HL7 International

ANSI

ANSI/HL7 PHRSFM, R2-2021
2021-10-12

HL7 EHRS-FM Release 2:

Personal Health Record System Functional Model,

Release 2

October 2021

Sponsored by:
Electronic Health Records Work Group

IMPORTANT NOTES:

HL7 licenses its standards and select IP free of charge. **If you did not acquire a free license from HL7 for this document,** you are not authorized to access or make any use of it. To obtain a free license, please visit http://www.HL7.org/implement/standards/index.cfm.

If you are the individual that obtained the license for this HL7 Standard, specification or other freely licensed work (in each and every instance "Specified Material"), the following describes the permitted uses of the Material.

A. HL7 INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS, who register and agree to the terms of HL7's license, are authorized, without additional charge, to read, and to use Specified Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part without paying license fees to HL7.

INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS wishing to incorporate additional items of Special Material in whole or part, into products and services, or to enjoy additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS as noted below, must become ORGANIZATIONAL MEMBERS of HL7.

B. HL7 ORGANIZATION MEMBERS, who register and agree to the terms of HL7's License, are authorized, without additional charge, on a perpetual (except as provided for in the full license terms governing the Material), non-exclusive and worldwide basis, the right to (a) download, copy (for internal purposes only) and share this Material with your employees and consultants for study purposes, and (b) utilize the Material for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, Compliant Products, in all cases subject to the conditions set forth in this Agreement and any relevant patent and other intellectual property rights of third parties (which may include members of HL7). No other license, sublicense, or other rights of any kind are granted under this Agreement.

C. NON-MEMBERS, who register and agree to the terms of HL7's IP policy for Specified Material, are authorized, without additional charge, to read and use the Specified Material for evaluating whether to implement, or in implementing, the Specified Material, and to use Specified Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part.

NON-MEMBERS wishing to incorporate additional items of Specified Material in whole or part, into products and services, or to enjoy the additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS, as noted above, must become ORGANIZATIONAL MEMBERS of HL7.

Please see http://www.HL7.org/legal/ippolicy.cfm for the full license terms governing the Material.

Ownership. Licensee agrees and acknowledges that **HL7 owns** all right, title, and interest, in and to the Trademark. Licensee shall **take no action contrary to, or inconsistent with**, the foregoing.

Licensee agrees and acknowledges that HL7 may not own all right, title, and interest, in and to the Materials and that the Materials may contain and/or reference intellectual property owned by third parties ("Third Party IP"). Acceptance of these License Terms does not grant Licensee any rights with respect to Third Party IP. Licensee alone is responsible for identifying and obtaining any necessary licenses or authorizations to utilize Third Party IP in connection with the Materials or otherwise. Any actions, claims or suits brought by a third party resulting from a breach of any Third Party IP right by the Licensee remains the Licensee's liability.

Following is a non-exhaustive list of third-party terminologies that may require a separate license:

Terminology	**Owner/Contact**
Current Procedures Terminology (CPT) code set	American Medical Association https://www.ama-assn.org/practice-management/cpt-licensing
SNOMED CT	SNOMED International http://www.snomed.org/snomed-ct/get-snomed-ct or info@ihtsdo.org
Logical Observation Identifiers Names & Codes (LOINC)	Regenstrief Institute
International Classification of Diseases (ICD) codes	World Health Organization (WHO)
NUCC Health Care Provider Taxonomy code set	American Medical Association. Please see www.nucc.org. AMA licensing contact: 312-464-5022 (AMA IP services)

Gary Dickinson, FHL7
Co-Chair, EHR Work Group
EHR Standards Consulting

Mark Janczewski, MD, MPH, FAAFP, FAMIA
Co-Chair, EHR Work Group
Medical Networks, LLC

Stephen Hufnagel, PhD
Co-Chair, EHR Work Group
Registry Clearinghouse

Feliciano 'Pele' Yu, MD, MSHI, MSPH, FAMIA
Co-Chair, EHR Work Group
University of Arkansas Medical Sciences

John Ritter, FHL7
Co-Chair, EHR Work Group, Project Team Facilitator

Michael Brody, DPM
Co-Chair, EHR Work Group
Registry Clearinghouse

Anneke Goossen, MScN
Publishing Facilitator
Results4Care

Michael van der Zel, BSc
Publishing Facilitator
UMCG

Table of Contents

Function List Component Descriptions

The Function List includes the following components:

Function ID # (Normative)	This is the unique identifier of a function in the Function List (e.g. CP.1.1) and should be used to uniquely identify the function when referencing functions. The Function ID also serves to identify the section within which the function exists (CP = Care Provision Section) and the hierarchy or relationship between functions (CP.1.1 is a sibling to CP.1.2, parent of CP.1.1.1 and child of CP.1). In many cases the parent is fully expressed by the children.
Function Type (Reference)	Indication of the line item as being a header (H) or function (F) or conformance criteria.
Header/Function Name (Normative)	This is the name of the Function and whilst expected to be unique within the Function List; it is not recommended to be used to identify the function without being accompanied by the Function ID. Example: Manage Medication List
Function Statement (Normative)	This is a brief statement of the purpose of this function. Whist not restricted to the use of structured language that is used in the Conformance Criteria (see below); the Statement should clearly identify the purpose and scope of the function. Example: Create and maintain patient-specific medication lists.
Description (Reference)	This is a more detailed description of the function, including examples if needed. Example: Medication lists are managed over time, whether over the course of a visit or stay, or the lifetime of a patient. All pertinent dates, including medication start, modification, and end dates are stored. The entire medication history for any medication, including alternative supplements and herbal medications, is viewable. Medication lists are not limited to medication orders recorded by providers, but may include, for example, pharmacy dispense/supply records, patient-reported medications and additional information such as age specific dosage.
Conformance Criteria (Normative)	Each function in the Function List includes one or more Conformance Criteria. A Conformance Criteria, which exists as normative language in this standard, defines the requirements for conforming to the function. The language used to express a conformance criterion is highly structured with standardized components with set meanings. The structured language used to define conformance clauses in the Function List are defined in the Glossary (Chapter 4).
R1.1 Reference (Reference)	Reference to the previous version of the Functional Model is included to support transition from one version to the next. The first 2 digits indicate the source document; FM = Functional Model, LM = Lifecycle Model. The remainder of the reference is to the function and, if applicable, conformance criteria.
Change Indicator	The change indicator shows the change from previous versions. This will be valued as follows: C - Changed D - Deleted N - New NC - No Change
Row #	A unique number for the row within the section.

1. Personal Health Section

Section Overview

Personal Health PHR-S functions are the subset of PHR-S functions that enable an individual to manage information about his or her healthcare. These functions provide direction as to the individual's ability to interact with a Personal Health Record in such a way so as to individualize the record and maintain a current and accurate record of his or her healthcare activities. The functions include activities such as managing wellness, prevention and encounters. These functions are designed to encourage and allow an individual to participate actively in their healthcare and better access the resources that allow for self-education and monitoring. All functions within the Personal Health Section have an identifier starting with "PH".

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
PH.0 Function	Personal Health			4
	Statement: Manage information and functions related to self care and provider-based care over time. **Description:** The personal health record (PHR) may be represented via multiple approaches including a personally-maintained paper record or via electronic means; also, the PHR may be represented within different contexts, for example, a minimal history of major health-related events versus a record of daily health and wellness activities. The functions with this PHR-S FM are a superset of functionality that detail certain functions that might be present in various PHR System implementations. The functions provide for both personal observations and health management, as well as by the PHR Account Holder's healthcare providers. The PHR should present a view to the PHR-S Account Holder that is tailored to their level of health literacy and language ability. Many realms already support a PHR Account Holder's ability to withhold health information from providers and other persons at the PHR Account Holder's discretion. Personal Health functions accommodate those realms by providing the PHR Account Holder the ability to withhold such information. Some realms may require, through jurisdictional law, rules, or regulations, clear indications in the record that some information has been withheld. When jurisdictional law requires such indications, the system can display such indications. If the jurisdiction provides individuals with an option to indicate or not indicate that information has been withheld, the PHR Account Holder can exercise that option (e.g., turn on a flag or not turn on a flag). In the PHR-S FM, there are times when the actions/activities related to the PHR Account Holder may also apply to the PHR Account Holder Proxy. External data sources might include: an EHR system; a pharmacy; a care team member; a medical device; a paper scan of birth certificate; a wiki; a family member; a public health organization; a laboratory; a clinical trial study; a local high school health department. The external data could be structured or non-structured. The context for the arriving data could be due to a single event (such as an immunization) or due to a set of associated events (such as occurs during a transition of care). Example(s): The PHR Account Holder may desire to see a summary-of-care record or an ad hoc view of the health record (e.g., the list of medications that is referenced by providers or pharmacists.			
1.	The system SHALL capture, maintain, and render the explicit source of all data in the PHR-S (specifically including any metadata that identifies the author, creator, or custodian of the data).			5
2.	The system SHALL provide the ability for the PHR Account Holder to control-access to the PHR Account Holder's self-created data (including the intended and/or permitted use of the data) according to organizational policy and/or jurisdictional law (e.g., depending on the vendor's terms-and-conditions-of-use agreement or the system's configuration parameters).			6
3.	The system SHALL audit each access to the PHR Account Holder's data according to organizational policy and/or jurisdictional law.			7
4.	The system SHOULD provide the ability for the PHR Account Holder to control access to the PHR-S by restricting the input of data from external sources.			8
5.	The system SHOULD provide the ability for the PHR Account Holder to analyze and determine whether to accept or reject data arriving from an external source according to organizational policy and/or jurisdictional law.			9
6.	The system SHOULD manage data arriving from an external source by accepting or rejecting the data based on predefined rules and according to organizational policy and/or jurisdictional law. For example, the PHR-S rejects data that was sent from the local clinic that has not been accepted by the PHR Account Holder after three months.			10
7.	The system SHALL provide the ability for the PHR Account Holder to control access to the PHR Account Holder's data by removing access to the PHR Account Holder's data according to organizational policy and/or jurisdictional law. Note: access to the PHR Account Holder's data could be controlled at a global and/or granular level.			11
8.	The system SHALL provide the ability to control access to the PHR Account Holder's data by restricting its use and/or disclosure according to user role, organizational policy, and/or jurisdictional law.			12
9.	The system SHALL transmit an indication that information has been withheld by the PHR Account Holder to any stakeholder with whom the information is shared according to organizational policy and/or jurisdictional law.		C	13
10.	The system SHOULD NOT transmit an indication that information has been withheld by the PHR Account Holder to any stakeholder with whom the information is shared unless required according to organizational policy and/or jurisdictional law.		C	14

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
11.	The system SHOULD provide the ability for the PHR Account Holder to capture, maintain, and render the reason that the PHR Account Holder is withholding certain information from the downstream user. For example, the PHR Account Holder could choose to not share information with members of his care team that inadvertently appears in his record (such as a record that has arrived from an unknown individual).		N	15
12.	The system MAY render an indication regarding the sort order of a list according to scope of practice, organizational policy, and/or jurisdictional law. Note: Since the user's assumptions regarding the sort order of a given list might be a patient safety issue, and since there are many lists that could be presented in various sort orders within a PHR system, an indicator can be presented for any list whose sort order could result in a troublesome interpretation of that list.		N	16
13.	The system MAY provide the ability for authorized users to configure a default sort order for given lists (e.g., to reduce the confusion when the same list is sorted by severity one day and then by date-of-onset the next day) according to scope of practice, organizational policy, and/or jurisdictional law.		N	17
14.	The system MAY provide the ability to render lists in an ad hoc (dynamic, real-time) user-selected sort order (e.g., to reduce the confusion when the same list is sorted by severity one day and then by date-of-onset the next day by a different user) according to scope of practice, organizational policy, and/or jurisdictional law.		N	18
15.	IF an organization and/or jurisdiction provides individuals with an option to transmit (or not transmit) an indication that information has been withheld, THEN the system SHOULD provide the ability for the PHR Account Holder to exercise that option.			19
16.	IF the system has imported or received information from an external source that the PHR Account Holder identifies as possibly being incorrect, inappropriate, out-of-date, incomplete, skewed, undesired, or not preferred, THEN the system SHOULD provide the ability to mask that information according to user preference and/or consent, organizational policy, and/or jurisdictional law.			20
17.	The system MAY provide the ability for the PHR Account Holder to present information that has been captured from an external system (but not yet stored) and determine to remove that information according to organizational policy and/or jurisdictional law. (Note: This "information staging" approach enables the PHR Account Holder to filter out unwanted (or incorrect) data, but also enables the PHR Vendor to log the arrival of the data and audit the corresponding action that the PHR Account Holder takes. The vendor is free to deposit the data into the PHR or keep it in a staging area outside the PHR Account Holder's account.)			21
PH.1 Function	PHR Account Holder Profile			22
	Statement: Manage PHR Account Holder demographics, preferences, Advance Directives, consent directives and authorizations. **Description:** The person that is the subject of the personal health record is referred to as the PHR Account Holder. The PHR Account Holder may also be represented by the parent/guardian, or a designated representative (proxy) assigned by the PHR Account Holder or otherwise authorized entity. The PHR includes relevant demographic information and other administrative statements necessary to provide care such as Advance Directives or consents for care. Example(s): Display and maintain demographics or preferences such as the PHR Account Holder's preferred first name or religious preferences.			
PH.1.1 Function	Identify and Maintain a PHR Account Holder Record			23
	Statement: Unambiguously identify the PHR Account Holder; correctly link the information with the PHR Account Holder and vice-versa. **Description:** The PHR Account Holder must be confident that the system can reliably and uniquely identify them and provide access to their health record. Nothing precludes the PHR Account Holder from having more than one PHR such as a tethered PHR-S with their Primary Care Provider and a separate self-maintained PHR. The following functions apply to a single PHR system (PHR-S).			
1.	The system SHOULD present a user guide or training material to assist the PHR Account Holder in installing, initializing, registering, or operating their PHR.		C	24
2.	The system SHALL provide the ability to store more than one unique identifier for each PHR Account Holder's record. For example, the PHR Account Holder may have received health information from multiple caregivers, each caregiver having a unique Patient Identifier for that PHR Account Holder (also known as an Account Number). When the PHR Account Holder shares information with an individual caregiver, the PHR Account Holder may desire to utilize the Patient Identifier that is known to that specific caregiver.			25
3.	The system SHOULD provide the ability to capture, store, and integrate and/or link the PHR Account Holder's unique identifiers from multiple external sources (e.g., medical record number, insurance account number, or voluntary unique identifiers).			26
4.	The system SHALL provide the ability to uniquely identify a PHR Account Holder.			27
5.	The system SHOULD provide the ability (through a controlled method) to capture, integrate, and/or link information that is determined to be the PHR Account Holder's information that is stored in external systems. Note: A controlled method enables the PHR Account Holder to choose a course of action from a limited set of actions. For example, the PHR-S could provide a controlled method by which the PHR Account Holder could choose to link to an external DICOM image, but import the Report regarding that DICOM image instead.			28

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
6. IF health information has been incorrectly associated with a PHR Account Holder, THEN the system SHALL provide the ability to annotate the information as being erroneous (or as believed to be erroneous) in the PHR Account Holder's account in which it was incorrectly associated, and represent that information as being erroneous.				29
7. IF health information has been incorrectly associated with a PHR Account Holder, THEN the system SHOULD provide the ability to transmit information regarding the error to the source of the information according to organizational policy and/or jurisdictional law.				30
8. The system SHOULD provide the ability to archive, delete, and/or purge part or all of a PHR Account Holder's information (e.g., information that is obsolete, inactive, or nullified) according to user preference and/or consent, organizational policy (e.g., according to a statement of terms and conditions), and/or jurisdictional law.				31
PH.1.2 Function	Manage PHR Account Holder Demographic Information			32
Statement: Enable the PHR Account Holder to manage the PHR Account Holder's demographic information. **Description:** The system should maintain the current demographic data set that unambiguously defines the PHR Account Holder including personal attributes and contact information (including emergency contact, next-of-kin information, and insurance information sufficient to meet the information needs required to provide health care services, and if applicable, facilitate the need to locate family members in the event of an emergency or to expedite next-of-kin notification). Example(s): Maintain current contact information, emergency contact information/next-of-kin information, and registration information including physical addresses, telephone numbers, and email addresses.				
1. The system SHALL capture the PHR Account Holder's demographic information.				33
2. The system SHALL store and retrieve the PHR Account Holder's demographic information as discrete data.				34
3. The system SHALL provide the ability to import and/or receive the PHR Account Holder's demographic data from existing digital sources (including, for example, from a provider's EHR-S or a health plan system).				35
4. The system SHOULD provide the ability to enter or update demographic data that has not been synchronized with other source systems.				36
5. The system SHALL provide the ability to render a PHR Account Holder's demographic data according to user preference and/or consent, organizational policy, and/or jurisdictional law.				37
6. The system SHOULD store historical values of demographic data (e.g., various residence addresses, or marital status changes).				38
7. The system SHALL present identifying information with any presentation of the PHR Account Holder's data (unless the information has been tagged as needing to be de-identified) according to organizational policy and/or jurisdictional law. For example, the PHR Account Holder's name ought to appear on each screen to help a mother distinguish the screen displays of the PHRs for each of her minor children. Another example is that the PHR Account Holder's name should not appear -- and the information should be de-identified -- when the information is being shared with a research organization.				39
8. IF one PHR Account Holder has certain information in common with a second PHR Account Holder, THEN the system SHOULD provide the ability to auto-populate the second PHR Account Holder's information with certain common information from the first PHR Account Holder's account according to user role, organizational policy, and/or jurisdictional law. For example, a mother may auto-populate her infant's resident address information using her own resident address information.				40
9. The system SHOULD provide the ability for the PHR Account Holder to annotate demographic data with text comments.				41
10. The system SHOULD provide the ability for the PHR Account Holder to control access to demographic information.				42
PH.1.3 Function	Manage PHR Account Holder and Family Preferences			43
Statement: Enable the PHR Account Holder to add certain preferences that he or she wants health care providers to know. **Description:** PHR Account Holders may hold certain religious or philosophical views that impact how they wish to be treated or how they might respond to treatment choices. These preferences should be captured, prominently displayed, and made available during the care process. For example, a person may hold certain preferences regarding eating certain foods (e.g., avoidance of meats; preference for vegetables); taking certain therapeutic serums derived from animals; use of a pig-valve for valve replacement; use of human or animal tissues (e.g., skin tissue or bone). Example(s): A religiously-based proscription of blood transfusion is a commonly encountered example of a PHR Account Holder preference.				
1. The system SHALL provide the ability to capture, maintain, and render the PHR Account Holder's preferences (e.g., language, religion, ethnicity, spiritual practices, or cultural practices) according to organizational policy and/or jurisdictional law.				44

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
2.	The system SHOULD provide the ability to capture, maintain, and render family preferences (such as preferred language, religion, spiritual practices and culture) for example, to support clinical decision making activities.			45
3.	The system SHALL provide the ability to capture, maintain, and/or render PHR Account Holder and family preferences as they pertain to current treatment plans according to user preference and/or consents, organizational policy, and/or jurisdictional law.		C	46
4.	The system SHOULD provide the ability to update care guidelines and options based on documented PHR Account Holder and family preferences, including clinical guidelines and treatment options (e.g., treatment for individuals who refuse blood transfusions).			47
5.	The system MAY provide the ability to present care guidelines and options relating to documented PHR Account Holder and family preferences, including clinical guidelines and treatment options.			48
6.	The system SHOULD provide the ability to integrate PHR Account Holder preferences with appropriate health education materials (e.g., dietary advice based on dietary preference).			49
7.	The system SHOULD provide the ability to integrate documentation of PHR Account Holder preferences, such as living wills, specific consents or releases, and other Advance Directives.			50
PH.1.4 Function	Manage PHR Account Holder Advance Directives			51
	Statement: Enable the PHR Account Holder to create or input Advance Directives for care under various circumstances. **Description:** The PHR Account Holder along with their immediate family should periodically assess their health status and formally state in writing how they wish to be cared for in different circumstances. This is particularly useful when the end of life is predictably near to avoid inappropriate or undesired care.			
1.	The system SHALL provide the ability to render an indication that Advance Directives or organ donation preferences exist for the PHR Account Holder. For example, a PHR Account Holder may desire to inform a new care provider of the existence of an organ donation preference. Also, in an emergency care situation, the emergency care provider might desire to know whether the PHR-S contains an Advance Directive for the PHR Account Holder.			52
2.	The system SHOULD provide the ability to render an indication of the type of Advance Directives completed for the PHR Account Holder (such as living will, durable power of attorney, preferred interventions for known conditions, organ donation, or the existence of a "Do Not Resuscitate order", or organ donation preferences) according to organizational policy and/or jurisdictional law, or according to the recipient's scope of practice.			53
3.	The system SHOULD provide the ability to capture, maintain, and render the PHR Account Holder's Advance Directives documents and "Do Not Resuscitate" orders or organ donation preferences according to organizational policy and/or jurisdictional law, or according to the recipient's scope of practice to support clinical decision making activities.			54
4.	The system SHALL provide the ability to maintain metadata (e.g., the type of the document, the time and date document was created, and the document currently in effect) for the PHR Account Holder's Advance Directives documents, "Do Not Resuscitate" orders, and/or organ donation preferences according to organizational policy and/or jurisdictional law.			55
5.	The system SHOULD provide the ability to render an indication regarding the date that Advance Directives or organ donation preferences were last reviewed by the PHR Account Holder or by their legal guardian or power of attorney.			56
6.	The system SHOULD provide the ability to render the name and the relationship of the party completing the Advance Directive or organ donation preferences for the PHR Account Holder.			57
7.	The system SHALL manage the date and time that Advance Directives or organ donation preferences were stored and/or changed in the PHR-S.			58
8.	The system SHOULD provide the ability to manage information regarding the location and the source of legal documentation regarding Advance Directives or organ donation preferences.			59
PH.1.5 Function	Manage Consents and Authorizations			60
	Statement: Enable the PHR Account Holder to manage consent directives and authorizations. **Description:** A variety of consent directives and authorizations are needed to provide healthcare services. Each institution such as an emergency room, each provider, or each health care service such as an operative procedure may require its own informed consent be captured, displayed, and verified before care can be provided. The consent directives may be externally sourced with copies made available for the PHR Account Holder to capture and store. Some consent directives or authorizations may be authored by the PHR Account Holder granting authorizations such as a parent granting ad hoc authorization for emergency care for a child. Note: The system FM is agnostic to any specific consent/authorization approach. For example, consent/authorization directives may apply to the data in the PHR itself or could integrate with an external access control service. Note: A consent and privacy framework is best described in a functional profile (i.e., a subset) of the PHR-S FM and ought to be specified in accordance to organizational policy and/or jurisdictional law. Therefore, it is assumed that a consent and privacy model will be specified by the functional profile. Example(s): Maintain current authorizations in relation to specific health record functions. The PHR Account Holder may desire to see the authorizations associated with a specific clinical activity, such as treatment or surgery, along with that event in the PHR Account Holder's PHR-S.			

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
1.	The system SHALL provide the ability for the PHR Account Holder to capture an indication that a PHR Account Holder has completed applicable consent directives and authorizations according to organizational policy and/or jurisdictional law.			61
2.	The system SHOULD provide the ability to capture information regarding the external location of the PHR Account Holder's applicable consent directives and authorizations according to user preference, organizational policy, and/or jurisdictional law.			62
3.	The system SHOULD provide the ability to manage consent directives and authorizations according to user preference, organizational policy, and/or jurisdictional law (e.g., capturing the PHR Account Holder's personal representative's authority (such as a note from the PHR Account Holder or a pointer to a legal document) to enable decisions to be made on behalf of the PHR Account Holder).			63
4.	The system SHALL provide the ability to manage an indication that a PHR Account Holder has granted access, withheld access, or revoked access to applicable consent directives and authorizations according to user preference, organizational policy, and/or jurisdictional law.			64
5.	The system MAY provide the ability to manage consent and authorization forms on-line according to user preference, organizational policy, and/or jurisdictional law.			65
6.	The system SHOULD provide the ability to render consent and authorization forms (including, for example, in print-format) according to user preference, organizational policy, and/or jurisdictional law.			66
7.	The system MAY render electronic copies of authorization and/or consent directives associated with a specific clinical activity, such as a treatment or surgery according to user preference, organizational policy, and/or jurisdictional law.			67
8.	The system SHOULD provide the ability to render electronic copies of authorization and/or consent directives chronologically according to user preference, organizational policy, and/or jurisdictional law.			68
9.	The system SHOULD provide the ability to manage documentation related to a PHR Account Holder Proxy's consent or authorization according to user preference, organizational policy, and/or jurisdictional law.			69
10.	The system SHOULD provide the ability to capture information that identifies the signer (and co-signer, if any) of a consent and/or authorization document according to user preference, organizational policy, and/or jurisdictional law.			70
PH.1.6 Function	Manage PHR Account Status			71
	Statement: Enable a PHR Account Holder to open or close a PHR Account, or to transfer PHR information from one PHR Account to another PHR Account. **Description:** A PHR Account Holder may possess one or more PHR accounts over a lifetime, and may have multiple PHR accounts open simultaneously. The PHR system, therefore, needs to provide the ability to open or close a PHR account on a PHR Account Holder's behalf, and to transmit a copy of PHR account data to other PHR systems.			
1.	The system SHALL provide the ability to authorize and authenticate a PHR Account Holder to create or activate a new PHR Account according to organizational policy and/or jurisdictional law.			72
2.	The system SHALL provide the ability to control access to a PHR Account Holder's Account by capturing information regarding the closure or deactivation of a PHR Account according to organizational policy and/or jurisdictional law.			73
3.	The system SHOULD transmit confirmation of the PHR Account Holder's account closure to the PHR Account Holder according to PHR Account Holder preference, organizational policy, and/or jurisdictional law.			74
4.	The system SHOULD provide the ability to transmit the PHR Account Holder's account information (specifically, the PHR Account Holder's account data such as the person's name and address, birth date, gender, and credit card number) to another PHR-S according to organizational policy and/or jurisdictional law. For example, the PHR Account Holder might want to create a new, but empty, PHR Account by transmitting certain account metadata.			75
5.	The system SHOULD provide the ability to transmit the PHR Account Holder's account information (specifically, the PHR Account Holder's demographic data, historical health records, pictures, reports, lists, educational research, etc.) to another PHR-S according to organizational policy and/or jurisdictional law. For example, the PHR Account Holder might desire to populate an empty PHR Account by transmitting certain health data content to the empty account.			76
6.	IF the system transmits a copy of the PHR Account Holder's account information to another PHR system, THEN the system MAY also transmit audit-related and/or log-related information for the PHR Account Holder's account to the other PHR system according to organizational policy and/or jurisdictional law.			77
7.	IF the system transmitted PHR Account metadata, and/or PHR data, and/or audit/log data to another system, THEN the system SHALL transmit a confirmation of the PHR Account Holder's account transfer to the PHR Account Holder.			78
8.	IF the system transmitted PHR Account metadata, and/or PHR data, and/or audit/log data to another system, THEN the system SHALL provide the ability to receive and render a notification/			79

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
	acknowledgement (from the receiving system) to the PHR Account Holder regarding the status of the intended account transfer (e.g., success, failure, or partial failure of the transfer).			
	9. The system MAY provide the ability to transmit a notification to the PHR Account Holder that the PHR Account Holder's account has experienced a period of inactivity and is scheduled to be purged according to the PHR Account Holder's preference and/or consent, organizational policy, and/or jurisdictional law.			80
	10. The system MAY provide the ability to purge the PHR Account Holder's account after a period of inactivity according to the PHR Account Holder's preference and/or consent, organizational policy, and/or jurisdictional law.			81
	11. The system MAY provide the ability for the PHR Account Holder to purge the PHR Account Holder's account according to the PHR Account Holder's preference and/or consent, organizational policy, and/or jurisdictional law (e.g., after confirmation of the PHR Account Holder's request to purge the account according the PHR vendor's Terms-Of-Service agreement).			82
PH.2 Function	Manage Historical Clinical Data and Current State Data			83
	Statement: Historical health information as well as current health status should be captured and maintained in the health record. **Description:** To obtain historical information to populate the PHR, the PHR Account Holder may use strategies that include entering historical information directly or importing at least part of this data from outside electronic data sources. An outside service such as an employer, insurance plan, provider or care delivery organization may sponsor a particular PHR and add data to the record from their data sources. The PHR Account Holder may use similar strategies to populate their current state information.			
	1. The system SHALL capture and maintain metadata that identifies the author, source, and custodian of the data in the PHR.			84
	2. The system SHALL conform to TI.2 (Auditable Records).		C	85
	3. The system SHOULD provide the ability for the PHR Account Holder to annotate any externally-sourced data with text comments.			86
PH.2.1 Function	Manage PHR Account Holder Originated Data			87
	Statement: Manage information sourced or input directly by the PHR Account Holder. **Description:** PHR data, including personal observations and most specific data elements (such as allergies and intolerances or problems), may be entered directly by the PHR Account Holder. The source of all data is captured and, in this case, self-entered data, should be so labeled. These data elements may possess more or less credibility when entered by the PHR Account Holder. When appropriate, patient-entered data should be structured and codified. Paper-based information (such as a health card or a laboratory report) may be captured in the form of a scanned image and kept in the record, organized, and/or indexed for retrieval. Example(s): When a problem in the problem list is entered by the PHR Account Holder, it is labeled as such in order to distinguish this problem from others that resulted from a provider's clinical diagnosis.			
	1. The system SHALL conform to RI.1.1.1 (Originate and Retain Record Entry) in order to capture unstructured PHR Account Holder -originated data.			88
	2. The system SHALL conform to RI.1.1.1 (Originate and Retain Record Entry) in order to capture structured PHR Account Holder -originated data.			89
	3. The system SHALL conform to RI.1.1.1.1 (Evidence of Record Entry Originate / Retain Event) in order to manage metadata that identifies the author of the data (e.g., the PHR Account Holder as author or a provider as author), or the source of the data (e.g., the name and location of an external system that authored and transmitted the data), or the generator of the data (e.g., the Unique Device Identifier and metadata of a medical device that authored the data).		C	90
	4. The system SHOULD render PHR Account Holder -originated data for use by care providers.			91
	5. The system MAY provide the ability to capture an indication that a provider has verified the accuracy of consumer-originated data and has included it as a record in the EHR-S.			92
	6. The system MAY provide the ability for the PHR Account Holder to annotate PHR Account Holder -sourced data with text comments.			93
	7. The system MAY provide the ability for the PHR Account Holder to update PHR Account Holder-sourced data with text comments.			94
PH.2.2 Function	Manage Data from External Administrative Sources			95
	Statement: Manage information from administrative data sources such as insurance plans and pharmacy benefit managers. **Description:** PHR Account Holder data can be collected from many sources (including administrative sources). For example, the PHR Account Holder's health insurance plan may directly offer health-related information or may enable the PHR system to derive selected clinical information from financial transactions to the extent that health insurance claims include relevant data. Similarly, selected medication records may be available from Pharmacy Benefits Management services.			
	1. The system SHOULD provide the ability to capture data from claims and other administrative data sources.			96
	2. IF the system provides the ability to capture data from claims and other administrative data sources, THEN the system SHALL provide the ability for the PHR Account Holder to manage		C	97

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
	that data according to scope of practice, organizational policy, and/or jurisdictional law. Note: The PHR Account Holder ought to be able to perform some data manipulation -- but no other data manipulation -- on the data received. For example, the PHR Account Holder ought to be able to annotate certain data, but not edit it.			
	3. The system MAY provide the ability to determine that duplicate data exists that references the same clinical events from different sources and present a notification to the PHR Account Holder that the duplicate data exists (e.g., so that the PHR Account Holder can hide or delete the duplicate data). For example, one copy of a picture of a laceration may be hidden if two identical copies are received: one from the Emergency Response personnel and another from the Emergency Department.			98
PH.2.3 Function	Manage Data and Documentation from External Clinical Sources			99
	Statement: Enable the PHR Account Holder to capture and manage historical clinical information. **Description:** The system shall capture structured and unstructured documents and data from outside clinical sources, index, and store them. Data and Documentation from External Clinical Sources may be indexed by contained structured attributes (such as the name of the source laboratory, or the date that the document was created), or manually by the PHR Account Holder (or proxy) by annotating those documents or data with a standard or custom indexing tag. Example(s): Clinical information may include: laboratory results, radiographic images, EKG, or scanned documents that are captured, annotated and stored, as coded and structured documents or unstructured documents.			
	1. The system SHOULD provide the ability to capture externally-sourced clinical documentation as structured content including the original, updates, and addenda.			100
	2. IF information is received through any electronic interface or is electronically referenced, THEN the system SHOULD provide the ability to render that information upon request.			101
	3. The system SHOULD provide the ability to capture provider-sourced electronic documents including original, updates, and addenda. Examples of provider-sourced electronic documents include: Discharge instructions, x-rays of teeth, or pictures of lacerations.			102
	4. The system SHOULD provide the ability to link documentation and annotations with structured content (e.g., an office visit, phone communication, e-mail consultation, laboratory result, problem, or diagnosis).			103
	5. The system SHALL present data and documentation that was captured from External Clinical Sources.			104
	6. The system SHOULD provide the ability to render structured or unstructured documents based on filter, search, and/or sort criteria.			105
	7. The system SHOULD conform to RI.1.1.1 (Originate and Retain Record Entry) in order to capture unstructured data and documentation from external clinical sources.			106
	8. The system SHALL conform to RI.1.1.1 (Originate and Retain Record Entry) in order to capture structured data and documentation from external clinical sources.			107
	9. The system SHALL authenticate transmission contents of clinical data received from any external source.			108
	10. The system SHOULD transmit acknowledgment of the receipt of clinical data from external sources.			109
	11. The system SHOULD transmit a notification to the PHR Account Holder of the successful receipt and integration of clinical data from external sources according to the PHR Account Holder's preference and/or consent, organizational policy, and/or jurisdictional law.			110
PH.2.4 Function	Produce and Present Ad Hoc Views of the Personal Health Record			111
	Statement: Provide for standard and customizable views of the Personal Health Record. **Description:** The PHR system may offer a standard set of views of the PHR Account Holder's data. One such view may be a summary screen or "dashboard" that allows the PHR Account Holder to monitor his or her healthcare progress. The system should also provide the ability for the PHR Account Holder to assemble custom views to meet their needs such as adding a glucose monitoring module to their dashboard view. Example(s): "The system MAY provide the ability to create customized views of summarized information based on sort and filter controls for custom or other parameters." "Display all clinical documents containing the word "thyroid"."			
	1. The system SHOULD provide the ability to render customized views of information based on sort and filter controls for chronology, reverse chronology, date or date range, condition, provider, and care setting.			112
	2. The system SHOULD provide the ability for Authorized PHR Users to render customized views of summarized information based on sort and filter controls for custom or other parameters.			113
	3. The system MAY provide the ability to render reports or views of all data based on searching on standardized or customized index tags.			114
	4. The system MAY maintain a text-based index of the entire record for searching on any word or phrase in the Personal Health Record.			115

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
5. The system SHOULD provide the ability to save multiple customized views for more rapid display of information by the PHR Account Holder.				116
6. The system SHOULD provide the ability for Authorized PHR Users to maintain individual custom views for their future PHR access.				117
7. The system SHOULD present summarized views and reports customized by the PHR Account Holder.				118
8. The system SHOULD provide the ability to present reminders and alerts in a view that is selected by the PHR Account Holder.				119
9. The system SHOULD provide the ability for Authorized PHR Users to maintain individual summary views for their future PHR access.				120
PH.2.5 Function	Manage Historical and Current State Data		C	121

Statement: Maintain the summary lists depicting the PHR Account Holder's current medical state and history.

Description: The current state data set is a data model of the PHR Account Holder that is useful to the PHR Account Holder, but is particularly useful to any healthcare provider who is asked by the PHR Account Holder for help. These data characterize the PHR Account Holder in current time and is useful in the evaluation of new conditions and predictive of how they might respond to treatments and/or therapies. Receiving these data in the PHR in an electronic and automated fashion may obviate having to recreate the data manually with every new encounter. For many of these elements, the PHR Account Holder is the primary authority. The following data elements are examples of information that is managed over time, across encounters with providers, and for particular health conditions:

- Problems (including Diagnoses)
- Medications
- Test Results
- Allergies and intolerances
- Medical history
- Surgical history
- Immunizations
- Family history
- Genetic information
- Social history, including family relationship and work information.
- Providers' notes

Work information could be defined using the Occupational Data for Health (ODH) data elements:

- Current employment status (e.g., employed for wages);
- Current job data: job employment type (e.g., self-employed), occupation and industry with the start and end dates, employer name and location, job duties, work schedule;
- Usual, or longest-held, occupation and industry, with duration and start date.

Specific complaints, history of present illness, review of systems, and the physical examination are more episodic and encounter specific.

Example(s): Current Problems, Medications taken, allergies, immunizations, past medical illnesses, surgeries, family history, and social history including habits along with recent diagnostic studies provide data useful for directing care.

1. The system SHOULD provide the ability for the PHR Account Holder and other Authorized PHR Users to render information about the PHR Account Holder's health conditions according to user role, organizational policy, and/or jurisdictional law.			122
2. The system SHOULD provide the ability for the PHR Account Holder to manage user-configuration parameters regarding their preferences for rendering PHR Account Holder information according to organizational policy and/or jurisdictional law.			123

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
PH.2.5.1 Function	Manage Problem Lists		C	124

Statement: Manage the PHR Account Holder's health problem list and provide the ability to manage the problem list over time in accordance with organizational policy and/or jurisdictional law.

Description: Problems are a core feature of the patient record that provides structure and direct management. Problems may include diagnoses. The PHR Account Holder, along with his or her (medical) advisors, may wish to establish their own guidelines regarding who can add or change self-entered problems on the primary list. The PHR Account Holder may wish to maintain his or her own list of problems authored themselves or from non-traditional providers that have no correlation in allopathic medicine. As in other criteria, all data must have source attribution so as to distinguish patient-entered data from provider-entered data.

The PHR Account Holder could have problems (or conditions) could be short-term or long-term. An example of a short-term condition is a febrile seizure or a single head injury; an example of a long-term condition is a genetic condition such as seizure-disorder (epilepsy) or repeated head trauma (e.g., professional boxing).

Problem List information needs to be communicated to the care team because problem history information could influence the way that medications and therapies are prescribed.

Regardless of the duration of the condition, the way that medications and therapies are prescribed by clinicians, as well as nutrient intake considerations, ought to be part of the PHR system. For example, a person who has a history of seizure(s) needs to share that information with relevant members of the care team throughout that person's lifetime.

Information about problems (or conditions) could be verified by diagnostic studies or collected via self-assessments.

The PHR Account Holder's problems (or conditions), either genetic or acquired, might cause contraindications with respect to medications, nutrients, or therapies. As a result, members of the care team may need to be informed during decision making activities. Members of the care team may also need to receive education regarding certain problems or conditions.

Example(s): Problem list items may include: chronic conditions, diagnoses, allergies or intolerances, or symptoms, both past and present, as well as disability status or functional status and all pertinent dates, including date of onset, diagnosis, changes and resolution.

1. The system SHALL provide the ability to manage all problems associated with a PHR Account Holder.			125
2. The system SHALL provide the ability to manage a history of all problems associated with the PHR Account Holder according to user preference, organizational policy, and/ or jurisdictional law (e.g., a PHR-Account-Holder desires to delete the history of a problem after three years but a federal law indicates that the record cannot be deleted before seven years).			126
3. The system SHALL provide the ability to capture the date that the problem was documented.			127
4. The system SHOULD provide the ability to capture the chronicity (e.g., chronic or acute/self-limiting) of a problem.			128
5. The system SHALL provide the ability to capture the source, date and time of all updates to the problem list.			129
6. The system SHOULD provide the ability to manage the deactivation of a problem according to organizational policy and/or jurisdictional law.			130
7. The system SHOULD provide the ability to manage the reactivation of a previously deactivated problem.			131
8. The system SHOULD provide the ability to render inactive or resolved problems (e.g., so that a list of childhood earaches (that are no longer problematic for the adult) can be quickly viewed).			132
9. The system SHOULD provide the ability to render the problem list based on a manually-specified order.			133
10. The system SHOULD provide the ability to link episode, encounters, orders, interventions, including medications and/or other treatments, and/or notes with one or more problems.		C	134
11. The system MAY provide the ability to manage the consolidation or grouping of multiple problems or related problems under a single problem.			135
12. IF problems are combined or consolidated, THEN the system SHOULD maintain any links with episode encounters, orders, interventions, including medications and/or other treatments, or notes previously set.		C	136
13. The system SHOULD provide the ability for the PHR Account Holder to annotate problems.			137
14. The system MAY provide the ability to capture a priority, importance, rank, and/or severity score for problems as defined in a classification scheme.			138
15. IF the system provides the ability to score problems in a classification scheme, THEN the system SHALL conform to function RI.1.1 (Record Lifecycle) to define classification schemes.		C	139
16. The system SHOULD provide the ability to render a problem list ordered by importance or severity of the problems.			140
17. The system SHOULD provide the ability to present a problem list truncated by the number of entries.			141
18. The system MAY provide the ability to link regimen therapy taken (either provider-initiated or PHR Account Holder initiated) and outcomes with a problem. For example, the PHR Account Holder may link the use of St. John's Wort and jogging with the problem of severe migraine headaches.			142

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
19.	The system MAY tag and render an indication that automated logic will not be applied against problems that were entered in free-text format. For example, the system discloses that it will not examine a free-text description of the PHR Account Holder's migraine headaches (or allergies) with respect to the PHR Account Holder's medication list.			143
20.	The system MAY conform to PH.5.4 (Integration with Third Party Clinical Decision Support Services) to analyze possible changes to health conditions across multiple factors (e.g., if a woman becomes pregnant she might need to temporarily limit the amount of tuna consumed that have high levels of mercury; or a person who gains an great deal of weight might need to resume taking insulin or adjust the dose of Levothyroxine taken).			144
PH.2.5.2 Function	Manage Medication List			145
	Statement: Manage the PHR Account Holder's medication list. **Description:** Medication lists are managed over time, whether over the course of a visit or stay, or the lifetime of a patient. All pertinent dates, including medication start, modification, and end dates can be stored. Medication histories, (for example, alternative supplements, over-the-counter medications, and herbal medications) may be relevant for review. Medication lists are not limited to medication orders recorded by providers, but may include, for example, pharmacy dispense/supply records, patient-reported medications, and additional information such as age-specific dosage. Example(s): The system maintains a medication list that may be followed by the PHR Account Holder and referenced by his or her providers and pharmacists. Copies of the PHR medication list may be kept by their providers in their EHRs.			
1.	The system SHALL provide the ability to capture PHR Account Holder -specific medication data from a provider's EHR system, a pharmacy system, or from other sources.		C	146
2.	The system SHOULD provide the ability to capture and update a fill status for each prescription.			147
3.	The system SHOULD provide the ability to capture dates associated with medications such as start date, fill date, and end date (e.g., so that a PHR Account Holder can keep track of multiple refills for a long-running prescription).			148
4.	The system SHALL provide the ability to capture medications that are not on the PHR Account Holder's existing medication list(s) or the existing medication history(s).			149
5.	The system SHOULD provide the ability for the PHR Account Holder to render a notification to a prescriber or provider that the PHR Account Holder believes that a medication was erroneously captured or duplicated.		C	150
6.	The system SHOULD provide the ability to capture and update a dispensing status for each medication order.			151
7.	The system SHALL present the list of medications to be self-administered.			152
8.	The system SHOULD provide the ability to render the timing, route of administration, and dose of all medications on the medication list.			153
9.	The system MAY provide the ability to capture available instructions regarding the administration of selected items on the medication list (e.g., by receiving administration instruction from the family physician, or by downloading information from the pharmacy).			154
10.	IF the system captures available instructions regarding the administration of selected items on the medication list, THEN the system MAY provide the ability for the PHR Account Holder to render available instructions regarding the administration of selected items on the medication list (e.g., to help the PHR Account Holder determine whether to discuss with their provider adjusting the dosing of Warfarin after receiving the results of an updated International Normalized Ratio (INR) laboratory test).		C	155
11.	The system SHOULD render a notification to the PHR Account Holder regarding a specific medication administration subject to the PHR Account Holder's preconfigured modalities for transmitting various types of notifications. For example, on a specific date/time via text message, or for a specific event (such as strenuous exercise via email), or for a specific condition (such as failure to complete an activity of daily living via a phone call to a family member).		C	156
12.	The system SHOULD provide the ability to capture medication self-administration details (e.g., timestamps, observations, complications, and/or the reason that a medication dose was not taken). For example, a mother could capture an indication that her baby was unwilling or unable to swallow a pill/liquid.			157
13.	The system SHOULD provide the ability for the PHR Account Holder to transmit a request for a medication refill to a pharmacy, or to the prescribing provider (if refills are not available for the given prescription).			158
14.	The system SHOULD provide the ability to annotate the medication list with text comments (e.g., a mother might note that the child is afraid of needles or cannot swallow the large red pill, or the PHR Account Holder might note that the medication works quite well, or that the medications are being shared with other people).			159
15.	The system MAY provide the ability to render a medication list containing only medications selected by the PHR Account Holder.			160
16.	The system SHOULD provide the ability for the PHR Account Holder to update the medication list by indicating those medications that are actually being taken.			161

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
17.	The system SHOULD provide the ability for the PHR Account Holder to maintain the medication list by updating the status of the medication self-administration (e.g., “no longer being taken” or “completed the regime”).			162
18.	The system SHOULD provide the ability to capture, maintain, and render prescription and non-prescription items (including dietary supplements) as discrete data and/or as lists.			163
19.	The system MAY provide the ability to receive current medications and a medication history from an external source (e.g., an EHR system, an insurance plan, a payer, or a pharmacy).			164
20.	The system SHOULD provide the ability to receive, maintain, and render information from an external source (e.g., from an EHR system or from a pharmacy system) regarding the difference between medications that were ordered and medications that were actually dispensed.			165
21.	The system MAY provide the ability to capture instructions regarding the cessation of selected items on the medication list. For example, the PHR Account holder could receive instructions from the family physician, the pharmacist, or from the medication manufacturer regarding behaviors that are permitted based on the cessation of a given medication. Another example is that the PHR Account Holder could be informed that the use of a blood thinner (e.g., Warfarin) must not be stopped abruptly. Finally, the PHR Account Holder could be informed that it is necessary to take the full course of a given prescribed medication.		C	166
PH.2.5.3 Function	Manage Test Results		C	167

Statement: Manage results of diagnostic tests including inpatient, ambulatory and home monitoring tests.

Description: Recent diagnostic studies further define the PHR Account Holder's current state. The system should capture, display, and maintain the results of tests and diagnostic studies, as limited by legal requirements or organizational policy. These will include laboratory tests with multiple line items such as test panels. Each individual item of a panel result should allow individual annotation. Other studies including diagnostic imaging studies should be included. Some tests such as colonoscopy or coronary artery catheterization will be derived from an encounter in PH.1.6 but the test results should be listed here.

A useful display will show brief test titles with dates and a simple flag to denote an abnormal component of the test. This gives the reviewer a quick understanding on which tests have been done, which tests were abnormal and which tests are out of date and may need to be repeated.

The EHR system is considered to be a more proper repository for a provider's orders than the PHR system. However, the PHR system may be the proper repository for “Direct-To-Consumer” laboratory tests that are ordered by the PHR Account Holder. Also, standing, recurring, or lifetime orders may be kept in the PHR (perhaps as part of a Care Plan). PHRs should be able to capture the fact that orders were made (either by a clinician or by a consumer) and link given test results to their corresponding orders.

Example(s): The results reporting list should inform the PHR Account Holder of the date of the most recent EKG or prostate cancer screening test and indicate the existence of abnormal findings.

1.	The system SHALL provide the ability to capture, maintain, and render test results according to organizational policy and/or jurisdictional law.			168
2.	The system SHALL provide the ability to render test results filtered by factors that support results management, such as type of test and date range.			169
3.	The system SHOULD present normal and abnormal ranges as reported by the source of the test result.			170
4.	The system SHOULD provide the ability to render test results via various filtering techniques (e.g., normalcy ranges for laboratory results: critical, abnormal, or normal; high versus low; or smallest to largest).			171
5.	The system SHOULD provide the ability to present numerical test results in graphical form in order to promote the comparison of test results.		C	172
6.	The system SHOULD provide the ability to render test results grouped in a logical manner (e.g., over a particular time frame or in relation to a particular problem).			173
7.	The system SHOULD provide the ability to analyze various information (e.g., test results, diagnoses, conditions, personal goals, therapy goals, and/or vital signs) using decision support algorithms and render possible courses of action.		C	174
8.	IF the system contains the electronic laboratory order, THEN the system SHOULD link test results to a specific order according to organizational policy and/or jurisdictional law.		C	175
9.	The system SHOULD provide the ability for the PHR Account Holder to annotate test results (e.g., "I do not understand the reason for this test", "This test result might be invalid because I was supposed to fast, but I ate full meals during the testing period", or "A second opinion was obtained and the consultant believes that these test results are erroneous").			176
10.	The system SHOULD provide the ability to render normal and/or abnormal test result ranges (as reported by the source of the test results).			177
11.	The system MAY present a reference to an image (e.g., an EKG tracing) that is associated with corresponding test results.			178

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
PH.2.5.4 Function	Manage Allergy, Intolerance, and Adverse Reaction List			179
	Statement: Manage the PHR Account Holder's list of known allergens and adverse reactions with all pertinent information. **Description:** Allergies, intolerances, sensitivities, and adverse reactions must be reviewed with every new prescription to avoid an allergic reaction. Environmental and food allergens should be listed and maintained here, as well as allergies to bee sting, sunlight, or substances (e.g., latex, metal, or contrast media (such as dye). Example(s): The system SHALL provide the ability to enter, store, update and display information related to allergic and adverse reactions or intolerances to drug and non-drug allergens or substances.			
1.	The system SHALL provide the ability to manage information related to allergy, intolerance, and adverse reaction to drugs, foods, or environmental triggers as unique, discrete entries (including, for example, substances such as latex, metal, and contrast media (such as dye)).			180
2.	The system SHOULD provide the ability to capture the reason for entry of the allergy, intolerance or adverse reaction.			181
3.	The system SHALL provide the ability to manage information related to allergic and adverse reactions to drug and non-drug allergens or substances.			182
4.	The system SHALL provide the ability to manage information regarding the reaction type.			183
5.	The system SHALL provide the ability to manage information regarding the severity of a reaction.			184
6.	The system SHOULD provide the ability to maintain associated allergic reactions to the prevention protocols and/or medications being taken.			185
7.	The system SHALL provide the ability to manage an indication regarding the negation of a health reaction (e.g., No Known Allergies (NKA), No Known Drug Allergies (NKDA), No Known Food Allergies (NKFA), No Known Sensitivities, or No Known Intolerances).		C	186
8.	The system SHOULD provide the ability to capture the source of allergy, intolerance, and adverse reaction information.			187
9.	The system SHOULD provide the ability to capture and maintain an indication regarding the deactivation of an item on the allergy, intolerance, and/or adverse reaction lists.		C	188
10.	The system SHOULD provide the ability to capture the reason for the deactivation of an item on the allergy, intolerance, and/or adverse reaction lists.			189
11.	The system SHOULD present allergies, intolerances and adverse reactions that have been deactivated.			190
12.	The system MAY provide the ability to present the list of allergies, intolerances, and/or adverse reactions in an order that is defined by the PHR Account Holder.			191
13.	The system SHALL provide the ability to capture and maintain the date on which allergy information was entered.			192
14.	The system SHOULD provide the ability to capture and maintain the approximate date of the allergy, intolerance, sensitivity, and/or adverse reaction occurrence.			193
15.	The system MAY provide the ability to render a standard adverse reaction report within a jurisdiction (e.g., a standard report regarding an adverse reaction to a vaccine). For example, an adverse reaction report could be transmitted to a public health organization.			194
PH.2.5.5 Function	Manage Immunization List		C	195
	Statement: Manage the Account Holder's immunization data and associated capabilities including reminders, alerts, compliance, and administration. **Description:** Immunization records can be maintained in the PHR-S. The list of immunizations can be associated with the health maintenance care plans in PH.1.3.3 maintaining a prospective immunization schedule for routine recommendations. In addition, vaccinations in preparation for foreign travel and episodic public health outbreaks such as bird flu vaccinations can be maintained here. Also, some jurisdictions accept titers or specific dates of infection as proof of adequate protection. Immunization information can be shared with national registries in order to support public health / population health stakeholder requirements. Example(s): The system SHOULD provide the ability to associate standard codes with discrete data elements associated with an immunization.			
1.	The system SHALL provide the ability to manage immunization histories associated with a PHR Account Holder.			196
2.	The system SHOULD capture as discrete data elements data associated with any immunization (this might include certification that the immunization was administered) according to organizational policy and/or jurisdictional law.			197
3.	The system SHOULD provide the ability to capture standard codes with discrete data elements associated with an immunization.			198
4.	The system SHOULD provide the ability to maintain standard codes with discrete data elements associated with an immunization.			199

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
5. The system SHOULD provide the ability to capture immunization administration details, such as date, route of administration, type, lot number, manufacturer, and the identity of the immunization administrator.				200
6. The system SHALL provide the ability to capture the currently recommended date for an immunization booster dose with each immunization if needed.				201
7. The system SHOULD provide the ability to render a PHR Account Holder's immunization history (e.g., when reporting to appropriate authorities such as public health immunization registries, schools, or day-care centers) according to organizational policy and/or jurisdictional law.				202
PH.2.5.6 Function	Manage Medical History			203
Statement: Manage the PHR Account Holder's medical history. **Description:** Significant or serious past medical illnesses and hospitalizations can be referenced in this list with a brief description and date. The past medical history list can also display standard life event reporting such as birth history used in pediatrics, for example: NVD at 36 weeks APGAR 7 and 9 (Normal vaginal delivery after 36 weeks gestation with APGAR scores of 7 and 9 at one and three minutes) and reproductive history used primarily by gynecologists: G4, P3, Ab1, postmenopausal (4 pregnancies, 3 live deliveries, 1 lost pregnancy, now postmenopausal). Medical Histories are typically created by healthcare professionals to summarize aspects of a given healthcare event, diagnosis, or condition (for example, appendectomy or diabetes). Example(s): The system SHOULD provide the ability to annotate the medical history.			
1. The system SHALL provide the ability to manage (either detailed or summary) medical history information (including the presence or absence of various conditions or symptoms and any associated annotations) that may exist in the provider(s) EHR-S or other systems according to organizational policy and/or jurisdictional law. Note: Medical History information can either be imported from a provider's system or entered by the PHR Account Holder, and includes the metadata regarding the creation, modification, viewing, extraction, or deletion of a record.				204
2. The system SHOULD provide the ability to capture and transmit a request for correction / amendment to a medical history (where the medical history was captured from an external source). For example, a report could be created by the PHR Account Holder that asserts that the provider's information is incorrect and sent to the provider with a recommendation that the provider's information must be repaired.				205
3. The system SHOULD provide the ability to capture and transmit to an external system a request for deletion/deprecation of erroneous PHR Account Holder's information (e.g., insertion of information into the PHR Account Holder's record that is of another person).				206
4. The system SHOULD provide the ability for the PHR Account Holder to annotate the medical history with text comments.				207
5. The system SHALL provide the ability to enter missing information in subsequent changes to the medical history.				208
6. IF medical history -related information is captured, THEN the system SHALL conform to PH.2.1 (Manage PHR Account Holder Originated Data) to identify the author/source/custodian of the information.				209
7. IF medical history-related information is captured, THEN the system SHALL conform to PH.6.1 (PHR Account Holder Health Data Derived from Administrative and Financial Sources) to identify the author/source/custodian of the information.				210
8. IF medical history-related information is captured, THEN the system SHALL conform to TI.2.2 (Auditable Records) to identify the author/source/custodian of the information.			C	211
PH.2.5.7 Function	Manage Surgical History		C	212
Statement: Manage the PHR Account Holder's history of surgical procedures. **Description:** The list of past procedures is a useful summary of what has been done in the past and anatomic changes have occurred that might influence current assessments and treatments. It is important to capture any surgical implants and associated lot/serial numbers for tracking/reporting purposes. For example, the consumer might desire to inform the provider that surgery was performed on the left arm (which was broken), not the right arm.			
1. The system SHALL provide the ability to manage the surgical history including the presence or absence of elements and associated annotations that may exist in the provider(s) EHR or other systems, according to organizational policy and/or jurisdictional law.				213
2. The system MAY provide the ability to capture, maintain, and transmit a request-for-correction to surgical history that was captured from an external source. Note: There could be multiple types of errors, both unintentional and intentional; the errors could also reside in multiple storage locations (primary, secondary, and intermediary); the errors could also reside in current records or in archived records; there could also be multiple sources (author, custodian-of-record, transcriptionist).				214
3. The system SHOULD provide the PHR Account Holder with the ability to annotate the surgical history with text comments.				215

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
4. The system SHOULD provide the ability to enter missing information regarding the surgical history list.				216
5. The system MAY provide the ability to manage implant information (e.g., by collecting device-identification numbers for a hip, lens, or breast implant; or by capturing the date of the implant).			C	217
6. The system MAY provide the ability to tag surgical history information (e.g., by category type (such as “implant”) or by procedure type (such as "excision" or "biopsy")).			C	218
PH.2.5.8 Function	Maintain Family History		C	219
Statement: Manage the PHR Account Holder's Family Health History. **Description:** The family history traditionally imparts the PHR Account Holder with certain risks and probabilities of illnesses that have a familial component. The major illnesses and cause of death of primary family members should be captured and displayed. For some illnesses of the PHR Account Holder a negative family history is also pertinent such as for cancer.				
1. The system SHALL provide the ability to manage family history according to organizational policy and/or jurisdictional law.				220
2. The system SHOULD provide the ability to capture, maintain, and transmit a request-for-correction to family history that was captured from an external source. Note: There could be multiple types of errors, both unintentional and intentional; the errors could also reside in multiple storage locations (primary, secondary, and intermediary); the errors could also reside in current records or in archived records; there could also be multiple sources (author, custodian-of-record, transcriptionist).				221
3. The system SHOULD provide the ability for the PHR Account Holder to annotate the family history with text comments (e.g., "Great-grandmother Alice was lost at sea” and that "Uncle Robert disagrees with the cause-of-death attributed to great-grandmother Alice".)			C	222
4. The system SHALL provide the ability to enter missing information regarding the family history.				223
5. The system MAY provide the ability to exchange family history entries with the PHR Accounts of other family members according to user preference and/or consent, user role, organizational policy, and/or jurisdictional law.				224
PH.2.5.9 Function	Manage Personal Genetic Information		C	225
Statement: Manage the Account Holder’s genetic information. **Description:** Limited personal genetic information is becoming available and it is anticipated that a much richer actionable data set will derive from current research. This function serves as a placeholder to take advantage of the scientific breakthroughs as they become available.				
1. The system MAY manage results of specific genetic tests, genetic markers, or findings according to user preference and/or consent, user role, organizational policy, and/or jurisdictional law.				226
2. The system MAY capture and present known genetically-based illnesses according to user preference and/or consent, user role, organizational policy, and/or jurisdictional law.				227
3. The system MAY capture and present a known single allele carrier status of a recessive genetic trait or diseases according to user preference and/or consent, user role, organizational policy, and/or jurisdictional law.				228
PH.2.5.10 Function	Manage Social History			229
Statement: Manage the PHR Account Holder's social history including, health related habits and risk factors. **Description:** The social history provides a profile with a number of characteristics that help define the PHR Account Holder's background and health risks. This information can be collected in, or related to, a health risk assessment. The PHR Account Holder is the primary author and authority of these topics commonly included in the social history: - Education - Work information such as: - - current employment status (e.g., employed for wages); - - current job data: job employment type (e.g. self-employed), occupation and industry with the start and end dates, employer name and location, job duties, work schedule; - - usual, or longest-held, occupation and industry, with duration and start date. - Family relationship (e.g., parent or sibling) - Marital status, care giver resources at home - Disability status or functional status - Living arrangement such as private home, adult family home, nursing home, or homelessness - Habits including smoking, alcohol, recreational drugs, use of seatbelts, helmets, hazardous sports, sexual practices - Travel history - Hazardous exposure such as asbestos, radiation exposure, sun exposure. Example(s): The system SHALL provide the ability to for the PHR Account Holder to maintain an accurate and current view of his or her health habits and risks.			

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
1.	The system SHALL provide the ability to manage the PHR Account Holder's social history according to organizational policy and/or jurisdictional law. For example: the PHR Account Holder's smoking history or work history can be informative to the PHR Account Holder's provider.		C	230
2.	IF the system captures the PHR Account Holder's social history from an external source, THEN the system MAY hide any flags or other indication(s) that the PHR Account Holder withheld information received from an external source (e.g., the PHR Account Holder might receive information from the therapist of a support group for people who have a family member who abuses alcohol, but could desire not to share that information with the PHR Account Holder's dentist).		C	231
3.	The system MAY provide the ability to capture, maintain, and transmit a request for correction to the PHR Account Holder's social history that was captured from an external source.			232
4.	The system MAY provide the ability to annotate the PHR Account Holder's social history.			233
5.	The system SHALL provide the ability to enter missing information regarding the PHR Account Holder's social history.			234
6.	The system SHOULD provide the ability to control-access to an external tool(s) that can support the translation of the PHR Account Holder's self-described job or profession into a standard code and/or data element (e.g., via an established vocabulary or code set).		N	235
PH.2.5.11 Function	Nutrition and Diet Information			236

Statement: Manage the PHR Account Holder's nutrition and diet-related information.

Description: Nutrition is related to health and wellness as well as chronic diseases. People want to record and monitor their food and nutrient intake including any nutritional supplements because they are trying to manage their weight, maintain their fitness level, or demonstrate progress towards the goals in their nutrition care plan. Diet and nutrient histories, (e.g., diet, nutritional supplements, enteral and parenteral feedings, vitamin and mineral supplements, history of breastfeeding, and other intake) may be relevant for review. Diet and nutrient lists are not limited to diet, enteral feeding, and vitamin and mineral supplement orders recorded by providers, but may include, for example, food and nutrient intake records, diet recommendations provided by a registered dietitian/nutritionist, and additional information such as weight, height, and Body Mass Index (BMI).

Example(s): The system maintains a food and nutrition history list that may be followed by the PHR Account Holder and referenced by his or her providers and Registered Dietitians. Copies of the PHR food and nutrition history list may be kept by their providers in their EHR systems.

Example(s): The system maintains a list of nutrition and diet-related information including food intake records, nutrient analysis summary records, energy balance data and nutrition care recommendations that may be followed by the PHR Account Holder and referenced by his or her providers including a Registered Dietitian.

1.	The system SHALL provide the ability for the PHR Account Holder to manage information regarding the PHR Account Holder's nutrition and/or diet.			237
2.	The system SHALL provide the ability for the PHR Account Holder to manage concerns (either self-generated concerns or concerns that were expressed by others) that relate to the PHR Account Holder's nutrition and/or diet.			238
3.	The system SHOULD provide the ability for the PHR Account Holder to capture his or her nutrition and diet information (specifically, current intake of foods and/or nutrients).			239
4.	The system SHOULD provide the ability for the PHR Account Holder to capture his or her nutrition and diet information (specifically, past history of intake of foods and/or nutrients (e.g., anorexic during teenage years; vegetarian from age 5 to 10).			240
5.	The system SHOULD provide the ability for the PHR Account Holder to import diet- and nutrition -related data from a provider's EHR system or from other sources (e.g., diet-related instructions from a provider; diet-related orders; or diet-related information that appears on an assessment).			241
6.	The system SHOULD provide the ability to capture, maintain, and render nutritional supplements, multi-vitamins, and herbal products as discrete data and/or as lists.			242
7.	The system SHOULD provide the ability to analyze drug-herb interactions and render a notification or alert regarding potentially harmful interactions.			243
8.	The system MAY provide the ability to analyze and render nutritional information (e.g., by calculating nutrient values for items or total daily intake summaries for macronutrients and micronutrients such as Energy (Kcal), Protein (grams), Carbohydrates (grams), Fat (grams), Saturated Fat (grams), Calories from Fat, Sodium (milligrams) and various vitamins (A, C, D, E, etc.)).			244
9.	The system MAY provide the ability to exchange food intake information and/or nutritional analysis data with third-party applications that have been authorized by the PHR Account Holder for such data exchange. For example, nutritional analysis information in the PHR that may be exchanged with external applications may include: - Total Calories (kcal or Cal) - Protein (g) - Carbohydrate (g) - Fat (g) - Plus Vitamins and Minerals. For example, food intake information in the PHR-S that may be exchanged with external applications may include foods and beverages (and portion sizes) that were actually consumed by the PHR Account Holder.			245
10.	The system SHOULD provide the ability for the PHR Account Holder to capture, maintain, and render physical activity information (which may include information regarding energy expended).			246
11.	The system MAY provide the ability to render (e.g., track, graph, chart, show an interpretive picture) the PHR Account Holder's ENERGY EXPEDITURE/BALANCE to show daily and/or weekly			247

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
	average kilo-calories or kilo-joules consumed and expended (if intake and energy expenditure data has been captured).			
12.	The system MAY provide the ability to capture information from physical exercise and/or training devices or applications that track physical activity and exercise information along with energy expenditure totals. For example, total workout summary information may include: - Date - Activity (e.g., running or swimming) - Duration (e.g., thirty minutes) - Distance (e.g., two kilometers) - Location (e.g., local street or swimming pool) - Intensity (based on five-point heart rate zones) (e.g., moderate or intense) - Speed (e.g., minutes-per-kilometer for running or miles-per-hour for bicycling) - Exercise-related physical measurements (e.g., minutes of significant exercise per week, or in the U.S., Exercise-Vital-Sign as defined by the American College of Sports Medicine).			248
13.	The system SHOULD provide the ability to capture, maintain, and render educational information that can promote the PHR Account Holder's understanding of the prescribed diet or nutrition care recommendations. For example, if the PHR Account Holder has a congenital disease, an acquired intolerance related to metabolism (e.g., Acquired Lactose Intolerance, Celiac Disease or Non-Celiac Gluten-Sensitivity), or an inborne error of metabolism (e.g., Glucose-6-Phoshate Dehydrogenase Deficiency (G6PD), Phenylketonuria (PKU), or Maple Syrup Urine Disease), then the PHR system might offer corresponding education.		C	249
14.	The system MAY provide the ability to analyze, determine, and render information regarding possible interactions between nutrients and allergies, intolerances, adverse reactions, sensitivities, problems, conditions, allergy cross-reactivity, genetic-status, time of ingestion, and genetic-predispositions. Therefore, the timing of medication administration need to carefully consider relative to other factors, such as food or supplement intake (or food or supplement withholding). For example, a PHR Account Holder who is pregnant could be informed that she should avoid consuming certain types of fish such as swordfish, shark or mackerel, and eat only limited amounts of tuna while pregnant due to the possibility of increased mercury exposure to the fetus. Another example, is that a person who is allergic to bananas, avocado, chestnut, and kiwi is also very likely to be allergic to latex. Another example is that a person who is on an anti-retroviral medication might need to wait one hour after taking the medication before ingesting calcium or magnesium supplements.			250
PH.3 Function	Wellness, Preventive Medicine, and Self Care			251
	Statement: Assist the PHR Account Holder with maintaining his or her wellness and management of their health conditions. **Description:** A competency of the personal health record is to encourage thoughtful, prospective management of our own health maintenance and conditions. Example(s): The system should maintain a life-long schedule for surveillance evaluations, clinical trials, and other healthcare information-related research studies.			
PH.3.1 Function	Manage Personal Clinical Measurements and Observations		C	252
	Statement: Provide the ability for the PHR Account Holder to enter personally-sourced data and to make it available electronically to authorized Health Care Provider(s) or other Authorized Users or applications. **Description:** The system should provide various ways for the PHR Account Holder to record self-generated health observations. Example(s): The system SHALL capture Account Holder's self-reported physical symptoms and daily functioning as structured or unstructured data.			
PH.3.1.1 Function	Manage Personal Observations and Care		C	253
	Statement: Provide the ability for the PHR Account Holder to enter personally-sourced data and to make it available electronically to authorized health care provider(s) or other authorized users or applications. **Description:** A PHR system can help a PHR Account Holder capture and maintain self-generated health observational information. That observational information can appear in structured and unstructured formats and/or as several media types. of observational methods could include structured or unstructured text documents, audio files from telephone devices, calendar entries, text messages, scanned or digital images (including photographs), and personal drawings. Example(s): The system SHALL capture Account Holder's self-reported health observations such as symptoms, vital signs and other physical conditions.			
1.	The system SHALL provide the ability for the PHR Account Holder to capture self-generated health observations (e.g., symptoms, vital signs, physical observations, direct-to-consumer laboratory studies, home health devices, (e.g., a blood sugar measurement device or a telemetric cardiac measurement device)).		C	254
2.	The system SHOULD provide the ability to capture the PHR Account Holder's self-measured and externally-sourced vital signs (e.g., blood pressure, temperature, heart rate, respiratory rate, and severity of pain) according to organizational policy and/or jurisdictional law.			255
3.	The system MAY capture other self-reported clinical measures (e.g., peak expiratory flow rate, size of lesions, or oxygen saturation) as discrete elements of structured or unstructured data.			256
4.	The system MAY provide the ability to capture the PHR Account Holder's self-reported mental health status according to organizational policy (e.g., using certain privacy and security protections). For example, the PHR Account Holder might note that the medication that has been		C	257

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
	prescribed by his physician is causing feelings of anger and depression (and suicidal ideation). If the PHR Account Holder shares that information with a healthcare organization, that organization might note that the PHR Account Holder's self-reported mental health status must be masked for members of the care team who do not have explicit permissions to view that data (i.e., only authorized health care provider(s)). The vendor organization that hosts the PHR system software might have a policy that states that that the PHR Account Holder's self-reported mental health status will not be exported without explicit consents and/or authorizations by the PHR Account Holder.			
	5. IF the system provides the ability to capture the PHR Account Holder's self-reported mental health status, THEN the system SHOULD provide the ability to capture corresponding consents and/or authorizations regarding the transmission of the PHR Account Holder's self-reported mental health status information according to organizational policy and/or jurisdictional law.		N	258
	6. The system SHOULD provide the ability to maintain educational information that can be used by the PHR Account Holder to understand his or her condition(s).			259
	7. The system SHOULD provide the ability to maintain educational information that can be used by the PHR Account Holder to understand and choose from various self-care options.			260
PH.3.1.2 Function	Communication with Home Monitoring Devices		C	261
	Statement: Provide the ability for the PHR Account Holder to capture and view home monitoring device data and to make it available electronically to authorized health care provider(s) or other authorized users or applications. **Description:** A variety of commercial devices are being developed to help monitor health conditions and compliance with care plans. Some of these commercial devices may offer standard electronic interfaces including wireless connectivity that may be captured by the system and integrated into the PHR. Simple examples include a pedometer recording walking activity, a continuous glucose monitor, a sleep apnea monitor and CPAP (Continuous Positive Airway Pressure) machine, and a pill dispensing device that prompts and records medication compliance. Medical Devices collect health information about an individual which may be exported to the PHR system, the EHR system, or another system. Depending on the purpose and capabilities of a given medical device, the device may be able to share its data with these systems in various formats, ranging from raw (unformatted) data, to coded / mapped values, to fully summarized and formatted reports. Furthermore, the systems may need to collect the data from the medical device in multiple formats. For example, a diabetic PHR Account Holder may use a PHR system to see a summary report from a blood pressure device that states, “Your blood pressure is very high today. Contact your physician immediately”, while an EHR system may require raw blood pressure data values from the past two weeks for the cardiologist. The same medical device may generate glucose values that are of interest to the PHR Account Holder’s registered dietitian/nutritionist. These values may be combined with values from other medical devices to create synthesized reports that are richer in content and value than those reports resulting from devices whose information cannot be synthesized. This level of power requires that the PHR system interact with medical devices in sophisticated ways, including: the ability to configure the medical device data input according to granularity, type, format, frequency, etc. of data collected; the ability to code or map data; the ability to summarize, filter, or merge data; the ability to route data to pre-designated role-types; the ability to tailor the data according to role-types; and the ability to transform the data into alerts or notifications. As the ability of the PHR system to manage medical device data increases, so does the value of the medical device data – and of the PHR system itself. Medical device -related gains made by the PHR system can, and should, be shared with EHR (and other) systems. The PHR system ought to be able to respond to a rules-engine request from an EHR (or other) system so that the PHR system can tailor its interactions with medical devices. For example, if the patient’s weight has increased more than 2% in the last week, the EHR system could recommend that the PHR system request blood pressure reports once an hour from a medical device, rather than once a day. Configuration of Medical-Device-Reports (exchanged between EHR and PHR systems) may be necessary (e.g., to cover, raw data, formatted data, summarized data, or filtered data). Reports may also be processed according to frequency or tailored by role (e.g., a daily report regarding weight sent to a registered dietitian/nutritionist, versus a weekly summary sent to a cardiologist). These reports may be merged with other reports and shared with multiple recipients. Example(s): The Account Holder may download blood sugar monitor data and transmit it to a healthcare provider.			
	1. The system SHOULD provide the ability to manage metadata regarding electronic home monitoring devices (e.g., serial number, unique device identifier, or name of the device).		C	262
	2. The system SHOULD provide the ability to manage information collected from home monitoring devices as part of the personal health record.			263
PH.3.2 Function	Manage Account Holder Implemented Care Plans			264
	Statement: Assist the PHR Account Holder to develop, manage, and adhere to (or comply with) his or her own care plans. **Description:** The PHR Account Holder may develop care plans related to health and wellness (such as training programs for sports) as well as to ameliorate a health condition. Self-developed care plans can be integrated into a comprehensive health and wellness plan. Example(s): Develop and implement an exercise program for optimizing cardiac fitness based on age, gender, and other health risks.			
	1. The system SHOULD provide the ability to manage the PHR Account Holder's self-generated care plans. Note: self-generated care plans can be constructed based on external recommendations from sources such as an established relationship with a care provider, an educational tool, or another informational resource.			265
	2. The system SHOULD provide the ability to maintain structured templates for the PHR Account Holder or the PHR Account Holder Proxy to design specific wellness care plans.			266

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
3.	The system SHOULD provide the ability to manage self-developed care plans with tasks, alerts, reminders, and calendar entries.			267
4.	The system MAY provide the ability to capture compliance with self-generated care plans and render notifications or alerts when the PHR Account Holder is out of compliance.			268
5.	The system MAY provide the ability to capture, maintain, and render information regarding the effectiveness of self-generated care plans.		N	269
6.	The system SHOULD provide the ability to integrate all care plans into one set of tasks, reminders, and calendar entries.			270
7.	The system SHOULD conform to function PH.6.7 (Manage Patient-Specific Care and Treatment Plans) in order to enable the PHR Account Holder to manage care plans that support treatments (e.g., treatments that need to be adjusted based on geographic location such as warm versus cold climate), physical body conditions (e.g., weight increases or decreases), long-term illnesses (e.g., diabetes), or health and wellness goals. Furthermore, provider-generated care plans might need to be adjusted when the PHR Account Holder alters a self-generated care plan. Finally, the providers who generated care plans might need to be notified when a certain care plan has been added, changed, or deleted.		N	271
8.	The system SHOULD conform to function PH.6.8 (Patient-Specific Care, Instructions, Treatment Plans, Guidelines and Protocols) in order to enable the PHR Account Holder to manage care plans that support treatments (e.g., treatments that need to be adjusted based on geographic location such as warm versus cold climate), physical body conditions (e.g., weight increases or decreases), long-term illnesses (e.g., diabetes), or health and wellness goals. Furthermore, provider-generated care plans might need to be adjusted when the PHR Account Holder alters a self-generated care plan. Finally, the providers who generated care plans might need to be notified when a certain care plan has been added, changed, or deleted.		N	272
9.	The system SHOULD conform to PH.3.3 (Manage Provider Implemented Care Plans) to accommodate the inclusion of the consumer-generated care plan with provider-generated care plans.		N	273
10.	The system SHOULD conform to PH.6.3 (Communications Between Provider and PHR Account Holder and/or PHR Account Holder Proxy) in order to promote the effective coordination of care plan elements and to communicate care plan changes to selected providers.		N	274
PH.3.3 Function	Manage Provider-Initiated Care Plans			275

Statement: Enable the PHR Account Holder to capture, record, and display Account Holder specific care plans received from authorized health care providers. An authorized health care provider's care plan(s) are typically provider-initiated, provider-defined, provider-rendered, and provider-implemented.

Description: Care plans may encompass a wide variety of styles, goals, and complexities, grouped into three categories: health maintenance, health restoration, and chronic disease management. Examples of the three categories of care plans include:

- Health Maintenance: The base care plan is a lifelong wellness plan that may specify age- and/or gender- specific health surveillance, an immunization schedule, and a diet and exercise program. It can be customized to accommodate specific health risks (such as hazardous exposures or genomic indicators).

- Health Restoration: Natural conditions (such as pregnancy) or acute illnesses may occur that require the management of specific diagnostic and/or therapeutic measures.

- Chronic Disease Management: Chronic disease care plans cover long term conditions (e.g., Type 1 diabetes).

Multiple care plans, treatment plans, or health activities (including those that are self-generated) need to be managed/reconciled in order to enable the prioritization/reconciliation of care plans: based on relative health outcomes and risk, based on a timewise ordering of care plans, based on a condition-related ranking of care plans, based on changes to insurance coverage of health care plan services, or based on potential contraindications that arise from conflicting care plans goals or methods.

There might also be certain restrictions against sharing health information in the case of infants or teenagers who might require special health information exchange protections.

Example(s): Capture and maintain a diabetic treatment plan that contains the pertinent staging details and multimodality plans in one place that can better coordinate the care by the diabetes-support team including the PHR Account Holder's Primary Care Provider.

1.	The system SHOULD provide the ability to capture provider-generated PHR Account Holder -specific care plan regimens and/or treatments (e.g., information regarding orders, therapies, wound care, or habit changes).			276
2.	The system SHOULD provide the ability to track updates to the PHR Account Holder's care plans, regimens, and treatments (e.g., including information regarding authors, creation date, version history, references, and sources as available).			277
3.	The system SHOULD provide the ability to present care and treatment plans captured from providers in their original format.			278
4.	The system SHOULD provide the ability to present a list of care plans and instructions indexed by provider, problem, and date.			279
5.	The system SHOULD provide the ability to manage care and treatment plans captured from provider(s) with tasks, alerts, reminders, and calendar entries.			280

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
6.	The system MAY capture compliance with provider-generated care plans and render notifications or alerts to the PHR Account Holder when the PHR Account Holder is out of compliance.			281
7.	The system MAY transmit out-of-compliance notifications or alerts to the originating provider and/ or to a person who is acting in the role of a provider (e.g., a registered dietitian/nutritionist who creates and signs a diet-order).			282
8.	The system SHOULD provide the ability to maintain decision support recommendations for care plans and treatment protocols that are sensitive to the context of PHR Account Holder data (e.g., peak flow, weight, blood pressure, food preferences).			283
9.	The system MAY provide the ability to analyze potentially conflicting decision support recommendations for care plans and treatment protocols (including self-generated care-plans) and present those potentially conflicting decision support recommendations for care plans and treatment protocols (e.g., if a provider-generated diabetic foot treatment plan recommends 20 days between formal examinations and an automated PHR system decision support module recommends 90 days between formal examinations, then the provider should be informed of the conflicting recommendations).		N	284
10.	IF the systemhas determined that potentially conflicting decision support recommendations for care plans and treatment protocols, THEN the system MAY provide the ability to transmit a request to a provider to harmonize those potentially conflicting decision support recommendations for care plans and treatment protocols.		N	285
11.	The system MAY provide the ability to capture order details for the PHR Account Holder in a manner that promotes understanding and compliance with an order.			286
12.	The system SHOULD provide the ability to capture externally-sourced (care plan -related) instructions or references to documents containing those instructions.			287
13.	The system SHOULD provide the ability to capture details on further care such as follow up, return visits, and appropriate timing of further care.			288
14.	The system MAY provide the ability to manage multiple care plans, treatment plans, or health activities (including those care plans, treatment plans, or health activities that are self-generated) according to user preferences and/or consents, organizational policy, and/or jurisdictional law.		N	289
PH.3.4 Function	Manage Medications			290

Statement: Assist the PHR Account Holder to manage his or her individual medications.

Description: Medications are a key modality of care plans. They provide significant benefit but also a risk of harm if not used appropriately. The original selection of medications as well as obtaining refills and renewals take up much of the PHR Account Holder's time. They can use their PHR-S to help manage their medications prescriptions, refills, and renewals.

Example(s): The system should provide the ability to communicate the refills/renewals requests to the pharmacy and the health care provider(s) or applications in a secure fashion.

1.	The system SHOULD provide the ability to determine and render, for a specific prescription medication, information regarding the level of insurance coverage that is offered by the PHR Account Holder's pharmacy benefit plan.			291
2.	The system SHOULD provide the ability to transmit refills/renewals requests to the pharmacy or the prescribing Health Care Provider(s) or applications (e.g., renewal of request for vitamins, contact lens solution, or insulin) according to organizational policy and/or jurisdictional law. NOTE: These transmissions may need to be performed in a secure manner, depending on the type of request.			292
3.	The system SHOULD provide the ability to transmit the PHR Account Holder's medication refill request to the pharmacy or pharmacy benefit manager according to organizational policy and/or jurisdictional law. Note: Some prescription refill requests for certain substances that are categorized as "controlled substances" (under certain jurisdictional law), are unable to be supported via electronic means (due to the possibility of fraud or abuse).			293
4.	The system SHOULD provide the ability to transmit the PHR Account Holder's request for prescription renewals to the Health Care Provider(s).			294
5.	The system MAY provide the ability to receive any communication about the request of the prescription refill or renewal from the pharmacy and/or from the Health Care Provider(s).			295
6.	The system SHOULD provide the ability to render an indication (e.g., notification or alert) that a medication is due for renewal or refill using information from internal and/or external sources according to organizational policy and/or jurisdictional law. Note: Requests for the renewal or refill of controlled substances may require special information handling considerations.			296
7.	The system SHOULD provide the ability to uniquely tag any medication on the medication list that is due for a refill using information from internal and/or external sources. Note: Information regarding controlled substances may require special consideration. Note: The information could be tagged either manually by the PHR Account Holder or transparently via the reception of information from an external source (such as a clinician).			297
8.	The system SHOULD provide the ability to uniquely tag any medication on the medication list that is due for a renewal using information from internal and/or external sources.			298
9.	The system SHOULD provide the ability to present the status of the refill or the renewal of the prescription to the PHR Account Holder.			299

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
10.	The system SHALL provide the ability to manage medication instructions received from the ordering clinician, pharmacist, or other authorized source.			300
11.	The system SHOULD provide the ability to manage weight-specific doses for over-the-counter and prescribed medications (e.g., pediatric doses, Aspirin for heart disease prevention).			301
12.	The system SHOULD provide the ability to determine recommendations for required immunizations and booster doses, including self-administered immunizations and when they are due, based on current immunization guidelines.			302
13.	The system SHOULD provide the ability to determine recommendations for required immunizations and booster doses based on the PHR Account Holder's risk factors.			303
14.	The system SHALL present the list of medications to be self-administered.			304
15.	The system SHALL provide the ability to capture medication administration details (including caregiver and/or self-administration details).			305
16.	The system SHALL provide the ability to manage all medications associated with a PHR Account Holder according to organizational policy and/or jurisdictional law.			306
17.	The system MAY provide the ability to render an indication to selected health care professional(s) that there is a possible need to harmonize and/or reconcile medications.		N	307
18.	The system SHOULD provide the ability for the PHR Account Holder to enter a self-prescribed medicinal or therapeutic means (e.g., a self-prescribed medication, nutritional supplement, and/or herbal supplement) onto the medication list.		N	308
PH.3.5 Function	Manage Tools and Functions to Assist Self Care			309

Statement: Provide various functions to allow the Account Holder to manage their health care events.

Description: The healthcare activities required of the Account Holder may be minimal and manageable. For some they may be complex, confusing, and overwhelming. Keeping track of multiple overlapping problems, providers, and care plans will take organization to manage successfully. Using the commonly understood desktop tools can aid the Account Holder to break down complicated processes into more manageable tasks and organize them. These tools may include:

- The health calendar
- The task list
- The contact list
- Reminders
- Alerts
- Recommendations

Example(s): Implement a complex care plan in the form of tasks, reminders, alerts, and calendar entries.

PH.3.5.1 Function	Manage Health Calendar			310

Statement: Provide a health calendar to record and display health care events.

Description: A health calendar provides a method to view time related healthcare activity both in the future as scheduled events and in the past as historic events. It is a handy and well understood format. The calendar can also be used as a data input device, mimicking the paper calendar where clinical observations (such as gallbladder attacks or menstrual periods) can be written directly onto a calendar and captured as a timed note. This idea was put forward from usability studies with lay people how they would like to interact with their PHR.

Example(s): IF a health calendar function is provided, THEN future appointments and other timed events SHOULD be displayed on the health calendar.

1.	The system MAY maintain a health calendar function for recording and displaying scheduled health appointments or events.			311
2.	IF a health calendar function is provided, THEN the system SHOULD present future appointments and other timed events on the health calendar.			312
3.	IF a health calendar function is provided, THEN the system SHOULD provide the ability to annotate directly onto the health calendar as date stamped text entries.			313
4.	IF a health calendar function is provided, THEN the system MAY present care plans (e.g., lifelong immunization schedules or cancer surveillance tests) as health calendar entries.			314
PH.3.5.2 Function	Manage Tasks			315

Statement: Healthcare events or activities that require the PHR Account Holder's participation can be organized as tasks.

Description: Care plans and other health care activities can be broken down into specific steps or tasks and organized on a task list that may be sorted by priority, date and time, problem, provider, and so forth. The task list entries should serve as an index to their supporting documents.

Example(s): Directions for a dressing change at a specific time of day can be displayed as an entry on the task list.

1.	The system SHOULD provide the ability for the PHR Account Holder to manage self-care, health maintenance, preventive, and wellness tasks, including the management of task status (e.g., performed, rescheduled, or canceled).			316

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
2. The system SHOULD provide the ability to determine a set of tasks for the PHR Account Holder based on a previously-defined set of business rules.				317
3. The system SHOULD provide the ability to capture, maintain, and render an indication of the status of tasks (e.g., completed or performed). For example, the dressing for a laceration needs to be changed every three days, but the PHR Account Holder failed to note yesterday that the dressing was successfully changed as required. Another example is the requirement to post an indication to the PHR system regarding daily compliance with dietary guidelines.				318
4. The system SHOULD provide the ability to render tasks in a sorted manner (e.g., by status or priority) according to user-preference, organizational policy, and/or jurisdictional law.				319
5. The system SHOULD present each task with a brief description and date on a task list included on the PHR Account Holder's summary view or dashboard.				320
6. The system SHOULD provide the ability for the PHR Account Holder to capture, maintain, and render descriptions of health-related tasks (and associated dates/times for those tasks).			N	321
7. The system SHOULD provide the ability to capture, maintain, and render communications that were received from others who are performing tasks (e.g., an indication from a member of a care team who completed or performed a certain task).			N	322
8. The system SHOULD conform to TI.7 (Workflow Management) to manage workflows and tasks that involve communications with others.			N	323
PH.3.5.3 Function	Manage a Registry and Directory of Actors			324

Statement: Each individual or entity that accesses the PHR-S should be identified in a directory that contains contact information and specific access rights.

Description: The PHR Account Holder should have control of who has access to his or her PHR-S. All entities that send information to or request information from the PHR-S should be identified for proper authentication and authorization. The PHR Account Holder may establish specific access rights for each actor or groups such as all emergency room physicians. The list of actors may be used to capture contact information for those without digital capability as well. Potential actors may include but are not limited to:

- PHR Account Holder Proxy
- Trusted relatives, friends, and caregivers.
- Healthcare providers that are part of the Account Holder’s team.
- Former providers and new providers not yet seen.
- Insurance plans.
- Pharmacy Benefits Manager, Pharmacies.
- Public health registries.
- Other registries including cancer, transplant and research.
- Hospitals, laboratories and diagnostic imaging centers.

All PHR data is associated with a source and all sources should be identified and maintained as long as the data is maintained.

All entities making a request for information or receiving information should be identified.

Example(s): Each provider should be registered before being granted access rights to the PHR-S.

1. The system SHALL maintain a directory of all Authorized PHR Users (e.g., actors or organizations) that have requested or have been granted access to the PHR Account Holder's account including data providers and PHR Account Holder Proxies that supply information for possible import into the PHR-S.				325
2. The system SHALL conform to section S.1.3 (Manage Health Care Provider Information), S.4.2 (Registry Notification and Management), S.4.3 (Manage Donor Information), S.4.5 (Manage PHR Account Holder Reminder Information Updates), PH.6.6 (Referrals and Referral Process (CC05 mentions a registry that lists people who abuse the healthcare system)) in order for the PHR Account Holder to control access rights to specific sections of the PHR-S for each actor in the directory according to user-preference, organizational policy, and/or jurisdictional law.				326
3. The system SHALL conform to functions in the Supportive Services Section that manage directory-related and/or registry-related information (e.g., information regarding a provider or a pharmacy).				327
PH.3.5.4 Function	Manage Reminders		C	328

Statement: Present the PHR Account Holder with reminders either sent by external sources or internally generated from information in the PHR-S.

Description: The PHR Account Holder will want to manage reminders sent by external sources (such as the PHR Account Holder’s provider(s)) or generated from information in the PHR (such as guideline-based reminders, prescription refills, or appointment reminders). A reminder is a notification of an upcoming event or activity that usually requires an action by the PHR Account Holder. Reminders may be displayed on a view in the PHR (such as the summary dashboard) and may also be displayed by other electronic means (such sent to an e-mail account).

Example(s): The system SHOULD send a reminder of an upcoming appointment as a text message to the PHR Account Holder’s cellular telephone.

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
1.	The system SHALL present the PHR Account Holder with reminders of scheduled events.			329
2.	The system SHALL manage timely reminders from PHR Account Holder provider(s) to include notifications for services, tests or actions that are due or overdue.			330
3.	The system SHOULD provide the ability to capture a history of notifications.			331
4.	The system MAY provide the ability to manage the PHR Account Holder's response(s) to notifications and/or reminders.			332
5.	The system MAY provide the ability to manage the PHR Account Holder's reason(s) for overriding a notification and/or reminder.			333
6.	The system MAY provide the ability to transmit to the sender of a notification and/or reminder the PHR Account Holder's response to that notification and/or reminder.			334
7.	The system SHOULD provide the ability to track PHR Account Holder-configured notifications and/or reminders.			335
8.	The system SHOULD provide the ability to manage PHR Account Holder notifications and/or reminders based on configuration options (e.g., repetitions or timing of the activity).			336
9.	The system MAY provide the ability to present options for the PHR Account Holder to configure preferences for notifications and/or reminders (e.g., posting on the PHR summary screen, e-mail, or text messages to another e-mail account or device).			337
10.	The system SHOULD provide the ability to update the content of notifications, guidelines, reminders, and associated reference materials.			338
11.	The system SHOULD provide the ability to receive and update content of notifications, guidelines, reminders, and associated reference materials from the PHR Account Holder's provider(s).			339
12.	The system MAY provide the ability to manage the lifecycle of the states of the notifications and/or reminders.			340
13.	The system SHOULD provide the ability to update the established criteria that trigger the reminders.			341
14.	IF indications for specific preventive services and accompanying reminders were previously captured, THEN the system SHALL present reminders to the PHR Account Holder of all specific preventive services (e.g., a follow up examination that is scheduled in the coming week).			342
15.	The system SHOULD provide the ability to receive secure messages of reminders or notifications from the PHR Account Holder's provider(s) to remind the PHR Account Holder of tests or actions that are due or overdue.			343
16.	The system SHOULD provide the ability to update a repetitive reminder by dismissing the reminder.			344
17.	The system SHOULD provide the ability to transmit a notification to the PHR Account Holder or the PHR Account Holder's designated representative that a reminder was not acknowledged.			345
PH.3.5.5 Function	Manage Health Alerts			346
	Statement: Notify the PHR Account Holder of an event or situation that may need immediate action. **Description:** Alerts may be generated by processes both internal to the PHR-S and external from outside sources such as a provider or governmental authority. Alerts may be issued in real time or may be used after an event is past due, when a situation may require a response. Alerts are also used to notify of potentially dangerous situations such as drug interaction alerts or public health alerts. Example(s): Notify the Account Holder with alerts to a public health emergency situation.			
1.	The system SHOULD track alerts.			347
2.	The system MAY provide the ability to manage the PHR Account Holder's response(s) to alerts.			348
3.	The system MAY provide the ability to manage the PHR Account Holder's reason(s) for overriding an alert.			349
4.	The system MAY provide the ability to transmit to the sender of an alert the PHR Account Holder's response to that alert.			350
5.	The system SHOULD provide the ability to track PHR Account Holder -configured alerts.			351
6.	The system SHOULD provide the ability to manage PHR Account Holder alerts based on configuration parameters.			352
7.	The system SHOULD present a number of options for the PHR Account Holder to configure how they prefer to receive alerts including posting on the PHR summary screen, as well as e-mail or text messages to another e-mail account or device.			353
8.	The system SHOULD provide the ability to update content of alerts and associated reference materials.			354
9.	The system SHOULD provide the ability to receive and update alerts from PHR Account Holder's provider(s).			355
10.	The system MAY provide the ability to manage the lifecycle of the states of the alerts.			356
11.	The system SHOULD provide the ability to update the established criteria that trigger the alerts.			357
12.	IF indications for specific preventive services and accompanying alerts were previously captured, THEN the system SHALL present alerts to the PHR Account Holder of all specific preventive services that are due.			358

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
13.	The system MAY provide the ability to render a list of all preventive services and the recommended timeframes that are due based on care plans that have been received or that exist within the PHR-S (e.g., some care plans may be imported from various care providers, another care plan may be self-generated by the PHR Account Holder).			359
14.	The system MAY provide the ability for the PHR Account Holder to maintain the severity level(s) for alerts (e.g., high, medium, or low priority alerts). For example, an internal clinical decision support algorithm may offer an alert to the PHR Account Holder that his blood pressure has exceeded the recommended range for his age and sex; another example is that the PHR Account Holder receives an alert from the PHR Account Holder's pharmacy's system that a medication needs to be refilled or that an existing prescription is about to expire. The PHR Account Holder could also choose to temporarily disable the presentation of low priority alerts while on vacation.			360
15.	IF the PHR Account Holder changes the severity level of an alert, THEN the system SHOULD provide the ability to transmit a notice to a member of the PHR Account Holder's care team informing them that the PHR Account Holder has changed the severity level of an alert. NOTE: This transaction could be a reimbursable care-provision event for the care team member. Also, a PHR Account Holder who abides by the recommendations offered by health care alerts could be rewarded with lower premium payments (due to decreased risk of non-compliance).		N	361
PH.3.5.6 Function	Manage Recommendations		C	362
	Statement: Capture and track provider recommendations for future care. **Description:** In many care activities, recommendations are made for specific future activities. They are easy to let slip by and lose track of them. A thoughtful and documented reason for not following a particular recommendation should be captured to help manage liability risk. Some recommendations may be controversial and there are reasons not to follow them. It is useful to keep a list of recommendations as a separate check on future care to be managed with the help of the PHR Account Holder's provider. Example(s): - The radiologist recommends a repeat mammogram in six months rather than the usual twelve months. - The Primary Care Provider recommends seeing a surgeon for occasional gallbladder attacks. - A screening colonoscopy is recommended after age fifty. - Annual screening or tests based on the PHR Account Holder's occupational risk factors.			
1.	The system SHALL provide the ability to capture recommendations from encounter and diagnostic studies in structured documents according to organizational policy and/or jurisdictional law (e.g., HIV results may need to be delayed from being sent directly to the PHR System, so that the provider has time to communicate with the patient directly).			363
2.	The system SHOULD provide the ability to capture a recommendation, the identity of the recommending provider, the date of the recommendation, and the date suggested to perform the recommended action.			364
3.	The system SHOULD provide the ability to link a recommendation entry with the corresponding original document (e.g., a recommendation to lose ten pounds should be linked to a document that contains the PHR Account Holder's most recent BMI readings).			365
4.	The system MAY provide the ability to render a pending (or future) recommendation (e.g., so that a provider might be able to create a future-order or reminder, or to document the reason that the recommendation was dismissed).			366
PH.3.6 Function	Population Health and Wellness			367
	Statement: The system may serve as a communication tool to help control public health risks and promote population wellness, as well as to target conditions for a specific population demographic and the PHR Account Holder specifically. **Description:** A formal and well-defined communication channel between public health agencies and the PHR Account Holder's PHR-S is useful. It provides for monitoring public health threats through data and observations captured within the PHR-S. Additionally, it alerts the PHR Account Holder to take corrective actions in response to public health threats. Example(s): The system SHOULD provide the PHR Account Holder the ability to subscribe to population health web site information.			
PH.3.6.1 Function	Public Health Reporting			368
	Statement: Provide reporting to authorized public health agencies as required by applicable jurisdictional law. **Description:** Government authorities with the mandate of preserving the health of the population have a need for early detection of public health threats such as identifying the early stages of an avian flu pandemic. This may require periodic reporting of certain de-identified personal health information (PHI). Other epidemiological studies for public health issues as well as public or private medical research studies may also request de-identified PHI. Certain public health reporting requires identified PHI and contact information for urgent epidemiologic investigations and countermeasures (such as for a resistant Tuberculosis outbreak). Note: When transmitting de-identified bio-surveillance data to a Public Health system, the receiver should understand the possibility that a single case may be inadvertently counted twice: once as an identified case from an EHR system, and once as a de-identified case from a PHR system. Example(s): The system SHALL conform to function S.3.3.1 (Manage Consents and Authorizations) regarding epidemiological investigations of clinical health within a population.			

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
1. The system SHOULD provide the ability to export de-identified and/or anonymized data for bio-surveillance and public health reporting to legally authorized public health agencies with appropriate consent according to organizational policy and/or jurisdictional law.				369
2. The system SHOULD provide the PHR Account Holder the ability to manage a subscription to population health web site information.				370
3. The system SHOULD capture alerts or warnings regarding population health threats.				371
4. IF providing de-identified data to legally authorized public health agencies, THEN the system SHALL conform to function S.3.3.1 (Manage Consents and Authorizations) regarding “Epidemiological Investigations of Clinical Health Within a Population" when providing de-identified data to legally authorized public health agencies.				372
5. The system SHOULD provide the ability for the PHR Account Holder to render information from population health web sites.				373
6. The system SHOULD provide the ability to de-identify data requested by public health agencies including appropriate consent.				374
7. The system MAY provide the ability to render notification to the PHR Account Holder regarding data requests from Public Health Agencies.				375
PH.3.6.2 Function	Public Health Risk Alerts			376
Statement: Support health risk alerts from authorized sources. **Description:** Alerts of a public health threat can be delivered by a Health Authority through a variety of channels, one of which can be to PHR Account Holders who provided prior consent for this service. The advantage of this modality is that the alerts can be prioritized to any special vulnerabilities of the PHR Account Holder based upon the Health Authority’s pre-existing claims data. More comprehensive background information and an action plan can then be included (such as alerts from government agencies regarding medications or devices). Example(s): Poor air quality alerts from governmental authorities are electronically sent to the registered PHR-S of a PHR Account Holder with a sensitive lung condition to take countermeasures.			
1. The system SHOULD provide the ability to manage health risk notifications from public health authorities or other external authoritative sources (e.g., an unstructured text-based message could be received regarding an influenza outbreak; a structured / codified message could be received that could be used in a clinical analysis engine that could route the notification to the PHR Account Holder's primary caregiver; or an alert could be received regarding a failing medical device that the PHR Account Holder uses that is identified via a Unique Device Identifier).			C	377
2. The system SHOULD provide the ability to render notifications of health risk to the PHR Account Holder.				378
3. The system MAY provide the ability to present specific actions to be taken by the PHR Account Holder based on a public health risk alert.				379
4. The system MAY provide the ability to manage notifications from social / community health organizations regarding services that might be expected / anticipated by the PHR Account Holder (e.g., the interruption of the daily distribution of food to the PHR Account Holder from a community service organization).			N	380
PH.4 Function	Manage Health Education		C	381
Statement: Provide reliable education and information customized to the PHR Account Holder based on the information in the PHR to help the PHR Account Holder explore treatment or wellness options. **Description:** A wide variety of educational materials are available and the problem is to identify authoritative sources that provide relevant information for the PHR Account Holder's age, sex, job, medical conditions, wellness goals, and health literacy. The system should be able to take a request for information and screen the available libraries of educational materials against clinical information in the PHR-S (including social history such as work information) without inadvertently or unknowingly divulging personal health information to those other systems. Example(s): - Provide breast feeding instructions in alternate languages for a new mother. - Provide educational material on asbestos or pesticide exposure, or healthy habits for workers on a rotating shift, based on data about a person's job.			
1. The system SHOULD provide the ability to maintain educational materials assumed appropriate for the level of health literacy and language of the PHR Account Holder or the PHR Account Holder Proxy.				382
2. The system SHOULD provide the ability to capture, maintain, and render evidence-based healthcare recommendations, with documentation of the sources of those recommendations, according to PHR Account Holder preference and/or consent, organizational policy, and/or jurisdictional law.				383
3. The system SHOULD provide the ability to capture, maintain, and render information about wellness, health goals, disease management, treatments, occupational risk factors, and related information that is relevant for a specific PHR Account Holder according to PHR Account Holder preference and/or consent, organizational policy, and/or jurisdictional law.			C	384

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
4.	The system SHOULD provide the ability to render educational information (that has been captured into the PHR) via a keyword search (e.g., presenting educational materials that contain the phrase "treatments for fractures").		C	385
5.	The system SHOULD provide the ability to render health educational information (that has been captured into the PHR) from external sources.			386
6.	IF the health education information is externally-based, THEN the system SHOULD provide the ability to capture and maintain a reference to that information (e.g., capture a hyperlink to a website that contains educational information regarding asthma).		C	387
7.	The system SHOULD provide the ability to maintain a reference (e.g., a hyperlink) to a library of educational material regarding a health concern, condition, occupational risk factors, or diagnosis.		C	388
8.	The system SHOULD provide the ability to manage applicable educational materials.			389
9.	The system SHOULD provide the ability to render multilingual educational material.			390
10.	The system MAY provide the ability to render PHR Account Holder educational materials using alternative modes to accommodate PHR Account Holder sensory capabilities (e.g., to accommodate difficulties in seeing, hearing, or distinguishing colors).		C	391
11.	The system SHOULD provide the ability to integrate guidelines and protocols captured in PH.5.1 (Manage Guidelines and Protocols) with the education files in specific searches.			392
12.	The system SHOULD provide the ability to capture and maintain educational material that was sent by an external entity. For example, a care giver might offer diet-related educational information to the PHR Account Holder; a pharmacy might send the PHR Account Holder educational material about a new medicinal product; the PHR Account Holder might locate an educational article on the Internet and place a copy in the PHR.			393
13.	The system MAY provide the ability for the PHR Account Holder to transmit educational material to external entities.			394
14.	The system SHOULD provide the ability to determine and present contextually-relevant educational materials based on possible courses of action suggested by an algorithm (e.g., a clinical decision-making algorithm) or other authoritative sources (e.g., a provider or a trusted educational service). For example, an algorithm that performs drug interaction checking might recognize a need to provide the PHR Account Holder with education regarding the signs and symptoms of an anaphylactic allergic reaction; expected changes related to nutritional intake (e.g., change in urine or stool color); possible changes related to medication side effects (e.g., itching and nausea for narcotic pain medication); potential organ failure (e.g., decreased urine output); or suggestions regarding the elimination of interferences (e.g., taking a medication one hour before taking a mineral supplement such as calcium, magnesium, or iron). This education is most essential when a new medication has been added to the patient's medication list which the patient has not taken before or when the PHR Account Holder first begins using the PHR system.			395
15.	The system MAY provide the ability to capture an indicator that the PHR Account Holder intends to receive, is receiving, or has received health education information and/or health educational services regarding a certain health problem and/or condition.			396
16.	The system MAY provide the ability to transmit an indicator to the PHR Account Holder's care plan team member(s) that the PHR Account Holder intends to receive, is receiving, or has received health education information and/or health educational services regarding a certain health problem and/or condition.			397
17.	IF certain regulations or legislation require the use of external health educational enhancements (on behalf of the PHR Account Holder), THEN the system MAY provide the ability to manage the use of technology that provides such health education (e.g., INFOBUTTON in the U.S.A.) according to PHR Account Holder preference and/or consent, organizational policy, and/or jurisdictional law.		N	398
18.	The system MAY provide the ability to present an indication that the health educational material that has been captured by the PHR-S has been vetted by a health information authority (e.g., presenting the stamp-of-approval offered by the Health-On-The-Net information-vetting organization) according to PHR Account Holder preference and/or consent, organizational policy, and/or jurisdictional law.		N	399
19.	The system MAY provide the ability to capture and render metadata regarding health educational material that has been captured by the PHR-S (e.g., the author or authoring organization, the author's credentials, the date-of-issue, and/or the date-of-last-review) according to PHR Account Holder preference and/or consent, organizational policy, and/or jurisdictional law.		N	400

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
PH.5 Function	PHR Account Holder Decision Support			401

Statement: Provide self-care -related decision support appropriate to the use of the PHR-S in self-care, home health, and remote settings.

Description: The PHR Account Holder may wish to seek assistance from diagnostic decision support tools, drug interaction checking, or published guidelines at the appropriate level of health literacy. The intent of this function is to provide the PHR Account Holder with education regarding sophisticated (or clinically complex) problems and also for more common (or more easily understood) problems, as well as support for assuming care of minor conditions. This function should also support the need for professional caregivers to govern, manage, respond to, or override self-care decisions made by the PHR Account Holder regarding acute or chronic conditions.

The PHR System could support the PHR Account Holder's need to understand particular medication- and nutrition- related handling and intake/administration requirements. These considerations could appear during drug-interaction checking, decision making educational investigations, care plan communications, and identification of duplicate therapies.

Example(s): The system should provide assistance to select an appropriate Internet based decision support tool to provide guidance in managing a young child with vomiting and fever.

PH.5.1 Function	Manage Guidelines and Protocols			402

Statement: Guidelines for general direction in managing a specific problem or condition can be acquired from a variety of sources for improved decision making.

Description: Guidelines help provide general direction to manage specific health risks or problems. They may be used by the PHR Account Holder to research a specific condition to verify that appropriate care is being provided. They may also be used to help self-manage minor conditions.

Example(s): Capture guidelines from the Internet for non-operative management of lower back pain.

1. The system SHOULD provide the ability to capture and maintain PHR Account Holder -specific health or treatment guidelines from healthcare providers or other trusted electronic healthcare sources.			403
2. The system SHOULD provide the ability to update PHR Account Holder -specific care plans and guidelines (e.g., isometric exercises in a business office versus swimming in a home pool).		C	404
3. The system SHOULD capture the source of the guideline.			405
4. The system SHOULD provide the ability for the PHR Account Holder to annotate the guideline.			406
5. The system SHOULD provide the ability to manage functionality that supports the PHR Account Holder's self-care plans that are based on guidelines (e.g., a task list, calendar entry, regularly scheduled alert, and/or reminders to perform a certain task).			407
6. The system MAY render an alert or reminder when the PHR Account Holder is out of compliance with a guideline.			408
7. The system MAY provide the ability for external stakeholders (e.g., including a PHR Account Holder Proxy, a physical exercise coach, or a registered dietitian/nutritionist) to present the PHR Account Holder's self-generated care plan(s) and transmit recommendations to the PHR Account Holder (e.g., a nutritionist offers recommendations regarding the PHR Account Holder's weight control plan that is based on a weight-control guideline). Note: The PHR Account Holder is able to accept or reject recommendations from external stakeholders regarding possible adjustment to the PHR Account Holder's self-generated care plan. The PHR Account Holder's self-generated care plan is different than the professional caregiver's care plan.		N	409

PH.5.2 Function	Drug Interaction Checking			410

Statement: Display warnings and severity levels of potential adverse interactions based on the data in the PHR Account Holder's medication and allergy list.

Description: Drug interaction and drug interference checking is a responsibility of the prescribing provider. However, the PHR Account Holder may be taking new over-the-counter medications or new prescription medications from providers without access to e-prescribing and may want to check for interactions and/or interferences. A complete interaction and interference check would take into consideration other prescribed medications, over-the-counter medications, allergies, relevant health conditions, age, weight, gender, diet and nutrition (e.g., mineral supplements, grapefruit juice, or pomegranate juice), environmental factors (e.g., phototoxic skin reactions to sunlight), absorption considerations (e.g., calcium interference with drug absorption), timing considerations (e.g., take immediately before sleeping), activity considerations (e.g., take before performing physical exercise), and relevant laboratory values such as creatinine clearance and liver function tests.

Example(s): Each time a new medication or a new allergy is entered into the PHR, perform an automated check for potential interactions among all of the current medication and allergy entries in the PHR.

1. The system SHOULD provide the ability to determine and render an alert to the PHR Account Holder regarding potential contraindications between prescribed medications (i.e., those medications that have already been captured onto the PHR Account Holder's current medication list) and over-the-counter (i.e., non-prescription) medications being considered for self-treatment.		C	411
2. The system SHOULD provide the ability to determine (possible) allergies, sensitivities, adverse reactions, interferences with medications, and/or intolerances to medications to facilitate allergy interaction checking decision support for medication (e.g., over-the-counter medication or		C	412

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
	a prescribed medication) orders including both prescribed medication and over-the-counter medication. For example, the PHR Account Holder might desire to compare the medications that are prescribed by two members of the PHR Account Holder's care team, in order to learn about potential adverse reactions. Each time a new medication or a new allergy is entered into the PHR, the PHR-S could perform an automated check for potential interactions among all of the current medication and allergy entries in the PHR. Also, the PHR-S could analyze possible reactions for medications that appear within "families" or classes of medications. A complete interaction and interference check would take into consideration other prescribed medications, over-the-counter medications, allergies, relevant health conditions, age, weight, gender, diet and nutrition (e.g., mineral supplements, grapefruit juice, or pomegranate juice), environmental factors (e.g., phototoxic skin reactions to sunlight), absorption considerations (e.g., calcium interference with drug absorption), timing considerations (e.g., take immediately before sleeping), activity considerations (e.g., take before performing physical exercise), and relevant laboratory values such as creatinine clearance and liver function tests.			
3.	The system SHOULD provide the ability to determine drug-drug interactions for all medications in the medication list (including prescribed and/or over-the-counter medications).			413
4.	The system SHOULD provide the ability to maintain a list of drug interaction warnings that was presented to a PHR Account Holder.			414
5.	The system SHOULD provide the ability to manage alerts (including overriding an alert) for adverse interactions or allergic reactions.			415
6.	The system MAY provide the ability to maintain the severity level at which warnings ought to be displayed.			416
7.	The system SHOULD provide the ability to determine and render duplicate therapies, such as two forms of the same medication (e.g., Percocet and acetaminophen), two medications with the same mechanism of action (e.g., two antihypertensives), or two medications in the same classification (e.g.,, two anticoagulants).			417
8.	The system MAY provide the ability to analyze and render educational information regarding the interaction between medications and nutrient intake. For example, when the system recognizes that the patient is taking an anti-coagulant (e.g., Coumadin) or a Non-Steroidal Anti-Inflammatory Drug (NSAID), then the system could offer education regarding the need to consider avoiding the intake of pomegranate juice, grapefruit juice, or alcoholic beverages.		N	418
9.	The system MAY provide the ability to manage the reason for the capture, update, or removal of the allergy, no-longer-allergic, intolerance, sensitivity, and/or adverse reaction to drugs and/or medications.		N	419
10.	The system SHOULD provide the ability to manage the source of allergy, intolerance, and/or adverse reaction information to drugs and/or medications (e.g., the source could be another system, a care provider, or the PHR Account Holder).		N	420
11.	The system MAY provide the ability to tag as deactivated an allergy, intolerance, and/or adverse reaction to drugs and/or medications.		N	421
12.	The system MAY provide the ability to capture as discrete data the reason for deactivation of an allergy, intolerance, and/or adverse reaction to drugs and/or medications.		N	422
13.	The system MAY provide the ability to render an allergy, intolerance, and/or adverse reaction to drugs and/or medications that has been tagged as deactivated.		N	423
14.	The system SHALL provide the ability to capture and render the date on which allergy to drug and/ or medication information was entered.		N	424
15.	The system MAY provide the ability to capture and render the approximate date of the allergy occurrence to drugs and/or medications.		N	425
16.	The system MAY provide the ability to capture and render that the allergies to drugs and/or medications are "Unknown" or "Unable to Assess Allergies".		N	426
17.	The system MAY provide the ability to capture and render the reason for "Unknown" or "Unable to Assess Allergies" to drugs and/ or medications.		N	427
18.	The system MAY provide the ability to tag records and render that the allergies are "Unknown" or "Unable to Assess Allergies" and need to be updated.		N	428
19.	The system SHOULD provide the ability to capture free text allergies, intolerances, or adverse reactions and render them in a manner that distinguishes them from coded allergy, intolerance, or adverse reaction entries.		N	429
20.	The system SHOULD tag and render an indication that automated interaction checking (e.g., drug-allergy checking) will not be applied against allergies, intolerances, and/or adverse reactions that were entered in free text format.		N	430
21.	The system MAY provide the ability to render historical information regarding drug-interactions and/or drug-interferences (e.g., showing the incidences of skin reactions that occurred when a certain medication was used at various times in the past few decades).		N	431
22.	The system MAY provide the ability to render historical information regarding the actions taken by the PHR Account Holder in response to drug-interactions and/or drug-interferences.		N	432
23.	The system MAY provide the ability to link an allergy, intolerance, and/or adverse reaction with diagnostic results (e.g., laboratory or allergy test result).		N	433

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
24. The system MAY capture an indication that the PHR Account Holder was presented with, and acknowledged, a drug interaction and/or drug interference notification.			N	434
PH.5.3 Function	Care-Related Decision Support		C	435
Statement: Provide decision support tools (including clinical decision support, best practice guidelines and/or recommendations from payers, employers, researchers, professional associations, or public health organizations). **Description:** The system should aid the PHR Account Holder with making his or her self-assessments and treatment plans for self-care. Some decision support algorithms are straightforward and can be provided as part of the PHR-S service. Others may be more complex and are detailed in function PH.5.4 (Integration with Third Party Clinical Decision Support Services). For example, a child's weight and height can be plotted on a growth curve chart which graphically displays growth progress. Another example, is the ability for a pregnant woman to plot weight changes over time against a norm.				
1. The system SHOULD provide the ability to render information regarding health guidelines and best practices.				436
2. The system MAY provide the PHR Account Holder the ability to analyze health data and context-driven assessments in comparison to practice standards in order to prompt additional testing, possible diagnoses, or adjunctive treatment.				437
3. The system SHOULD provide the ability to capture from an authoritative source (e.g., provider EHR-S or a care management PHR-S) rules related to abnormal trends.				438
4. The system MAY provide the PHR Account Holder the ability to analyze health data and context-driven assessments in comparison to practice standards in order to prompt additional testing, possible diagnoses, or adjunctive treatment.				439
5. The system MAY provide the PHR Account Holder the ability to analyze assessment data in correlation with the data in the PHR Account Holder's problem list.				440
6. The system MAY render a notification to the PHR Account Holder to request additional assessments, testing, or adjunctive treatment.				441
7. The system MAY render a notification to the PHR Account Holder to follow a provider-designated care plan related to assessment results (e.g., peak flow results, blood glucose readings, weight, or blood pressure).				442
8. The system MAY provide the ability to integrate health information contained in the PHR with appropriate health education materials (e.g., consumer self-identified as a smoker vis-à-vis smoking cessation materials sent to the PHR-S).				443
PH.5.4 Function	Integration with Third Party Clinical Decision Support Services			444
Statement: Provide the ability to query external clinical decision support services designed for the lay consumer. **Description:** A variety of clinical decision support services are currently available for professional use; a growing number of these services are becoming available for lay use. The primarily focus of these services is to assist with making an assessment and then recommending a treatment protocol. Example(s): Provide access to clinical decision support services that provide differential diagnoses and advice for further management for common complaints such as sore throat or cough.				
1. The system SHOULD provide the ability for the PHR Account Holder to manage their registration(s) to a third-party clinical decision support service(s) (e.g., the name of the service, the Internet address of the service, the date of the registration, the status of the registration) according to user preference, organizational policy, and/or jurisdictional law. NOTE: The identification of third-party clinical decision support services could be handled either by the PHR Account Holder, the vendor, or both.				445
2. The system SHOULD provide the ability for the PHR Account Holder to tag the PHR-S information that is shared with a third-party clinical decision support service.				446
3. The system SHOULD provide the ability for the PHR Account Holder to render responses to specific structured questions from a third-party clinical decision support service.				447
4. The system MAY provide the ability to analyze problems/conditions (in terms of the onset and/or duration, frequency/pattern, and impact on Activities of Daily Living of the condition/problem) and render findings/issues/alerts to the PHR Account Holder (for possible transmission to a member of the care team) according to user preference, organizational policy, and/or jurisdictional law. The ingredients of this analysis might only appear (collectively) in the PHR Account Holder's PHR. The results of such an analysis could be shared with certain members of the PHR Account Holder's care team for consideration. For example, the PHR Account Holder becomes less physically active and wonders why, the PHR system can analyze the PHR Account Holder's conditions and suggest that the increased amount of joint pain as a possible factor.		N		448
5. The system MAY provide the ability to analyze medications and therapies that are prescribed by clinicians and render findings/issues/alerts to the PHR Account Holder (for possible transmission to a member of the care team) according to user preference, organizational policy, and/or jurisdictional law. The ingredients of this analysis might only appear (collectively) in the PHR Account Holder's PHR. The results of such an analysis could be shared with certain members of the PHR Account Holder's care team for consideration. For example, the PHR Account Holder		N		449

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
	begins eating bananas and wonders why the medication being consumed does not seem to be as effective; the PHR system analyzes the nutrient-drug interaction as a possible factor.			
6.	The system MAY provide the ability to analyze exacerbating factors (e.g., environmental or emotional factors) and render findings/issues/alerts to the PHR Account Holder (for possible transmission to a member of the care team) according to user preference, organizational policy, and/or jurisdictional law. The ingredients of this analysis might only appear (collectively) in the PHR Account Holder's PHR. The results of such an analysis could be shared with certain members of the PHR Account Holder's care team for consideration. For example, the PHR Account Holder begins feeling depressed and wonders why; the PHR system analyzes the PHR Account Holder's recent birth of a child as a possible factor.		N	450
7.	The system MAY provide the ability to analyze the nutrients that are consumed and render findings/ issues/alerts to the PHR Account Holder (for possible transmission to a member of the care team) according to user preference, organizational policy, and/or jurisdictional law. The ingredients of this analysis might only appear (collectively) in the PHR Account Holder's PHR. The results of such an analysis could be shared with certain members of the PHR Account Holder's care team for consideration. For example, the PHR Account Holder begins eating bananas and wonders why the medication being consumed does not seem to be as effective; the PHR system analyzes the nutrient-drug interaction as a possible factor.		N	451
8.	The system MAY provide the ability to analyze the genetic profile of the PHR Account Holder and render findings/issues/alerts to the PHR Account Holder (for possible transmission to a member of the care team) according to user preference, organizational policy, and/or jurisdictional law. The ingredients of this analysis might only appear (collectively) in the PHR Account Holder's PHR. The results of such an analysis could be shared with certain members of the PHR Account Holder's care team for consideration. For example, the PHR Account Holder begins to feel sluggish and wonders why; the PHR system analyzes the PHR Account Holder's genetic profile and offers sickle cell anemia as a possible factor.		N	452
9.	The system MAY render an alert or notification to certain members of the PHR Account Holder's care team regarding the results of problem/condition analyses (including the components of those analyses) according to user preference, organizational policy, and/or jurisdictional law.		N	453
PH.5.5 Function	PHR Account Holder Configured Alerts, Reminders, and/or Notifications			454
	Statement: Alerts, reminders, and/or notifications are configured by the PHR Account Holder based on a variety of triggers or conditions. **Description:** The PHR Account Holder may desire to configure specific alerts, reminders, notifications, and/or notices (e.g., to promote compliance with physician orders, manage chronic conditions, perform routine health care measurements, or meet personal wellness goals). Note that the quantity, timing, or priority of such notices might also need to be configured. Example(s): The system SHOULD provide the ability to present medication recommendations based on findings related to a physician's diagnosis.			
1.	The system SHOULD provide the ability to manage (e.g., by creating, capturing, correcting, updating) alerts, reminders, and/or notifications.		N	455
2.	The system SHOULD provide the ability to capture, maintain, and render configuration parameters regarding alerts, reminders, and/or notifications.		N	456
PH.5.6 Function	Manage Updated Orders, Recommendations, or Alternative Care Plans		C	457
	Statement: Manage Updated Orders, Recommendations, or Alternative Care Plans. **Description:** The PHR Account Holder might need to receive updated orders or recommendations from care team members; or receive alternative care plan recommendations as the PHR Account Holder's conditions (or goals) change or when different modalities-of-care are recommended or chosen; or as elements of the PHR Account Holder's care plan change. For example, a physician might recommend an alternate drug if the physician notices that the price of the currently-prescribed drug increases dramatically or that the current drug is proving to be less effective than previously experienced. By accepting this new drug, the PHR Account Holder might then need to reconfigure the PHR system to present reminders for the PHR Account Holder to take the medication every third day instead of once-a-week.			
1.	The system SHOULD provide the ability to manage updated orders, updated recommendations, and/or alternative care plans.		N	458
2.	The system SHOULD provide the ability to manage updated orders (e.g., by presenting updated recommendations for medication regimens based on new findings related to a physician's diagnosis, or by presenting updated recommended laboratory monitoring protocols with respect to the use of a particular medication (e.g., by presenting a recommendation to send a blood sample to the laboratory every two days when using insulin)).		N	459
3.	The system SHOULD provide the ability to manage updated recommendations (e.g., by presenting recommendations for medication regimens based on findings related to a physician's diagnosis).			460
4.	The system SHOULD provide the ability to manage alternative treatments (or proposed alternative treatments) (e.g., by presenting alternative treatments in medications on the basis of updated practice standards, updated costs, updated formularies, and/or updated protocols).			461

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
PH.6 Function	Manage Encounters with Providers			462

Statement: Manage information for scheduling, preparation, and assimilation of knowledge gained by encounters with providers.

Description: Each interaction with a provider, including office visits, virtual visits, hospitalizations, telephone conversations, or diagnostic procedures, comprise an encounter. Some encounters are non-discretionary such as emergent admission to a level 1 trauma center. Many encounters are initiated by providers in the course of care such as a scheduled chemotherapy treatment. Some encounters are initiated by the PHR Account Holder requiring additional steps facilitated by their PHR-S.

Example(s): The Account Holder makes a self-assessment that his or her chest pain warrants urgent evaluation and telephones an ambulance service. Access to the PHR Account Holder's PHR information is provided to the ambulance crew and emergency room staff. The resulting assessments, updates to the current data set including problems, procedures, and medications, and new care plans from the hospital evaluation are then incorporated into the PHR Account Holder's PHR-S during or shortly after the encounter concludes. The Primary Care Provider receives an alert to the changes.

PH.6.1 Function	PHR Account Holder Health Data Derived from Administrative and Financial Sources			463

Statement: The system should capture and manage financial information related to the encounter.

Description: Tracking the personal costs of healthcare can be complex. Charges are typically discounted by the insurance plan to allowed charges. They will pay a portion of allowed charges with the PHR Account Holder being responsible for the rest. A given encounter such as a hospitalization will have multiple charges from several providers. Capturing the Explanation Of Benefits from the insurance plan can help monitor the expenses.

Example(s): The system should capture charge information and payment data from the Explanation Of Benefits (EOB) and associate it with the encounter records stored in the PHR-S.

1.	The system SHOULD provide the ability to capture and maintain information related to financial data and the current balances from the PHR Account Holder's health-related financial accounts.			464
2.	The system SHOULD provide the ability to capture a request for the correction (e.g., if the data is known to be incorrect) and/or annotation (e.g., if another opinion exists regarding the correctness of the data) of the administrative or financial data.			465
3.	The system SHOULD provide the ability to capture financial details and link those details to each clinical encounter or billable service (e.g., charges, allowed charges, or payments made by an insurance plan or by the PHR Account Holder).			466
4.	The system MAY provide the ability for the PHR Account Holder to render financial and administrative data and the data about those health-related accounts.			467
5.	The system MAY provide the ability to render a notification to the PHR Account Holder of any changes to the financial data or health-related accounts.			468
6.	IF health data is derived from administrative and financial data, THEN the system SHALL provide the ability to capture data about, and a reference to, the source of the health data.			469
7.	The system MAY provide the ability to capture metadata about certain PHR Account Holder's health data that was derived from administrative and financial data, and link that metadata with the corresponding health data. For example, the fact that the PHR Account Holder broke a leg could be derived from an invoice from an insurance company that describes a procedure performed at the provider's site of a pin being inserted into a leg; the derived health data (the fact about the broken leg) needs to be associated with the financial data (the invoice) and with administrative data (the provider's site).		C	470
8.	IF certain health data was derived from administrative and financial data, THEN the system SHALL provide the ability to render that health data to Authorized PHR Users, including metadata regarding the administrative and financial data from which that health data was derived.			471
9.	The system MAY provide the ability to render information from interactions with the PHR Account Holder's insurance coverage systems (e.g., employer's benefit system or the insurance company's benefit information system).			472

PH.6.2 Function	Manage Self-Assessments (i.e., Symptoms)			473

Statement: Manage information related to self-assessments.

Description: The PHR Account Holder may make a self-assessment regarding certain symptoms they may be experiencing, concluding that they need an encounter with a provider. This self-assessment should include a specific reason or reasons for the encounter (referred to as the chief complaint(s)) and personal observations or measurements that might be germane to the encounter.

Example(s): The system SHALL provide the ability to document self-assessments using standard self-assessments germane to the age, gender, developmental state, and health condition as appropriate.

1.	The system SHOULD provide the ability to capture self-assessments.			474
2.	The system SHOULD provide the ability to capture self-assessments using templates (if available).			475
3.	The system SHOULD provide the ability to capture self-assessments using standard self-assessments germane to the age, gender, developmental state, and health condition as appropriate.			476
4.	The system SHOULD provide the ability to capture data relevant to a standard self-assessment.			477

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
5. The system SHOULD provide the ability to capture PHR Account Holder's self-reported physical symptoms and daily functioning as structured or unstructured data.				478
6. The system SHOULD provide to ability to capture PHR Account Holder's self-reported mental health status as structured or unstructured data.				479
7. The system MAY provide the ability to capture other self-reported clinical measures (e.g., peak expiratory flow rate, size of lesions, or oxygen saturation).				480
8. The system MAY analyze and present percentile values when data with normative distributions are entered.				481
9. The system MAY render normal ranges for data based on age and other parameters (such as height, weight, ethnic background, or gestational age).				482
PH.6.3 Function	Communications Between Provider and PHR Account Holder and/or PHR Account Holder Proxy			483
Statement: The system should enable the PHR Account Holder to capture information in preparation for an encounter with a provider and to support ongoing interactions with that provider. The system should enable the PHR Account Holder to request appointments with health care providers and capture information in preparation for the encounter. **Description:** The PHR Account Holder may fulfill specific requests for data or obtain requested diagnostic studies prior to the formal encounter. This may include providing PHR-S access to the new provider. The provider could also communicate with various members of the PHR Account Holder's care team. Example(s): The PHR Account Holder MAY fill out a current Review Of Systems (ROS) template questionnaire and specific chief complaint related questions as part of the History of Present Illness (HPI) prior to the encounter.			
1. The system SHALL provide the ability to capture and maintain communications between providers and the PHR Account Holder and/or the PHR Account Holder's Proxy according to organizational policy and/or jurisdictional law.				484
2. The system SHOULD provide the ability to manage scanned documents based on the document type (e.g., based on the quality, format, origin, completion status, or intended diagnostic use (e.g., a screening versus a diagnostic breast examination)).				485
3. The system SHOULD provide the ability to capture and maintain communications (e.g., date, entity, or details of communication) that were originated by the PHR Account Holder or Authorized PHR User.				486
4. The system SHALL provide the ability to capture, maintain and render PHR authorization information (e.g., to support a designee's claim that the designee is authorized to receive PHR Account Holder-related health information).				487
5. The system SHOULD render to the PHR Account Holder a notification of the arrival of a provider-originated communication.				488
6. The system SHOULD provide the ability to exchange communications between providers and PHR Account Holders using a secure connection.				489
7. The system SHALL conform to PH.6.3 (Communication Between Provider and PHR Account Holder and/or the PHR Account Holder's Representative) in order to exchange information.				490
8. The system SHALL conform to TI.1.8 (Patient Privacy and Confidentiality) to support adherence to various levels of confidentiality when exchanging information.				491
9. The system SHOULD provide the ability to tag a set of elements within the PHR Account Holder's self-generated care plan that the PHR Account Holder intends to send to selected care team members.			N	492
10. IF the PHR Account Holder is creating a self-generated care plan, THEN the system SHOULD provide the ability for the PHR Account Holder to tag a set of selected care team members (to whom the PHR Account Holder intends to send certain information).			N	493
11. The system SHOULD provide the ability to transmit a tagged set of elements within the PHR Account Holder's self-generated care plan to a tagged set of selected care team members.			N	494
PH.6.4 Function	Data and Documentation from External Clinical Sources		C	495
Statement: The system should capture, index, and store documentation related to the encounter. **Description:** Most encounters generate documentation that can be captured in the PHR-S. Additional supporting data such as diagnostic reports or consultations may be included. A prolonged hospitalization encounter may encompass numerous structured or unstructured documents. Example(s): The system should capture, index, and store encounter information, including the encounter document or summary, laboratory results, radiographic images, PACS, EKG, and scanned documents.				
1. IF information is received through any electronic interface or is electronically referenced, THEN the system SHALL present it upon request, according to organizational policy and/or jurisdictional law.				496
2. The system SHALL provide the ability to capture externally-sourced electronic clinical documentation including original, updates and addenda, according to organizational policy and/or jurisdictional law.			C	497

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
3. The system SHOULD provide the ability to capture and maintain externally-sourced electronic clinical documentation and annotations with structured content including problems, diagnoses, office visit, phone communication, e-mail consultations and laboratory results.				498
4. IF externally-sourced electronic clinical documentation is captured from encounters with providers, THEN the system SHALL provide the ability to present that documentation to the PHR Account Holder.				499
5. The system SHOULD provide the ability to render notes based on filters, search, or sort criteria.				500
6. The system SHOULD provide the ability to exchange data using documentation templates.			C	501
PH.6.5 Function	Provider Assessments			502
Statement: Enable the PHR Account Holder to capture provider assessments and their supporting documentation such that the PHR Account Holder or another provider may independently review the assessments. **Description:** The provider may make assessments (observations, working hypotheses, differential diagnoses, or definitive diagnoses) derived from the new clinical information obtained during the encounter supplemented by additional PHR information including the current state data set. These assessments will direct further diagnostic, therapeutic, and health maintenance care. Example(s): The system MAY provide the ability to compare assessment data entered during the encounter and the accessed health evidence-based guidelines and best practices.				
1. The system SHALL provide the ability to capture and maintain health assessment data needed to support an assessment.				503
2. The system SHOULD provide the ability to capture standardized assessments that correspond to the problem list (including new problems defined during the encounter).				504
3. The system SHOULD provide the ability for the PHR Account Holder to annotate an assessment.				505
4. The system MAY provide the ability to capture evidence-based standardized assessments (e.g., data-collection instruments, engines, templates, or forms); practice standards; or other generally-accepted, verifiable, and regularly-updated clinical sources (e.g., updated clinical protocols for evaluation or treatment).				506
5. The system MAY provide the ability to determine and render appropriate assessment data to be entered during the encounter.				507
6. The system MAY determine and render appropriate health evidence-based guidelines and best practices.				508
PH.6.6 Function	Referrals and Referral Process			509
Statement: Manage information related to referrals for the PHR Account Holder's benefit and convenience. **Description:** For many referrals to other provider organizations, the PHR Account Holder must manage data, approvals, and appointments related to the referral. The PHR Account Holder may need to ensure that relevant data are received by the provider for the referral encounter. The PHR Account Holder may need to interact with his or her insurance company to secure authorization for payment for a referral to a provider. Examples of methods of transmittal include: secure email or enhanced data sharing. Examples of target referrals includes: referral service organization processing referrals on behalf of multiple healthcare providers that could be regional or jurisdictional. Example(s): The system SHOULD provide the ability to include test and procedure results with a referral.				
1. The system SHOULD provide the ability to transmit clinical and administrative data (e.g., insurance information) as part of the referral process to the provider who is receiving the referral.				510
2. The system SHOULD provide the ability to render test and procedure results with a referral.				511
3. The system SHOULD provide the ability for the PHR Account Holder to control access to the PHR Account Holder's information by allowing temporary privileges to the referring provider or provider's representative (e.g., viewing, printing, downloading, or exporting).				512
4. The system SHOULD provide the ability to transmit clinical data, administrative data, test results, and/or procedure results to the provider who is the target of a referral or to a referral service.				513
PH.6.7 Function	Patient-Specific Care, Instructions, Care Plans, Treatment Plans, Guidelines and Protocols		C	514
Statement: The system should facilitate the development of provider-generated care plans and the capture of provider-generated discharge instructions, and facilitate their capture and integration by the PHR-S. **Description:** The provider may develop and recommend a specific care plan and/or treatment plan that is tailored to the PHR Account Holder's particular circumstances including information in his or her PHR-S. The care plan and/or treatment plan may require input from several providers developed over multiple encounters. This includes enabling authorized Health Care Provider(s) to generate, communicate and record specific instructions, including discharge instructions, instructions about diet, clothing, transportation assistance, convalescence, follow-up with physician, and other related instructions. Types of providers that may offer instructions include: medical provider, social worker, physical therapist, respiratory therapist, occupational therapist, pharmacist, or a nurse.				
1. The system SHALL provide the ability to capture externally-sourced instructions or references to documents containing those instructions. Examples of instructions include: Patient-specific Care Instructions, Discharge Instructions, Treatment Plan instructions, Guidelines and/or Protocols, ad hoc instructions that were created by the provider, or institutional educational/instructional				515

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
	materials. Examples of externally-sourced instructions might include: documents, websites, pictures, videos, and/or sounds.			
2.	IF the system has captured externally-sourced instructions or references to documents containing those instructions, THEN the system MAY provide the ability to integrate those instructions as business rules and/or workflow rules. Examples of instructions include: Patient-specific Care Instructions, Discharge Instructions, Treatment Plan instructions, Guidelines and/or Protocols, ad hoc instructions that were created by the provider, or institutional educational/instructional materials. Examples of externally-sourced instructions might include: documents, websites, pictures, videos, and/or sounds.		N	516
3.	The system SHOULD provide the ability to capture details on further care (such as follow up, return visits, and appropriate timing of further care).			517
4.	The system SHOULD provide the ability to analyze and present abnormal trends with respect to the PHR Account Holder's expected or desired health or wellness outcomes (e.g., the PHR Account Holder could be alerted that the care plan anticipates a weight reduction of 1/2 pound (0.2 kg) per week, but the PHR Account Holder is actually gaining weight; or that blood glucose levels have exceeded 150 milligrams per deciliter for more than one week).			518
5.	The system MAY provide the ability to update site-specific and PHR Account Holder care plans and guidelines (e.g., isometric exercises in office versus swimming in home pool).			519
6.	The system MAY provide the ability for the PHR Account Holder to capture and maintain site-specific and PHR Account Holder care plans and guidelines (e.g., isometric exercises in office versus swimming in home pool).			520
7.	The system MAY determine, track and render alerts, notifications and reports about variances from care plans, guidelines, and discharge instructions. For example, a PHR Account Holder Representative could receive a text message notification, indicating that the PHR Account Holder failed to acknowledge compliance with a certain care plan, guideline, or discharge instruction.			521
PH.6.8 Function	Manage Patient-Specific Care and Treatment Plans			522
	Statement: The system should facilitate the capture and implementation of the care plan in the PHR-S. **Description:** Once a care plan is developed it should be incorporated into the PHR-S. The care plan may be limited in scope or comprehensive involving multiple providers, encounters, institutions, and years of time. Example(s): A comprehensive breast cancer treatment plan may include multiple diagnostic imaging staging studies, surgical procedures, a chemotherapy protocol, details of the radiation therapy plan, plastic surgery reconstruction and long-term post therapy surveillance plan to be posted in the PHR-S and referenced by the cancer care team.			
1.	The system SHOULD provide the ability to capture PHR Account Holder-specific plans of care and treatment (e.g., information about orders or therapies).			523
2.	The system SHOULD provide the ability to capture updates to the PHR Account Holder's plan of care and treatment including authors, creation date, version history, references and sources as available.			524
3.	The system MAY provide the ability to capture adequate order details to promote the PHR Account Holder's understanding and compliance with the order.			525
4.	The system SHOULD provide the ability to present care and treatment plan recommendations in terms of the PHR Account Holder's health-related data (e.g., peak flow, weight, blood pressure, or dietary preferences) at the option or control of the PHR Account Holder or PHR Account Holder Proxy.			526
5.	The system SHOULD provide the ability to transmit care plans, care instructions, treatment plans, guidelines, and protocols (or portions of those items) to selected stakeholders (e.g., sharing a new fitness plan with members of the care team, or sharing a care plan with a new member of the care team) according to user preference, organizational policy, and/or jurisdictional law.			527

2. Personal Health Support Section

Section Overview

Supportive PHR-S functions are the subset of PHR-S functions that assist with the administrative and financial requirements associated with the delivery of healthcare. Supportive PHR-S functions also provide input to systems that perform medical research, promote public health, and seek to improve the quality of healthcare delivered. All functions within the Supportive Section have an identifier starting with “S”.

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
S.1 Function	Provider Information			529
	Statement: The purpose of this section is to provide the system support to obtain a list of providers in an area and/or within a health plan panel and then maintain, or provide access to, current provider information. **Description:**			
S.1.1 Function	Manage Selection of Providers		C	530
	Statement: Support a PHR Account Holder in seeking providers who may meet their healthcare requirements. **Description:** In seeking healthcare, the system should support the PHR Account Holder being able to obtain a list(s) of providers by geographic area and/or within a dental or medical plan panel. Further, the PHR Account Holder should be able to sort providers by attributes including, but not limited to: - specialty; - office hours; - telehealth-oriented encounters; - sex; - language; - methods of information selection; - methods of information sharing; - and (possible) payment information. The PHR Account Holder should be able to maintain, or provide access to, current provider information. A PHR Account Holder may desire to research (because of a planned household relocation to another geographic area) a diagnosis requiring highly specialized care by healthcare providers and or healthcare facilities that are in limited availability. The system should be flexible on alternative sources of information allowing the PHR Account Holder to review providers who might best meet the individual’s needs. Consider also, that if various types of providers, care-team members, or social-affinity groups might be involved with the PHR Account Holder's health, then various methods of information selection, information sharing, and (possible) payment information might also need to be accommodated within the PHR system. As a result, the PHR system ought to support a rich, extended set of caregivers such as: - Social Networking Groups that are oriented towards health maintenance and recovery, wellness, and health goals; - Personal Health Support Groups (e.g., weight, drugs, behavioral health, mental health, or diabetes support) - Exercise and Physical Training specialists - School Nurses - Nutritionists/Dietitians - Care managers (e.g., in-home therapists, or discharge planners) - Community health worker (either professional or volunteer) (e.g., neighbors, public health workers, health representatives, health screeners, or non-traditional healthcare workers) - A mobile health clinic provider Note: Some of these extended caregivers might offer PHR data entry services on behalf of the PHR Account Holder.			
1.	The system SHOULD provide the ability to link to multiple sources of healthcare provider and healthcare system information.			531
2.	The system SHOULD provide the ability to render information based on one or more provider attributes.			532
3.	The system MAY provide the ability to render information regarding available health benefit plan provider panel(s) based on one or more attributes.			533
4.	The system MAY provide the ability to present insurance information regarding a selected provider versus a health plan provider panel (in order to help the PHR Account Holder choose between an in-network versus an out-of-network provider). For example, the PHR Account Holder may desire to compare prices of certain specialists, compare the credentials of the specialists, identify the level of experience, research comments regarding the provider's quality of service, or evaluate the provider's caseload panel.			534
5.	The system SHALL manage the provider’s contact/business information.			535

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
6.	The system MAY provide the ability to capture provider participation in payer networks.			536
7.	The system MAY provide the ability to capture provider participation in payer benefit plan products.			537
8.	The system MAY provide the ability to capture a healthcare provider privilege status at a healthcare facility.			538
9.	The system MAY provide the ability to analyze a healthcare provider's credential information (e.g., to verify the accuracy of the stated credential).			539
10.	The system MAY provide the ability to transmit a request to subscribe to a (health-oriented) Social Networking Group, a Health Support Group, or a health research organization according to user-preference, organizational policy, and/or jurisdictional law.		N	540
11.	The system MAY provide the ability to manage personal health information in the health-coaching (including fitness training and/or exercise management) environment according to user-preference, organizational policy, and/or jurisdictional law (e.g., a health-coach might need to know the PHR Account Holder's health goals, physical limitations, natural human language, pregnancy status, age, and weight).		N	541
12.	The system MAY provide the ability to exchange selected personal health information with a school health information system according to user-preference, organizational policy, and/or jurisdictional law (e.g., a parent might use the PHR system to share their child's diabetes information, diet order (e.g., feeding instructions, timing, or schedule) meal plan, or allergy restriction with the school nurse and with the child's pediatrician in keeping with Family Educational Rights and Privacy legislative requirements).		N	542
13.	The system MAY provide the ability to exchange selected personal health information with a community health worker according to user-preference, organizational policy, and/or jurisdictional law (e.g., a parent might use the PHR system to share their children's demographic information with a disaster relief worker after a flood; a PHR Account Holder Proxy might use the PHR system to share information about their elderly parent's health status with a community health worker who is analyzing community risk for potentially unhealthful airborne exposures).		N	543
14.	The system MAY provide the ability for the PHR Account Holder to exchange selected health information with virtual encounter groups. Examples of virtual encounter groups include: - telehealth-oriented encounters with providers; - Social Networking Groups that are oriented towards health maintenance and recovery, wellness, and health goals; - Support Groups (e.g., weight, drugs, behavioral health, mental health, or diabetes support); or - Care Managers (e.g., a care-manager who offers virtual assessments or reviews, or who provides discharge planning services, or who serves as a PHR information management or data-curation concierge).		N	544
S.1.2 Function	Manage PHR Account Holder Provider's Information		C	545

Statement: Manage contact information for the PHR Account Holder's current and past health care providers.

Description: A system should maintain both current and past contact information about a provider. The system may also collect and maintain background information about a provider such as academic credentials, certifications and specialties. Healthcare providers may be individuals, teams, or organizations such as clinics.

The system should allow the PHR Account Holder to manage information regarding teams of providers. A team of providers may be a group of healthcare physicians practicing in the same healthcare facility. For example, a primary care provider, an orthopedic specialist, physiatrist and physical therapy may comprise a team at a facility during an acute hospitalization. A team of providers could also be designated by the PHR Account Holder based on a disease process. For example, in the case of extended care after a motor vehicle accident with extreme facial injury, the team may be comprised of a dentist, an orthodontist, a maxilla-facial specialist, and orthopedist, a reconstructive specialist and a chiropractor. These healthcare providers may not be part of a healthcare facility, but all may be instrumental in the complete care of the individual, requiring coordination by the PHR Account Holder.

Note: It is likely true that information about a given provider (or provider organization) might be difficult for the PHR Account Holder to obtain, curate, and validate. However, such information might prove to be useful, for example, for historical or research purposes.

1.	The system SHALL provide the ability to manage the PHR Account Holder's provider's contact information.			546
2.	The system MAY provide the ability to manage background information regarding the PHR Account Holder's providers.			547
3.	The system MAY provide the ability to maintain provider-related information as part of an existing provider-defined care team(s).			548
4.	The system SHOULD provide the ability to capture information necessary to identify primary and secondary practice locations or offices of providers to support communication and access.			549
5.	The system MAY provide the ability to manage provider's scheduled work hours at each location.			550
6.	The system MAY provide the ability to maintain providers as part of the PHR Account Holder's team(s).			551
7.	The system MAY provide the ability to manage healthcare provider credentials.			552
8.	The system MAY provide the ability to maintain the provider as active or previous/past member of the PHR Account Holder care team.			553

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
S.1.3 Function	Manage Health Care Provider Information			554
	Statement: Support the import or retrieval of data necessary to identify a healthcare provider. **Description:** This information will assist the PHR Account Holder in contacting a provider to schedule appointments and ask health-related questions. The provider roles include, but are not limited to, physician, nurse and physical therapist.			
	1. The system SHOULD provide the ability to capture information regarding a provider's location or contact information regarding a facility.			555
	2. The system SHOULD provide the ability to manage information regarding a provider's location, contact information, hours of operation, role as a member of the PHR Account Holder's care team, and authorizations attributed to the provider.			556
	3. The system MAY provide the ability for the PHR Account Holder to hide or mask selected elements of the provider's identifying information according to the PHR Account Holder's authorization, organizational policy, and/or jurisdictional law. For example, the PHR Account Holder might desire to mask the physician's specialty as a drug counselor.			557
	4. IF a directory service is available, THEN the system SHOULD update a provider's current information via that directory service.			558
S.1.4 Function	Manage Provider Transparency Information			559
	Statement: Support the import or retrieval of data necessary to review available quality, performance, and cost measurements regarding providers. **Description:** A variety of stakeholders offer consumers the ability to evaluate the credentialing, quality, performance, and cost. Having ready access to the information will assist the consumer in their evaluation and selection of providers. Note: Healthcare provider transparency information that has been received or imported from external sources must not be altered by the PHR Account Holder.			
	1. The system SHOULD provide the ability to import or receive healthcare provider transparency information that the PHR Account Holder can use to assess the healthcare provider's quality, performance, and cost.			560
	2. The system SHOULD provide the ability to present healthcare provider transparency information that has been imported or received from an external source.			561
S.1.5 Function	Manage Healthcare Facility Information			562
	Statement: Support the import or retrieval of data necessary to identify a healthcare facility. **Description:** This information will assist the PHR Account Holder in identifying where a facility is located and in contacting a facility to schedule appointments. These facilities may be local or remote from the PHR Account Holder. The facility types include, but are not limited to, hospitals, clinics, same day surgery centers.			
	1. The system SHOULD provide the ability to manage information on facility location or contact information on a facility's premises.			563
S.1.6 Function	Manage Healthcare Facility Transparency Information			564
	Statement: Support the import or retrieval of data necessary to review available quality, performance, and cost measurements regarding healthcare facilities. **Description:** A variety of stakeholders offer consumers the ability to evaluate the quality, performance, and cost. Having ready access to the information will assist the consumer in their evaluation and selection of healthcare facility. Note: Healthcare facility transparency information that has been received or imported from external sources must not be altered by the PHR Account Holder.			
	1. The system SHOULD provide the ability to import or receive healthcare facility transparency information that the PHR Account Holder can use to assess health care quality, performance, and cost.			565
	2. The system SHOULD provide the ability to present healthcare facility transparency information that has been imported or received from an external source.			566
S.1.7 Function	Manage Surveys on the Healthcare Experience			567
	Statement: Enable the PHR Account Holder to respond to surveys on his or her healthcare experience. **Description:** This feature would enable providers, payers and PHR Account Holders to assess and provide feedback on areas such as the perceived patient-centeredness of care, satisfaction and performance, and the transparency efforts to improve quality of care. The receipt of a health survey does not imply that the member must participate in the survey. The system may simply direct the PHR Account Holder to a separate, external survey tool, or may provide the capacity to manage the entire survey process in which a member chooses to participate.			
	1. The system SHOULD provide the ability to render notification to the PHR Account Holder that a survey is available.			568

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
2. The system SHOULD provide the ability for the PHR Account Holder to manage participation in a survey (e.g., to subscribe or unsubscribe to a survey).				569
3. The system MAY provide the ability to capture the results of PHR Account Holder survey responses from external survey tools.				570
4. The system MAY provide the ability to manage one or more survey(s) that capture PHR Account Holder responses.				571
5. The system MAY provide the ability to manage the survey results.				572
S.2 Function	Financial Management			573
Statement: The purpose of this section is to provide the system support in managing financial information related to benefit plan coverage and service utilization. **Description:**				
S.2.1 Function	Capture and Read Health Insurance Account and Benefit Information			574
Statement: Enable the PHR Account Holder to request and/or receive and read information on their general health insurance benefits. **Description:** PHR Account Holders may want to centralize administrative information related to the insurance accounts that he/she participate in. Administrative information such as group, group number, policy number, member identification number, effective and termination dates, probationary periods, pre-existing condition constraints, prior authorization or referral requirements and others are important data for provider offices for billing purposes. Current and prior insurance coverage information is important for correct billing and payment. Detail of multiple coverages allows for coordination of benefits information to be easily provided. The ability to capture information of separate riders such as extra major medical coverage or cancer specific coverages in addition to routine benefit plans assists the PHR Account Holder in better knowledge and utilization of the financial resources available for payments. The system should allow the PHR Account Holder to display patient responsibility and benefit plan covered costs – both estimated and final – for a given event (e.g., test, procedure, surgery, or provider appointment). In newer plan types such as Consumer Directed Health Plans (CDHP), this information will help the PHR Account Holder determine the financial implications of his/her treatment options, alternative treatment options and provide information that may be needed by the provider.				
1. The system SHOULD provide the ability to capture health insurance benefit information.				575
2. The system SHOULD provide the ability to render health insurance benefit information.				576
3. The system SHOULD provide the ability to manage multiple payer sources of health insurance benefits information.				577
4. The system SHOULD capture insurance type (e.g., medical or dental).				578
5. The system SHOULD provide the ability to capture insurer(s) contact information.				579
6. The system MAY provide the ability for a PHR Account Holder to determine and present estimated PHR Account Holder responsibility and insurance covered costs for an healthcare-related event.				580
7. The system SHOULD provide the ability for a PHR Account Holder to determine and present final PHR Account Holder responsibility and insurance determination for an event.				581
8. The system SHOULD provide the ability to store, determine, and present (i.e., track) multiple categories of account distributions related to the varied financial implications of funds usage in Consumer-Directed Health Plan (CDHP) accounts according to the PHR Account Holder's authorization, organizational policy, and/or jurisdictional law.			C	582
S.2.2 Function	Manage Health Insurance Plan Benefit Information		C	583
Statement: Enable the PHR Account Holder to capture, read, update and remove access to health insurance benefit information including but not limited to past, current and future (if known) benefit plans. **Description:** Robust management features allow the PHR Account Holder to actively maintain their health insurance benefits information for selected benefits related to PHR Account Holder coverage needs. Over an extended period of time, with the likelihood of multiple insurance providers, it may be important for there to be information management capability for the varied payer sources, varied levels of benefit information, and varied levels of coverage including allowed coverages, exclusions, and limitations on specific coverages. Information management capabilities may include analytics regarding the PHR Account Holder's desired care such as: the selection of the most appropriate insurance plan for the current disease or injury; or the amount of deductibles that can be expected under varying insurance plans. Out-of-date or non-current insurance plan and benefit information can be used to compare different benefit packages, costs, and/or expenses over time resulting in a better understanding of health care as it pertains to health insurance coverage.				
1. The system SHOULD provide the ability to capture selected insurance benefit information that is pertinent to the PHR Account Holder's needs.				584
2. The system SHOULD provide the ability to maintain the selected health insurance benefit information.				585
3. The system SHOULD provide the ability for the PHR Account Holder to capture and render updates made to selected insurance plan benefit information that is pertinent to the PHR Account Holder's needs. For example, the PHR Account Holder might receive information regarding changes in deductible amounts, categories of coverage (e.g., new medicines or new therapies being covered), terms-of-coverage (e.g., changes in co-pay amounts), prior authorization requirements,			C	586

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
	and updates to the list of health care providers that are within the insurance carrier's network (including specific facilities and providers).			
4.	The system SHOULD provide the ability to manage health insurance benefit information from multiple payer sources.			587
5.	The system MAY provide the ability to link to the health insurance benefit PHR-S as the source for multiple categories of account distributions which may be related to the varied financial implications of funds usage in accounts (such as Consumer-Directed Health Plans).			588
6.	The system MAY provide the ability to manage multiple categories of account distributions which may be related to the varied financial implications of funds usage in accounts (such as Consumer-Directed Health Plans).			589
7.	The system MAY provide the ability to capture preauthorization requirements for medications and health services specific to the PHR Account Holder's policies.			590
8.	The system MAY provide the ability to capture, store, and render referral requirements. Note: Referral requirements are those requirements that must be met by a healthcare provider as specified by the healthcare payer or a care-coordinating entity. A care-coordinating entity consists of a group of healthcare professionals who have formally agreed to manage the healthcare of a patient.			591
9.	The system MAY provide the ability to capture and present an indication that an insurance coverage / benefit / deductible-amount / co-pay amount has changed (e.g., by receiving a notice from an insurance providers of the existence of a new benefit, an expired benefit, or a changed benefit.)		N	592
S.2.3 Function	Manage Standard Reporting		C	593
	Statement: Enable PHR Account Holders or authorized designees to request and read pre-configured, packaged reports of PHR information. **Description:** PHR Account Holders may request standard, pre-configured, packaged reports. The purpose is not for PHR interchange but rather for PHR Account Holder's analysis of his/her health related financial and administrative data, and for sharing (if desired).			
1.	The system SHOULD provide the ability to render standard reports of structured clinical and administrative and financial data using either internal or external reporting tools.			594
2.	The system SHOULD provide the ability to maintain report parameters based on data sorted or filtered by the PHR Account Holder or by the PHR-S settings.			595
3.	The system MAY provide the ability to render information from unstructured clinical and administrative data in the report generation process using internal or external tools.			596
4.	The system (or an external application using data from the PHR-S) MAY provide the ability to maintain report parameters for generating subsequent reports.			597
5.	The system (or an external application using data from the PHR-S) MAY provide the ability to update one or more parameters of a saved report specification when generating a report using that specification.			598
S.2.4 Function	Manage Ad Hoc Reporting		C	599
	Statement: Allow PHR Account Holders or authorized designees to request and read ad hoc reports of PHR information. **Description:** PHR Account Holders may request ad hoc, non-standard reports. The purpose is not for PHR interchange but rather for PHR Account Holder's analysis of his/her health related financial and administrative data, and for sharing (if desired).			
1.	The system SHOULD provide the ability for the authorized PHR Account Holder to render ad hoc reports of the PHR.			600
2.	The system SHOULD provide the ability for the authorized PHR Account Holder to render customized reports of summarized information based on sort and filter controls for date or data range, problem, or other clinical data element or categories (e.g., medications or providers).			601
3.	The system SHOULD provide the ability to maintain ad hoc reports for future retrieval and use.			602
4.	The system SHOULD provide the ability to maintain summarized information through customized reports based on prioritization of chronology, problem or other pertinent information of importance to the authorized PHR Account Holder.			603
5.	The system SHALL manage data visibility for PHR Account Holder Proxies using confidentiality-related preferences that were previously established by the PHR Account Holder for all ad hoc reporting capabilities.			604
6.	The system MAY provide the ability to render consolidated reports across family members (e.g., children).			605
7.	The system SHOULD conform to TI.1.1 (Entity Authorization).		C	606
8.	The system SHALL conform to TI.2 (Auditable Records).		C	607
9.	The system (or an external application using data from the PHR-S) MAY provide the ability to capture and maintain parameters for ad hoc reports.		N	608

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
S.3 Function	Administration Management			609
	Statement: The purpose of this section is to provide the system support in managing the PHR-S and the interaction with other PHR and EHR systems. It also serves as a set of functions to manage documentation related to the PHR-S as well as legal documents that affect or may affect the PHR Account Holder. **Description:**			
S.3.1 Function	Manage Interoperability of PHR Account Holder Demographics			610
	Statement: Support the ability to capture or have interactions with other systems, applications and modules to enable the creation and maintenance of demographic information. **Description:** The PHR Account Holder demographic data set is needed to support identification and to enhance the prospect for interoperability. The PHR Account Holder should be able to request or make changes to their demographic data and allow for export of all or parts of the demographic data to other systems.			
	1. The system MAY provide the ability to manage demographic information through interaction with other systems, applications, and modules.			611
	2. The system MAY render notification to the PHR Account Holder of added and updated demographic changes, as a result of interaction with other systems, applications, and modules.			612
	3. The system SHOULD provide the ability for a PHR Account Holder to transmit requests for maintenance of the PHR Account Holder's demographic information to the PHR Sponsoring Organization. Note: A PHR Sponsoring Organization is an organization that acquires and offers a PHR Account to those constituents who are, for example, members, subscribers, or employees of that organization.		C	613
	4. The system MAY provide the ability for a PHR Account Holder to transmit requests for maintenance of the PHR Account Holder's demographic information in other external systems (e.g., a Health Information Exchange, a healthcare payer, or a care-coordinating entity). Note: A care-coordinating entity consists of a group of healthcare professionals who have formally agreed to manage the healthcare of a patient.			614
S.3.2 Function	Manage PHR Conditions of Use			615
	Statement: Outline the sponsor requirements for use of the system. **Description:** The terms and conditions outline the sponsor requirements in using the application. The terms and conditions may include items such as copyright information, trademarks and intellectual property, third party links, indemnification, privacy, limitation of liability, term and termination and other miscellaneous provisions. The PHR Account Holder should be notified of the expectations of the sponsor and have the opportunity to agree to the requirements and any changes to the requirements. The Conditions of Use document also helps indemnify the PHR sponsor against certain misuse of the data. For example, a published article on diabetes may contain a copyright notice that forbids the storage of that article on a computer without first paying for the article. The Conditions of Use document would inform the PHR Account Holder that the sponsor does not support copyright infringement.			
	1. The system SHOULD provide the ability for the PHR Account Holder to enter an indication of an agreement to the Conditions-of-Use when the PHR-S is initially used by the PHR Account Holder.			616
	2. The system SHALL render a notification to the PHR Account Holder that changes occurred to the Conditions-of-Use documents according to organizational policy and/or jurisdictional law.			617
	3. The system SHOULD provide the ability to present changes that occurred to the Conditions-of-Use documents (e.g., the actual document, or an audit, or a summary, or an overview of the changes) according to organizational policy and/or jurisdictional law.			618
	4. The system SHOULD provide the ability to render the Conditions-of-Use.			619
	5. The system SHALL provide the ability for the PHR Account Holder to render a notification to the PHR-S vendor and/or sponsor(s) as part of the process to seek redress regarding the vendor and/or sponsor‘s failure to meet performance expectations as specified in the Conditions-of-Use agreements (including reporting PHR-S errors, failures, abuse, fraud, or other issues).			620
	6. The system SHOULD provide the ability to maintain a list of PHR-S administrators and personnel to receive, manage, and respond to emails and telephone calls regarding PHR-S errors, failures, abuse, fraud, or any other PHR Account Holder issues with the PHR-S Terms and Conditions-of-Use agreements.			621
S.3.3 Function	Manage Legal and other Related Documents			622
	Statement: Manage legal and other related documents that allow or restrict the use or disclosure of the PHR Account Holder’s information. **Description:** The PHR system should allow for the entry of documents related to the use or disclosure of the PHR Account Holder’s information. These documents may include scanned images or electronic images sent via attachment. The system does not judge the authenticity of the document. The PHR Account Holder should ensure they have the original document or approved copy of a document or other images. The system allows for multiple instances of the same document (e.g., multiple authorizations). The system allows document to be retired (for example, by moving the documents to an archival service and deleting those documents locally). Retired documents may continue to be tracked. The system allows for the removal of documents at the PHR Account Holder’s discretion.			

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
S.3.3.1 Function	Manage Consents and Authorizations			623
	Statement: Maintain Consents and Authorization directives/statements for any entity that may or may not have access to the PHR Account Holder's PHR-S. **Description:** The PHR Account Holder may have Consents and/or Authorization directives that allow or prohibit certain entities from access to part or all of the PHR. Directives may take different forms including documents or system flags on Consent Authorization. The Consent or Authorization requirements would be maintained in accordance with user role, organizational policy and/or jurisdictional law. Based on that, the Consent or Authorization might contain the details of the entity that may be authorized to use, or may be prohibited from using the PHR-S. The Consent or Authorization may detail to the record, field or class, the data available to be used or disclosed. The entities that the Consent or Authorization applies to may or may not be current PHR Account Holders of the PHR-S.			
	1. The system SHALL provide the ability to capture Consents and Authorizations according to organizational policy and/or jurisdictional law.			624
	2. The system SHALL provide the ability to determine the entity to which the Consent or Authorization applies.			625
	3. The system SHALL provide the ability to determine a section or sections of the PHR Account Holder's information to which the Consent or Authorizations applies (e.g., the demographic data section, the medication list, or history of illness section).			626
	4. The system SHOULD provide the ability to determine individual elements of records to which the Consent or Authorization applies.			627
	5. The system SHOULD provide the ability to determine the time period within which the Consent or Authorization is enforced.			628
	6. The system SHOULD provide the ability to render Consents and Authorizations to another PHR-S, an EHR-S, or elsewhere (e.g., to a printer).			629
	7. The system SHOULD provide the ability to import Consents and Authorizations through electronic interfaces (e.g., scanning or faxing).			630
	8. The system MAY provide the ability to link to external Consents and Authorizations (e.g., in an external EHR-S).			631
S.3.3.2 Function	Manage End-of-Life Documents and Other Advance Directives			632
	Statement: Manage documents that provide direction for end-of-life care and manage other types of Advance Directives. **Description:** The PHR Account Holder may want to capture and maintain documents that pertain to end-of-life care and to capture and maintain other types of Advance Directives. End-of-life documents include but are not limited to: Advance Directive for Healthcare; Power of Attorney for Healthcare and Physician Order for Life Sustaining Treatment. The system should allow for multiple occurrences of a document and the ability to archive documents. The documents maintained will depend on the jurisdictional law. The documents may or may not reside in the PHR-S. The document may be scanned images, structured documents or simply a notation on the location of the original (hardcopy or original).			
	1. The system SHOULD provide the ability to capture documents related to end-of-life care and other types of Advance Directives.			633
	2. The system SHOULD provide the ability to render a list of end-of life documents sorted by one or more defined data elements.			634
	3. The system MAY provide the ability to tag a document as Active or Non-Active by category of document.			635
	4. The system SHOULD maintain the end-of-life document and/or a note that specifies that document's location.			636
S.3.3.3 Function	Manage Documents for Personal Representation			637
	Statement: Manage documents that designate those authorized to act on behalf of the PHR Account Holder. **Description:** The PHR Account Holder may want to capture and maintain documents that pertain to designating those authorized to act on behalf of PHR Account Holder for healthcare. Examples include but are not limited to: Guardianship, Legal Custodial Parent, Executor or Trustee. The system should allow for multiple occurrences of a document and the ability to archive documents. The documents maintained will depend on the jurisdictional law. The documents may or may not reside in the PHR-S. The document may be scanned images, structured documents or simply a notation that specifies the location of the original (hardcopy or original).			
	1. The system SHOULD provide the ability to capture, maintain, and render Consents, Authorizations, and other documentation authorizing individuals and/or PHR Account Holder Proxies to act on behalf of the PHR Account Holder with regard to healthcare or the PHR-S.			638
	2. The system SHOULD provide the ability to render a list of documents designating those authorized to act on behalf of the PHR Account Holder sorted by one or more defined data elements.			639
	3. The system MAY provide the ability to tag a document designating those authorized to act on behalf of the PHR Account Holder as Active or Non-Active by category of document.			640
	4. The system SHOULD maintain the document designating those authorized to act on behalf of the PHR Account Holder and/or a note that specifies that document's location.			641

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
S.3.4 Function	Manage Data Masking for Sensitive or Selective Information		C	642
	Statement: Allow the PHR Account Holder or authorized designee to mask data on a selective, record, field-by-field, or class basis as one aspect of controlling access to personal health data. The PHR Account Holder has the ability to determine what PHR information is available to an authorized designee. **Description:** The PHR Account Holder or designee needs the ability to protect sensitive information by masking specific content without deleting the information. Example(s): The PHR Account Holder wants to make the fact of Sexually Transmitted Disease or pregnancy known if and only if she arrives at an emergency room unconscious.			
	1. The system SHOULD provide the ability for the PHR Account Holder to tag records, data fields, or data classes that will not display intelligibly unless viewed by condition-based Authorized PHR Users under conditions specified by the PHR Account Holder. Examples of a condition-based Authorized PHR User include: An individual that the PHR Account Holder specifies, an Emergency Care provider, or a PHR Account Holder's smartphone that is accessed within an Emergency Department.			643
	2. The system MAY provide the ability for the PHR Account Holder to manage data visibility at differ degrees of data discoverability by masking, hiding, and/or de-identifying data according to user preference, organizational policy, and/or jurisdictional law. For example: medication information may be masked with asterisks; mental health records may be undiscoverable by those who do not have a need-to-know. Examples of data-masking visibility conditions include: type of healthcare provider (e.g., administrator versus clinician), location of care being received (e.g., a local clinic versus an Emergency Department), time (e.g., weekday versus weekend for a provider), past healthcare service received (e.g., earlier substance abuse therapy; therapy regarding significant weight loss).		C	644
	3. The system SHOULD provide the ability to authenticate systems that are requesting personal health information to ensure the requesting system has the ability to protect masked data according to the PHR Account Holder's preferences and consent, organizational policy, and/or jurisdictional law.			645
	4. The system SHOULD provide the ability to transmit data to other systems that support the ability to protect masked data.		C	646
	5. The system MAY provide the ability to render a notification to the PHR Account Holder that masking selected information may result in unintended consequences or medical harm (e.g., by providing information that is incomplete for a physician who is engaged in the medication-ordering process).			647
S.3.5 Function	Manage PHR Output		C	648
	Statement: Enable the PHR Account Holder or authorized designee to manage and generate PHR output. **Description:** The PHR Account Holder may request PHR output which may include standard and ad hoc reports in hardcopy or electronic formats. This output may be for the PHR Account Holder's analysis of his/her health related financial and administrative data, and for sharing of the PHR information for any purposes the PHR Account Holder deems appropriate.			
	1. The system SHALL provide the ability to render reports consisting of all or part of an individual's PHR.			649
	2. The system SHOULD provide the ability to determine the records or reports that are considered the formal health record for disclosure purposes.			650
	3. The system SHOULD conform to function RI.1 (Manage Record Lifecycle and Lifespan) to ensure that updates to unstructured Health Record Information are tracked.		C	651
	4. The system SHOULD conform to function RI.1 (Manage Record Lifecycle and Lifespan) to ensure that updates to Structured Health Record Information are tracked.		C	652
	5. The system SHOULD provide the ability to render hardcopy and electronic report summary information (e.g., procedures, medications, laboratory results, immunizations, allergies, or vital signs).			653
	6. The system SHOULD provide the ability to render reports in both chronological and specified records elements order.			654
S.3.6 Function	Manage PHR Data Import and Export			655
	Statement: Allow the PHR Account Holder to manage the import to and export of data from a PHR-S. **Description:** A PHR Account Holder needs to prescribe how data is exchanged with other systems including how data is imported to the PHR-S, and the parameters for data export (e.g., who, when, or the extent of data). Some import and export functions may be one-time events; other exchanges, for example, may occur at regular intervals (such as via a subscription service). The PHR Account Holder should be able to determine the information or data that he/she will accept into the PHR. The system should record the acknowledgement or refusal of data sent to the Account Holder's PHR-S. Use of exported data should be constrained according its intended and permitted purpose of use (e.g., as described in the PHR-S manufacturer's Terms of Service and Terms of Use agreements). Example(s): The PHR Account Holder may desire to inform her General Practitioner that the PHR Account Holder has received a proposed dietary regimen from a Registered Dietitian / Nutrition specialist. The PHR Account Holder may also desire to send a copy of the proposed nutrition care plan to the General Practitioner.			

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
1.	The system SHOULD provide the ability to exchange PHR Account Holder data content with another PHR system.			656
2.	The system SHOULD provide the ability to exchange PHR Account Holder data content with other systems.		C	657
3.	The system SHOULD provide the ability to exchange PHR Account Holder data content with other systems.			658
4.	The system SHOULD provide the ability for the PHR Account Holder to determine entities from which data may be imported into the PHR-S.			659
5.	The system SHOULD provide the ability for the PHR Account Holder to determine entities to which data may be exported from the PHR-S.			660
6.	The system SHOULD provide the ability for the PHR Account Holder to exchange information with an entity on a one-time basis.			661
7.	The system SHOULD provide the ability for the PHR Account Holder to exchange information with an entity on a recurring basis.			662
8.	The system SHOULD provide the ability for the PHR Account Holder to annotate incoming information.			663
9.	The system SHOULD provide the ability for the PHR Account Holder to render a notification (i.e., an acknowledgment) of the receipt or the refusal to receive information that was sent from another system.			664
10.	The system SHALL conform to TI.1.5 (Non-Repudiation) to promote provenance regarding professionally-sourced clinical information.		C	665
S.3.7 Function	Manage New, Additional, or Other Use Request		C	666
	Statement: Support the formal and routine request for PHR Account Holder health record information for new, additional, or other uses. **Description:** Provide hardcopy and electronic output that supports the needs of a variety of new, additional, or other uses such as: annual immunization requests from schools/camps, application processing for disability requests, validation of compliance with treatment regimens. This mechanism should be provided for both chronological and specified record element output. An auditable record of these requests and associated exports may be maintained by the system. The system has the capability of providing a report of accounting of disclosures of the secondary PHR Account Holders in accordance with user role, organizational policy and/or jurisdictional law.			
1.	The system SHOULD provide the ability to capture information regarding the new, additional, or other use data-requestor (including the identity of the requestor, the requestor's intended use of the data, date of the request, and the date of the PHR Account Holder's response to that request) according to user role, organizational policy, and/or jurisdictional law.			667
2.	The system MAY provide the ability for the PHR Account Holder to control access by adding password protection to PHR Account Holder-defined exported information.			668
3.	The system SHOULD provide the ability to tag specific PHR information to be reviewed and acted upon by the authorized PHR Account Holder for the purpose of deactivation, destruction, or retention.		C	669
4.	The system SHALL provide the ability to render PHR Account Holder identifying information on each page of the reports generated.			670
5.	The system SHOULD provide the ability to export PHR records to a variety of PHR Account Holders using various platforms without needing special viewing software.			671
S.3.8 Function	Manage Requests for Release of Information		C	672
	Statement: Support requests for release of PHR Account Holder health record information. **Description:** Either the PHR Account Holder or the authorized designee may receive formal requests to release some or all of the PHR information. These requests may be ad hoc, or may also be routine, recurring requests that may be episodic or longer term. These requests may be related to patient care, administrative process, law enforcement or legal action. An auditable record of these requests and associated fulfillment(s) should be maintained by the system. The system should provide an accounting of PHR disclosures of the Release of Information Requests in accordance with user role, organizational policy and/or jurisdictional law.			
1.	The system SHOULD provide the ability to capture information regarding any individual or entity who requests PHR Account Holder data (including the identity of the requestor, stated reason for the request, the requestor's intended use of the data, date of the request, and the date of the PHR Account Holder's response to that request) according to user role, organizational policy, and/or jurisdictional law.			673
2.	The system SHOULD provide the ability to capture the Authorization or Consent associated with the request for release of information according to user role, organizational policy, and/or jurisdictional law.			674
3.	The system MAY provide the ability to manage the fulfillment status of requests.			675
4.	The system SHOULD manage recurring, standing requests for PHR information.			676
5.	The system MAY provide the ability for the PHR Account Holder to control access by adding password protection, purpose-of-use protection, and/or intention-of-use protection to PHR Account Holder-defined exported records.			677

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
6.	The system SHOULD provide the ability to render PHR Account Holder identifying information on each page of the reports generated.			678
7.	The system MAY provide the ability to export PHR records to a variety of PHR Account Holders using various platforms without needing special viewing software.			679
8.	The system SHOULD conform to function S.3.4 (Manage Data Masking for Sensitive or Selective Information) when masking any PHR data provided.			680
9.	The system SHOULD provide the ability to transmit electronic responses with unstructured and structured health record information.			681
10.	The system MAY conform to function TI.5.1 (Application, Structured-Message, and Structured-Document Interchange Standards) to enable data extraction in standard-based formats.		C	682
S.3.9 Function	Manage Information Views			683
Statement: Support PHR Account Holder -defined information views. **Description:** Views of information can be tailored for or by the PHR Account Holder (PHR Account Holder, caregiver or other authorized PHR account user) for their presentation preferences and to support personal or role-based workflows and purpose-of-use / intention-of-use requirements. Example(s): A PHR Account Holder may prefer to see summary information about medications, while a provider's view may include detailed information about current dosage and the PHR Account Holder's response to the medication over time.				
1.	The system SHOULD provide the ability for a PHR Account Holder to manage personal views of PHR information.			684
2.	The system MAY provide the ability to render role-based views of PHR information.			685
3.	The system MAY provide the ability for a PHR Account Holder to determine content of role-based views.			686
4.	The system MAY provide the ability to render purpose-of-use/intention-of-use-based views of PHR information.			687
5.	The system MAY provide the ability for a PHR Account Holder to determine content of purpose-of-use/intention-of-use-based views.			688
6.	The system MAY provide the ability for the PHR Account Holder to manage multiple customized views for more rapid display of information by the PHR Account Holder.			689
7.	The system MAY provide the ability to for a PHR Account Holder or Authorized PHR User to maintain individual custom views for future access.			690
S.4 Function	Manage Other Resources			691
Statement: The purpose of this section is to provide the system support to both allow the PHR Account Holder to participate in a variety of programs that may be directly related to areas of interest to the PHR Account Holder and to enable appropriate access and support for new, additional, or other uses of PHR information. **Description:**				
S.4.1 Function	Manage Clinical Research Information			692
Statement: Support a PHR Account Holder in clinical trials and provide research information. **Description:** In seeking healthcare, the system should support the PHR Account Holder being able to obtain a list(s) of available clinical trials/research. The PHR Account Holder should be able to refine trials by geographic area, by disease, by treatment, by sponsor and maintain, or provide access to, current clinical trial/research information. The system should also support the PHR Account Holder's participation in, and support of, appropriate new, additional, or other uses of their PHR information for clinical research which could include quality and performance analysis.				
S.4.1.1 Function	Capture Genomic/Proteomic Data and Documentation from External Clinical Sources			693
Statement: Incorporate genomic/proteomic data and documentation from external sources. **Description:** Mechanisms for incorporating external genomic/proteomic data and documentation (including identification of source) such as image documents, reports and other clinically relevant electronic data are available.				
1.	The system SHOULD provide the ability to capture relevant family genomic history.			694
2.	The system MAY capture and maintain genomic/proteomic information through interaction with other systems, applications, and modules.			695
3.	IF laboratory results are received through an electronic interface, THEN the system SHALL render the data elements upon request.			696
4.	IF laboratory results are received through an electronic interface, THEN the system SHALL capture and maintain the data elements in the PHR Account Holder record.			697
5.	The system MAY provide the ability to store imaged documents.			698
6.	The system SHOULD provide the ability to manage text-based externally-sourced documents and reports.			699

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
S.4.1.2 Function	Manage De-Identified Data Request Process		C	700
	Statement: Provide PHR Account Holder data in a manner that meets local requirements for de-identification. **Description:** When the PHR Account Holder desires to share his/her information in a de-identified state, the PHR Account Holder can export the data in a fashion that meets requirements for de-identification in that locale or realm. Example(s): If a person wants to participate in a study that will utilize de-identified data, then the system should provide the ability to de-identify this data according to the requirements of the study. In Germany, when a PHR Account Holder's subscription is cancelled, the PHR data may be maintained. But if the data is maintained, it must be maintained in a de-identified state or be pseudonymized (similar to the limited data set in the U.S. Privacy Rule).			
	1. The system SHOULD provide the ability for the PHR Account Holder to de-identify his or her information as needed to meet the requirements of a study or other request.			701
	2. The system SHOULD capture the source and date of a request for de-identified data.			702
	3. The system SHOULD provide the ability to capture the date of transmission, data transmitted, and the target of the de-identified data.			703
	4. The system SHOULD provide the ability to capture confirmation of the target's receipt of the data.			704
	5. The system SHOULD provide the ability to render the history of data transmissions.			705
	6. The system SHOULD provide the ability to de-identify data according to organizational policy and/ or jurisdictional law.			706
S.4.1.3 Function	Manage PHR Account Holder Notification of Clinical Trials			707
	Statement: Support member notification of clinical trials or research. **Description:** A PHR Account Holder should be notified of clinical trials in which they have an interest. The individual may obtain clinical trial information based on general description or specific description such as diagnosis or trial phase. A PHR Account Holder should be able to make their clinical and demographic data available for clinical trials and/or research matching.			
	1. The system SHOULD provide the ability to capture the PHR Account Holder's enrollment for clinical trial notifications.			708
	2. The system SHOULD provide the ability to capture the PHR Account Holder's consent to participate in a clinical trial.			709
	3. The system SHOULD provide the ability to receive clinical trial notifications.			710
	4. The system MAY provide the ability to export the data fields necessary to help qualify the PHR Account Holder as a clinical trial participant.			711
	5. The system SHOULD provide the ability to capture and render information regarding multiple sources of clinical trial and research information (e.g., links to multiple clinical trial websites).			712
	6. The system SHOULD provide the ability to extract and determine a focused search of trials by one or more attributes.			713
S.4.1.4 Function	Manage PHR Account Holder Enrollment in Clinical Trials or Research			714
	Statement: Support member enrollment in clinical trials or research. **Description:** The system should support a PHR Account Holder having the ability to enroll in clinical trials or research, The system should be able to capture administrative and consent requirements, trial or research questionnaires, data submissions and all alerts associated with a program. The PHR Account Holder should also have the ability to choose which programs they desire to participate in when notified of trial availability and high quality PHR Account Holder match.			
	1. The system SHOULD provide the ability to manage a PHR Account Holder's enrollment in a clinical trial or research program.			715
	2. The system SHOULD provide the ability to capture all administrative information about a clinical trial or research program.			716
	3. The system SHOULD provide the ability to render clinical trial or research participation sorted by categories.			717
	4. The system SHOULD provide the ability to capture alerts or notifications from the clinical trial program.			718
	5. The system SHOULD provide the ability to render prompts to the PHR Account Holder regarding clinical trial requirements.			719
	6. The system MAY provide the ability to render information regarding available health benefit plan clinical trial/research support.			720

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
S.4.2 Function	Registry Notification and Management			721
	Statement: Enable data sharing and communication with registries and manage the related information shared. **Description:** Support the automated transfer of formatted demographic and clinical information to disease-specific registries (and other notifiable registries) to enable PHR Account Holder to participate, if and as desired, in provider and public health monitoring and subsequent epidemiological analysis. The PHR Account Holder can export personal health information to disease-specific registries, other notifiable registries such as immunization registries, through standard data transfer protocols or messages. The PHR Account Holder can update and configure communication for new registries, or delete communication with an existing registry.			
	1. The system SHALL conform to function TI.1.1 (Entity Authentication).		C	722
	2. The system SHALL conform to function TI.1.3 (Entity Access Control).		C	723
	3. The system SHOULD provide the ability to manage information exchange and communication with registries.			724
	4. The system MAY provide the ability to exchange demographic and clinical information with disease-specific registries (and other notifiable registries) according to PHR Account Holder's preferences and/or consents, organizational policy, and/or jurisdictional law.			725
	5. The system MAY provide the ability to manage a pointer to PHR Account Holder registry information that might exist in a registry according to PHR Account Holder's preferences and/or consents, organizational policy, and/or jurisdictional law.			726
S.4.3 Function	Manage Donor Information			727
	Statement: Provide capability to capture and share needed information as a volunteer donor. **Description:** The PHR Account Holder is able to capture and share donor information (for products such as blood, organs, eggs, sperm, or stem cells). The PHR Account Holder can make this information available to donor matching agencies. This information may be in multiple formats, hardcopy output, standard messaging, display for authorized PHR Account Holders.			
	1. The system MAY provide the ability to capture and maintain demographic and clinical information needed for organ and/or tissue donation.			728
	2. The system MAY exchange documented demographic and clinical information about potential donations with appropriate outside parties.			729
	3. The system SHOULD provide the ability to render unstructured health record information.			730
	4. The system SHOULD provide the ability to render structured health record information.			731
	5. The system SHALL conform to S.3.3.1 (Manage Consents and Authorizations).			732
	6. The system MAY conform to function TI.5.1 (Application, Structured-Message, and Structured-Document Interchange Standards) to enable data extraction in standard-based formats.		C	733
S.4.4 Function	Manage PHR Account Holder Education Material Updates			734
	Statement: Receive and validate formatted inbound communications to facilitate and/or perform updating of PHR Account Holder education material. **Description:** Materials may include information about a diagnosis, recommended diets, associated PHR Account Holder health organizations, international vaccinations needed for travel, or web links to similar educational information. These materials would be provided electronically and may require validation prior to inclusion in the system.			
	1. The system SHALL receive updates to educational materials.			735
	2. The system MAY provide the ability to determine the validity of educational material prior to updating the educational material.		C	736
	3. The system MAY provide the ability to determine the applicability of educational material prior to updating the educational material. For example, a healthcare professional could offer information stating that the PHR Account Holder's use of non-alcoholic wine will not adversely affect the PHR Account Holder's pregnancy. Another example is that the PHR Account Holder may need to be reminded that milk must not be consumed within three hours of taking Tetracycline (when attempting to fight infection); also the PHR Account Holder could be reminded that antacids or iron supplements have a tendency to interfere with the absorption of various types of medicines.		N	737
S.4.5 Function	Manage PHR Account Holder Reminder Information Updates			738
	Statement: Receive and validate formatted inbound communications to facilitate updating of PHR Account Holder reminder information from external sources such as Cancer or Immunization Registries. **Description:** Information from outside groups, such as immunization groups or public health organizations, may periodically have and send updates of value to PHR Account Holders. The system should be capable of generating reminders based on the recommendations of these organizations. Reminders could be provided to PHR Account Holders by a number of means, including alerts or system generated email. A record of such reminders may become part of a PHR Account Holder's record. Example(s): Reminders could include a recommended immunization, prophylactic guidelines for treating Mitral Valve Prolapse disorder, or PHR Account Holder self-testing for disease.			

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
1.	The system SHOULD provide the ability to automatically receive inbound communications from external sources (e.g., from Cancer Registries or Immunization Registries) to facilitate updating of the PHR Account Holder's reminder-related information.		N	739
2.	IF the system has received an inbound communication from an external source (e.g., from Cancer Registry or Immunization Registry) regarding reminder-related information, THEN the system SHOULD provide the ability for the PHR Account Holder to transmit an acknowledgement of that inbound communication.		N	740
3.	IF the system has received inbound communications from external sources (e.g., from Cancer Registries or Immunization Registries) regarding reminder-related information, THEN the system SHOULD provide the ability for the PHR Account Holder to maintain that reminder-related information (e.g., by reviewing, editing, storing, harmonizing, updating, or deleting the information).		N	741
4.	The system MAY provide the ability to manage reminders automatically for PHR Account Holders meeting specific criteria (e.g., age, gender, or diagnosis). For example, the PHR Account Holder is a male and does not need to view reminders about annual mammograms; or the PHR Account Holder is diabetic and desires to receive and store reminders about foot examinations that will help assess circulatory health.			742
5.	The system MAY provide the ability to render reminders automatically to the PHR Account Holder (e.g., via email or voice message).			743
6.	The system SHOULD log reminder activity (e.g., by logging the fact the PHR-S transmitted a reminder message to the PHR Account Holder's email or mobile phone regarding an upcoming appointment).			744
S.4.6 Function	Manage Public Health Information			745
Statement: Manage the PHR Account Holder's use of PHR-related Public Health Information and/or services. **Description:**				
S.4.6.1 Function	Manage Public Health Related Updates			746
Statement: Provide the ability to update and maintain information regarding public health notifications. **Description:** Public health updates may be applicable to entire geographic regions or specific to a specific locale or diagnosis. The system should allow the PHR Account Holder to identify the types of public health updates that are of interest. The system should also allow a PHR Account Holder to be notified of other public health occurrences which may affect an entire population.				
1.	The system MAY provide the ability to render notifications to the PHR Account Holder based on the recommendations of public health authorities according to PHR Account Holder's preferences and/or consents, organizational policy, and/or jurisdictional law.			747
S.4.6.2 Function	Manage Access to Public Health Information Resources			748
Statement: Enable access to public health information resources. **Description:** PHR Account Holder shall have access to public health information resources. Example(s): A PHR Account Holder may want to receive general news releases from specific local, state and federal agencies. A PHR Account Holder may want to access information regarding public health resources for specific areas of interest such as birth control or hepatitis prevention.				
1.	The system SHOULD provide the ability for a PHR Account Holder to manage a subscription to Public Health information resources.			749
2.	The system MAY provide the ability to capture administrative information necessary to subscribe to Public Health Information resources.			750
3.	The system SHOULD provide the ability to render public health information resources sorted by enrollment date and category.			751
4.	The system SHOULD provide the ability to capture alerts and/or notifications from public health information resources according to organizational policy and/or jurisdictional law.			752
S.4.6.3 Function	Manage Access to Public Health Knowledge Bases			753
Statement: Enable access to public health knowledge bases. **Description:** PHR Account Holder shall have access to public health knowledge bases. Example(s): A PHR Account Holder may want to access up to date information from local, state and federal agencies regarding diabetes outcomes.				
1.	The system SHOULD provide the ability for a PHR Account Holder to manage a subscription to Public Health knowledge bases.			754
2.	The system MAY provide the ability to capture administrative information necessary to subscribe to public health information knowledge bases.			755
3.	The system SHOULD provide the ability to render public health knowledge bases sorted by enrollment date and category.			756

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
4. The system SHOULD provide the ability to capture alerts and/or notifications from public health knowledge bases according to organizational policy and/or jurisdictional law.				757
S.4.6.4 Function	Manage Enrollment in Public Health Programs			758
Statement: Provide the ability to enroll in public health programs. **Description:** The systems should support the ability of a PHR Account Holder to enroll in all available local, state and federal public health programs. Example(s): A PHR Account Holder would like to enroll in a local or regional maternal health program to receive care for pregnancy.				
1. The system SHOULD provide the ability for a PHR Account Holder to manage an enrollment in public health programs.				759
2. The system MAY provide the ability to capture administrative information necessary to enroll in public health programs.				760
3. The system SHOULD provide the ability to render public health programs sorted by enrollment date and category.				761
4. The system SHOULD provide the ability to capture notices from public health program offices according to organizational policy and/or jurisdictional law.				762
S.4.6.5 Function	Manage Enrollment in Public Health Notifications and Alerts			763
Statement: Support member subscriptions to public health notifications and alerts. **Description:** A PHR Account Holder should have the ability to subscribe to local, state or federal public health notifications and alerts. Example(s): The PHR Account Holder enrolls to receive public health alerts from a local or regional health department that has recently issued an alert for meningitis.				
1. The system SHOULD provide the ability for a PHR Account Holder to subscribe to public health notifications and alerts.				764
2. The system MAY provide the ability to capture administrative information necessary to subscribe to public health notifications and alerts.				765
3. The system SHOULD provide the ability to render public health notifications and alerts sorted by publishing date and category according to the PHR Account Holder's preferences and/or consents, user role, organizational policy, and/or jurisdictional law.				766
4. The system SHOULD provide the ability to capture notifications and alerts from public health agencies according to the PHR Account Holder's preferences and/or consents, user role, organizational policy, and/or jurisdictional law.				767
5. The system MAY provide the ability for the PHR Account Holder to maintain severity level(s) for alerts (e.g., high risk, medium risk, or low risk alerts).				768
6. The system MAY provide the ability for the PHR Account Holder to manage configuration parameters regarding the severity level(s) for alerts (e.g., receiving and/or presenting high risk, medium risk, or low risk alerts).				769
7. The system MAY provide the ability for the PHR Account Holder to manage configuration parameters regarding the reception of alerts by type (e.g., food-borne, travel-related, location-related, or elementary school age population).				770
S.4.6.6 Function	Enrollment in Public Health Surveys			771
Statement: Support access to public health surveys. **Description:** A PHR Account Holder will have the ability to participate in public health surveys and store their responses to those surveys. Example(s): The World Health Organization offers a survey to research the number of smokers who also have a specific related disease.				
1. The system SHOULD provide the ability for the PHR Account Holder to manage participation in public health surveys from local, state and federal agencies.				772
2. The system SHOULD provide the ability to capture administrative information necessary to enroll in public health surveys.				773
3. The system SHOULD provide the ability to determine public health surveys that apply to the PHR Account Holder according to the PHR Account Holder's preferences and/or consents, organizational policy, and/or jurisdictional law.				774
4. The system SHOULD provide the ability to capture PHR Account Holder responses to public health surveys.				775

3. Record Infrastructure Section

Section Overview

The Record Infrastructure Section consists of functions common to EHR System record management, particularly those functions foundational to managing record lifecycle (origination, attestation, amendment, access/use, translation, transmittal/ disclosure, receipt, de-identification, archive...) and record lifespan (persistence, indelibility, continuity, audit, encryption). The RI and TI Sections are identical between the PHR and EHR System Functional Models, reflecting the need for common and compatible record management and trust infrastructures. Note that there may be some functions more directly applicable to EHR systems than PHR systems. RI functions are core and foundational to all other functions of the Model (PH, S). RI functions may be implemented within the architecture of a single system or across a tightly coupled suite of systems (applications). All functions within the Record Infrastructure Section have an identifier starting with “RI”.

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1 Function	Record Lifecycle and Lifespan			777

Statement: Manage Record Lifecycle and Lifespan

Description: Actions are taken to support patient health. Actions are taken in provision of healthcare to individuals. Actions are taken as the result of rules-based PHR System algorithms. Actors (i.e., patients, providers, users, systems) take Actions. (Actions broadly encompass tasks, acts, procedures or services performed or provided.) The PHR System captures Actions taken and creates corresponding Record Entries. Record Entries provide persistent evidence of Action occurrence, context, disposition, facts, findings and observations. From the point of Record Entry origination to the end of its lifespan, the PHR System manages each Entry consistent with and according to scope of practice, organizational policy, and jurisdictional law. In support of individual health and in provision of healthcare to individuals, Actors perform Actions and Actions have corresponding Entries in the PHR Record, (i.e., Action instances are documented by Record Entry instances). Record Entries may be captured during the course of the Action or sometime thereafter. The Actor (author/source) of the Record Entry may be the same as an Actor performing the Action or not. The PHR-S Functional Model does not specify a particular relationship of Actions and corresponding Record Entries. It may be one to one, many to one or even one to many. Actions have associated metadata (e.g., who, what, when, where, why, how, under what conditions, in what context). The corresponding Record Entry captures this metadata along with other Action and Record Entry related information.

Each Record Entry also includes its own provenance metadata such as who (authoring Actor) and when (documented). Record Entries may be encapsulated to bind Actor (individual, organization, and/or system) signatures to data and metadata content and data/time of occurrence. Actions and related Record Entries capture a chronology of patient health and healthcare and also a chronology of operations and services provided in/by a healthcare enterprise. Record Entries reflect changes in health information from the time it was created, to the time it was amended, sent, received, etc. In this manner, each Record Entry serves as persistent evidence of an Action taken, enabling providers to maintain comprehensive information that may be needed for legal, business, and disclosure purposes. To satisfy these purposes, Record Entries must also be retained and persisted without alteration. Record Entries have both a lifecycle and a lifespan. Lifecycle Events include originate, retain, amend, verify, attest, access/view, de-identify, transmit/receive, and more. Lifecycle Events occur at various points in a Record Entry lifespan, always starting with a point of origination and retention (i.e., when the Entry is first created and stored). A Record Entry may have a pre and post Event state if content is modified. In this case, the original Record Entry is preserved (with signature binding) and a new Entry is created (with new signature binding). A Record Entry contains data and metadata, in multiple formats, following various conventions and standards. Included data may be tagged, and/or delimited, structured (concise, encoded, computable), or unstructured (free form, non-computable). Data may be encoded as text, document, images, audio, waveforms, in ASCII, binary or other encoding. Structured data may be characterized as being concise, encoded, computable, and may be divided into discrete fields.

Examples of structured health information include:

- patient residence (non-codified, but discrete field)
- diastolic blood pressure (numeric)
- coded laboratory result or observation
- coded diagnosis
- patient risk assessment questionnaire with multiple-choice answers.

Unstructured data may be characterized as being free form, and/or non-computable. Unstructured health record information is information that is not divided into discrete fields AND not represented as numeric, enumerated or codified data.

Examples of unstructured health record information include:

- text (text message to physician)
- word processing document (a letter from a family member)
- image (photograph of a patient or a scanned image of insurance card)
- multimedia (dictated report or a voice recording).

Context may determine whether data are structured or unstructured. For example, a progress note might be standardized and structured in some systems (e.g., Subjective/Objective/Assessment/Plan) but unstructured in other systems. The PHR System manages Record Lifecycle Events for each Record Entry, including pre and post Event record states, continuity, persistence and related Record Audit Logs.

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1.1 Function	Record Lifecycle			778
	Statement: Manage Record Lifecycle **Description:** As above References: - ISO 21089: Health Informatics -- Trusted End-to-End Information Flows - HL7 EHR Interoperability Model DSTU - HL7 Electronic Health Record Lifecycle Model DSTU			
	1. The system SHALL conform to function RI.1.2.1 (Manage Record Entries) as the final step to conclude each Record Lifecycle Event in RI.1.1 (Record Lifecycle) and all child functions.			779
RI.1.1.1 Function	Originate/Retain Record Lifecycle Event			780
	Statement: Originate and Retain Record Entry (1 instance) **Description:** Occurs when an agent causes the system to: a) initiate capture of potential record content, and b) incorporate that content into the storage considered a permanent part of the health record. Reference: ISO 21089-2018, Section 15.1.			
	1. The system SHALL provide the ability to capture (originate) a Record Entry instance corresponding to an Action instance and context.			781
	2. The system SHALL capture a unique instance identifier for each Record Entry.			782
	3. The system SHALL capture the signature event (e.g., digital signature) of the origination entry Author, binding signature to Record Entry content.			783
	4. The system SHALL provide the ability to capture both structured and unstructured content in Record Entries.			784
	5. The system SHALL provide the ability to capture Record Entries from information recorded during system downtime.			785
	6. The system SHOULD provide the ability to integrate Record Entries from Information recorded during system downtime.			786
	7. The system SHALL provide the ability to capture the date/time an Action was taken or data was collected if different than date/time of the Record Entry.			787
	8. The system SHOULD capture metadata that identifies the source of non-originated Record Entry (e.g., templated, copied, duplicated, or boilerplate information).			788
	9. The system MAY provide the ability to tag unstructured Record Entry content to organize it according to need, for example, in a time-related fashion or by application-specific groups (such as photographs, handwritten notes, or auditory sounds), or by order of relative importance.			789
	10. The system MAY capture and maintain a Record Entry encoded as a standards-based data object (e.g., HL7 Continuity of Care, other HL7 CDA R2 Document, ISO 13606 artifact).			790
	11. The system MAY capture and maintain a standards-based data object to mirror (be duplicate and synchronous with) internal Record Entry representation.			791
RI.1.1.1.1 Function	Evidence of Record Entry Originate/Retain Event			792
	Statement: Maintain Evidence of Record Entry Originate/Retain Event **Description:** Evidence of Record Entry Originate/Retain Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
	1. The system SHALL audit each occurrence when a Record Entry is originated and retained.			793
	2. The system SHALL capture identity of the organization where Record Entry content is originated.			794
	3. The system SHALL capture identity of the patient who is subject of Record Entry content.			795
	4. The system SHALL capture identity of the individual(s) who performed the Action documented in Record Entry content.			796
	5. The system SHALL capture identity of the user who entered/authored Record Entry content.			797
	6. The system SHALL capture identity of the system application which originated Record Entry content.			798
	7. IF the source of Record Entry content is a device, THEN the system SHALL capture identity of the device.			799
	8. The system SHALL capture the Action as evidenced by Record Entry content.			800
	9. The system SHALL capture the type of Record Event trigger (i.e., originate/retain).			801
	10. The system SHALL capture the date and time of Action occurrence as evidenced by Record Entry content.			802
	11. The system SHALL capture the date and time Record Entry content is originated.			803
	12. The system MAY capture the duration of the Action evidenced by Record Entry content.			804
	13. The system MAY capture the physical location of the Action evidenced by Record Entry content.			805

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
14. The system SHOULD capture identity of the location (i.e., network address) where Record Entry content is originated.				806
15. The system MAY capture the rationale for the Action evidenced by Record Entry content.				807
16. The system MAY capture the rationale for originating Record Entry content.				808
17. IF Record Entry content includes templates (boilerplate information) or copied (duplicated) information, THEN the system SHOULD capture the source of such content.				809
RI.1.1.2 Function	Amend (Update) Record Lifecycle Event			810
Statement: Amend (Update) Record Entry (1 instance) **Description:** Occurs when an agent makes any change to record entry content currently residing in storage considered permanent (persistent). Reference: ISO 21089-2018, Section 15.2.				
1. The system SHALL provide the ability to update (amend) Record Entry content.				811
2. The system SHALL maintain the original and all previously amended versions of the Record Entry, retaining each version instance without alteration.				812
3. The system SHALL capture a new uniquely identifiable version of the Record Entry, incorporating amended content.				813
4. The system SHALL capture the signature event (e.g., digital signature) of the amendment Author, binding signature to Record Entry content.				814
RI.1.1.2.1 Function	Evidence of Record Entry Amendment Event			815
Statement: Maintain Evidence of Record Entry Amendment Event **Description:** Evidence of Record Entry Amendment Event includes key metadata, ensures health record integrity (and trust) and enables record audit.				
1. The system SHALL audit each occurrence when a Record Entry is amended.				816
2. The system SHALL capture identity of the organization where Record Entry content is amended.				817
3. The system SHALL capture identity of the patient who is subject of amended Record Entry content.				818
4. The system SHALL capture identity of the user who entered/authored Record Entry content amendment.				819
5. The system SHALL capture identity of the system application which amended Record Entry content.				820
6. The system SHALL capture the type of Record Event trigger (i.e., amendment).				821
7. The system SHALL capture the date and time Record Entry content is amended.				822
8. The system SHOULD capture identity of the location (i.e., network address) where Record Entry content is amended.				823
9. The system SHOULD capture the rationale for amending Record Entry content.				824
10. The system SHALL capture a sequence identifier for amended Record Entry content.				825
11. The system SHOULD capture a reference (e.g., link, pointer) to pre-amendment data for each amended Record Entry.				826
RI.1.1.3 Function	Transform/Translate Record Lifecycle Event			827
Statement: Transform/Translate Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to change the form, language or code system used to represent record entry content. Reference: ISO 21089-2018, Section 15.3.				
1. The system SHALL provide the ability to render coded Record Entry content translated from one coding/classification system to another.				828
2. The system SHALL provide the ability to render coded Record Entry content translated from one value set to another.				829
3. The system MAY provide the ability to render Record Entry content translated from one human language to another.				830
4. The system SHOULD maintain the original and all previously amended versions of the Record Entry, retaining each version instance without alteration.				831
5. The system SHOULD capture a new uniquely identifiable version of the Record Entry, incorporating translated content.				832

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1.1.3.1 Function	Evidence of Record Entry Translate Event			833
Statement: Maintain Evidence of Record Entry Translate Event **Description:** Evidence of Record Entry Translate Event includes key metadata, ensures health record integrity (and trust) and enables record audit.				
1. The system SHALL audit each occurrence when Record Entry content is translated.				834
2. The system SHALL capture identity of the organization where Record Entry content is translated.				835
3. The system SHALL capture identity of the patient who is subject of translated Record Entry content.				836
4. IF a user initiated a Record Entry content translation, THEN the system SHALL capture identity of the user initiating Record Entry content translation.				837
5. The system SHALL capture identity of the system application which translated Record Entry content.				838
6. The system SHALL capture the type of Record Event trigger (i.e., translation).				839
7. The system SHALL capture the date and time Record Entry content is translated.				840
8. The system SHOULD capture identity of the location (i.e., network address) where Record Entry content is translated.				841
9. IF a user initiated a Record Entry translation, THEN the system MAY capture the rationale for translating Record Entry content.				842
10. The system SHALL capture a sequence identifier for translated Record Entry content.				843
11. The system SHALL capture the identifier and version of Translation Tools used for each translated Record Entry.				844
12. The system SHALL capture a reference (e.g., link, pointer) to pre-translation data for each Record Entry translation.				845
RI.1.1.4 Function	Attest Record Lifecycle Event			846
Statement: Attest Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to capture the agent's digital signature (or equivalent indication) during formal validation of record entry content. Reference: ISO 21089-2018, Section 15.4.				
1. The system SHALL conform to function TI.1.1 (Entity Authentication).				847
2. The system SHALL conform to function TI.1.2 (Entity Authorization).				848
3. The system SHALL provide the ability to attest (approve and apply signature to) Record Entry content by the author.				849
4. The system SHALL capture the signature event (e.g., digital signature) of the Attesting Author, binding signature to Record Entry content.				850
5. The system SHALL provide the ability to maintain any attestable Record Entry content added or changed with the content's author				851
6. The system SHALL present the status of attestable Record Entry content which has not been attested, conforming to function RI.1.3.1 (Record Pending State).				852
7. IF the attester is different than the author(s), THEN the system SHALL provide the ability to maintain Record Entry content by properly authenticated and authorized users different from the author (e.g., counter-signature) according to scope of practice, organizational policy, and/or jurisdictional law.				853
8. The system SHOULD provide the ability to manage digital signatures as the means for attestation.				854
9. IF more than one author contributed to the Record Entry content, THEN the system SHALL provide the ability to maintain all authors/contributors associated with their content.				855
10. IF Record Entry content is attested by someone other than the author, THEN the system SHALL maintain and display the author(s) and attester.				856
11. The system SHALL provide the ability to present a minimum set of information that identifies the author of Record Entry content according to scope of practice, organizational policy, and/or jurisdictional law (e.g., name, credential, and/or role (such as Karen Smith, RN)).				857
12. The system SHALL capture the signature type of the entity (individual, PHR or other system, or organization) sending Record Entry content.				858
13. The system SHALL capture the signature type of the entity (individual, PHR or other system, or organization) receiving Record Entry content.				859
14. The system SHALL capture all signature types of the entities through which Record Entry content has passed.				860

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1.1.4.1 Function	Evidence of Record Entry Attestation Event			861
Statement: Maintain Evidence of Record Entry Attestation Event **Description:** Evidence of Record Entry Attestation Event includes key metadata, ensures health record integrity (and trust) and enables record audit.				
1. The system SHALL audit each occurrence of Record Entry attestation (signature event).				862
2. The system SHALL capture identity of the organization where Record Entry content attestation (signature event) occurred.				863
3. The system SHALL capture identity of the patient who is subject of attested Record Entry content.				864
4. The system SHALL capture identity of the user attesting to Record Entry content (signature event).				865
5. The system SHALL capture identity of the system application in which Record Entry content attestation (signature event) occurred.				866
6. The system SHALL capture the type of Record Event trigger (i.e., attestation/signature event).				867
7. The system SHALL capture the date and time of Record Entry content attestation (signature event).				868
8. The system SHOULD capture identity of the location (i.e., network address) where Record Entry content attestation (signature event) occurred.				869
9. The system SHALL capture the data, document or other identifier for attested Record Entry content.				870
RI.1.1.5 Function	Access/View Record Lifecycle Event			871
Statement: Access/View Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to obtain and open a record entry for inspection or review. Reference: ISO 21089-2018, Section 15.5.				
1. The system MAY mask Record Entry content to access by authorized entities.				872
2. The system SHALL provide the ability to render Record Entry content, including original version and any subsequent amendments.				873
3. The system SHALL provide the ability to render Record Entry content down to the discrete element or item, including encoded fields.				874
RI.1.1.5.1 Function	Evidence of Record Entry View/Access Event			875
Statement: Maintain Evidence of Record Entry View/Access Event **Description:** Evidence of Record Entry View/Access Event includes key metadata, ensures health record integrity (and trust) and enables record audit.				
1. The system SHALL audit each occurrence when Record Entry content is viewed/accessed.				876
2. The system SHALL capture identity of the organization where Record Entry content is viewed/ accessed.				877
3. The system SHALL capture identity of the patient who is subject of the viewed/accessed Record Entry content.				878
4. The system SHALL capture identity of the user who viewed/accessed Record Entry content.				879
5. The system SHALL capture identity of the system application in which Record Entry content is viewed/accessed.				880
6. The system SHALL capture the type of Record Event trigger (i.e., view/access).				881
7. The system SHALL capture the date and time Record Entry content is viewed/accessed.				882
8. The system SHOULD capture identity of the location (i.e., network address) where Record Entry content is viewed/accessed.				883
9. The system MAY capture the rationale for viewing/accessing Record Entry content (e.g., emergency access).				884
10. The system SHALL capture the data, document or other identifier for the viewed/accessed Record Entry content.				885
11. The system MAY capture whether the data/document viewed/accessed is a primary source record (e.g., patient's record) or an aggregated report (e.g., summary report including multiple patients).				886
12. The system SHALL capture when a Record Entry content view/access occurrence is known to be a disclosure, according to scope of practice, organizational policy, and/or jurisdictional law.				887
13. The system SHOULD capture known and applicable permissions regarding Record Entry content viewed/accessed including confidentiality codes, patient consent authorizations, privacy policy pointers.				888

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1.1.6 Function	Report (Output) Record Lifecycle Event			889
	Statement: Report (Output) Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to produce and deliver record entry content in a particular form and manner. Reference: ISO 21089-2018, Section 15.6.			
	1. The system SHOULD provide the ability to render Record Entry content (e.g., as a report) retaining original, unaltered content and signature bindings, Action and Record Entry provenance and metadata.			890
	2. The system SHALL provide the ability to render Record Entry extracts, including content, context, provenance and metadata.			891
	3. The system SHALL provide the ability to capture the identity of the patient or the individual subject who is the target of Record Entry content that is presented/reported.			892
	4. IF the identity of a specific recipient has been stored, THEN the system SHOULD render protected Record Entry content based on established permissions and according to scope of practice, organizational policy, and/or jurisdictional law.			893
	5. IF known and explicit as to Record Entry content being output/reported, THEN the system SHOULD transmit corresponding authorizations and patient consent permissions.			894
	6. The system SHALL conform to function TI.1.6 (Secure Data Exchange).			895
	7. The system SHALL provide the ability to extract Record Entry content prior to output/report, conforming to function RI.1.1.13 (Extract Record Entry Content).			896
	8. The system SHALL provide the ability to de-identify Record Entry content prior to output/report, conforming to function RI.1.1.10 (De-Identify Record Entries).			897
	9. The system SHALL provide the ability to render updates (new versions) of Record Entry Content to known recipients of prior versions of that Record Entry Content according to scope of practice, organizational policy, and/or jurisdictional law.			898
RI.1.1.6.1 Function	Evidence of Record Entry Output/Report Event			899
	Statement: Maintain Evidence of Record Entry Output/Report Event **Description:** Evidence of Record Entry Output/Report Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
	1. The system SHALL audit each occurrence when an output (e.g., report, screen shot) is generated from Record Entry content.			900
	2. The system SHALL capture identity of the organization where output/report is generated from Record Entry content.			901
	3. The system SHALL capture identity of the patient who is subject of the Record Entry(ies) populating the output/report generated.			902
	4. The system SHALL capture identity of the user who generated the output/report of Record Entry content.			903
	5. The system SHALL capture identity of the system application from which the output/report is generated.			904
	6. The system SHALL capture the type of Record Event trigger (i.e., output/report).			905
	7. The system SHALL capture the date and time the output/report is generated.			906
	8. The system SHOULD capture identity of the location (i.e., network address) where the output/ report is generated.			907
	9. The system MAY capture the rationale for generating the output/report.			908
	10. The system MAY capture the data, document, or other identifier for the output/report generated.			909
	11. The system SHALL capture when a Record Entry content output/report occurrence is known to be a disclosure, according to scope of practice, organizational policy, and/or jurisdictional law.			910
	12. The system SHOULD capture known and applicable permissions regarding Record Entry content output/reported including confidentiality codes, patient consent authorizations, privacy policy pointers.			911
RI.1.1.7 Function	Disclose Record Lifecycle Event			912
	Statement: Disclose Record Entry Content (1 or more instances) **Description:** Occurs when an agent causes the system to release, transfer, provision access to, or otherwise divulge record entry content. Reference: ISO 21089-2018, Section 15.7.			
	1. The system SHALL provide the ability to capture the identity of the patient or individual subject to whom Record Entry content was transmitted/disclosed.			913

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
2.	The system SHALL capture a log entry for disclosure of protected Record Entry content, according to scope of practice, organizational policy, and/or jurisdictional law.			914
3.	IF the identity of a specific recipient has been stored, THEN the system SHOULD render protected Record Entry content based on established permissions and according to scope of practice, organizational policy, and/or jurisdictional law.			915
4.	IF known and explicit as to Record Entry content being transmitted, THEN the system SHOULD transmit corresponding authorizations and patient consent permissions.			916
5.	The system SHALL conform to function TI.1.6 (Secure Data Exchange).			917
6.	The system SHALL provide the ability to extract Record Entry content prior to disclosure, conforming to function RI.1.1.13 (Extract Record Entry Content).			918
7.	The system SHALL provide the ability to de-identify Record Entry content prior to disclosure, conforming to function RI.1.1.10 (De-Identify Record Entries).			919
RI.1.1.7.1 Function	Evidence of Record Entry Disclosure Event			920
	Statement: Maintain Evidence of Record Entry Disclosure Event **Description:** Evidence of Record Entry Disclosure Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
1.	The system SHALL audit each occurrence when Record Entry content is disclosed according to scope of practice, organizational policy, and/or jurisdictional law.			921
2.	The system SHALL capture identity of the organization from which Record Entry content is disclosed.			922
3.	The system SHALL capture identity of the patient who is subject of Record Entry content disclosed.			923
4.	The system SHALL capture identity of the user initiating disclosure of Record Entry content.			924
5.	The system SHALL capture identity of the system application from which Record Entry content is disclosed.			925
6.	The system SHALL capture the type of Record Event trigger (i.e., disclose).			926
7.	The system SHALL capture the date and time Record Entry content is disclosed.			927
8.	The system SHOULD capture identity of the location (i.e., network address) where Record Entry content is disclosed.			928
9.	The system SHOULD capture the rationale for disclosing Record Entry content.			929
10.	The system MAY capture the data, document or other identifier for Record Entry content disclosed.			930
11.	The system SHALL capture that this is an occurrence when Record Entry content is known to be disclosed, according to scope of practice, organizational policy, and/or jurisdictional law.			931
12.	The system SHOULD capture known and applicable permissions regarding Record Entry content disclosed including confidentiality codes, patient consent authorizations, privacy policy pointers.			932
RI.1.1.8 Function	Transmit Record Lifecycle Event			933
	Statement: Transmit Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to send record entry content from one (EHR/PHR/other) system to another. Reference: ISO 21089-2018, Section 15.8.			
1.	The system SHOULD provide the ability to transmit Record Entry content to external systems, retaining original, unaltered content and signature bindings, Action and Record Entry provenance and metadata.			934
2.	The system SHALL provide the ability to transmit Record Entry extracts to external systems, including content, context, provenance and metadata.			935
3.	The system SHALL provide the ability to capture the identity of the patient or individual subject to whom Record Entry content was transmitted.			936
4.	IF a specific recipient is known, THEN the system SHOULD transmit protected Record Entry content based on established permissions and according to scope of practice, organizational policy, and/or jurisdictional law.			937
5.	IF known and explicit as to Record Entry content being transmitted, THEN the system SHOULD transmit corresponding authorizations and patient consent permissions.			938
6.	The system SHALL conform to function TI.1.6 (Secure Data Exchange).			939
7.	The system SHALL provide the ability to extract Record Entry content prior to transmittal, conforming to function RI.1.1.13 (Extract Record Entry Content).			940
8.	The system SHALL provide the ability to de-identify Record Entry content prior to transmittal, conforming to function RI.1.1.10 (De-Identify Record Entries).			941
9.	The system SHALL provide the ability to transmit updates (new versions) of Record Entry Content to known recipients of prior versions according to scope of practice, organizational policy, and/or jurisdictional law.			942

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
10.	The system SHALL provide the ability to transmit with each exchange the most recent or all versions of Record Entry Content according to scope of practice, organizational policy, and/or jurisdictional law.			943
RI.1.1.8.1 Function	Evidence of Record Entry Transmit Event			944
	Statement: Maintain Evidence of Record Entry Transmit Event **Description:** Evidence of Record Entry Transmit Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
1.	The system SHALL audit each occurrence when Record Entry content is transmitted.			945
2.	The system SHALL capture identity of the organization from which Record Entry content is transmitted.			946
3.	The system SHALL capture identity of the patient who is subject of Record Entry content transmitted.			947
4.	The system SHALL capture identity of the user initiating transmission of Record Entry content.			948
5.	The system SHALL capture identity of the system application which transmitted Record Entry content.			949
6.	The system SHALL capture identity of the system application which received Record Entry content.			950
7.	The system SHALL capture the type of Record Event trigger (i.e., transmit).			951
8.	The system SHALL capture the date and time Record Entry content is transmitted.			952
9.	The system SHOULD capture identity of the location (i.e., network address) from which the Record Entry is transmitted/disclosed.			953
10.	The system SHALL capture the location (network address) to which the Record Entry is transmitted/disclosed.			954
11.	The system MAY capture the rationale for transmitting Record Entry content.			955
12.	The system SHALL capture the type of Record Entry content transmitted/disclosed (e.g., original, amended, updated data).			956
13.	The system MAY capture the data, document or other identifier for transmitted/disclosed Record Entry.			957
14.	The system MAY capture data elements for transmitted/disclosed Record Entry.			958
15.	The system SHALL capture when a Record Entry transmit occurrence is known to be a disclosure, according to scope of practice, organizational policy, and/or jurisdictional law.			959
16.	The system SHOULD capture known and applicable permissions regarding Record Entry content transmitted including confidentiality codes, patient consent authorizations, privacy policy pointers.			960
RI.1.1.9 Function	Receive/Retain Record Lifecycle Event			961
	Statement: Receive/Retain Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to a) initiate capture of data content from elsewhere, and b) incorporate that content into the storage considered a permanent part of the health record. Reference: ISO 21089-2018, Section 15.9.			
1.	The system SHOULD provide the ability to capture and maintain Record Entry content from external systems, retaining and persisting original unaltered content and signature bindings, Action and Record Entry provenance and metadata.			962
2.	The system SHALL provide the ability to capture and maintain Record Entry extracts from external systems, retaining and persisting source, identity, record content, corresponding provenance and metadata.			963
3.	The system SHALL provide the ability to capture the identity of the patient or individual subject to whom Record Entry content was received.			964
4.	IF received with Record Entry content, THEN the system SHOULD control subsequent data access to that permitted by corresponding authorizations and patient consents.			965
RI.1.1.9.1 Function	Evidence of Record Entry Receive/Retain Event			966
	Statement: Maintain Evidence of Record Entry Receive/Retain Event **Description:** Evidence of Record Entry Receive/Retain Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
1.	The system SHALL audit each occurrence when externally-sourced Record Entry content is received and retained.			967
2.	The system SHALL capture identity of the organization transmitting Record Entry content received and retained.			968
3.	The system SHALL capture identity of the organization receiving transmitted Record Entry content.			969
4.	The system SHALL capture identity of the patient who is subject of received Record Entry content.			970

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
5. IF the system supports user verification of receipt of externally-sourced Record Entry content, THEN the system SHALL capture identity of the user accepting receipt of the transmitted Record Entry content.				971
6. The system SHALL capture identity of the system application which transmitted Record Entry content.				972
7. The system SHALL capture identity of the system application which received Record Entry content.				973
8. The system SHALL capture the type of Record Event trigger (i.e., receive).				974
9. The system SHALL capture the date and time Record Entry content is received.				975
10. The system SHOULD capture identity of the location (i.e., network address) where the Record Entry content is received.				976
11. The system MAY capture the rationale for accepting receipt of transmitted Record Entry content.				977
12. The system SHALL capture the type of Record Entry content received (e.g., original, amended, updated data).				978
13. IF an internal identifier is assigned to data/documents received from an external source, THEN the system MAY capture the data, document or other identifier for the Record Entry received.				979
14. The system MAY capture data elements for the Record Entry received.				980
RI.1.1.10 Function	De-Identify (Anononymize) Record Lifecycle Event			981
Statement: De-Identify (Anononymize) Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to scrub record entry content to reduce the association between a set of identifying data and the data subject in a way that may or may not be reversible. Reference: ISO 21089-2018, Section 15.10.				
1. The system SHALL provide the ability to de-identify Record Entry content according to scope of practice, organizational policy, and/or jurisdictional law.				982
RI.1.1.10.1 Function	Evidence of Record Entry De-Identification Event			983
Statement: Maintain Evidence of Record Entry De-Identification Event **Description:** Evidence of Record Entry De-Identification Event includes key metadata, ensures health record integrity (and trust) and enables record audit.				
1. The system SHALL audit each occurrence when Record Entry content is de-identified.				984
2. The system SHALL capture identity of the organization where Record Entry content is de-identified.				985
3. The system SHALL capture identity of the patient who is subject of de-identified Record Entry content.				986
4. The system SHALL capture identity of the user de-identifying Record Entry content.				987
5. The system SHALL capture identity of the system application which de-identified Record Entry content.				988
6. The system SHALL capture the type of Record Event trigger (i.e., de-identify).				989
7. The system SHALL capture the date and time Record Entry content is de-identified.				990
8. The system SHOULD capture identity of the location (i.e., network address) where Record Entry content is de-identified.				991
9. The system MAY capture the rationale for de-identifying Record Entry content.				992
10. The system MAY capture the data, document or other identifier for de-identified Record Entry content.				993
RI.1.1.11 Function	Pseudonymize Record Lifecycle Event			994
Statement: Pseudonymize Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to remove record entry content to reduce the association between a set of identifying data and the data subject in a way that may be reversible. Reference: ISO 21089-2018, Section 15.11.				
1. The system SHALL provide the ability to de-identify patient Record Entries by pseudomizing patient Record Entries (or associating them with a new identity) according to scope of practice, organizational policy, and/or jurisdictional law.				995
RI.1.1.11.1 Function	Evidence of Record Entry Pseudomynization Event			996
Statement: Maintain Evidence of Record Entry Pseudomynization Event **Description:** Evidence of Record Entry Pseudomynization Event includes key metadata, ensures health record integrity (and trust) and enables record audit.				
1. The system SHALL audit each occurrence when a Record Entry content is pseudomynized.				997

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
2. The system SHALL capture identity of the organization where Record Entry content is pseudomynized.				998
3. The system SHALL capture identity of the patient who is subject of pseudomynized Record Entry content.				999
4. The system SHALL capture identity of the user pseudomynizing Record Entry content.				1000
5. The system SHALL capture identity of the system application which pseudomynized Record Entry content.				1001
6. The system SHALL capture the type of Record Event trigger (i.e., pseudomynize).				1002
7. The system SHALL capture the date and time Record Entry content is pseudomynized.				1003
8. The system SHOULD capture identity of the location (i.e., network address) where the Record Entry content is pseudomynized.				1004
9. The system MAY capture the rationale for pseudomynizing Record Entry content.				1005
RI.1.1.12 Function	Re-identify Record Lifecycle Event			1006
Statement: Re-Identify Record Entries that were previously de-identified or pseudonymized (1 or more instances) **Description:** Occurs when an agent causes the system to restore information to data that allows identification of information source and/or information subject. Reference: ISO 21089-2018, Section 15.12.				
1. The system SHALL provide the ability to re-identify (or associate original identity with) Record Entry content according to scope of practice, organizational policy, and/or jurisdictional law.				1007
RI.1.1.12.1 Function	Evidence of Record Entry Re-Identification Event			1008
Statement: Maintain Evidence of Record Entry Re-Identification Event **Description:** Evidence of Record Entry Re-Identification Event includes key metadata, ensures health record integrity (and trust) and enables record audit.				
1. The system SHALL audit each occurrence when Record Entry content is re-identified.				1009
2. The system SHALL capture identity of the organization where Record Entry content is re-identified.				1010
3. The system SHALL capture identity of the patient who is subject of re-identified Record Entry content.				1011
4. The system SHALL capture identity of the user re-identifying Record Entry content.				1012
5. The system SHALL capture identity of the system application which re-identified Record Entry content.				1013
6. The system SHALL capture the type of Record Event trigger (i.e., re-identify).				1014
7. The system SHALL capture the date and time Record Entry content is re-identified.				1015
8. The system SHOULD capture identity of the location (i.e., network address) where Record Entry content is re-identified.				1016
9. The system MAY capture the rationale for re-identifying Record Entry content.				1017
RI.1.1.13 Function	Extract Record Lifecycle Event			1018
Statement: Extract Record Entry content to produce subsets, derivations or aggregations (1 or more instances) **Description:** Occurs when an agent causes the system to selectively pull out a subset of record entry content, based on explicit criteria. Reference: ISO 21089-2018, Section 15.13.				
1. The system SHALL provide the ability to extract Record Entry content to produce subsets, derivations, summaries or aggregations according to scope of practice, organizational policy, and/ or jurisdictional law.				1019
2. The system SHALL provide the ability to de-identify Record Entries during extraction in accordance with function RI.1.1.10 (De-Identify Record Entries).				1020
3. The system SHALL provide the ability to extract Record Entry content based on queries with selection criteria, for example, key words, date/time range, full text search.				1021
4. The system SHALL provide the ability to extract metadata associated with Record Entry content.				1022
5. The system SHOULD provide the ability to extract, with parameterized selection criteria, across the complete data set that constitutes all Record Entries for a patient.				1023
6. The system SHOULD provide the ability to extract and present a full chronicle of the healthcare process from assembled Record Entries.				1024
7. The system SHOULD provide the ability to extract and present a full chronicle of healthcare delivered to a patient from assembled Record Entries.				1025
8. The system SHALL provide the ability to extract Record Entry content for various purposes, including administrative, financial, research, quality analysis and public health.				1026
9. The system SHOULD provide the ability to extract Record Entries for system migration.				1027

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
10.	The system SHOULD provide the ability to manage a set of over-riding parameters to exclude sensitive or privileged Record Entry content from extraction.			1028
11.	The system MAY provide the ability to extract unstructured Record Entry content and convert it into structured data.			1029
RI.1.1.13.1 Function	Evidence of Record Entry Extraction Event			1030
	Statement: Maintain Evidence of Record Entry Extraction Event **Description:** Evidence of Record Entry Extraction Events includes key metadata, ensures health record integrity (and trust) and enables record audit.			
1.	The system SHALL audit each occurrence when Record Entry content is extracted.			1031
2.	The system SHALL capture identity of the organization where Record Entry content is extracted.			1032
3.	The system SHALL capture identity of the patient who is subject of extracted Record Entry content.			1033
4.	The system SHALL capture identity of the user extracting Record Entry content.			1034
5.	The system SHALL capture identity of the system application which extracted Record Entry content.			1035
6.	The system SHALL capture the type of Record Event trigger (i.e., extract).			1036
7.	The system SHALL capture the date and time Record Entry content is extracted.			1037
8.	The system SHOULD capture identity of the location (i.e., network address) where Record Entry content is extracted.			1038
9.	The system MAY capture the rationale for extracting Record Entry content.			1039
RI.1.1.14 Function	Archive Record Lifecycle Event			1040
	Statement: Archive Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to create and move archive artifacts containing record entry content, typically to long-term offline storage. Reference: ISO 21089-2018, Section 15.14.			
1.	The system SHALL archive Record Entries according to function RI.3 (Manage Record Archive and Restore).			1041
RI.1.1.14.1 Function	Evidence of Record Entry Archive Event			1042
	Statement: Maintain Evidence of Record Entry Archive Event **Description:** Evidence of Record Entry Archive Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
1.	The system SHALL audit each occurrence when Record Entry content is archived.			1043
2.	The system SHALL capture identity of the organization where Record Entry content is archived.			1044
3.	The system SHALL capture identity of the patient who is subject of archived Record Entry content.			1045
4.	The system SHALL capture an archive identifier for archived Record Entry content (e.g., nursing home inpatient stay from 3/15/2000 thru 6/10/2000).			1046
5.	The system SHALL capture identity of the user archiving Record Entry content.			1047
6.	The system SHALL capture identity of the system application which archived Record Entry content.			1048
7.	The system SHALL capture the type of Record Event trigger (i.e., archive).			1049
8.	The system SHALL capture the date and time Record Entry content is archived.			1050
9.	The system SHOULD capture identity of the location (i.e., network address) to which Record Entry content is archived.			1051
10.	The system MAY capture the rationale for archiving Record Entry content.			1052
11.	The system SHALL capture the set of Record Entry content to be archived.			1053
12.	The system MAY capture the data, document or other identifier for archived Record Entry content.			1054
13.	The system SHOULD capture the method and target media of archived Record Entry content.			1055
RI.1.1.15 Function	Restore Record Lifecycle Event			1056
	Statement: Restore Record Entries from archive (1 or more instances) **Description:** Occurs when an agent causes the system to recreate record entries and their content from a previous created archive artefact. Reference: ISO 21089-2018, Section 15.15.			
1.	The system SHALL provide the ability to restore (previously archived) Record Entries according to scope of practice, organizational policy, and/or jurisdictional law.			1057

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1.1.15.1 Function	Evidence of Record Entry Restore Event			1058
	Statement: Maintain Evidence of Record Entry Restore Event **Description:** Evidence of Record Entry Restore Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
	1. The system SHALL audit each occurrence when archived Record Entry content is restored.			1059
	2. The system SHALL capture identity of the organization where Record Entry content is restored.			1060
	3. The system SHALL capture identity of the patient who is subject of restored Record Entry content.			1061
	4. The system SHALL capture an archive identifier for restored Record Entry content (e.g., nursing home inpatient stay from 3/15/2000 thru 6/10/2000).			1062
	5. The system SHALL capture identity of the user restoring Record Entry content.			1063
	6. The system SHALL capture identity of the system application which restored Record Entry content.			1064
	7. The system SHALL capture the type of Record Event trigger (i.e., restore).			1065
	8. The system SHALL capture the date and time Record Entry content is restored.			1066
	9. The system SHOULD capture identity of the location (i.e., network address) from which Record Entry content is restored.			1067
	10. The system MAY capture the rationale for restoring Record Entry content.			1068
	11. The system MAY capture the data, document or other identifier for restored Record Entry content.			1069
RI.1.1.16 Function	Destroy/Delete Record Lifecycle Event			1070
	Statement: Destroy/Delete Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to permanently erase record entry content from the system. Reference: ISO 21089-2018, Section 15.16.			
	1. The system SHALL provide the ability to delete (destroy) Record Entries (e.g., those exceeding their legal retention period) according to scope of practice, organizational policy, and/or jurisdictional law.			1071
	2. The system SHALL provide the ability to tag Record Entries as missing.			1072
RI.1.1.16.1 Function	Evidence of Record Entry Destruction Event			1073
	Statement: Maintain Evidence of Record Entry Destruction Event **Description:** Evidence of Record Entry Destruction Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
	1. The system SHALL audit each occurrence when Record Entry content is destroyed according to scope of practice, organizational policy, and/or jurisdictional law.			1074
	2. The system SHALL capture identity of the organization where Record Entry content is destroyed.			1075
	3. The system SHALL capture identity of the patient who is subject of destroyed Record Entry content.			1076
	4. The system SHALL capture a destruction identifier for destroyed Record Entry content (e.g., nursing home inpatient stay from 3/15/2000 thru 6/10/2000).			1077
	5. The system SHALL capture identity of the user destroying Record Entry content.			1078
	6. The system SHALL capture identity of the system application which destroyed Record Entry content.			1079
	7. The system SHALL capture the type of Record Event trigger (i.e., destroy).			1080
	8. The system SHALL capture the date and time Record Entry content is destroyed.			1081
	9. The system SHOULD capture identity of the location (i.e., network address) where Record Entry content is destroyed.			1082
	10. The system MAY capture the rationale for destroying Record Entry content.			1083
	11. The system MAY capture the data, document or other identifier for destroyed Record Entry content.			1084
	12. The system MAY capture data elements for Record Entry content de-identified.			1085
RI.1.1.17 Function	Deprecate Record Lifecycle Event			1086
	Statement: Deprecate Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to tag record entry(ies) as obsolete, erroneous or untrustworthy, to warn against its future use. Reference: ISO 21089-2018, Section 15.17.			
	1. The system SHALL provide the ability to tag Record Entries as deprecated/retracted and indicating that they are invalid according to scope of practice, organizational policy, and/or jurisdictional law.			1087

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1.1.17.1 Function	Evidence of Record Entry Deprecation/Retraction Event			1088
Statement: Maintain Evidence of Record Entry Deprecation/Retraction Event **Description:** Evidence of Record Entry Deprecation/Retraction Event includes key metadata, ensures health record integrity (and trust) and enables record audit.				
1. The system SHALL audit each occurrence when Record Entry content is deprecated/retracted.				1089
2. The system SHALL capture identity of the organization where Record Entry content is deprecated/ retracted.				1090
3. The system SHALL capture identity of the patient who is subject of deprecated/retracted Record Entry content.				1091
4. The system SHALL capture identity of the user deprecating/retracting Record Entry content.				1092
5. The system SHALL capture identity of the system application which deprecated/retracted Record Entry content.				1093
6. The system SHALL capture the type of Record Event trigger (i.e., deprecate/retract).				1094
7. The system SHALL capture the date and time Record Entry content is deprecated/retracted.				1095
8. The system SHALL capture identity of the location (i.e., network address) where Record Entry content is deprecated/retracted.				1096
9. The system MAY capture the rationale for deprecating/retracting Record Entry content.				1097
RI.1.1.18 Function	Re-activate Record Lifecycle Event			1098
Statement: Re-activate Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to recreate or restore full status to record entries previously deleted or deprecated. Reference: ISO 21089-2018, Section 15.18.				
1. The system SHALL provide the ability to untag Record Entries that were previously tagged as being deleted or deprecated (or tag Record Entries as no longer being deleted that were previously deleted, or as no longer being deprecated that were previously deprecated) and thus reactivate those Record Entries according to scope of practice, organizational policy, and/or jurisdictional law.				1099
RI.1.1.18.1 Function	Evidence of Record Entry Re-Activation Event			1100
Statement: Maintain Evidence of Record Entry Re-Activation Event **Description:** Evidence of Record Entry Re-Activation Event includes key metadata, ensures health record integrity (and trust) and enables record audit.				
1. The system SHALL audit each occurrence when destroyed or deprecated Record Entry content is re-activated.				1101
2. The system SHALL capture identity of the organization where Record Entry content is reactivated.				1102
3. The system SHALL capture identity of the patient who is subject of reactivated Record Entry content.				1103
4. The system SHALL capture identity of the user reactivating Record Entry content.				1104
5. The system SHALL capture identity of the system application which re-activated Record Entry content.				1105
6. The system SHALL capture the type of Record Event trigger (i.e., re-activate).				1106
7. The system SHALL capture the date and time Record Entry content is re-activated.				1107
8. The system SHOULD capture identity of the location (i.e., network address) where Record Entry content is re-activated.				1108
9. The system MAY capture the rationale for re-activating Record Entry content.				1109
RI.1.1.19 Function	Merge Record Lifecycle Event			1110
Statement: Merge Record Entries (2 or more instances) **Description:** Occurs when an agent causes the system to combine or join content from two or more record entries, resulting in a single logical record entry. Reference: ISO 21089-2018, Section 15.19.				
1. The system SHALL provide the ability to harmonize or integrate patient Record Entries by logically merging patient Record Entries according to scope of practice, organizational policy, and/or jurisdictional law.				1111

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1.1.19.1 Function	Evidence of Record Entry Merge Event			1112
	Statement: Maintain Evidence of Record Entry Merge Event **Description:** Evidence of Record Entry Merge Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
1.	The system SHALL audit each occurrence when Record Entries are merged (e.g., same patient, multiple sets of record entries).			1113
2.	The system SHALL capture identity of the organization where Record Entries are merged.			1114
3.	The system SHALL capture identity of the patient who is subject of merged Record Entries.			1115
4.	The system SHALL capture the identifier for the source set of Record Entries.			1116
5.	The system SHALL capture the identifier for the target set of Record Entries.			1117
6.	The system SHALL capture identity of the user merging Record Entries.			1118
7.	The system SHALL capture identity of the system application which merged Record Entries.			1119
8.	The system SHALL capture the type of Record Event trigger (i.e., merge).			1120
9.	The system SHALL capture the date and time Record Entries are merged.			1121
10.	The system SHALL capture identity of the location (i.e., network address) where Record Entries are merged.			1122
11.	The system MAY capture the rationale for merging Record Entries.			1123
12.	The system MAY capture the data, document or other identifier for merged Record Entries.			1124
RI.1.1.20 Function	Unmerge Record Lifecycle Event			1125
	Statement: Unmerge Record Entries previously merged (2 or more instances) **Description:** Occurs when an agent causes the system to reverse a previous record entry merge operation, rendering them separate again. Reference: ISO 21089-2018, Section 15.20.			
1.	The system SHALL provide the ability to update multiple patient Record Entries that were previously harmonized or integrated by unmerging them according to scope of practice, organizational policy, and/or jurisdictional law.			1126
RI.1.1.20.1 Function	Evidence of Record Entry Unmerge Event			1127
	Statement: Maintain Evidence of Record Entry Unmerge Event **Description:** Evidence of Record Entry Unmerge Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
1.	The system SHALL audit each occurrence when merged Record Entries are unmerged.			1128
2.	The system SHALL capture identity of the organization where Record Entries are unmerged.			1129
3.	The system SHALL capture identity of the patient who is subject of unmerged Record Entries.			1130
4.	The system SHALL capture the identifier for the source set of Record Entries.			1131
5.	The system SHALL capture the identifier for the target set of Record Entries.			1132
6.	The system SHALL capture identity of the user unmerging Record Entries.			1133
7.	The system SHALL capture identity of the system application which unmerged Record Entries.			1134
8.	The system SHALL capture the type of Record Event trigger (i.e., unmerge).			1135
9.	The system SHALL capture the date and time Record Entries are unmerged.			1136
10.	The system SHOULD capture identity of the location (i.e., network address) where Record Entries are unmerged.			1137
11.	The system MAY capture the rationale for unmerging Record Entries.			1138
12.	The system MAY capture the data, document or other identifier for unmerged Record Entries.			1139
RI.1.1.21 Function	Link Record Lifecycle Event			1140
	Statement: Link Record Entries (2 or more instances) **Description:** Occurs when an agent causes the system to connect related record entries. Reference: ISO 21089-2018, Section 15.21.			
1.	The system SHALL provide the ability to link patient Record Entries logically according to scope of practice, organizational policy, and/or jurisdictional law.			1141

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1.1.21.1 Function	Evidence of Record Entry Link Event			1142
	Statement: Maintain Evidence of Record Entry Link Event **Description:** Evidence of Record Entry Link Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
	1. The system SHOULD audit each occurrence when Record Entries are linked to another entry/ object (e.g., Record Entries in an external system).			1143
	2. The system SHOULD capture identity of the organization where Record Entries are linked.			1144
	3. The system SHOULD capture identity of the patient who is subject of linked Record Entries.			1145
	4. The system SHOULD capture identity of the user linking Record Entries.			1146
	5. The system SHOULD capture identity of the system application which linked Record Entries.			1147
	6. The system SHOULD capture the type of Record Event trigger (i.e., link).			1148
	7. The system SHOULD capture the date and time Record Entries are linked.			1149
	8. The system SHOULD capture identity of the location (i.e., network address) where Record Entries are linked.			1150
	9. The system MAY capture the rationale for linking Record Entries.			1151
RI.1.1.22 Function	Unlink Record Lifecycle Event			1152
	Statement: Unlink Record Entries (2 or more instances) **Description:** Occurs when an agent causes the system to disconnect two or more record entries previously connected, rendering them separate (disconnected) again. Reference: ISO 21089-2018, Section 15.22.			
	1. The system SHALL provide the ability to update multiple patient Record Entries by unlinking them according to scope of practice, organizational policy, and/or jurisdictional law.			1153
RI.1.1.22.1 Function	Evidence of Record Entry Unlink Event			1154
	Statement: Maintain Evidence of Record Entry Unlink Event **Description:** Evidence of Record Entry Unlink Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
	1. The system SHOULD audit each occurrence when linked Record Entries are unlinked from another entry/object.			1155
	2. The system SHOULD capture identity of the organization where Record Entries are unlinked.			1156
	3. The system SHOULD capture identity of the patient who is subject of un-linked Record Entry.			1157
	4. The system SHOULD capture identity of the user unlinking Record Entries.			1158
	5. The system SHOULD capture identity of the system application which unlinked Record Entries.			1159
	6. The system SHOULD capture the type of Record Event trigger (i.e., unlink).			1160
	7. The system SHOULD capture the date and time Record Entries are unlinked.			1161
	8. The system SHOULD capture identity of the location (i.e., network address) where Record Entries are unlinked.			1162
	9. The system MAY capture the rationale for unlinking Record Entries.			1163
RI.1.1.23 Function	Add Legal Hold Record Lifecycle Event			1164
	Statement: Add Legal Hold to Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to tag or otherwise indicate special access management and suspension of record entry deletion/destruction, if deemed relevant to a lawsuit or which are reasonably anticipated to be relevant or to fulfill organizational policy under the legal doctrine of "duty to preserve". Reference: ISO 21089-2018, Section 15.23.			
	1. The system SHALL provide the ability to manage a specified set of patient Record Entries during period of legal hold, marking as to on hold status and preventing alteration according to scope of practice, organizational policy, and/or jurisdictional law.			1165
RI.1.1.23.1 Function	Evidence of Record Entry Legal Hold Event			1166
	Statement: Maintain Evidence of Record Entry Legal Hold Event **Description:** Evidence of Record Entry Legal Hold Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
	1. The system SHOULD audit each occurrence when a set of Record Entries are placed on legal hold.			1167

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
2. The system SHOULD capture identity of the organization where Record Entries are placed on legal hold.				1168
3. The system SHOULD capture identity of the patient who is subject of Record Entries placed on legal hold.				1169
4. The system SHOULD capture the identifier for the set of Record Entries placed on legal hold.				1170
5. The system SHOULD capture identity of the user placing Record Entries on legal hold.				1171
6. The system SHOULD capture identity of the system application which placed Record Entries on legal hold.				1172
7. The system SHOULD capture the type of Record Event trigger (i.e., placed on legal hold).				1173
8. The system SHOULD capture the date and time Record Entries are placed on legal hold.				1174
9. The system SHOULD capture identity of the location (i.e., network address) from which Record Entries are placed on legal hold.				1175
10. The system MAY capture identity of the location (i.e., network address) in which Record Entries on legal hold are placed.				1176
11. The system MAY capture the rationale for placing Record Entries on legal hold.				1177
12. The system MAY capture the data, document or other identifier for Record Entries placed on legal hold.				1178
RI.1.1.24 Function	Remove Legal Hold Record Lifecycle Event			1179
Statement: Remove Legal Hold from Record Entries (1 or more instances) **Description:** Occurs when an agent causes the system to remove a tag or other cues for special access management had required to fulfill organizational policy under the legal doctrine of "duty to preserve". Reference: ISO 21089-2018, Section 15.24.				
1. The system SHALL provide the ability to update the legal hold status of patient Record Entries by releasing the patient Record Entries from legal hold according to scope of practice, organizational policy, and/or jurisdictional law.				1180
RI.1.1.24.1 Function	Evidence of Record Entry Legal Hold Removal Event			1181
Statement: Maintain Evidence of Record Entry Legal Hold Removal Event **Description:** Evidence of Record Entry Legal Hold Removal Event includes key metadata, ensures health record integrity (and trust) and enables record audit.				
1. The system SHOULD audit each occurrence when a set of Record Entries are released from legal hold.				1182
2. The system SHOULD capture identity of the organization where Record Entries are released from legal hold.				1183
3. The system SHALL capture identity of the patient who is subject of Record Entries released from legal hold.				1184
4. The system SHALL capture identity of the user releasing Record Entries from legal hold.				1185
5. The system SHALL capture identity of the system application which released Record Entries from legal hold.				1186
6. The system SHOULD capture the type of Record Event trigger (i.e., released from legal hold).				1187
7. The system SHALL capture the date and time Record Entries are released from legal hold.				1188
8. The system SHOULD capture identity of the location (i.e., network address) where Record Entries are released from legal hold.				1189
9. The system MAY capture the rationale for releasing Record Entries from legal hold.				1190
RI.1.1.25 Function	Verify Record Entries			1191
Statement: Verify Record Entries (1 or more instances) **Description:** Verify Record Lifecycle Event - occurs when an agent causes the system to confirm compliance of data or data objects with regulations, requirements, specifications, or other imposed conditions based on organizational policy. Reference: ISO 21089-2018, Section 15.25.				
1. The system SHALL conform to function TI.1.1 (Entity Authentication).				1192
2. The system SHALL conform to function TI.1.2 (Entity Authorization).				1193
3. The system SHALL provide the ability to verify Record Entry content.				1194
4. The system SHALL provide the ability to maintain any verified Record Entry content added or changed with the content's author.				1195
5. The system SHALL present the status of verified Record Entry content which has not been verified, conforming to function RI.1.3.1 (Record Pending State).				1196

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
6.	IF the verifier is different than the author(s), THEN the system SHALL provide the ability to maintain Record Entry content by properly authenticated and authorized users different from the author according to scope of practice, organizational policy, and/or jurisdictional law.			1197
7.	IF more than one author contributed to the Record Entry content, THEN the system SHALL provide the ability to maintain all authors/contributors associated with their content.			1198
8.	IF Record Entry content is verified by someone other than the author, THEN the system SHALL maintain and display the author(s) and verifier(s).			1199
9.	The system SHALL provide the ability to present a minimum set of information that identifies the author of Record Entry content according to scope of practice, organizational policy, and/or jurisdictional law (e.g., name, credential, and/or role (such as Karen Smith, RN)).			1200
RI.1.1.25.1 Function	Evidence of Record Entry Verification Event			1201
	Statement: Maintain Evidence of Record Entry Verification Event **Description:** Evidence of Record Entry Verification Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
1.	The system SHALL audit each occurrence of Record Entry verification.			1202
2.	The system SHALL capture identity of the organization where Record Entry content verification occurred.			1203
3.	The system SHALL capture identity of the patient who is subject of verified Record Entry content.			1204
4.	The system SHALL capture identity of the user verifying Record Entry content			1205
5.	The system SHALL capture identity of the system application in which Record Entry content verification occurred.			1206
6.	The system SHALL capture the type of Record Event trigger (i.e., verification event).			1207
7.	The system SHALL capture the date and time of Record Entry content verification.			1208
8.	The system SHOULD capture identity of the location (i.e., network address) where Record Entry content verification occurred.			1209
9.	The system SHALL capture the data, document or other identifier for verified Record Entry content.			1210
RI.1.1.26 Function	Encrypt Record Entries			1211
	Statement: Encrypt Record Entries (1 or more instances) **Description:** Encrypt Record Lifecycle Event - occurs when an agent causes the system to encode record entry content in a cipher. Reference: ISO 21089-2018, Section 15.26.			
1.	The system SHALL provide the ability to render encrypted Record Entry content based on a cipher.			1212
2.	The system SHOULD maintain the original and all previous versions of the Record Entry, retaining each version instance without alteration.			1213
3.	The system SHOULD capture a new uniquely identifiable version of the Record Entry, incorporating encrypted content.			1214
RI.1.1.26.1 Function	Evidence of Record Entry Encryption Event			1215
	Statement: Maintain Evidence of Record Entry Encryption Event **Description:** Evidence of Record Entry Encryption Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
1.	The system SHALL audit each occurrence when Record Entry content is encrypted.			1216
2.	The system SHALL capture identity of the organization where Record Entry content is encrypted.			1217
3.	The system SHALL capture identity of the patient who is subject of encrypted Record Entry content.			1218
4.	IF a user initiated a Record Entry content encryption, THEN the system SHALL capture identity of the user initiating Record Entry content encryption.			1219
5.	The system SHALL capture identity of the system application which encrypted Record Entry content.			1220
6.	The system SHALL capture the type of Record Event trigger (i.e., encryption).			1221
7.	The system SHALL capture the date and time Record Entry content is encrypted.			1222
8.	The system SHALL capture identity of the location (i.e., network address) where Record Entry content is encrypted.			1223
9.	IF a user initiated a Record Entry encryption, THEN the system MAY capture the rationale for encrypting Record Entry content.			1224
10.	The system SHALL capture a sequence identifier for encrypted Record Entry content.			1225
11.	The system SHOULD capture the identifier and version of Encryption Tools used for each encrypted Record Entry.			1226
12.	The system SHOULD capture a reference (e.g., link, pointer) to pre-encrypted data for each Record Entry encryption.			1227

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1.1.27 Function	Decrypt Record Entries			1228
	Statement: Decrypt Records Entries (1 or more instances) **Description:** Decrypt Record Lifecycle Event - occurs when an agent causes the system to decode record entry content from a cipher. Reference: ISO 21089-2018, Section 15.27.			
	1. The system SHALL provide the ability to render decrypted Record Entry content based on a cipher.			1229
	2. The system SHOULD maintain the original and all previous versions of the Record Entry, retaining each version instance without alteration.			1230
	3. The system SHOULD capture a new uniquely identifiable version of the Record Entry, incorporating decrypted content.			1231
RI.1.1.27.1 Function	Evidence of Record Entry Decryption Event			1232
	Statement: Maintain Evidence of Record Entry Decryption Event **Description:** Evidence of Record Entry Decryption Event includes key metadata, ensures health record integrity (and trust) and enables record audit.			
	1. The system SHALL audit each occurrence when Record Entry content is decrypted.			1233
	2. The system SHALL capture identity of the organization where Record Entry content is decrypted.			1234
	3. The system SHALL capture identity of the patient who is subject of decrypted Record Entry content.			1235
	4. IF a user initiated a Record Entry content decryption, THEN the system SHALL capture identity of the user initiating Record Entry content decryption.			1236
	5. The system SHALL capture identity of the system application which decrypted Record Entry content.			1237
	6. The system SHALL capture the type of Record Event trigger (i.e., decryption).			1238
	7. The system SHALL capture the date and time Record Entry content is decrypted.			1239
	8. The system SHOULD capture identity of the location (i.e., network address) where Record Entry content is decrypted.			1240
	9. IF a user initiated a Record Entry decryption, THEN the system MAY capture the rationale for decrypting Record Entry content.			1241
	10. The system SHALL capture a sequence identifier for decrypted Record Entry content.			1242
	11. The system SHOULD capture the identifier and version of decryption Tools used for each decrypted Record Entry.			1243
	12. The system SHOULD capture a reference (e.g., link, pointer) to pre-decrypted data for each Record Entry decryption.			1244
RI.1.2 Function	Record Lifespan			1245
	Statement: Manage Record Lifespan **Description:** Record Lifecycle Events (Function RI.1.1) are those required to manage Record Entries in persistent storage over the full course of Record Lifespan (Section RI.1.2). See Section RI.1.1 , Record Lifecycle, for further description.			
RI.1.2.1 Function	Manage Record Entries			1246
	Statement: Manage/Persist Record Entries (Multiple instances) **Description:** Occurs upon Record Entry origination/retention and thereafter on a continuous and uninterrupted basis for lifespan of each Record Entry. - Ensures long-term retention and preservation of EHR Record Entries, without alteration. Reference: ISO 21089, Section 12.2.2			
	1. The system SHALL manage each Record Entry as a persistent, indelible (unalterable) data object, including its revision history.			1247
	2. The system SHALL manage (persist) each Record Entry for its applicable retention period according to scope of practice, organizational policy, and/or jurisdictional law.			1248
	3. The system SHALL manage (persist) the full set of identity, event and provenance Audit Metadata for each Record Entry, conforming to lifecycle events in function RI.1.1 (Record Lifecycle) and metadata requirements in function TI.2.1.1 (Record Entry Audit Triggers).			1249
	4. The system SHALL manage (persist) the attestation/signature event (e.g., digital signature) of each Record Entry conforming to function RI.1.1.4 (Attest Record Entry Content).			1250
	5. The system SHALL manage Record Entries with data content in standard and non-standard formats.			1251
	6. The system SHALL manage Record Entries containing both structured and unstructured data.			1252

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
7.	The system SHOULD manage Record Entry content with tagged or delimited elements including data formatted as text, documents, images, audio, waveforms, in ASCII, binary and other encodings.			1253
8.	The system SHOULD manage Record Entries in clinical and business contexts.			1254
9.	The system SHOULD provide the ability to manage sets of clinical and business context data, to be captured in or linked to Record Entries.			1255
10.	The system SHOULD provide the ability to extract all available elements included in the definition of a legal medical record (including Audit Log Entries and the decoded translation of anything stored only in code form) according to scope of practice, organizational policy, and/or jurisdictional law.			1256
11.	The system MAY provide the ability to tag specific Record Entries for deletion according to scope of practice, organizational policy, and/or jurisdictional law.			1257
12.	IF allowing tags for specific Record Entry deletion, THEN the system SHALL provide the ability to manage the set of tagged Entries, allowing review and confirmation before actual deletion occurs according to scope of practice, organizational policy, and/or jurisdictional law.			1258
13.	IF allowing tags for specific Record Entry deletion, THEN the system SHALL provide the ability to delete Entries according to scope of practice, organizational policy, and/or jurisdictional law.			1259
14.	IF allowing tags for specific Record Entry deletion, THEN the system SHALL provide the ability to render confirming notification that the destruction occurred according to scope of practice, organizational policy, and/or jurisdictional law.			1260
15.	The system MAY provide the ability to maintain Record Entries by undeleting the Record Entries according to scope of practice, organizational policy, and/or jurisdictional law.			1261
16.	The system MAY transmit record destruction date information along with existing data when transmitting Record Entries (or extracts) to another entity.			1262
17.	The system SHOULD manage health care information for organizations that have multiple facilities according to scope of practice, organizational policy, and/or jurisdictional law.			1263
18.	The system MAY tag and render patient information that has been not been previously presented to the clinician.			1264
19.	IF the system tags patient information from internal or external systems that has not been previously presented to the clinician, THEN the system MAY present a notification to that clinician in accordance with user role and according to scope of practice, organizational policy, and/or jurisdictional law.			1265
RI.1.2.2 Function	Manage Record Entries for Legal Hold			1266
	Statement: Manage/Preserve Record Entries for Legal Hold (Multiple instances) **Description:** Occurs when a set of Record Entries is designated to be held for legal purposes or proceedings. - Ensures preservation of a set of Record Entries for a designated time, held without alteration.			
1.	The system SHALL conform to function RI.1.1.23 (Place Record Entries on Legal Hold).			1267
2.	The system SHALL conform to function RI.1.1.24 (Release Record Entries from Legal Hold).			1268
3.	The system SHALL provide the ability to control access to data/records during legal hold, preventing un-auditable alteration or unauthorized use for preservation purposes.			1269
4.	The system SHALL provide the ability to maintain records beyond normal retention period according to scope of practice, organizational policy, and/or jurisdictional law.			1270
5.	The system SHOULD provide the ability to capture the reason for preserving records beyond the normal retention period.			1271
6.	The system SHOULD provide the ability to render a legal hold notice identifying who to contact for questions when a user attempts to alter a record on legal hold.			1272
7.	The system MAY provide the ability to render Record Entry content preserved for a legal hold by type, class or encounter (e.g., medical Record Entry or report, e-mail, metadata, etc.), conforming to function RI.1.1.13 (Extract Record Entry Content).			1273
RI.1.3 Function	Record States			1274
	Statement: Manage Record States **Description:** Record Entries may reside in various states that must be managed. An important underlying principle for managing record states is the need to retain Record Entries that have been viewed for patient care purposes even if the Entry has not been completed or attested. This principle has important legal impact because it provides an account of what the provider viewed and relied on for clinical decision-making. For example, if Record Entry content was available in pending state and a clinician used the information to make decisions, it is important to retain the pending version even after the final version was available. Determining if Record Entry content was used for patient care may be challenging. Access logs could provide a mechanism to determine if the information was used.			

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1.3.1 Function	Manage Record Pending State			1275
	Statement: Manage Record Entries during the various states of completion. **Description:** Record Entries may reside in various states that must be managed. An important underlying principle for managing record states is the need to retain Record Entries that have been viewed for patient care purposes even if it has not been completed or attested. This principle has important legal impact because it provides a record of what the provider relied on for clinical decision-making. For example, if a Record Entry was available in pending state and a clinician accessed the information to make decisions, it is important to retain the pending version even after the final version was available. Determining if the Record Entry was accessed for patient care may be challenging. Access logs should show if the information was accessed/viewed.			
	1. The system SHOULD provide the ability to manage the length of time a Record Entry can be in a pending or inactive state before being administratively closed.			1276
	2. The system MAY present a notification to the author or designate that a Record Entry will be administratively closed after a designated period of time.			1277
	3. The system MAY present pending Record Entries in accordance with the organization's business rules.			1278
	4. IF the system displays pending Record Entries, THEN the system SHALL tag and present that a Record Entry is pending or incomplete.			1279
	5. The system SHOULD provide the ability to update a Record Entry status to one of: - complete, - complete while retaining incomplete version of the Entry if viewed for patient care or used by the system, - mark as erroneous and retain if Entry used for patient care or by the system, or - discard if Entry never viewed for patient care purposes.			1280
	6. The system SHOULD provide the ability to manage administrative closure of a Record Entry after a period of inactivity according to scope of practice, organizational policy, and/or jurisdictional law.			1281
	7. The system SHALL capture a date/time stamp and identify the author each time a Record Entry is updated including when opened, when updated, with the signature event and when officially closed, conforming to function TI.2.1.1 (Record Entry Audit Triggers).			1282
RI.1.3.2 Function	Manage Record Entry Amended, Corrected and Augmented State			1283
	Statement: Manage Record Entries amended, corrected or augmented after finalization (or signature/attestation). **Description:** Clinicians need the ability to correct, amend or augment Record Entries once they have been completed. When an amendment, correction or augmentation has been made, principles for documentation practices require that the original documentation must be accessible, readable, and unobliterated. A user must have a clear indication that modifications have been made to an Record Entry. There is optionality in how a system may identify a Record Entry that has been corrected or amended -- a flag or indicator could be displayed, the text could be in a different font, etc. The original Record Entry is not required to be displayed, but can be linked or traced back. The original Record Entry and each successive amendment, correction or augmentation should be retained for the legally prescribed timeframe as defined by scope of practice, organizational policy, and/or jurisdictional law.			
	1. The system SHALL provide the ability to update a Record Entry for purposes of amendment, correction or augmentation, conforming to function RI.1.1.2 (Amend Record Entry Content).			1284
	2. The system SHALL provide the ability to tag a Record Entry as an amendment, a correction of erroneous information and the reason, or an augmentation to supplement content.			1285
	3. The system SHALL capture, maintain and render the corresponding date, time, and user specifying when and by whom a Record Entry was amended, corrected, or augmented, conforming to function RI.1.1.2.1 (Evidence of Record Entry Amendment Event).			1286
	4. The system SHALL present the current version and provide a link or clear direction for accessing previous version(s) of the Record Entry.			1287
	5. The system SHALL manage all versions of the Record Entry for the legal retention period, conforming to function RI.1.2.1 (Manage Record Entries).			1288

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
RI.1.3.3 Function	Manage Record Entry Succession and Version Control			1289
	Statement: Manage successive Record Entry versions over time. **Description:** The system must have a mechanism to handle versions and succession of Record Entries (such as a preliminary and final laboratory reports, amended or corrected documents). Versioning and succession management is based on Record Entry content, and/or status change over time. A version may be one of: 1) A completed and attested Record Entry; 2) A Record Entry completed and attested which has been modified one or more times; 3) A Record Entry that has been viewed for clinical decision-making purposes by an individual other than the author; 4) A Record Entry that has been captured in an incomplete state per organization business rules and updated over time (i.e., a preliminary laboratory test); 5) A Record Entry that electively, according to the author, must be preserved in the current state at a given point in time (i.e., History and Physical). Certain types of Record Entries are typically handled in versions, for example: - Laboratory results (preliminary and final) - Dictated reports - Work ups (over course of days) The prior version of Record Entries should be retained for the legally prescribed timeframe as defined by scope of practice, organizational policy, and jurisdictional law.			
	1. The system SHOULD provide the ability to manage Record Entries that become new versions when their state changes (e.g., augmented, amended, corrected, etc.).			1290
	2. The system SHALL provide the ability to update a Record Entry and save it as a new version.			1291
	3. The system SHALL capture, maintain and render the date, time and user for the original and each updated version of the Record Entry.			1292
	4. The system SHALL manage the succession of Record Entries in chronological version order.			1293
RI.1.3.4 Function	Manage Record Entry Retraction			1294
	Statement: Remove a record entry from view if it is deemed erroneous and cite the reason. **Description:** Record retraction is used to reverse changes that have been made to existing Record Entries. Once a Record Entry has been retracted, it is no longer visible in standard queries, though it remains accessible in PHR audit records, should evidence ever be required for legal or other exceptional circumstances. Canada Health Infoway provides the following definition for retraction: This mechanism allows an existing record to be "removed" from the PHR if it is deemed erroneous. It can also be used to reverse changes that have been made to an existing record. Once a record has been retracted, it is no longer visible in standard queries, though it remains accessible in PHR audit records should evidence ever be required for legal or other exceptional circumstances. After retracting an erroneous record, a user has the ability to resubmit a corrected record with no visible indication that there was ever a previous version. Retract generally has significant constraints upon its use because of the risks of removing data from a patient's record that might have been used by others in making decisions. The specifics will vary by jurisdiction, and potentially even by type of data. There are times that a PHR Record Entry is created then found to be erroneous, i.e., the record may belong to another individual. In these cases, it is necessary to remove that record from view (storing it in case it may be needed for litigation or investigation purposes, etc.). After retracting an erroneous record, a user has the ability to resubmit a corrected record with no visible indication that there was ever a previous version.			
	1. The system SHALL provide the ability to hide a Record Entry from view and retain it such that it is only visible upon specific request and with appropriate authorization.			1295
	2. The system SHOULD provide the ability to capture users who viewed a Record Entry prior to its retraction and notify them of the retraction.			1296
	3. The system SHOULD provide the ability to capture and retain the reason why a Record Entry was retracted.			1297
	4. The system SHALL conform to function RI.1.1.17 (Deprecate/Retract Record Entries).			1298
RI.1.4 Function	Record Completeness			1299
	Statement: Manage Record Completeness **Description:** The PHR-S must provide the ability for an organization to define minimum elements and timeframes for completion at the report level and at the record level. Provide a report that identifies completion and timeliness status by patient/ health record number or other specified parameters. Prior to disclosure for legal proceedings or other official purposes, an organization analyzes the health record for completeness. PHR systems must provide the ability to define a minimum set of content to be analyzed for timeliness and completeness and provide a report of the status.			
	1. The system SHALL provide the ability to manage timeframes for completion of specified Record Entry content according to organizational business rules.			1300
	2. The system SHOULD provide the ability to tag by patient/health record number the completeness status of specified Record Entry content noting identified deficiencies.			1301

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
3.	The system SHOULD provide the ability to render a report by patient/health record number indicating the completeness status of specified Record Entry content noting identified deficiencies.			1302
4.	The system SHOULD provide the ability to render a visual indicator denoting that the content of a specified Record Entry content is incomplete according to organizational business rules.			1303
5.	The system SHOULD provide the ability to render a reminder to clinicians for the completion of specified Record Entry content (at the data or report level) according to organizational business rules (e.g., complete attestation, complete a section).			1304
RI.2 Function	Record Synchronization			1305

Statement: Manage Record Synchronization

Description: A PHR-S may consist of a set of components or applications; each application manages a subset of the health information. Therefore it is important that, through various interoperability mechanisms, a PHR-S maintains all the relevant information regarding the health record in synchrony. For example, if a physician orders an MRI, a set of diagnostic images and a radiology report will be created. As a result, the patient demographic information, the order for MRI, the diagnostic images associated with the order, and the report associated with the study must all be synchronized in order for the clinicians to receive a synchronized view the complete record (with respect to time and geographic location).Date and time need to be consistent across the applications that are part of the PHR system.

Synchronization demonstrates a sequence and chain of events for reconstruction and is relevant during a legal proceeding. Maintenance of synchronization activities could be relevant during a legal proceeding.

Note: Standards exist for Consistent Date and Time.

1.	The system SHALL conform to function TI.5.1 (Application and Structured-Document Interchange Standards).			1306
2.	The system SHOULD conform to function TI.3 (Registry and Directory Services).			1307
3.	The system SHOULD provide the ability to link Record Entries to external information.			1308
4.	The system SHOULD store the location of each known Record Entry in order to enable authorized access to a complete logical health record if the PHR is distributed among several applications, services, or devices within the PHR-S.			1309
5.	The system SHALL provide the ability to manage date and time-related information between applications, components, services, systems, and devices.			1310
RI.3 Function	Record Archive and Restore			1311

Statement: Manage Record Archive and Restore

Description: PHR Record Entries must be transitioned over its lifecycle from online data structures to near-line or off-line data structures. The archive function performs this transition of Record Entries from an online, production PHR-S to offline storage for information that is not being purged/destroyed. The system must provide such archive and restore functions to extract and preserve indefinitely, Record Entries selected to be removed from the live production PHR-S database and retained.

Record Entries must be archived and restored in such a manner as to permit them to be returned to their original or similar information structures. Archived Record Entries must also include corresponding metadata to ensure logical and semantic consistency of the information for subsequent access upon restoration.

The archive function should provide both an automated, configurable capability as well as a user-invoked archival function to enable selected Record Entries to be preserved, or flagged for preservation.

In the first instance, rules are specified to enable the system to conduct archiving in an unattended fashion. This is often the case for periodic system maintenance requirements (e.g., nightly processing where archival, data summarization and possibly purging of information occurs). In the second instance the system should provide the ability to select Record Entries to be preserved for future reference and access, such as in the case where selected Entries need to be preserved and retained for litigation.

In restoring information, it may occur that Record Entries being restored are a subset of the Entries originally archived. For example, when all Record Entries for a patient encounter were archived and only a particular set of Record Entries related to a study or result are to be restored. The system may provide for such finer granularity of restoration.

Archiving and restoring of Record Entries must be performed in a timely fashion, consistent with the operational requirements of both PHR users and system and technology capabilities.

The system must enable compliance with records retention according to scope of practice, organizational policy or jurisdictional law.

1.	The system SHALL provide the ability to archive and restore Record Entries according to scope of practice, organizational policy, and/or jurisdictional law (e.g., to/from off-line or near-line media).			1312
2.	The system SHALL provide the ability for an authorized user to tag and untag Record Entries to be archived.			1313
3.	The system SHALL provide the ability to archive or restore metadata that is associated with Record Entries that have been archived or restored.			1314
4.	The system SHOULD provide the ability to enter a target destination when restoring Record Entries (e.g., original data location, temporary user storage, or a research/analysis database).			1315
5.	The system SHOULD provide the ability to tag Record Entries that will be retained or archived during the archival process.			1316
6.	The system SHOULD provide the ability to enter a schedule for archive and restore processing.			1317

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
7.	The system MAY provide the ability to restore selected portions of archived Record Entries.			1318
8.	The system SHALL provide the ability to manage (configure) archival parameters for Record Entries (e.g., what and when to archive).			1319

4. Trust Infrastructure Section

Section Overview

The Trust Infrastructure (TI) Section consists of functions common to a PHR System infrastructure, particularly those functions foundational to system operations, security, efficiency and data integrity assurance, safeguards for privacy and confidentiality, and interoperability with other systems. TI functions are core and foundational to all other functions of the Model (Care Provision, Care Provision Support, Population Health, Administrative Support and Record Infrastructure). Note extensive reference to TI functions in Overarching Criteria. TI functions may be implemented within the architecture of a single system or across a tightly coupled suite of systems (applications).All functions within the Trust Infrastructure Section have an identifier starting with “TI”. The RI and TI Sections are identical between the PHR and EHR System Functional Models, reflecting the need for common and compatible record management and trust infrastructures. Note that there may be some functions more directly applicable to EHR systems than PHR systems.

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
TI.1 Function	Security			1321
Statement: Manage PHR-S security. **Description:** PHR-S security consists of entity authentication, entity authorization, entity access control, patient access management, secure data exchange, attestation, patient privacy and confidentiality. PHR audit functions are described in TI.2 .				
TI.1.1 Function	Entity Authentication			1322
Statement: Authenticate PHR-S users, and/or entities before allowing access. **Description:** All entities accessing the PHR-S are subject to authentication. Examples of entity authentication, with varying levels of authentication rigor, include: - username/password; - digital certificate; - secure token; - biometrics.				
1. The system SHALL authenticate entities (e.g., users, organizations, applications, components, objects, and/or devices) accessing PHR-S protected resources (e.g., functions and data) according to scope of practice, organizational policy, and/or jurisdictional law, using an authentication mechanism such as an accredited Standards Development Organization-approved authentication standard (e.g., SAML, WS-Trust, Kerberos), username/password, digital certificate, secure token, biometric, or hardware-specific addressing mechanism. (See also ISO 22600.)				1323
2. The system SHALL manage authentication data/information securely (e.g., passwords or biometric data).				1324
3. The system SHALL maintain configurable conditions and rules which protect against invalid, possibly malicious, authentication attempts according to organizational policy, and/or jurisdictional law (e.g., consecutive invalid logon attempts).				1325
4. IF passwords are used to control access to the PHR-S, THEN the system SHALL provide the ability to maintain configurable timeframes (e.g., 180 days) for the reuse of passwords according to organizational policy, and/or jurisdictional law.				1326
5. IF passwords are used to control access to the PHR-S, THEN the system SHALL provide the ability to maintain a configurable limit on the reuse of recently used passwords (e.g., the last 5 passwords) according to organizational policy, and/or jurisdictional law.				1327
6. IF username/passwords are used to control access to the PHR-S, THEN the system SHALL maintain password strength rules (e.g., requiring a minimum number of characters and inclusion of alpha-numeric complexity).				1328
7. IF passwords are used to control access to the system, THEN the system SHALL capture the password using obfuscation techniques (e.g., during user password entry) according to scope of practice, organizational policy, and/or jurisdictional law.				1329
8. IF passwords are used to control access to the PHR-S, THEN the system SHALL manage password reset as an administrative function.				1330
9. IF user passwords are initially set or later reset by an administrator, THEN the system SHALL provide the ability to update password at the next successful logon.				1331
10. The system SHALL present limited feedback to the user during authentication.				1332
11. The system SHALL provide the ability to enter case-insensitive 'usernames' that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).				1333
12. IF passwords are used, THEN the system SHALL provide the ability to enter case-sensitive passwords that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).				1334

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
TI.1.2 Function	Entity Authorization			1335
	Statement: Manage set(s) of PHR-S access control permissions. **Description:** Entities are authorized to use components of a PHR-S in accordance with their scope of practice within local policy or legal jurisdiction. Authorization rules provide a proper framework for establishing access permissions and privileges for the use of a PHR system, based on user, role or context. A combination of these authorization categories may be applied to control access to PHR-S resources (i.e., functions or data), including at the operating system level. - User based authorization refers to the permissions granted to access PHR-S resources based on the identity of an entity (e.g., user or software component). - Role based authorization refers to the permissions granted to access PHR-S resources based on the role of an entity. Examples of roles include: an application or device (tele-monitor or robotic); or a nurse, dietitian, administrator, legal guardian, and auditor. - Context-based Authorization refers to the permissions granted to access PHR-S resources within a context, such as when a request occurs, explicit time, location, route of access, quality of authentication, work assignment, patient consents and authorization. See ISO 10181-3 Technical Framework for Access Control Standard. For example, a PHR-S might only allow supervising providers' context authorization to attest to entries proposed by residents under their supervision.			
	1. The system SHALL provide the ability to manage sets of access-control permissions granted to an entity (e.g., user, application, device) based on identity, role, and/or context according to scope of practice, organizational policy, and/or jurisdictional law.			1336
	2. The system SHALL conform to function TI.2 (Audit) to audit authorization actions as security events.			1337
	3. The system SHALL provide the ability to manage roles (e.g., clinician versus administrator) and contexts (e.g., legal requirements versus emergency situations) for authorization according to scope of practice, organizational policy, and/or jurisdictional law.			1338
	4. The system SHALL maintain a revision history of all entity record modifications.			1339
	5. The system MAY provide the ability to manage authorizations for the use of portable media in according to scope of practice, organizational policy, and/or jurisdictional law.			1340
TI.1.3 Function	Entity Access Control			1341
	Statement: Manage access to PHR-S resources. **Description:** To ensure access is controlled, a PHR-S must authenticate and check authorization of entities for appropriate operations.			
	1. The system SHALL conform to function TI.1.1 (Entity Authentication).			1342
	2. The system SHALL conform to function TI.1.2 (Entity Authorization).			1343
	3. The system SHALL provide the ability to manage system and data access rules for all PHR-S resources according to scope of practice, organizational policy, and/or jurisdictional law.			1344
	4. The system SHALL manage the enforcement of authorizations to access PHR-S resources.			1345
	5. The system SHALL control access to PHR-S resources after a configurable period of inactivity by terminating the session, or by initiating a session lock that remains in effect until the entity re-establishes access using appropriate identification and authentication procedures, according to organizational policy, and/or jurisdictional law.			1346
	8. The system SHOULD provide the ability to control-access to data, and/or functionality according to scope of practice, organizational policy, and/or jurisdictional law.			1355
	9. The system SHALL control-access to data, and/or functionality by using authentication mechanisms that comply with regulatory and policy guidelines (e.g.,by using a combination of Username and Password, Digital Certificates, Secure Tokens, and/or Biometrics).			1356
	10. The system MAY provide the ability to determine the identity of public health agencies for healthcare purposes through the use of internal, and/or external registry services or directories.			1357
	11. The system MAY provide the ability to determine the identity of healthcare resources (e.g., Meal Delivery services for home-based patients) and devices (e.g., wheelchairs) for resource management purposes through the use of internal, and/or external registry services or directories.			1358
TI.1.3.1 Function	Emergency Access Control			1347
	Statement: Manage emergency access to PHR-S resources. **Description:** The intent of Emergency Access Control is to mitigate the potential for impeding the provision of care in an emergency situation in accordance with organizational policy. For example, emergency access may include: - Single record entry (e.g., single laboratory results, single document, single view); - Single patient; - Single login session, multiple patients; - Site mode allowing simultaneous emergency access to all users. Logging of a user's activities should occur in the audit record/metadata. Reports of emergency access use for follow up are critical for compliance and monitoring.			

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
1.	The system SHALL provide the ability to capture emergency access (permission) rules according to scope of practice, organizational policy, and/or jurisdictional law.			1348
2.	The system MAY provide the ability to capture categories of emergency access criteria (e.g., 1) Single record entry such as single laboratory results, single document, single view; 2) Single patient; 3) Single login session, multiple patients; 4) Site mode allowing simultaneous emergency access to all users) according to scope of practice, organizational policy, and/or jurisdictional law.			1349
3.	The system SHALL manage emergency access by individual users based on criteria (e.g., defined rules and categories) according to organizational policy, and/or jurisdictional law.			1350
4.	The system SHALL provide the ability to maintain emergency access time limits according to scope of practice, organizational policy, and/or jurisdictional law.			1351
5.	The system MAY present periodic reminders to a system administrator to review user's emergency access privileges.			1352
6.	The system SHALL provide the ability to capture a reason for emergency access.			1353
7.	The system SHALL provide the ability to render an after action report for follow up of emergency access.			1354
TI.1.4 Function	Patient Access Management			1359
	Statement: Manage a patient's access to personal health information. **Description:** A healthcare delivery organization will be able to manage a patient's ability to view his or her PHR based on organization policy or jurisdictional law. Typically, a patient or their legal representative (e.g., guardian, surrogate) has the right to view his or her PHR.			
1.	IF organizational policy allows patient access to the PHR-S, THEN the system SHALL conform to function TI.1.3 (Entity Access Control).			1360
2.	IF organizational policy allows patient access to the PHR-S, THEN the system SHALL conform to function TI.1.2 (Entity Authorization).			1361
TI.1.5 Function	Non-Repudiation			1362
	Statement: Limit a PHR-S user's ability to deny (repudiate) data origination, transmission or receipt by that user. **Description:** A PHR-S allows data entry to a patient's electronic health record and it can be a sender or receiver of healthcare information. Non-repudiation is a way to guarantee that the source of the data/record cannot later deny that fact; and that the sender of a message cannot later deny having sent the message; and that the recipient cannot deny having received the message. Components of non-repudiation can include: - Digital signature, which serves as a unique identifier for an individual (much like a written signature); - Confirmation service, which utilizes a message transfer agent to create a digital receipt (providing confirmation that a message was sent, and/or received); - Timestamp, which proves that a document existed at a certain date and time; - The use of standardized timekeeping protocols (e.g., the Integrating the Healthcare Enterprise (IHE) Consistent Time Profile).			
1.	The system SHALL capture the identity of the entity taking the action according to scope of practice, organizational policy, and/or jurisdictional law.			1363
2.	The system SHALL capture time stamp of the initial entry, modification and exchange of data according to scope of practice, organizational policy, and/or jurisdictional law.			1364
3.	The system SHALL conform to function TI.2 (Audit) to prevent repudiation of data origination, transmission and receipt according to scope of practice, organizational policy, and/or jurisdictional law.			1365
4.	The system SHOULD conform to function RI.1.1.4 (Attest Record Entry Content) to ensure integrity of data and data exchange and thus prevent repudiation of data origination, transmission or receipt according to scope of practice, organizational policy, and/or jurisdictional law.			1366
TI.1.6 Function	Secure Data Exchange			1367
	Statement: Secure all modes of PHR data exchange. **Description:** Whenever an exchange of PHR information occurs, it requires appropriate security and privacy considerations, including data obfuscation as well as both destination and source authentication when necessary. For example, it may be necessary to encrypt data sent to remote or external destinations.			
1.	The system SHALL secure all modes of PHR data exchange.			1368
2.	The system SHALL conform to function TI.1.7 (Secure Data Routing).			1369
3.	The system SHOULD provide the ability to de-identify data.			1370
4.	The system SHALL encrypt and decrypt PHR data that is exchanged over a non-secure link.			1371
5.	IF encryption is used, THEN the system SHALL exchange data using recognized standards-based encryption mechanisms according to organizational policy, and/or jurisdictional law.			1372
6.	IF the PHR-S is the recipient of a secure data exchange, THEN the system SHOULD provide the ability to transmit an acknowledgment of the receipt of the data.			1373

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
7. The system SHALL provide the ability to determine static or dynamic addresses for known and authorized sources and destinations.				1374
TI.1.7 Function	Secure Data Routing			1375
Statement: Route electronically exchanged PHR data only to/from known and authenticated destinations/sources (according to applicable healthcare-specific rules and relevant standards). **Description:** A PHR-S needs to ensure that it is exchanging PHR information with the entities (applications, institutions, directories) it expects. This function depends on entity authorization and authentication to be available in the system. For example, a physician practice management application in a PHR-S might send claim attachment information to an external entity. To accomplish this, the application must use a secure routing method, which ensures that both the sender and receiving sides are authorized to engage in the information exchange. Known sources and destinations can be established in a static setup or they can be dynamically determined. Examples of a static setup are recordings of IP (Internet Protocol) addresses or recordings of DNS (Domain Name System) names. For dynamic determination of known sources and destinations, systems can use authentication mechanisms as described in TI.1. For example, the sending of a laboratory order from the PHR-S to a laboratory system within the same organization usually uses a simple static setup for routing. In contrast, sending a laboratory order to a reference laboratory outside of the organization will involve some kind of authentication process. Provision of a secure network infrastructure is beyond the scope of a PHR-S.				
1. The system SHALL conform to function TI.1.1 (Entity Authentication) to exchange PHR data only to and from known, authenticated sources and destinations.				1376
2. The system SHALL conform to function TI.2 (Audit) to capture audit information about changes to the status of sources and destinations.				1377
TI.1.8 Function	Patient Privacy and Confidentiality			1378
Statement: Enable the enforcement of the applicable jurisdictional and organizational patient privacy rules as they apply to various parts of a PHR-S through the implementation of security mechanisms. **Description:** Patients' privacy and the confidentiality of PHRs are violated if access to PHRs occurs without authorization. Violations or potential violations can impose tangible economic or social losses on affected patients, as well as less tangible feelings of vulnerability and pain. Fear of potential violations discourages patients from revealing sensitive personal information that may be relevant to diagnostic and treatment services. Rules for the protection of privacy and confidentiality may vary depending upon the vulnerability of patients and the sensitivity of records. Strongest protections should apply to the records of minors and the records of patients with stigmatized conditions. Authorization to access the most sensitive parts of a PHR is most definitive if made by the explicit and specific consent of the patient. Please see the definition of masking in the glossary. Organizational practices related to privacy and security jurisdictional laws could be called into question during a legal proceeding. Adherence to applicable laws supports the credibility and trustworthiness of the organization.				
1. The system SHALL provide the ability to maintain compliance with requirements for patient privacy and confidentiality according to scope of practice, organizational policy, and/or jurisdictional law (e.g., US HIPAA Privacy Rules, US Federal Conditions of Participation for Medicare/Medicaid Providers).				1379
2. The system SHALL conform to function TI.1.1 (Entity Authentication).				1380
3. The system SHALL conform to function TI.1.2 (Entity Authorization).				1381
4. The system SHALL conform to function TI.1.3 (Entity Access Control).				1382
5. The system SHALL conform to function TI.1.5 (Non-Repudiation).				1383
6. The system SHALL conform to function TI.1.6 (Secure Data Exchange).				1384
7. The system SHALL conform to function TI.2 (Audit).				1385
8. The system SHALL provide the ability to maintain varying levels of confidentiality according to patient preferences, user role, scope of practice, organizational policy, and/or jurisdictional law.				1386
9. The system SHALL provide the ability to mask parts of the electronic health record (e.g., medications, conditions, sensitive documents) from disclosure according to patient preferences, user role, scope of practice, organizational policy, and/or jurisdictional law.				1387
10. The system SHALL provide the ability to unmask (override a mask) in emergency or other specific situations in accordance with users' role, and according to scope of practice, organizational policy, and/or jurisdictional law.				1388
11. The system SHOULD provide the ability to maintain indicators (flags) to health record users that content has been masked in accordance with users' role, and according to scope of practice, organizational policy, and/or jurisdictional law.				1389
12. IF the system allows a user to unmask (override a mask) in an emergency or other specific situation, THEN the system SHALL provide the ability to capture the reason for unmasking or overriding the mask.				1390
13. The system SHALL provide the ability to manage patient consents to, or restrictions against, any access to data.				1391
14. The system SHALL provide the ability to manage a privacy policy according to patient preferences, user role, scope of practice, organizational policy, and/or jurisdictional law.				1392
15. The system SHALL provide the ability to control access by specified user(s) to a particular patient health record either by inclusion or exclusion according to patient preferences, user role, scope of practice, organizational policy, and/or jurisdictional law.				1393

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
TI.1.8.1 Function	Redact Patient Identifying Information			1394
	Statement: Maintain patient identities and conditions invisible to the public and other providers who do not have "need to know"# on public tracking screens. **Description:** A number of systems implement large tracking screens, common displays or dashboards to support workflows. In these applications, there is a need to create de-identified views for broadcast in common areas.			
	1. The system SHALL provide the ability to manage redaction of patient identities on publicly viewable status boards according to organizational policy, and/or jurisdictional law.			1395
TI.1.8.2 Function	Protect Individual Patient Identity			1396
	Statement: Flag patient identity as confidential to others. **Description:** Create a flag to indicate to all providers caring for the patient, as well as administrative staff who may receive phone calls from family members or others, the need to protect the identity of patients at risk of harm, or requesting similar anonymity. Despite best efforts of confidentiality, display should identify patients at particular risk of harm during stay (e.g., domestic violence).			
	1. The system SHALL provide the ability to maintain the designation of patients who require protection of their identity from others, including family, visitors, and non participating healthcare providers according to scope of practice, organizational policy, and/or jurisdictional law.			1397
TI.1.9 Function	System Operation Measurements			1398
	Statement: Manage the change of status of an external facility. **Description:** A health care delivery relies on services provided by other external facilities such as laboratories or Long Term Care facilities. The status of those facilities is subject to change for example: power outage, flooding or overcapacity. Therefore, the PHR system needs to capture the status of the external facilities, notify appropriate individuals / organizations or even change the workflow based on established business rules. Change of the status of an external facility is patient safety concern because a provider may need to adjust patient care or care workflows accordingly. For example, changes of status of external facility include: laboratory no longer accredited, laboratory power outage, Long Term Care facility at overcapacity. If laboratory loses accreditation an administrator needs to be notified to adjust the workflow. If status change is anticipated on regular basis, the system may automatically trigger workflow adjustment according to established business rule that take in consideration the status of the external facility. The example for later, the local Long Term Care facility may routinely exceed the capacity on the weekends; therefore, the business rule will accommodate for automatic workflow adjustments.			
	1. The system SHOULD provide the ability to manage the change of status of an external facility.			1399
TI.1.10 Function	Service Availability			1400
	Statement: Manage the ability to access, render and determine information related to Service Level Agreement. **Description:** A provider may need to be aware of certain Service Level Agreement information in order to mitigate patient safety-related risks that depend on system availability or system performance.			
	1. The system SHOULD provide the ability to manage Service Level Agreement information according to scope of practice, organizational policy, and/or jurisdictional law.			1401
	2. The system MAY provide the ability to render system availability statistics and system performance statistics as specified in the Service Level Agreement according to scope of practice, organizational policy, and/or jurisdictional law.			1402
TI.1.11 Function	Trusted Information Exchange Environment			1403
	Statement: Maintain a Trusted Information Exchange environment to enable common security measures among participants in the health information exchange. **Description:** A Trusted Information Exchange environment facilitates protected health information exchange by employing common user authentication across multiple systems, and/or organizations. A Trusted Information Exchange environment can help decrease risk and liability for participating members of the Trusted Information Exchange environment by ensuring that protected health information is consistently managed by all participants.			
	1. The system SHOULD provide the ability to manage applicable Trusted Information Exchange environment-related information according to scope of practice, organizational policy, and/or jurisdictional law. (See ISO 22600, 'Privilege Management and Access Control', Part 1, 'Overview and Policy Management'.)			1404

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
TI.2 Function	Audit			1405
	Statement: Audit Key Record, Security, System and Clinical Events **Description:** PHR Systems have built in audit triggers to capture key events in real-time, including events related to record management, security, system operations or performance or clinical situations. Event details, including key metadata (who, what, when, where), are captured in an Audit Log. Audit Review functions allow various methods of critical event notification as well as routine log review. Audit functions implement requirements according to scope of practice, organizational policy, and jurisdictional law.			
	1. The system SHALL conform to function TI.1.3 (Entity Access Control) to limit access to, or modification of, audit record information to appropriate entities according to scope of practice, organizational policy, and/or jurisdictional law.			1406
	2. The system SHALL conform to function TI.1.3 (Entity Access Control) to limit access to audit record information for purposes of deletion according to scope of practice, organizational policy, and/or jurisdictional law (e.g., limit access to only allow a specific system administrator to delete audit record information).			1407
TI.2.1 Function	Audit Triggers			1408
	Statement: Manage Audit Triggers **Description:** PHR Systems have built in audit triggers to capture key events in real-time. Audit triggers signal key: - Record management and lifecycle events; - Security events related to system and data safeguards, both routine and exceptional; - System events related to performance and operations, both routine and exceptional; - Clinical events with special log requirements.			
	1. The system SHALL audit key events, as specified in function TI.2.1 (Audit Triggers) and child functions, according to scope of practice, organizational policy, and/or jurisdictional law.			1409
	2. The system SHALL capture key Audit Metadata at each Audit Trigger, as specified in TI.2.1 (Audit Triggers) and child functions, according to scope of practice, organizational policy, and/or jurisdictional law.			1410
	3. The system SHALL capture an Audit Log Entry at each Audit Trigger as specified in TI.2.1 (Audit Triggers) according to scope of practice, organizational policy, and/or jurisdictional law.			1411
	4. The system SHALL capture the current master clock time to establish valid record date and time metadata.			1412
	5. The system MAY manage Audit Trigger logging using a common audit engine (e.g., using schema and transports such as specified in the Audit Log specification of IHE Audit Trails and Node Authentication (ATNA) Profile).			1413
TI.2.1.1 Function	Record Entry Audit Triggers			1414
	Statement: Manage Record Entry Audit Triggers **Description:** Record Entries are managed throughout their lifespan at various points in their lifecycle. Record Entry Audit Triggers are designed to capture Record Entry related events including key metadata (who, what, when, where, why). See Function RI.1 , Record Lifecycle.			
	1. The system SHALL conform to function RI.1 (Record Lifecycle) and its RI.1.x.1 Subsections to capture and maintain Record Entry Audit Metadata.			1415
	2. The system SHALL link an Audit Log Entry to each Record Entry according to scope of practice, organizational policy, and/or jurisdictional law.			1416
	3. The system SHALL harmonize Audit Log Entry Metadata and corresponding Record Entry Metadata to ensure they remain identical.			1417
TI.2.1.2 Function	Security Audit Triggers			1418
	Statement: Manage Security Audit Triggers **Description:** Security Audit Triggers are designed to capture security related events, both routine and exceptional, including key metadata (who, what, when, where, why).			
	1. The system SHALL provide the ability to enter the reason that access control functions are being overridden.			1419
	2. The system SHALL audit key events according to scope of practice, organizational policy, and/or jurisdictional law.			1420
	3. The system SHALL capture key Audit Metadata at each Audit Trigger according to scope of practice, organizational policy, and/or jurisdictional law.			1421
	4. The system SHALL capture an Audit Log Entry at each Audit Trigger according to scope of practice, organizational policy, and/or jurisdictional law.			1422

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
5. The system SHALL provide the ability to log system maintenance events for entry to, and exit from, the PHR system.				1423
6. The system MAY capture an Audit Log Entry at each Audit Trigger using a common audit engine, e.g., standards-based software.				1424
TI.2.1.2.1 Function	Security Event Security Audit Trigger			1425
Statement: Manage Audit Trigger initiated to track Security event. **Description:** Capture security events, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when security events are detected according to scope of practice, organizational policy, and/or jurisdictional law.				1426
2. The system SHALL capture identity of the organization.				1427
3. IF known, THEN the system SHALL capture identity of the user.				1428
4. The system SHALL capture identity of the system.				1429
5. The system SHALL capture the event initiating audit trigger.				1430
6. The system SHALL capture the date and time of the event initiating audit trigger.				1431
7. The system SHALL capture identity of the location (i.e., network address).				1432
8. The system MAY capture the rationale for the event initiating audit trigger.				1433
TI.2.1.2.2 Function	User Authentication to the System (Start user session) Security Audit Trigger			1434
Statement: Manage Audit Trigger initiated to track user authentication to the system (start user session). **Description:** Capture user authentication to the system (start user session), both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence of user authentication at logon (start session).				1435
2. The system SHALL capture identity of the organization.				1436
3. IF known, THEN the system SHALL capture identity of the user.				1437
4. The system SHALL capture identity of the system.				1438
5. The system SHALL capture the event initiating audit trigger.				1439
6. The system SHALL capture the date and time of the event initiating audit trigger.				1440
7. The system SHALL capture identity of the location (i.e., network address).				1441
8. The system SHALL capture the method of user authentication (e.g., user ID, password, biometrics, token, security question(s)).				1442
TI.2.1.2.3 Function	User Authentication (System Prompt for Password Change) Security Audit Trigger			1443
Statement: Manage Audit Trigger initiated to track user authentication (system prompt for password change). **Description:** Capture user authentication (system prompt for password change), both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence of user authentication when user is prompted to change password.				1444
2. The system SHALL capture identity of the organization.				1445
3. IF known, THEN the system SHALL capture identity of the user.				1446
4. The system SHALL capture the identity of the system.				1447
5. The system SHALL capture the event initiating audit trigger.				1448
6. The system SHALL capture the date and time of the event initiating audit trigger.				1449
7. The system SHALL capture identity of the location (i.e., network address).				1450
8. IF password change successful, THEN the system SHALL capture the new password.				1451
TI.2.1.2.4 Function	User Request to Change Password Security Audit Trigger			1452
Statement: Manage Audit Trigger initiated to track user request to change password. **Description:** Capture user request to change password, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence of user authentication when user requests password change.				1453
2. The system SHALL capture identity of the organization.				1454
3. IF known, THEN the system SHALL capture identity of the user.				1455
4. The system SHALL capture identity of the system.				1456
5. The system SHALL capture the event initiating audit trigger.				1457
6. The system SHALL capture the date and time of the event initiating audit trigger.				1458

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
7. The system SHALL capture identity of the location (i.e., network address).				1459
8. The system MAY capture the rationale for the event initiating audit trigger.				1460
9. IF password change successful, THEN the system SHALL capture the new password.				1461
TI.2.1.2.5 Function	User Log Out (End user session) Security Audit Trigger			1462
Statement: Manage Audit Trigger initiated to track user log out (end user session). **Description:** Capture user log out (end user session), both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence of user logout (end session).				1463
2. The system SHALL capture identity of the organization.				1464
3. IF known, THEN the system SHALL capture identity of the user.				1465
4. The system SHALL capture identity of the system.				1466
5. The system SHALL capture the event initiating audit trigger.				1467
6. The system SHALL capture the date and time of the event initiating audit trigger.				1468
7. The system SHALL capture identity of the location (i.e., network address).				1469
8. The system SHOULD capture how the session ended (e.g., user logout, timeout, loss of connection, administrator logout, system failure).				1470
TI.2.1.2.6 Function	User Access (Successful) Security Audit Trigger			1471
Statement: Manage Audit Trigger initiated to track user access (successful). **Description:** Capture user access (successful), both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when user access is successful.				1472
2. The system SHALL capture identity of the organization.				1473
3. IF known, THEN the system SHALL capture identity of the user.				1474
4. The system SHALL capture identity of the system.				1475
5. The system SHALL capture the event initiating audit trigger.				1476
6. The system SHALL capture the date and time of the event initiating audit trigger.				1477
7. The system SHALL capture identity of the location (i.e., network address).				1478
TI.2.1.2.7 Function	User Attempts to Access Data (Unsuccessful -- Access Denied) Security Audit Trigger			1479
Statement: Manage Audit Trigger initiated to track user attempts to access data (unsuccessful -- access denied). **Description:** Capture user attempts to access data (unsuccessful -- access denied), both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when user access is unsuccessful (denied).				1480
2. The system SHALL capture identity of the organization.				1481
3. IF known, THEN the system SHALL capture identity of the user.				1482
4. The system SHALL capture identity of the system.				1483
5. The system SHALL capture the event initiating audit trigger.				1484
6. The system SHALL capture the date and time of the event initiating audit trigger.				1485
7. The system SHALL capture identity of the location (i.e., network address).				1486
TI.2.1.2.8 Function	Extraordinary User Access (Break the Glass) Security Audit Trigger			1487
Statement: Manage Audit Trigger initiated to track extraordinary user access (break the glass). **Description:** Capture extraordinary user access (break the glass), both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when extraordinary access is successful (e.g., 'break the glass' scenario).				1488
2. The system SHALL capture identity of the organization.				1489
3. IF known, THEN the system SHALL capture identity of the user.				1490
4. The system SHALL capture identity of the system.				1491
5. The system SHALL capture the event initiating audit trigger.				1492
6. The system SHALL capture the date and time of the event initiating audit trigger.				1493
7. The system SHALL capture identity of the location (i.e., network address).				1494
8. The system SHALL capture the rationale for extraordinary user access.				1495

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
TI.2.1.2.9 Function	User Permissions (Authorization) Security Audit Trigger			1496
	Statement: Manage Audit Trigger initiated to track user permissions (authorization). **Description:** Capture user permissions (authorization), both routine and exceptional, including key metadata (who, what, when, where, why).			
1.	The system SHALL audit each occurrence when user permissions (authorizations) are granted, removed or updated.			1497
2.	The system SHALL capture identity of the organization.			1498
3.	IF known, THEN the system SHALL capture identity of the user.			1499
4.	The system SHALL capture identity of the system.			1500
5.	The system SHALL capture the event initiating audit trigger.			1501
6.	The system SHALL capture the date and time of the event initiating audit trigger.			1502
7.	The system SHALL capture identity of the location (i.e., network address).			1503
8.	The system SHOULD capture the rationale for granting, removing or updating user permissions.			1504
9.	The system SHALL capture identity of user to whom permissions apply.			1505
10.	The system SHALL capture the new set of applicable user permissions (authorizations).			1506
TI.2.1.3 Function	System Audit Triggers			1507
	Statement: Manage System Audit Triggers **Description:** System Audit Triggers are designed to capture system related events, both routine and exceptional, including key metadata (who, what, when, where, why).			
1.	The system SHOULD provide the ability to log system maintenance events for loading new versions of, or changes to, the clinical system.			1508
2.	The system SHOULD provide the ability to store system maintenance events for loading new versions of codes and knowledge bases.			1509
3.	The system SHOULD provide the ability to log system maintenance events for creating and restoring of backup.			1510
4.	The system SHOULD provide the ability to audit events in the case of detection of corrupt or dirty data.			1511
5.	The system SHALL provide the ability to audit the access and usage of systems, data, and organizational resources.			1512
6.	The system SHALL provide the ability to log system events at the hardware and software architecture level.			1513
7.	The system SHALL provide the ability to log system maintenance events for entry to, and exit from, the PHR system.			1514
8.	The system SHALL provide the ability to log system maintenance events for remote access connections including those for system support and maintenance activities for security and access purposes.			1515
TI.2.1.3.1 Function	System Event System Audit Trigger			1516
	Statement: Manage Audit Trigger initiated to track system events. **Description:** Capture system events, both routine and exceptional, including key metadata (who, what, when, where, why).			
1.	The system SHALL audit each occurrence when system events are detected according to scope of practice, organizational policy, and/or jurisdictional law.			1517
2.	The system SHALL capture identity of the organization.			1518
3.	IF known, THEN the system SHALL capture identity of the user.			1519
4.	The system SHALL capture identity of the system.			1520
5.	The system SHALL capture the event initiating audit trigger.			1521
6.	The system SHALL capture the date and time of the event initiating audit trigger.			1522
7.	The system SHALL capture identity of the location (i.e., network address).			1523
8.	The system MAY capture the rationale for the event initiating audit trigger.			1524
TI.2.1.3.2 Function	System Started System Audit Trigger			1525
	Statement: Manage Audit Trigger initiated to track system started event. **Description:** Capture system started event, both routine and exceptional, including key metadata (who, what, when, where, why).			
1.	The system SHALL audit each occurrence when system started.			1526
2.	The system SHALL capture identity of the organization.			1527
3.	IF known, THEN the system SHALL capture identity of the user.			1528

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
4. The system SHALL capture identity of the system.				1529
5. The system SHALL capture the event initiating audit trigger.				1530
6. The system SHALL capture the date and time of the event initiating audit trigger.				1531
7. The system SHALL capture identity of the location (i.e., network address).				1532
TI.2.1.3.3 Function	Back Up Started System Audit Trigger			1533
Statement: Manage Audit Trigger initiated to track back-up started event. **Description:** Capture back-up started event, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when database backup is initiated.				1534
2. The system SHALL capture identity of the organization.				1535
3. IF known, THEN the system SHALL capture identity of the user.				1536
4. The system SHALL capture identity of the system.				1537
5. The system SHALL capture the event initiating audit trigger.				1538
6. The system SHALL capture the date and time of the event initiating audit trigger.				1539
7. The system SHALL capture identity of the location (i.e., network address).				1540
TI.2.1.3.4 Function	Back Up Completed System Audit Trigger			1541
Statement: Manage Audit Trigger initiated to track back-up completed event. **Description:** Capture back-up completed event, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when database backup is completed.				1542
2. The system SHALL capture identity of the organization.				1543
3. IF known, THEN the system SHALL capture identity of the user.				1544
4. The system SHALL capture identity of the system.				1545
5. The system SHALL capture the event initiating audit trigger.				1546
6. The system SHALL capture the date and time of the event initiating audit trigger.				1547
7. The system SHALL capture identity of the location (i.e., network address).				1548
8. The system SHALL capture backup success or failure.				1549
TI.2.1.3.5 Function	Back Up Recovery Started System Audit Trigger			1550
Statement: Manage Audit Trigger initiated to track back-up recovery started event. **Description:** Capture back-up recovery started event, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when database recovery is initiated.				1551
2. The system SHALL capture identity of the organization.				1552
3. IF known, THEN the system SHALL capture identity of the user.				1553
4. The system SHALL capture identity of the system.				1554
5. The system SHALL capture the event initiating audit trigger.				1555
6. The system SHALL capture the date and time of the event initiating audit trigger.				1556
7. The system SHALL capture identity of the location (i.e., network address).				1557
TI.2.1.3.6 Function	Back Up Recovery Completed System Audit Trigger			1558
Statement: Manage Audit Trigger initiated to track back-up recovery completed event. **Description:** Capture back-up recovery completed event, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when database recovery is completed.				1559
2. The system SHALL capture identity of the organization.				1560
3. IF known, THEN the system SHALL capture identity of the user.				1561
4. The system SHALL capture identity of the system.				1562
5. The system SHALL capture the event initiating audit trigger.				1563
6. The system SHALL capture the date and time of the event initiating audit trigger.				1564
7. The system SHALL capture identity of the location (i.e., network address).				1565
8. The system SHALL capture backup recovery success or failure.				1566

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
TI.2.1.3.7 Function	Batch Job Started System Audit Trigger			1567
Statement: Manage Audit Trigger initiated to track batch job started event. **Description:** Capture system batch job started event, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when a batch job is initiated.				1568
2. The system SHALL capture identity of the organization.				1569
3. IF known, THEN the system SHALL capture identity of the user.				1570
4. The system SHALL capture identity of the system.				1571
5. The system SHALL capture the event initiating audit trigger.				1572
6. The system SHALL capture the date and time of the event initiating audit trigger.				1573
7. The system SHALL capture identity of the location (i.e., network address).				1574
TI.2.1.3.8 Function	Batch Job Completed System Audit Trigger			1575
Statement: Manage Audit Trigger initiated to track batch job completed event. **Description:** Capture batch job completed event, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when a batch job is completed.				1576
2. The system SHALL capture identity of the organization.				1577
3. IF known, THEN the system SHALL capture identity of the user.				1578
4. The system SHALL capture identity of the system.				1579
5. The system SHALL capture the event initiating audit trigger.				1580
6. The system SHALL capture the date and time of the event initiating audit trigger.				1581
7. The system SHALL capture identity of the location (i.e., network address).				1582
TI.2.1.3.9 Function	Maintenance Started System Audit Trigger			1583
Statement: Manage Audit Trigger initiated to track maintenance started event. **Description:** Capture maintenance started event, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when maintenance is initiated, including down time.				1584
2. The system SHALL capture identity of the organization.				1585
3. IF known, THEN the system SHALL capture identity of the user.				1586
4. The system SHALL capture identity of the system.				1587
5. The system SHALL capture the event initiating audit trigger.				1588
6. The system SHALL capture the date and time of the event initiating audit trigger.				1589
7. The system SHALL capture identity of the location (i.e., network address).				1590
TI.2.1.3.10 Function	Maintenance Completed System Audit Trigger			1591
Statement: Manage Audit Trigger initiated to track maintenance completed event. **Description:** Capture maintenance completed event, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence when maintenance is completed, including restart from down time.				1592
2. The system SHALL capture identity of the organization.				1593
3. IF known, THEN the system SHALL capture identity of the user.				1594
4. The system SHALL capture identity of the system.				1595
5. The system SHALL capture the event initiating audit trigger.				1596
6. The system SHALL capture the date and time of the event initiating audit trigger.				1597
7. The system SHALL capture identity of the location (i.e., network address).				1598
TI.2.1.3.11 Function	Resource Usage System Audit Trigger			1599
Statement: Manage Audit Trigger initiated to track resource usage event. **Description:** Capture resource usage event, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit usage of system resources (access, computational, storage, network) according to scope of practice, organizational policy, and/or jurisdictional law.				1600
2. The system SHALL capture identity of the organization.				1601
3. IF known, THEN the system SHALL capture identity of the user.				1602
4. The system SHALL capture identity of the system.				1603

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
5. The system SHALL capture the event initiating audit trigger.				1604
6. The system SHALL capture the date and time of the event initiating audit trigger.				1605
7. The system SHALL capture identity of the location (i.e., network address).				1606
TI.2.1.3.12 Function	System Maintenance Events -Local Access System Audit Trigger			1607
Statement: Manage Audit Trigger initiated to track system maintenance events -local access. **Description:** Capture system maintenance events -local access, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence of a system maintenance event with local access.				1608
2. The system SHALL capture identity of the organization.				1609
3. IF known, THEN the system SHALL capture identity of the user.				1610
4. The system SHALL capture identity of the system.				1611
5. The system SHALL capture the event initiating audit trigger.				1612
6. The system SHALL capture the date and time of the event initiating audit trigger.				1613
7. The system SHALL capture identity of the location (i.e., network address).				1614
TI.2.1.3.13 Function	System Maintenance Events - Remote Access System Audit Trigger			1615
Statement: Manage Audit Trigger initiated to track system maintenance events -remote access. **Description:** Capture system maintenance events -remote access, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence of a system maintenance event with remote access.				1616
2. The system SHALL capture identity of the organization.				1617
3. IF known, THEN the system SHALL capture identity of the user.				1618
4. The system SHALL capture identity of the system.				1619
5. The system SHALL capture the event initiating audit trigger.				1620
6. The system SHALL capture the date and time of the event initiating audit trigger.				1621
7. The system SHALL capture identity of the location (i.e., network address).				1622
TI.2.1.3.14 Function	System Maintenance - PHR or Clinical Software System Audit Trigger			1623
Statement: Manage Audit Trigger initiated to track system maintenance - PHR or clinical software. **Description:** Capture system maintenance - PHR or clinical software, both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence of a system maintenance event when PHR or clinical software is updated or re-configured.				1624
2. The system SHALL capture identity of the organization.				1625
3. IF known, THEN the system SHALL capture identity of the user.				1626
4. The system SHALL capture identity of the system.				1627
5. The system SHALL capture the event initiating audit trigger.				1628
6. The system SHALL capture the date and time of the event initiating audit trigger.				1629
7. The system SHALL capture identity of the location (i.e., network address).				1630
TI.2.1.3.15 Function	System Maintenance - Codes, Vocabulary, Knowledge, Rules System Audit Trigger			1631
Statement: Manage Audit Trigger initiated to track system maintenance of codes, vocabulary, knowledge and rules. **Description:** Capture system maintenance of codes, vocabulary, knowledge and rules - both routine and exceptional, including key metadata (who, what, when, where, why).				
1. The system SHALL audit each occurrence of a system maintenance event when codes, classification schemes, knowledge bases, clinical or business practice rules are updated or re-configured.				1632
2. The system SHALL capture identity of the organization.				1633
3. IF known, THEN the system SHALL capture identity of the user.				1634
4. The system SHALL capture identity of the system.				1635
5. The system SHALL capture the event initiating audit trigger.				1636
6. The system SHALL capture the date and time of the event initiating audit trigger.				1637
7. The system SHALL capture identity of the location (i.e., network address).				1638

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
TI.2.1.3.16 Function	Data Corruption System Audit Trigger			1639
	Statement: Manage Audit Trigger initiated to track data corruption events. **Description:** Capture data corruption event, including key metadata (who, what, when, where, why).			
	1. The system SHALL audit each occurrence or detection of data corruption.			1640
	2. The system SHALL capture identity of the organization.			1641
	3. IF known, THEN the system SHALL capture identity of the user.			1642
	4. The system SHALL capture identity of the system.			1643
	5. The system SHALL capture the event initiating audit trigger.			1644
	6. The system SHALL capture the date and time of the event initiating audit trigger.			1645
	7. The system SHALL capture identity of the location (i.e., network address).			1646
TI.2.1.4 Function	Clinical Audit Triggers			1647
	Statement: Manage Clinical Audit Triggers **Description:** Clinical Audit Triggers are designed to capture certain clinical events, both routine and exceptional, including key metadata (who, what, when, where, why).			
	1. The system SHALL provide the ability to track all clinical alerts.			1648
	2. The system SHALL provide the ability to track all acknowledgements of clinically-significant report changes.			1649
	3. The system SHOULD provide the ability to track when decision support alerts have been disabled.			1650
TI.2.1.4.1 Function	Clinical Alerts Clinical Audit Trigger			1651
	Statement: Manage Audit Trigger initiated to track clinical alerts. **Description:** Capture clinical alerts, both routine and exceptional, including key metadata (who, what, when, where, why).			
	1. The system SHALL audit each occurrence of a clinical alert according to scope of practice, organizational policy, and/or jurisdictional law.			1652
	2. The system SHALL capture identity of the organization.			1653
	3. IF known, THEN the system SHALL capture identity of the user.			1654
	4. The system SHALL capture identity of the system.			1655
	5. The system SHALL capture the event initiating audit trigger.			1656
	6. The system SHALL capture the date and time of the event initiating audit trigger.			1657
	7. The system SHALL capture identity of the location (i.e., network address).			1658
	8. The system SHOULD capture the rationale for the clinical alert.			1659
TI.2.1.4.2 Function	Acknowledgements of Clinically Significant Report Changes Clinical Audit Trigger			1660
	Statement: Manage Audit Trigger initiated to track acknowledgement of clinically significant report changes. **Description:** Capture acknowledgement of clinically significant report changes, both routine and exceptional, including key metadata (who, what, when, where, why).			
	1. The system SHALL audit each occurrence of an acknowledgement of clinically significant report changes according to scope of practice, organizational policy, and/or jurisdictional law.			1661
	2. The system SHALL capture identity of the organization.			1662
	3. IF known, THEN the system SHALL capture identity of the user.			1663
	4. The system SHALL capture identity of the system.			1664
	5. The system SHALL capture the event initiating audit trigger.			1665
	6. The system SHALL capture the date and time of the event initiating audit trigger.			1666
	7. The system SHALL capture identity of the location (i.e., network address).			1667
	8. The system SHOULD capture the rationale for significant report changes.			1668
TI.2.1.4.3 Function	Disable Decision Support Alerts Clinical Audit Trigger			1669
	Statement: Manage Audit Trigger initiated to track disabling of decision support alerts. **Description:** Capture disabling of decision support alerts, both routine and exceptional, including key metadata (who, what, when, where, why).			
	1. The system SHALL audit each occurrence when decision support alerts are disabled according to scope of practice, organizational policy, and/or jurisdictional law.			1670
	2. The system SHALL capture identity of the organization.			1671
	3. IF known, THEN the system SHALL capture identity of the user.			1672

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
4. The system SHALL capture identity of the system.				1673
5. The system SHALL capture the event initiating audit trigger.				1674
6. The system SHALL capture the date and time of the event initiating audit trigger.				1675
7. The system SHALL capture identity of the location (i.e., network address).				1676
8. The system SHALL capture the rationale for disabling clinical alerts.				1677
TI.2.2 Function	Audit Log Management			1678
Statement: Manage Audit Log **Description:** Audit Triggers create Audit Log entries. Audit Log entries are typically managed as persistent evidence of events occurring over time, including events pertaining to record management, security, system operations and performance, key clinical situations. Audit log entries capture event details, including key metadata (who, what, when, where).Audit log functions fulfill log maintenance and persistence requirements according to scope of practice, organizational policy, and jurisdictional law.				
1. The system SHALL provide the ability to capture audit log entries using a standards-based audit record format according to scope of practice, organizational policy, and/or jurisdictional law (e.g., IETF RFC 3881 'Internet Engineering Task Force, Request For Comment, Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications').				1679
2. The system SHOULD provide the ability to annotate or tag previously recorded audit log entries.				1680
3. The system SHOULD provide the ability to store audit log entry metadata (including related metadata). NOTE: Audit log entry metadata and related metadata ought to be stored in a secure fashion.				1681
4. The system SHALL provide the ability to log access to audit log entries, and/or metadata.				1682
TI.2.2.1 Function	Audit Log Indelibility			1683
Statement: Manage Audit Log Indelibility **Description:** Audit logs must be maintained in a persistent and indelible form according to scope of practice, organizational policy, and jurisdictional law.				
1. The system SHALL manage each Audit Log entry as a persistent, indelible (unalterable) data object including all metadata.				1684
TI.2.3 Function	Audit Notification and Review			1685
Statement: Notify of Audit Events, Review Audit Log **Description:** PHR system functions allow various methods of critical event notification (from audit triggers) as well as routine log review. Audit log notification and review functions implement requirements according to scope of practice, organizational policy, and jurisdictional law.				
1. The system SHALL provide the ability to render a report based on audit log entries.				1686
2. The system SHALL provide the ability to render reports based on ranges of system date and time that audit log entries were captured.				1687
3. The system SHOULD provide the ability to render audit log entry time stamps using UTC (based on ISO 8601).				1688
4. The system SHALL provide the ability to authorize emergency access to certain logs based on criteria such as individual work assignment, specific user role, specific reason(s), or a need to access a specific patient's information/record entries according to organizational policy and/or jurisdictional law.				1689
TI.3 Function	Registry and Directory Services			1690
Statement: Enable the use of registry services and directories to uniquely identify, locate and supply links for retrieval of information related to: - patients and providers for healthcare purposes; - payers, health plans, sponsors, and employers for administrative and financial purposes; - public health agencies for healthcare purposes, and- healthcare resources and devices for resource management purposes. **Description:** Registry and directory service functions are critical to successfully managing the security, interoperability, and the consistency of the health record data across a PHR-S. These services enable the linking of relevant information across multiple information sources within, or external to, a PHR-S for use within an application. This applies to directories/registries internal to the PHR-S as well as directories/registries external to the PHR-S. Transmission may occur automatically or manually and may include small or large amounts of data. Directories and registries support communication between PHR Systems and may be organized hierarchically or in a federated fashion. For example, a patient being treated by a primary care physician for a chronic condition may become ill while out of town. The new provider's PHR-S interrogates a local, regional, or national registry to find the patient's previous records. From the primary care record, a remote PHR-S retrieves relevant information in conformance with applicable patient privacy and confidentiality rules. An example of local registry usage is a PHR-S application sending a query message to the Hospital Information System to retrieve a patient's demographic data.				
1. The system SHALL provide the ability to manage internal registry services and directories.				1691

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
2.	The system SHALL provide the ability to exchange information with external registry services and directories.			1692
3.	The system SHALL provide the ability to exchange information securely with external registry services and directories.			1693
4.	The system SHALL conform to function TI.5.1 (Application and Structured-Document Interchange Standards) to exchange information with external registry services and directories.			1694
5.	The system SHOULD capture and render local registry services and directory information through standards-based interfaces.			1695
6.	IF the system communicates with external registry services and directories (i.e., external to a PHR-S), THEN the system SHOULD capture and render information using standards-based interfaces.			1696
7.	The system SHOULD provide the ability to determine the unique identity of a patient through the use of internal, and/or external registry services or directories.			1697
8.	The system MAY provide the ability to determine links to healthcare information regarding a patient through the use of internal, and/or external registry services or directories.			1698
9.	The system MAY provide the ability to determine the unique identity of a provider through the use of internal, and/or external registry services or directories.			1699
10.	The system MAY provide the ability to determine the identity of payers, health plans and sponsors for administrative or financial purposes through the use of internal, and/or external registry services or directories.			1700
11.	The system MAY provide the ability to determine the identity of employers for administrative or financial purposes through the use of internal, and/or external registry services or directories.			1701
TI.4 Function	Standard Terminology and Terminology Services			1702

Statement: Support semantic interoperability through the use of standard terminologies, standard terminology models and standard terminology services.

Description: The purpose of supporting terminology standards and services is to enable semantic interoperability. Interoperability is demonstrated by the consistency of human and machine interpretation of shared data and reports. It includes the capture and support of consistent data for templates and decision support logic.

Terminology standards pertain to concepts, representations, synonyms, relationships and computable (machine-readable) definitions. Terminology services provide a common way for managing and retrieving these items, including historically correct version interpretation. Terminology services need to support legal requirements for retrospective health record information and system data.

TI.4.1 Function	Standard Terminology and Terminology Models			1703

Statement: Employ approved standard terminologies to ensure data correctness and to enable semantic interoperability (both within an enterprise and externally).Support a formal standard terminology model.

Description: Semantic interoperability requires standard terminologies combined with a formal standard information model. An example of an information model is the HL7 Reference Information Model. Another example is the ISO/EN 13606 Electronic Health Record Communication.

A terminology provides semantic and computable identity to its concepts. Examples of terminologies that a PHR-S may support include: LOINC, SNOMED, ICD-9, ICD-10, and CPT-4.Terminologies are use-case dependent and may or may not be realm dependent. The key is that the standard be approved by all stakeholders. For example, terminologies for public health interoperability may differ from those for healthcare quality, administrative reporting, research, etc.

Formal standard terminology models enable common semantic representations by describing relationships that exist between concepts within a terminology or in different terminologies, such as exemplified in the model descriptions contained in the HL7 Common Terminology Services specification.

The clinical use of standard terminologies is greatly enhanced with the ability to perform hierarchical inference searches across coded concepts. Hierarchical Inference enables searches to be conducted across sets of coded concepts stored in a PHR-S. Relationships between concepts in the terminology are used in the search to recognize child concepts of a common parent. For example, there may be a parent concept, 'penicillin containing preparations' which has numerous child concepts, each of which represents a preparation containing a specific form of penicillin (Penicillin V, Penicillin G, etc.). Therefore, a search may be conducted to find all patients taking any form of penicillin preparation.

Clinical and other terminologies may be provided through a terminology service internal or external to a PHR-S.

1.	The system SHALL determine that clinical terms and coded clinical data exist in an approved standard terminology.			1704
2.	The system SHOULD provide the ability to receive and transmit healthcare data using formal standard information models and approved standard terminologies according to scope of practice, organizational policy, and/or jurisdictional law.			1705
3.	The system SHOULD provide the ability to manage data using a formal standard terminology model according to scope of practice, organizational policy, and/or jurisdictional law.			1706
4.	The system SHOULD provide the ability to determine hierarchical inferences (e.g., subsumption across coded terminology concepts that are expressed using standard terminology models).			1707

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
5.	The system SHALL provide the ability to manage terminology assets and supporting tools (internal or external to the PHR-S).			1708
6.	IF there is no recognized-standard terminology model available, THEN the system MAY provide the ability to manage data using a locally-defined standard terminology model.			1709
7.	The system SHOULD provide the ability to capture information into structured data formats using approved standard terminologies without the user requiring knowledge of the terminologies used.			1710
8.	The system SHOULD provide the ability to enter data using content that is common to the user, and allow for collection and presentation of text form data to meet the pre-determined purposes of others. Text forms should exclude cryptic or uncommon abbreviations.			1711
9.	The system SHOULD provide the ability to present standard terminology terms in a language which is appropriate for the user.			1712
10.	The system SHALL provide the ability to exchange data with other systems (internal or external to the PHR-S) using approved standard terminologies.			1713
TI.4.2 Function	Maintenance and Versioning of Standard Terminologies			1714

Statement: Enable version control according to scope of practice, organizational policy, and/or jurisdictional law to ensure maintenance of utilized standard terminologies. This includes the ability to accommodate changes to terminology sets as the source terminology undergoes its natural update process (new codes, retired codes, redirected codes). Such changes need to be cascaded to clinical content embedded in templates, custom formularies, etc., as determined by existing policy.

Description: Version control allows for multiple sets or versions of the same terminology to exist and be distinctly recognized over time. Standard terminologies are usually periodically updated, and concurrent use of different versions may be required. Ideally, the meaning of a concept never changes over time, but a concept can be deprecated, and replaced with a new concept in a new version. However, in some terminologies, the meaning of a concept can change over time. In any case, it is important that retrospective analysis and research maintains the ability to relate to the appropriate conceptual meaning. If the terminology encoding for a concept changes over time, it is also important that for legal health records, as well as for retrospective analysis and research, the different encodings can be correlated to ensure the permanence of the concept as originally captured. This does not necessarily imply that complete older versions of the terminology be kept in the PHR-S, only access to the changes needs to be maintained.

1.	The system SHALL provide the ability to manage data using different versions of standard terminologies.			1715
2.	The system SHALL provide the ability to update standard terminologies.			1716
3.	The system SHOULD maintain relationships among versions of a standard terminology to allow preservation of interpretation over time.			1717
4.	The system SHOULD provide the ability to receive and harmonize data from and transmit data to other systems that use known different versions of a terminology standard while preserving the meaning of that data.			1718
5.	The system SHALL provide the ability to update terminologies to a deprecated status.			1719
6.	The system SHALL provide the ability to update individual codes within a terminology to a deprecated status.			1720
7.	The system SHALL provide the ability to update terms with their equivalent when terminology is changed, where coded terminology content is embedded in clinical models (e.g., templates and custom formularies), when the terminology changes can be accomplished unambiguously, and if consistent with scope of practice, organizational policy, and/or jurisdictional law.			1721
8.	The system SHALL provide the ability to update standard terminologies used to enter clinical content (via templates, custom formularies, etc.)			1722
9.	The system SHALL maintain an audit log or a change history of code system to the individual code level, for versions used, dates implemented and updated to enable correct interpretation of historical data over time.			1723
TI.4.3 Function	Terminology Mapping			1724

Statement: Map or translate one terminology to another as needed by local, regional, national, or international interoperability requirements.

Description: The ability to map or translate one terminology to another is fundamental to an organization in an environment where several terminologies are in play to meet different purposes. It is a common occurrence that data is captured using one terminology, but is shared using another terminology.

Example: Within a healthcare organization there may be a need to map terminology concepts with the same semantic meaning to meet different purposes (e.g., between a PHR-S and an external laboratory system, or between a PHR-S and a billing system). Standard terminologies are evolving and maps will need to be adjusted to support this evolution and more sophisticated use of standard terminologies and maps over time.

Realm specific (including local, regional, national or international) interoperability requirements can also determine the need for terminology mapping, and in many cases terminology mapping services (internal or external) can be used to satisfy these requirements.

The interaction and mapping of terminologies may be called into question in a legal proceeding, when clinical decisions were documented or when semantic meaning could be misinterpreted. It is important to seek guidance, document and retain all mapping decisions for all types of terminology mapping, and to recognize when mapping may not be possible from one concept to another. The quality of mapping is dependent upon the skills and interpretation of standard terminologies and clinical information by mapping experts.

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
1. The system SHALL provide the ability to manage data using terminology maps which may be provided by terminology mapping services (internal or external).				1725
2. The system SHOULD provide the ability to update terminology maps using standard terminology services (internal or external).				1726
3. The system SHOULD provide the ability to render data quality and technical quality reports for a user to determine the validity of terminology mappings using approved mapping techniques.				1727
4. The system MAY provide the ability for a user to maintain custom terminology maps using approved mapping techniques where formal standard terminology maps are unavailable.				1728
5. The system MAY provide the ability for a user to maintain custom terminology maps to formal standard terminology maps in order to support historical data use.				1729
TI.5 Function	Standards-Based Interoperability			1730

Statement: Provide automated health care delivery processes and seamless exchange of clinical, administrative, and financial information through standards-based solutions.

Description: Interoperability standards enable certain applications to be shared among PHR systems, resulting in a unified (logical) view of a given PHR system where several disparate systems may actually be participating transparently. Interoperability standards also enable certain information to be shared among PHR systems (including information that resides in regional, national, or international information exchanges). Interoperability standards also promote timely and efficient information capture, use, and re-use, often reducing the cumulative workload of the broad set of stakeholders.

When health-related information is exchanged -- or when external applications are used to extend a PHR system -- the interoperability methods and underlying standards that were used in the process may need to be disclosed during a legal proceeding (especially when the resulting information becomes part of the patient's medical record).

TI.5.1 Function	Application, Structured-Message, and Structured-Document Interchange Standards			1731

Statement: Support a PHR system's ability to operate seamlessly with systems that adhere to recognized application interchange standards. These systems include other PHR systems, subcomponents of a PHR system, or other (authorized, non-PHR) systems.

Description: Since a health care organization typically has various external and internal interoperability requirements, it must use a set of corresponding interoperability or interchange standards that will meet its connectivity and information structure, format, and semantic requirements. Information should be exchanged -- and applications should provide functionality -- in a manner that appears to be seamless to the user. To be specific, if data is received from an external source that requires a user to manually copy-and-paste that data into multiple parts of the system, the exchange is not considered to be 'seamless'.

Examples of standards-based PHR information content and exchange methods include: standards-based data extracts, standards-based messages, standards-based documents (e.g., HL7 Clinical Document Architecture (CDA) documents), standards-based healthcare transactions, and standards-based images (e.g., Digital Imaging and Communication in Medicine (DICOM) documents).

Support for multiple interaction modes is needed to respond to differing levels of immediacy and types of exchange. For example, messaging is effective for many near-real time, asynchronous data exchange scenarios but may not be appropriate if the end-user is requesting an immediate response from a remote application.

A variety of interaction modes are typically supported such as:

- Unsolicited Notifications (e.g., Adam Everyman has arrived at the clinic for his scheduled appointment);
- Query/Response (e.g., Query: Is Adam Everyman known to the system? Response: Yes, Adam's medical record number is 12345678);
- Service Request and Response (e.g., Request: Laboratory Order for "Fasting Blood Sugar". Response: the results of the test);
- Information Interchange between organizations (e.g., in a regional health exchange or in a national health system);
- Structured/discrete clinical documents (e.g., a structured clinical note);
- Unstructured clinical document (e.g., dictated surgical note).

Standard terminology is a fundamental part of interoperability and is described in function TI.4 . Using a formal explicit information model further optimizes interoperability. An example of an information model is the HL7 Reference Information Model (RIM). Organizations typically need to deal with more than one information model and may need to develop a mapping between information models, a meta-model (that helps to explain and organize the various information models), or both.

TI.5.1.1 Function	Application Interchange Standards			1732

Statement: Support the ability to operate seamlessly with other systems by using applications, and/or structured messages and documents that adhere to interchange standards.

Description: Placeholder - Not Defined at this time

1. The system SHALL provide the ability to receive and transmit information using interchange standards as required by realm / local -specific profiles, and/or by recognized jurisdictional authorities.				1733
2. The system SHALL provide the ability to integrate with the operations of other systems that adhere to interchange standards as required by realm / local -specific authorities and/or by recognized jurisdictional authorities.				1734

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
3.	The system SHALL conform to function TI.4 (Standard Terminology and Terminology Services) including all child-functions, to support terminology standards according to scope of practice, organizational policy, and/or jurisdictional law.			1735
4.	IF a standard information model is not available, THEN the system SHOULD provide the ability to exchange information with other systems in a seamless manner by using a formal explicit information model.			1736
5.	The system MAY provide the ability to exchange information with other systems by using an explicit formal information model, and/or by using a standard coded terminology.			1737
6.	The system SHALL provide the ability to receive and transmit data using standard, coded terminology.			1738
7.	The system SHOULD provide the ability to export data using an explicit and formal information model in accordance with industry and governmental-mandated standards.			1739
8.	The system SHOULD provide the ability to import data using an explicit and formal information model in accordance with industry and governmental-mandated standards.			1740
9.	The system SHOULD provide the ability to harmonize data with another system.			1741
10.	The system SHOULD provide the ability to determine whether the information transmitted to another system has been successfully received by that other system.			1742
11.	The system SHALL store a log record of each data exchange (transaction) when transmitting information with external systems.			1743
TI.5.1.2 Function	Structured-Document Interchange Standards			1744
	Statement: Support the management of structured documents. **Description:** Structured documents are an important method of facilitating the exchange of information to support care. Documents are often considered to be more permanent in nature; messages are often considered to be more transitory in nature. Examples of structured documents include: a referral from a primary care physician to a specialist; a medical summary; a discharge instruction for the patient.			
1.	The system SHALL provide the ability to exchange structured documents according to scope of practice, organizational policy, and/or jurisdictional law.			1745
TI.5.1.3 Function	Structured-Message Interchange Standards			1746
	Statement: Support the management of structured messages. **Description:** Structured messages are an important method of facilitating the exchange of information to support care. Messages are often considered to be more transitory in nature; documents are often considered to be more permanent in nature.			
1.	The system SHALL provide the ability to manage structured messages according to scope of practice, organizational policy, and/or jurisdictional law.			1747
TI.5.2 Function	Interchange Standards Versioning and Maintenance			1748
	Statement: Support various versions of an interchange standard. **Description:** Interchange standards characteristically change throughout their lifecycles; those changes are often tagged with 'version' numbers. PHR systems need to control the various versions of interchange standards that are used within a PHR implementation and accommodate changes that arise with each version. For example, if an organization migrates to version 2.5 of HL7's messaging standard, it may choose to utilize that version's specimen or blood bank information capabilities. The organization may also find that certain fields have been retained for backwards compatibility only or withdrawn altogether. The PHR-S needs to be able to handle all of these possibilities. Standards typically evolve in such a way as to protect backwards compatibility. On the other hand, sometimes there is little, or no, backwards compatibility when an organization may need to replace an entire standard with a new methodology. An example of this is migrating from HL7 v2 to HL7 v3. Interchange standards that are backward compatible support exchange among senders and receivers who are using different versions. Version control ensures that those sending information in a later version of a standard consider the difference in information content that can be interchanged effectively with receivers, who are capable of processing only earlier versions. That is, senders need to be aware of the information that receivers are unable to capture and adjust their business processes accordingly. Version control enables multiple versions of the same interchange standard to exist and be distinctly recognized over time. Since interchange standards are usually periodically updated, concurrent use of different versions may be required. Large (and/or federated) organizations typically need to use different versions of an interchange standard to meet internal organizational interoperability requirements. For example, the enterprise-wide standard might use HL7 v2.5 for laboratory messages, but some regions of the enterprise might be at a lower level. It should be possible to retire deprecated interchange standards versions when applicable business cycles are completed while maintaining obsolete versions. An example use of this is for possible claims adjustment throughout the claim's life cycle. When interchange standards change over time, it is important that retrospective analysis and research correlate and note gaps between the different versions' information structures to support the permanence of concepts over time.			

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
1.	The system SHALL provide the ability to exchange information with other systems that use different versions of interchange standards.			1749
2.	The system SHALL provide the ability to exchange information based on updated (or reconfigured) interchange standards and/or based on updated business needs.			1750
3.	The system SHOULD provide the ability to tag an interchange standard as being deprecated.			1751
4.	The system SHOULD provide the ability to integrate with other systems that use previously-supported versions of an interoperability standard according to scope of practice, organizational policy, and/or jurisdictional law.			1752
TI.5.3 Function	Standards-Based Application Integration			1753

Statement: Integrate applications in a standards-based manner.

Description: A PHR-S often consists of multiple applications. Some of those applications may be within the PHR-S; others may be external to the PHR-S. The user of the PHR-S often benefits when those applications are integrated. Application integration can be accomplished in an ad-hoc fashion or in a standards-based fashion.

The method(s) by which applications may be integrated within an organization depends on that organization's approach to application integration. A given organization could conceivably employ multiple application integration approaches to meet various application integration requirements.

1.	The system SHALL provide the ability to integrate applications in a standards-based fashion when the system is composed of, and/or is extended by disparate applications.			1754
2.	The system SHOULD provide the ability to integrate user (or system) authentication for the purposes application context management (e.g., Graphical User Interface application integration via HL7's Context Management Standard from the Clinical Context Object Work Group (CCOW)).			1755
TI.5.4 Function	Interchange Agreements			1756

Statement: Support the use of Interchange Agreements to specify the rules, responsibilities, expectations, and methods by which Interchange Agreement partners may exchange information.

Description: Systems that wish to communicate with each other must agree on certain parameters/criteria that will govern an information exchange process. Interchange agreements enable partnering systems to discover, negotiate, and utilize those parameters/criteria. A PHR-S can use this information to define how data will be exchanged between the sending and the receiving partners. Interchange services and capabilities can be discovered in an automated fashion.

Entity directories can be used to determine the address, profile, and data exchange requirements of known, and/or potential Interchange Agreement partners. Entity registries can be used to determine the security, addressing, and reliability requirements between potential Interchange Agreement partnering systems.

1.	The system SHALL exchange information with Interchange Agreement partners based on interoperability agreement descriptions.			1757
2.	IF an interchange agreement description specifies the use of a certain standard, THEN the system SHOULD exchange information using the standard specified by the interchange agreement description according to scope of practice, organizational policy, and/or jurisdictional law.			1758
3.	The system MAY conform to function TI.3 (Registry and Directory Services) to interact with registries, and/or directories to determine the address, profile, and data exchange requirements of known, and/or potential partners.			1759
4.	The system MAY analyze and present interchange service descriptions and capabilities according to scope of practice, organizational policy, and/or jurisdictional law.			1760
5.	The system SHOULD provide the ability to manage Interchange Agreements that have been established with Interchange Agreement partners.			1761
TI.5.5 Function	System Integration			1762

Statement: Support the integration of the PHR system with related systems.

Description: Within a given organization (for example, an institution, facility , or integrated care-delivery network), a PHR system may be directly integrated with other systems (for example, a laboratory Information System, Radiology System, Pharmacy System, or Hospital Information System). Conversely, a PHR system may access these other systems indirectly by integrating with a system that serves as the central routing mechanism for the organization. For example, the PHR system may be integrated with the Hospital Information System which then routes the PHR system's orders to a laboratory , pharmacy, or radiology service.

Depending on the type of information that is exchanged within an integrated-system environment, certain heuristics may be needed that will help govern the information exchange process.

1.	The system SHALL provide the ability to integrate the PHR system with other systems (e.g., a laboratory Information System, Radiology System, Pharmacy System, or Hospital Information System) according to scope of practice, organizational policy, and/or jurisdictional law.			1763
2.	The system SHOULD provide the ability to exchange discrete information (e.g., problem list, medication, and/or allergy information) with an integrated system data repository.			1764
3.	The system SHOULD provide the ability to exchange clinical documents with an integrated system Clinical Document Repository.			1765

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
4. The system MAY exchange information with systems that are integrated with the PHR system using heuristics that are defined by, and according to scope of practice, organizational policy, and/ or jurisdictional law.				1766
TI.6 Function	Business Rules Management			1767
Statement: Manage the ability to create, update, delete, view, and version business rules including institutional preferences. Apply business rules from necessary points within a PHR-S to control system behavior. A PHR-S audits changes made to business rules, as well as compliance to and overrides of applied business rules. **Description:** PHR-S business rule implementation functions include decision support, diagnostic support, workflow control, and access privileges, as well as system and user defaults and preferences. A PHR-S supports the ability of providers and institutions to customize decision support components such as triggers, rules, or algorithms, as well as the wording of alerts and advice to meet realm specific requirements and preferences.			
1. The system SHALL provide the ability to manage business rules.				1768
2. The system SHOULD provide the ability to enter, import, or receive business rules to guide system behavior.				1769
3. The system SHOULD provide the ability to maintain business rules and their components.				1770
4. The system SHOULD provide the ability to tag decision support rules as inactive / obsolete or to remove them according to scope of practice, organizational policy, and/or jurisdictional law.				1771
5. The system SHOULD provide the ability to render business rules.				1772
6. The system SHOULD provide the ability to manage diagnostic decision support rules that guide system behavior according to scope of practice, organizational policy, and/or jurisdictional law.				1773
7. The system SHOULD provide the ability to manage workflow control rules that guide system behavior according to scope of practice, organizational policy, and/or jurisdictional law.				1774
8. The system SHOULD provide the ability to manage access privilege rules that guide system behavior according to scope of practice, organizational policy, and/or jurisdictional law.				1775
9. The system SHOULD provide the ability to manage other rules (for example, monitoring rules, user defaults rules and preferences rule) that guide system behavior according to scope of practice, organizational policy, and/or jurisdictional law.				1776
10. The system SHALL provide the ability to determine system behavior based upon defined business rules.				1777
TI.7 Function	Workflow Management			1778
Statement: Support workflow management functions including both the management and set up of work queues, personnel lists, and system interfaces as well as the implementation functions that use workflow-related business rules to direct the flow of work assignments. **Description:** Workflow management functions that a PHR-S supports include: - Distribution of information to and from internal and external parties; - Support for task-management as well as parallel and serial task distribution; - Support for notification and task routing based on system triggers; and-Support for task assignments, escalations and redirection in accordance with business rules. Workflow definitions and management may be implemented by a designated application or distributed across a PHR-S.			
1. The system SHALL provide the ability to manage workflow business rules including work queues, personnel lists, and system interfaces.				1779
2. The system SHOULD provide the ability to determine workflow assignments based on workflow-related business rules.				1780
3. The system MAY provide the ability to manage human resources (i.e., personnel lists) for workflow queues.				1781
4. The system MAY exchange information with external systems (for example, Human Resources system or Staff Management system) to support the management of human resources.				1782
5. The system MAY exchange information with external systems (for example, Human Resources system or Staff Management system) to support the management of workflow queues (task lists).				1783
6. The system MAY provide the ability to exchange workflow related information with an external system.				1784
7. The system MAY provide the ability to render notifications and tasks based on system triggers.				1785
8. The system MAY determine and render an updated priority of tasks on the workflow (task list) queue in accordance with business rules, and according to scope of practice, organizational policy, and/or jurisdictional law.				1786
9. The system MAY determine and render an update to the tasks, and/or execution path on the workflow (task list) queue in accordance with business rules, and according to scope of practice, organizational policy, and/or jurisdictional law.				1787
10. The system MAY determine and render an update to the assignment of the resources to workflow (task list) queue in accordance with business rules, and according to scope of practice, organizational policy, and/or jurisdictional law.				1788

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
11.	The system SHOULD provide the ability to render a notification of a workflow update.			1789
12.	The system MAY provide the ability to render a notification of a workflow update including the details of the update.			1790
13.	The system SHOULD provide the ability to transmit a workflow (task list) queue update request to an external system.			1791
14.	The system SHOULD provide the ability to receive a workflow (task list) queue update response from an external system.			1792
TI.8 Function	Database Backup and Recovery			1793

Statement: Provide for the ability to backup and recover the PHR system.

Description: To enable the preservation of the PHR database and its data, functionality needs to be present to record a copy of the database and its contents to offline media as well as the recovery of the system from a backup copy and resumption of normal system operation. The backup must preserve both data as well as database structure and definition information sufficient to recover a complete functional PHR system. Database components may include, but not be limited to application data, security credentials, log/audit files, and programs; ultimately all PHR components necessary to provide a full and complete operating environment. Finally, the backup must be capable of being used during recovery processing to restore an exact copy of the PHR system as of a particular instant in time. This is a requirement to be able to preserve logical consistency of information within the recovered PHR system.

In providing for this capability the system may include multiple backup, and/or redundancy solutions such as fail-over architecture, database journaling, transaction processing, etc.

The backup and recovery function must address both physical system failure (i.e., failure of PHR system hardware) as well as logical system failure (e.g., database corruption). To support the requirement that the PHR system be available whenever it is needed within the design parameters of the system and provide reliability and redundancy of the PHR database and its data, the backup function shall not impact user functionality or appreciably impact user performance.

The backup function may include features which permit multiple processes and technologies to perform its task. This may include multiple backup technologies such as tape, disk, cloud, etc. Also, multiple architectures such as redundancy, online, near-line and off-line media.

1.	The system SHALL provide the ability to backup and recover PHR information according to scope of practice, organizational policy, and/or jurisdictional law.			1794
2.	The system SHALL provide the ability to backup and recover all database contents including programs and all software components necessary to permit a complete PHR to be recovered. (i.e., 'full' backup and recovery)			1795
3.	The system MAY provide the ability to backup and recover PHR information using alternative backup methods in addition to a full backup/recovery (e.g., incremental, differential, reverse delta, or continuous).			1796
4.	The system MAY provide the ability to backup PHR information according to a defined schedule of storage media rotation.			1797
5.	IF the PHR user requirements specify that the PHR system be available continuously, THEN the system SHALL provide the ability to backup PHR information concurrently with the normal operation of the PHR application.			1798
6.	The system SHOULD provide the ability to backup PHR information to a remote location.			1799
7.	The system MAY provide the ability to backup PHR information to more than one storage media (e.g., disk, tape, or cloud).			1800
8.	The system MAY provide the ability to encrypt backup data.			1801
TI.9 Function	System Management Operations and Performance			1802

Statement: Manage the change of status of an external facility and the ability to access, render and determine information related to Service Level Agreement.

Description: A health care delivery relies on services provided by other external facilities such as laboratories or Long Term Care facilities. The status of those facilities is subject to change for example: power outage, flooding or overcapacity. Therefore, the PHR system needs to capture the status of the external facilities, notify appropriate individuals / organizations or even change the workflow based on established business rules. Change of the status of an external facility is patient safety concern because a provider may need to adjust patient care or care workflows accordingly. For example, changes of status of external facility include: laboratory no longer accredited, laboratory power outage, Long Term Care facility at overcapacity. If laboratory loses accreditation an administrator needs to be notified to adjust the workflow. If status change is anticipated on regular basis, the system may automatically trigger workflow adjustment according to established business rules that take into consideration the status of the external facility. The example for later, the local Long Term Care facility may routinely exceed the capacity on the weekends; therefore, the business rule will accommodate for automatic workflow adjustments. A provider may need to be aware of certain Service Level Agreement information in order to mitigate patient safety-related risks that depend on system availability or system performance.

1.	The system SHOULD provide the ability to manage the change of status of an external facility.			1803
2.	The system SHOULD provide the ability to manage Service Level Agreement information according to scope of practice, organizational policy, and/or jurisdictional law.			1804
3.	The system MAY provide the ability to render system availability statistics and system performance statistics as specified in the Service Level Agreement according to scope of practice, organizational policy, and/or jurisdictional law.			1805

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
TI.10 Function	Standard or Preferred Clinical Models and Clinical Model Services			1806

Statement: Employ approved standard clinical models and clinical model service to ensure data correctness and to enable semantic interoperability (both within an enterprise and externally). Support sets of formal standard clinical models and/or clinical model services.

Description: Clinical Model specification. Semantic interoperability requires in addition to standard terminologies that give the meaning to concepts in the PHR also the structural format of data elements, code bindings, relationships, and data types, and their units and value sets where applicable. To allow the vast clinical variations to be facilitated in a PHR system, clinical model specifications are used. Such clinical models adhere to formal standard information models such as templates adhering to the HL7 Reference Information Model, or archetypes according the ISO/EN 13606 Electronic Health Record Communication. However, recently additional clinical models are expressed independent of such standard information models. Examples include models from the Clinical Information Modeling Initiative and ISO TS 13972 based Detailed Clinical Models.

A clinical model typically specifies the required data element(s) for one or more clinical concepts. The data elements will get unique identifying codes from terminologies as is explained in TI 4. Examples of clinical models include blood pressure, body weight, Apgar score, Glasgow Coma Scale, physical exam, and laboratory result.

Clinical Model Services specification.

The use of clinical models in a PHR system can vary. The clinical models can be used to specify which data elements should be visible in the user interface, which values should be allowed to select from pull down menus or check boxes. For record keeping, clinical models can define which data elements should be stored (for instance besides the values the user sees on the screen) and which terminology codes should in addition be stored with the data to maintain the meaning. Also, the clinical models can be used to specify the data exchange for a given use case.

Clinical models may be provided through a clinical model service internal or external to a PHR-S. Typical functions of clinical model services include the runtime provisions of the single clinical model or sets of clinical models. It is also possible to provide specifications for single data elements, and where applicable (versions) of value sets used to populate the data in the PHR-S in a standard manner. In addition, the clinical model service could provide mappings between values from different value sets, e.g., between different versions of value sets, or alternatively mappings between data elements, e.g., from source to target.

TI.10.1 Function	Standard or Preferred Clinical Models			1807

Statement: Employ approved standard or Preferred Clinical Models to ensure structured data correctness and to enable semantic interoperability (both within an enterprise and externally). Support a standard or Preferred Clinical Models model.

Description: Healthcare is shifting from supply-oriented care to more demand / patient-oriented integrated care. The focus is the patient and the integrated care he needs executed by one or more healthcare provider(s) in one or more organizations. Information on the patient must be shared by these healthcare providers and organizations. The PHR system must be focused on a problem-oriented recording in an integrated PHR system. This recording should take place in the care process and seamlessly fit in the workflow of the healthcare professional. When the information is properly recorded in the PHR, these information can be reused: by other healthcare providers, for deriving quality information, financial information and for research. For this purposes the use of widely accepted international standards is necessary.

Clinical Models are used to capture functional, semantic (non-technical) agreements for the standardization of information used in the care process. The purpose of the standardization is that this information from the care process is reused for other purposes such as quality registration, transfer or patient-related research. A Clinical Model is an information model in which a care-based concept is described in terms of the data elements from which that concept exists, the data types of those data elements, the binding to a (standard) terminology, etc.

Clinical models are information models of minimal clinical concepts, each containing multiple data with agreed content, structure and mutual relationship.

The binding to a terminology provides semantic and computable identity to its concepts. Examples of terminologies that a PHR-S may support include: LOINC, SNOMED, ICD-9, ICD-10, and CPT-4. See also Function TI.4 Standard Terminology and Terminology Services.

The key is that the standard be approved by all stakeholders. For example, a standard Clinical Model for 'Problem'. The information that is recorded in the PHR according to the Clinical Model can be reused for other purposes as quality registration, transfer or patient-related research.

1. The system SHALL provide the ability to exchange data with other systems (internal or external to the PHR-S) using approved standard or preferred clinical models or compositions of clinical models (e.g patient summary, follow-up message).			1808
2. The system SHALL determine that clinical terms and coded clinical data exist in an approved Clinical Model.			1809
3. The system SHOULD provide the ability to receive and transmit healthcare data using formal standard information models and approved standard or preferred clinical models according to scope of practice, organizational policy, and/or jurisdictional law.			1810
4. The system SHOULD provide the ability to manage data using a standard or preferred clinical model according to scope of practice, organizational policy, and/or jurisdictional law.			1811
5. The system SHALL provide the ability to manage clical model assets and supporting tools (internal or external to the PHR-S).			1812
6. IF there is no recognized-standard or preferred clinical model available, THEN the system MAY provide the ability to manage data using a locally-defined clinical model.			1813

Section/Id#: Type:	Header/Function Name Conformance Criteria	Reference	Chg Ind	Row#
7.	The system SHOULD provide the ability to capture information into structured data formats using approved standard or preferred clinical models without the user requiring knowledge of the clinical models used.			1814
8.	The system SHOULD provide the ability to enter data using content that is common to the user, and allow for collection and presentation of text form data to meet the pre-determined purposes of others. Text forms should exclude cryptic or uncommon abbreviations.			1815
9.	The system SHOULD provide the ability to present the terms used in standard or preferred clinical models in a language which is appropriate for the user.			1816
TI.10.2 Function	Maintenance and Versioning of Standard or Preferred Clinical Models			1817
	Statement: Enable version control according to scope of practice, organizational policy, and/or jurisdictional law to ensure maintenance of utilized standard or preferred clinical models. This includes the ability to accommodate changes to clinical models as the source clinical model undergoes its update process. Such changes need to be cascaded to clinical content embedded in templates, custom formularies, etc., as determined by existing policy. **Description:** Version control allows for multiple sets or versions of the same clinical model to exist and be distinctly recognized over time. Standard clinical models can be updated, and concurrent use of different versions may be required. Ideally, the meaning of a clinical model never changes over time, but a clinical model can be deprecated, and replaced with a new clinical model in a new version. It is important that retrospective analysis and research maintains the ability to relate to the appropriate clinical model. If the meaning of a clinical model changes over time, it is also important that for legal health records, as well as for retrospective analysis and research, the different meaning can be correlated to ensure the permanence of the information as originally captured. This does not necessarily imply that complete older versions of the clinical model be kept in the PHR-S, only access to the changes needs to be maintained.			
1.	The system SHALL provide the ability to manage data using different versions of standard or preferred clinical models.			1818
2.	The system SHALL provide the ability to update standard or preferred clinical models.			1819
3.	The system SHOULD maintain relationships among versions of a standard or preferred clinical models to allow preservation of interpretation over time.			1820
4.	The system SHOULD provide the ability to receive and harmonize data from and transmit data to other systems that use known different versions of a standard or preferred clinical model while preserving the meaning of that model.			1821
5.	The system SHALL provide the ability to update clinical models to a deprecated status.			1822
6.	The system SHALL provide the ability to update individual data elements within a clinical model to a deprecated status.			1823
7.	The system SHALL provide the ability to update terms with their equivalent when terminology is changed, where coded terminology content is embedded in clinical models (e.g., templates and custom formularies), when the terminology changes can be accomplished unambiguously, and if consistent with scope of practice, organizational policy, and/or jurisdictional law. NEEDS REVIEW			1824
8.	The system SHALL provide the ability to update standard or preferred clinical models used to enter clinical content (via templates, custom formularies, etc.)			1825
9.	The system SHALL maintain an audit log or a change history of clinical models to the individual clinical model, for versions used, dates implemented and updated to enable correct interpretation of historical data over time.			1826
TI.10.3 Function	Clinical Model Mapping			1827
	Statement: Map or translate one clinical model to another as needed by local, regional, national, or international interoperability requirements. **Description:** The ability to map or translate one clinical model to another is fundamental to an organization in an environment where several clinical models are in play to meet different purposes. It is a common occurrence that data is captured using one clinical model, but is shared using another clinical model.			
1.	The system SHALL provide the ability to manage data using clinical model maps which may be provided by mapping services (internal or external).			1828
2.	The system SHOULD provide the ability to update clinical model maps using standard clinical model services (internal or external).			1829
3.	The system SHOULD provide the ability to render data quality and technical quality reports for a user to determine the validity of clinical model mappings using approved mapping techniques.			1830
4.	The system MAY provide the ability for a user to maintain custom clinical model maps using approved mapping techniques where formal standard clinical model maps are unavailable.			1831
5.	The system MAY provide the ability for a user to maintain custom clinical model maps to formal standard clinical model maps in order to support historical data use.			1832