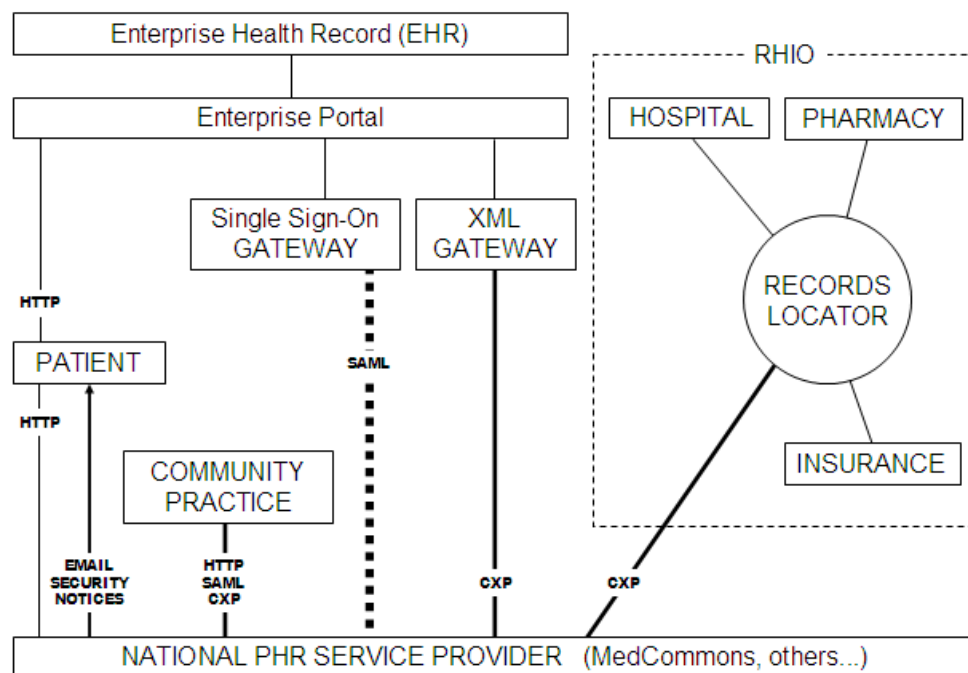




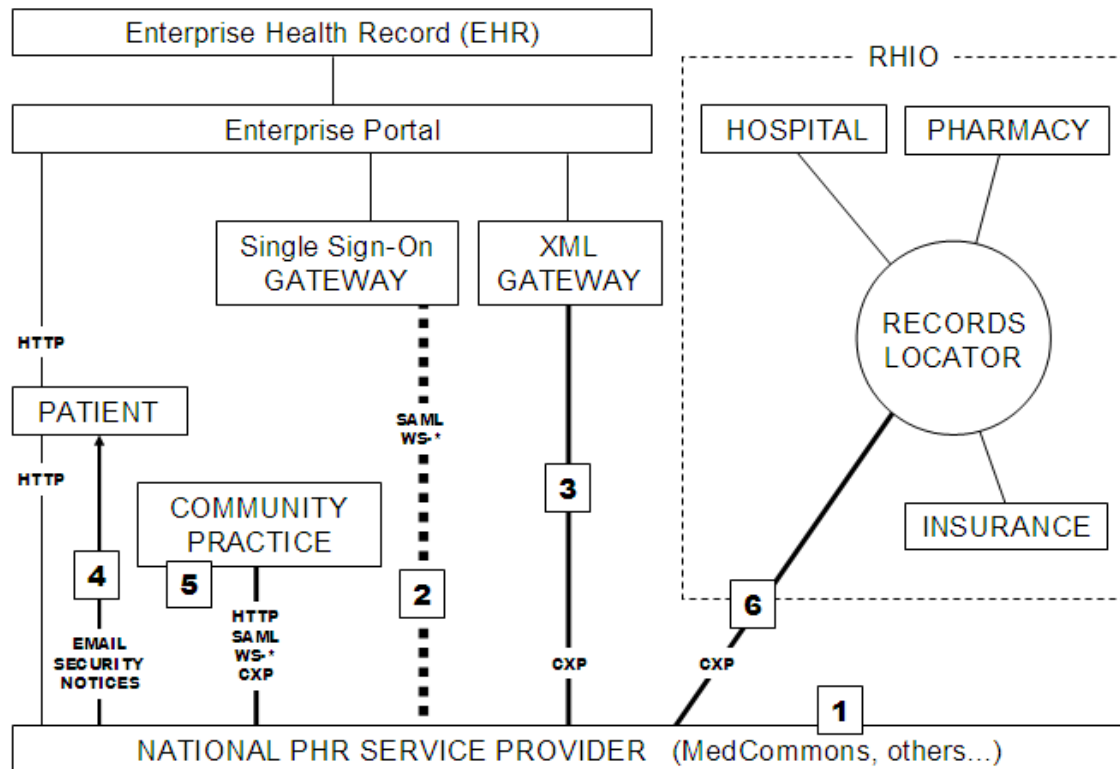
Consumer-Centered Interoperability

A system for regional and national health records interoperability built around existing web services standards and a patient-centered architecture inspired by the HITSP Consumer Empowerment Use Case.



CONTENTS

- I. Introduction
- II. [A Consumer Perspective on Health Care Interoperability Standards](#)
- III. [CCR Compatible Product Gallery as of January 2006](#)
- IV. [MedCommons – A Patient-Centric Exoskeleton for the NHIN](#)
- V. [Federated Identity Management and CXP – MedCommons White Paper – March 2006](#)
- VI. [CXP - Commons eXchange Specification 1.0 – March 2006](#)
- VII. [HITSP-Consumer Empowerment Use Case – January 18, 2006](#)
- VIII. [Consumer Reports Investigates Health Privacy – March 2006](#)



The diagram illustrates how enterprise portals could interoperate with community-based health information resources using open standards and under informed patient consent.

Some of the benefits include:

1. Unlike a typical RHIO, MedCommons indexes absolutely no private information and does not participate in master patient index arrangements that are presumed by typical RHIOs.
2. Support for two-factor authentication and SAML standard single sign-on provides a strong forensic audit trail for identity assertions across the Enterprise – MedCommons boundary.
3. CXP Web service protocol is standards based and transparent to CCR and future XML-based PHR interoperability standards per market demand.
4. MedCommons sends simple, privacy-safe emails notices to the patient each time their PHR account is accessed or updated by anyone.
5. The patient and community practitioners can access the patient's PHR using any modern web browser or via CXP-compatible PHR and EHR software.
6. MedCommons provides an informed consent mechanism for the patient to forward information to a RHIO.

© MedCommons 2006 except:

CCR Compatible Product Gallery © American Academy of Family Physicians

CXP Protocol and sample code is released under Creative Commons Attribution License 2.5

A Consumer Perspective on Health Care Interoperability Standards

Adrian Gropper, MD

MedCommons¹

March 3, 2006

At the intersection of consumer empowerment and the forthcoming national health information network, a battle is underway between standards and policies that are driven by integration and interoperability concerns. As a physician working to develop tools for healthcare providers for over 30 years, I find myself on four standards organizations representing enterprise technology (HL7 /IHE), consumer technology (Liberty Alliance), physicians (ASTM-CCR) and government policy (HITSP). To complete the set, I also should attend with the benefits administrators (X12) and figure out where engineers (IEEE) fit in. All of these groups are accredited by ANSI and all are trying to protect their stakeholders interest in the domain of interoperable and patient-focused primary health records².

The scope of integration is at the heart of the debate. Few would argue against integration of components that make up a single device, laboratory or treatment. People prefer cell phones that integrate email, a calendar and address book. A surgical suite where instruments were incompatible would be more than inconvenient, it would be dangerous. Adverse Drug Events (ADE) , the most frequently cited problem that health information systems can solve, are from the patient's perspective failures to coherently integrate diagnostic and therapeutic input.

As the scope of integration moves beyond the individual or a small team and becomes an enterprise or workflow "solution" it forces compromise by restricting the ability for a professional to choose her own tools. In the broad marketplace of knowledge workers, the Mac vs. PC debate is one classic example of the limitations of integration and the need for interoperability at a professional level. Yet, in the healthcare domain, radiologists are typically convinced to use workstations from a single vendor, clinicians are restricted to a particular *Enterprise* Medical Records workstation and community clinics are pushed to adopt the EMR of the region's dominant enterprise in the name of quality.

¹ Dr. Gropper is Chief Science Officer of MedCommons Inc.

² Primary health records are defined here as the authoritative information of interest to a primary care practitioner including physicians and allied health professionals. Specialty records such as billing, scheduling or intermediate laboratory results are excluded. As defined, primary health records also exclude information that is not specific to a particular patient such as might be found on the Internet by the patient or physician themselves.

In healthcare, as in the broader market, professional preference defines the boundary where integration principles become ineffective and standards become the basis of interoperability. The time has come to recognize that standards “harmonization” and other mandated integration principles do not result in practical interoperability among diverse professionals. This explains the apparent market failure of the open standards process that is driving the recently constituted federal HITSP initiative. For example, if primary care physicians want to define the standard for communicating a primary health record between one clinical workstation and another it is futile to insist on additional requirements based on the assumption that these workstations are integrated on any particular larger scale.

In the Internet age, world-wide interoperability will emerge spontaneously as professionals begin to insist on choosing their tools as individuals. A number of medical societies have already agreed on a standard, the CCR, which serves their need for comparable pay-for-performance measures across diverse practice situations. Other professional groups may develop other standards in the future, but in the long run, empowered consumers themselves may choose the mix of privacy and interoperability that will become the primary health record standard and all successful enterprises will have to deal with that.

CCR-Compatible Product Gallery

March 3, 2006

There are many EHR, PHR, and other health-IT vendors that are working toward the ASTM Continuity of Care Record (CCR) Standard (E2369-05). We have asked members of the Partners for Patients companies and those companies that are part of the CCR Acceleration Task Force to provide us with the estimated delivery time for CCR compliant products. We have aggregated them into the table below. Since this dates are estimates, they are subject to change, yet we will try to keep them as up-to-date as possible.

We have also provided links to example CCRs from companies that have provided them. You can view them in their native XML format by clicking on the "XML" link and you can see them transformed into a Web page by clicking on the "HTML" link.

If you are an EHR or PHR vendor and want to join the CCR Acceleration Task Force, please send an email to centerforhit@aafp.org

Continue to come back to this page frequently, as there will be many additions to this page for the next weeks and months.

			CCR Export*		Accept & View CCRs*		CCR Import*	
Vendor	Product	Sample CCR	Version	Release Date	Version	Release Date	Version	Release Date

We're awaiting permission from AAFP to reproduce this section.

Until then, please visit:

<http://www.centerforhit.org/x1556.xml>

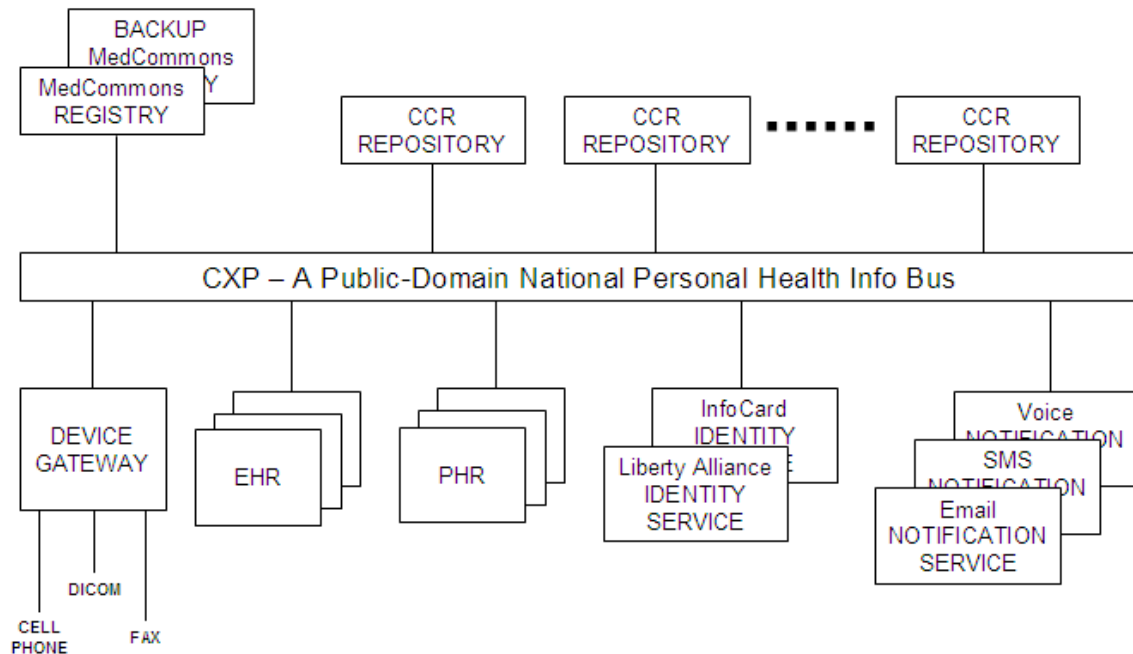
for an up-to-date list of CCR-Compatible Products.



MedCommons – A Patient-Centric ExoSkeleton for the NHIN

The interconnection of disparate healthcare enterprises into a cohesive NHIN is a large undertaking that is currently under evaluation and prototyping by the federal government [1]. MedCommons provides a lightweight means for adding patient-centric services to current generation PHR and EHR systems, Laboratory and Personal Medical Devices, RHIOs and the various putative NHIN prototype efforts.

MedCommons creates an exoskeleton over existing enterprise and personal IT systems by blending distributed patient health record storage, with simple, secure communications protocols for connecting legacy systems, and a flexible approach to managing patient Identity on a national scale. The exoskeleton grows incrementally yet independently of the NHIN by adding additional resources only as patient coverage increases.



- **Storage:** Copying source content into a distributed document repository and a centralized registry keeps things simple, and builds confidence in the archival nature of the service. MedCommons is patient-centric because each patient has an account and maintains a collection of key documents and consents. Source content is left untouched, and is normally never referenced again by MedCommons, as at least one copy is maintained by the service in a document repository. Access to an account is strictly controlled, with notification alerts to the account holder every time the account is referenced.
- **Communications:** The primary means for inserting and retrieving documents is the Commons Exchange Protocol, or CXP, which is an open WS-* based standard sponsored by the CCR Accelerator Group [2]. Third party PHR, EHR and device vendors utilize CXP to send and receive CCRs and other XML formatted documents into accounts. To achieve interoperability between all parties, it is necessary to minimize the number of duplicative document types, but for now MedCommons will support CCRs, PDFs, DICOM, and whatever else the market demands.

- **Identity:** The techniques for identification of individuals are quite varied. At the simplest level, anyone can self-register for a plain MedCommons account with a username and password and an optional two-factor cell phone identity check. At the other end of the spectrum, MedCommons supports federated identity management systems from Liberty Alliance and will ultimately support Microsoft InfoCard as well [3]. Federated identity allows large enterprises to participate in Single Sign-On with MedCommons, as well as dynamically securing the CXP protocols. With federation, it is possible to integrate large communities of patients such as RHIOs directly into MedCommons.
- **Notification:** In a multi-enterprise environment, some of the responsibility for monitoring security will fall on the patient or clinician themselves. MedCommons integrates a lightweight email notification function that alerts the patient to changes in their account and to access of their information without divulging the information itself. This notification functionality can also serve as a means of contacting a patient to request informed consent to a disclosure that otherwise would not be covered by HIPAA direct patient care regulations.

The MedCommons Family of Services

The exoskeleton is both a platform for the NHIN and a useful point-to-point transport medium unto itself, capable of providing useful, patient-centric, cost reducing, quality improving value right now, well in advance of the formulation of the NHIN. The ecosystem consists of the Core MedCommons Service, and the MedCommons Partner Systems and Services.

Core MedCommons Service

The operational MedCommons service, at <http://medcommons.net/> consists of a pair of replicated MedCommons Document Registries and a scaleable collection of application servers at two diversely situated data centers, and a widely distributed collection of MedCommons Document Repositories in both these locations and also in partner and select customer locations. The service ensures that multiple separately encrypted copies of all documents are maintained by MedCommons according to patient account preferences for both backup and performance purposes.

A small re-brandable AJAX-based user interface is offered as part of the MedCommons service to allow access to the patient's account, to view any previously stored content, to send and receive secure healthcare communications, and to control access to her personal health information by healthcare providers. A similar interface is available to healthcare providers to display a restricted view of patient content. But MedCommons is not in the user interface business. Instead, the primary means for access to MedCommons content is via the user interfaces of the PHR and EHR systems, enterprise portals, and other 3rd party configurations via CXP and additional MedCommons specific web services.

Optional DICOM support for radiology and cardiology is offered as part of the MedCommons service for owners of DICOM devices and PACS systems that wish to utilize MedCommons directly from within their existing workstation vendor environment. A standard feature of MedCommons for all users is a web-based, FDA approved, AJAX display of DICOM content with easy to use tools for image manipulation. However, long term DICOM storage in MedCommons Repositories is a premium feature.

Optional FAX mailboxes may be established for any MedCommons account. This allows the patient to distribute a fax number for his healthcare providers to supply source documents if there is no other direct means. The Faxes are rendered as PDF documents for archival storage.

Optional re-brandable Mobile Device support will allow appropriately configured cell phones and PDAs to collect personal healthcare data on a periodic basis and automatically integrate into a MedCommons account.

Partner Systems and Services

The attraction and efficacy of a common ecosystem depends largely on the ease of integration. Most third party software integrates with MedCommons via CXP and standard web service protocols. The storage model for different types of partners can vary: For some single user systems such as a PHR the MedCommons Account might be considered the primary repository for healthcare content. Multi-patient systems such as an EHR or Practice Management System will typically consider MedCommons as a secondary store, and require an explicit “Export” from the application. Lab and personal mobile devices will typically utilize CXP in a message push mode, to upload values into a patient’s account at the completion of some workflow event that is managed separately from MedCommons.

Enterprise Portals can integrate with MedCommons via MedCommons JSR-168 supplied portlets, or CXP can be incorporated directly into the portal. Many portals will also include a third party Identity System for Single Sign-On within the Enterprise and MedCommons (via Liberty Alliance or Microsoft InfoCard), and for securing MedCommons web service communications within the enterprise user community.

RHIOs integrate with MedCommons by incorporating CXP based applications such as EHRs, PHRs, into their networks, and by utilizing a Federated Identity Service to establish MedCommons Accounts for patients and providers.

All MedCommons Partners are presumed to run their own direct customer support call centers, with a 2nd tier help desk and case repository provided via at <http://medcommons.net/?p=support>

Built-in MedCommons Applications

There are three inbuilt MedCommons Applications that are available to all patients directly from www.medcommons.net or through a PHR or EHR system

- Free Emergency CCR Service – allows any user to manage and carry a wallet card to provide immediate access to critical emergency healthcare information from any Emergency Room. The card can also be branded and printed by any partner PHR or EHR system.
- Free Commons Service – allows any document to be anonymously and temporarily stored within MedCommons, for access by any PHR or EHR system via CXP. Within thirty days, documents must be moved to a patient account, or are permanently deleted.
- Paid Accounts Service – subscription based accounts holding a lifetime of personal medical content, including complex content such as DICOM, laboratory device reports, optional faxes. A set of MedCommons specific web services are available for management of accounts, including Single Sign-On, from PHR and EHR systems.

Conclusion

The MedCommons family of services combines distributed storage, standard protocols for document exchange, and federated identity management to produce a platform for support of next-generation, networked healthcare applications and communities including EHRs, PHRs, Enterprise Portals, RHIOs, and HMOs. This set of services forms a patient centric exoskeleton for the forthcoming NHIN, which can shape itself incrementally and evolve in advance any formal NHIN direction and without changes to existing privacy and consumer protection statutes.



CXP – A Patient-Centric Document Transfer Protocol Supporting Federated Identity Management

MedCommons White Paper
March 2006

Abstract

CXP is a protocol for the structured and reliable exchange of standards compliant xml based Healthcare Records and Messages between Patients, Providers, Payors, and medical Devices. Based on SOAP and optionally, WS* standards, CXP achieves a high degree of security via support of both hardwired TLS connections and dynamic WS-*/SAML based operations over a federated identity network such as the Liberty Alliance or Microsoft InfoCard.

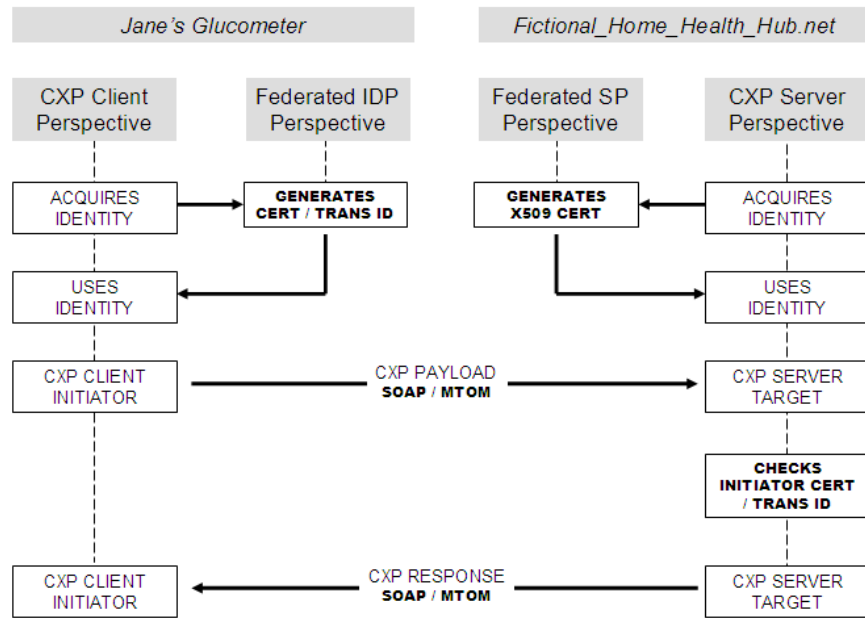
The payload in a typical CXP exchange is one or more structured XML documents, with additional unstructured document types (notably PDFs) included as attachments. The XML formats supported include CCR, and will cover CCD and CDA if applicable. The CXP Server often front-ends a document repository and may be configured to validate incoming payloads against specific XSD schemas, interact with one or more registries, or perform enterprise specific processing.

CXP Overview

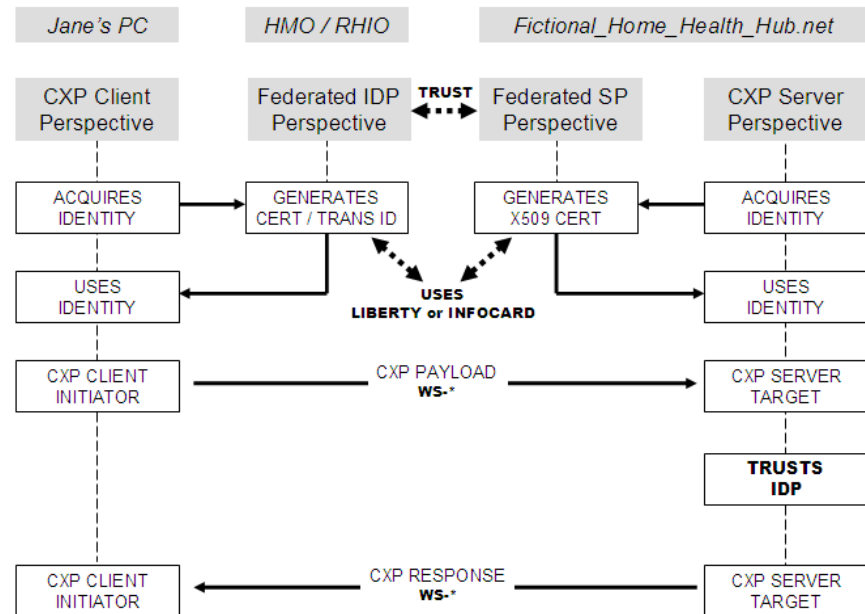
The Commons Exchange Protocol (CXP) is a TCP based end to end HealthCare Aware Protocol allowing two parties to structure a spontaneous and reliable constrained exchange of standards-based, patient-focused healthcare information. It can be utilized over plain http or SSL, over locked-down certificate based TLS connections, or preferably via a Federated Identity Management scheme such as the Liberty Alliance or Microsoft InfoCard, each with increasing levels of trust. CXP is defined on top of existing standards including SOAP with or without MTOM, and the WS-* family of web services protocols. CXP permits PHR and EHR vendors to utilize basic GET, PUT, and DELETE services to exchange and validate structured data and metadata in common formats including CCR, CCD, CDA, and any other XML based schema.

Use Cases

Importantly, the CXP interface afforded to PHR and EHR vendors is neutral with regard to the presence or absence of particular WS-* features including identity, security, and discovery services. This allows vendors to construct simple client implementations of their applications that assume only SOAP is present, yet lets larger enterprises, software vendors and service vendors to immediately gain benefits from additional complex services layered above CXP built around Liberty, InfoCard and WS-* supported protocols.

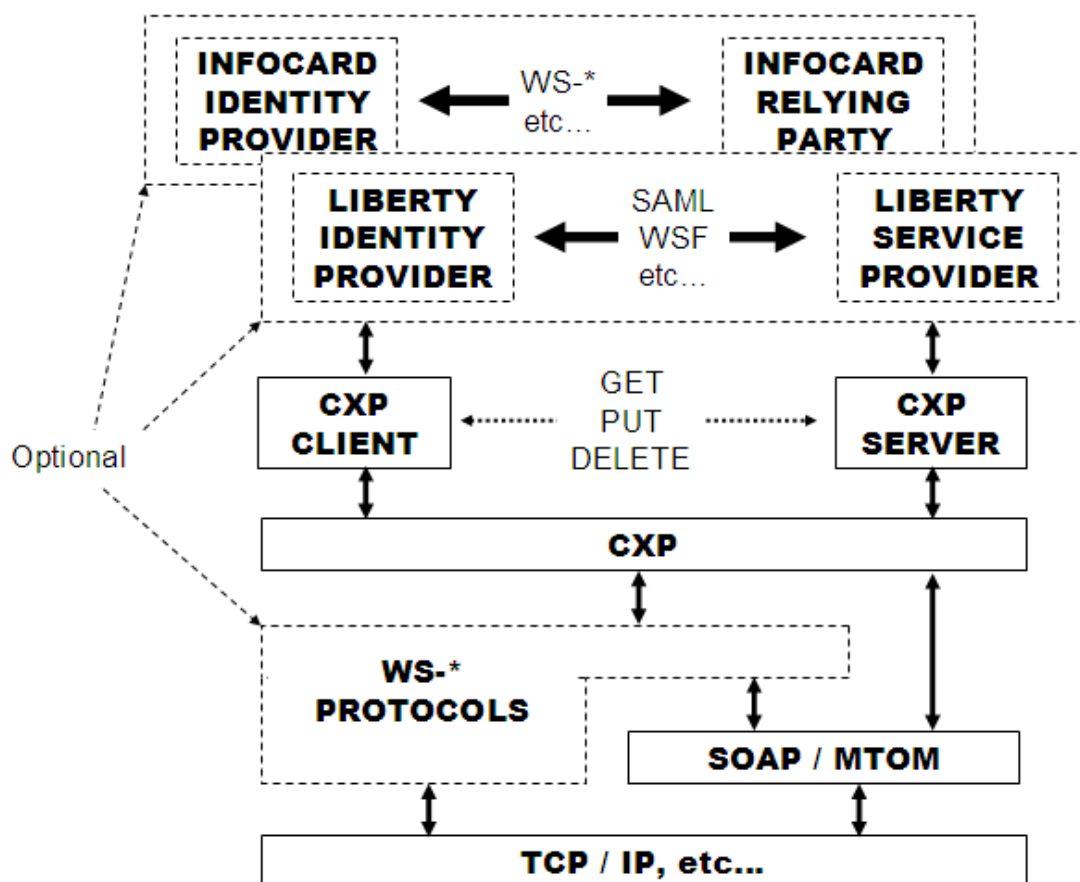


Thus, for example, the same CXP protocol is used between (a) the glucometer on Jane's belt and a network based Fictional Home Healthcare Hub service at <http://fhhh.net> and (b) the HealthStuff PHR used by Jane to access her personal healthcare account from her Liberty-Friendly HMO. In the first case, the trust relationship between the client and server is established by a PKI cert in Jane's glucometer, that is honored, or possibly issued, by the FHHH service. In the second case, the trust relationship is between Jane's IDP (her HMO) and the FHHH Service Provider via the bilateral Liberty Alliance business agreements.



Architecture

To achieve connectivity, each end of a CXP connection must support the same SOAP/MTOM/WS-* Protocol selection depending on the requirements of the federated identity management provider, if any.



There is a well defined and standard separation between CXP Clients and Servers; clients make requests, servers process requests and respond. Although nothing precludes a program from being both a CXP Client and Server, typically they have distinct roles within a distributed healthcare network. Normally, a CXP Server is the front door for a document repository and may also optionally interact with one or more registries behind the scenes.

CXP requires that each Client party initiating a transaction supply an opaque Sender identity token and that both parties maintain an audit log of each CXP transaction so that the logs of each party can be conjoined for forensic problem and dispute resolution. These tokens may be hardwired shared secrets, or otherwise obtained dynamically via methods outside CXP, as for example, from SAML or InfoCard.

Identity Federation

But it is more interesting to consider CXP when used in conjunction with a Federated Identity Service such as Liberty Alliance or Microsoft's InfoCard. In this case, the two parties establish a static trust relationship within the framework of the Federation Service, and dynamically use SAML2.0 and SOAP based WS-* to communicate CXP payloads. The Client side initiator of a CXP transaction obtains an opaque Sender identity token from the Liberty or InfoCard IDP and passes it along to his counterpart (the Liberty Service Provider or InfoCard Relying Party) as above. But instead of hard coded secrets, or cumbersome certificates, the federation services permit dynamic interconnection of CXP participants who have signed

bilateral business agreements and demonstrated technical compliance.

If a CXP Server is owned or otherwise associated with a Liberty Alliance Service Provider or InfoCard Relying Party, then that CXP Server can be exclusively available to only those CXP Clients whose Identity has been vetted by a trusted Identity Provider and has a pre-established bilateral trust relationship with the Service Provider/Relying Party. This allows not only for the federation of Identity outside of CXP itself, but allows small software and device vendors to benefit from the enhanced security and trust models of the Liberty and InfoCard.

Once a Identity Provider of any variety signs an agreement with a Liberty Alliance Service Provider or an InfoCard Relying Party and their technical infrastructures have been upgraded as necessary to support WS-* and SAML2.0 then the CXP Server can begin to offer services to the IDP users. If the Service Provider/Relying Party application presents a User Interface in addition to the CXP interface, then the single sign-on (SSO protocols) will likely be utilized between the service and the IDP, without regard to CXP. If the only protocol is CXP, then the WSF-2.0 protocols are utilized to allow secure and authenticated remote web service calls.

To support a network the size of the NHIN it will be necessary to run many CXP Servers in front of many repositories under a single Service Identity. In this case a single x509v3 Cert can be shared by the entire farm and WS-* redirection protocols may be utilized to put all of the servers under a single public name. The CXP client connects to the service and is transparently redirected to the appropriate server.

Alternatively, when the CXP Server is a Document Repository, and there is a separate Document Registry, the CXP transaction initiator (the document source) may choose to have an initial conversation (WSF2.0) with the Registry (e.g. a Liberty Service Provider or InfoCard Relying Party) to determine which Repository to contact. In this case there is an implied transfer of trust from the Registry to the Repository and the CXP protocol is then utilized as documented herein. When using a Federated Identity Service this initial conversation is mandatory and supplies the same opaque Sender identity token.

Registry Options

Finally – CXP may be used as a low-complexity, simple mechanism for document storage/retrieval from other types of registries and repositories. The use of multiple registry parameter blocks permits opt-in on the part of the call initiator to other repository models such as the ebXML-based IHE-XDS.

The leverage gained from federation by both identity providers and service providers towards the establishment of an NHIN are enormous. The identity providers can focus on membership, verification, and personalization. The service providers can focus on safe, cost effective healthcare.

Commons eXchange Protocol

Version 1.0

Commons eXchange Protocol.....	5
Overview.....	6
Protocol.....	7
Possible Architectures.....	8
Architecture A: System registry and repository.....	8
Architecture B: Simple End-to-End communication.....	8
Architecture C: System with multiple registries.....	9
API.....	10
Data Definitions.....	10
CXP Messages.....	12
Security.....	13
Data Encryption.....	13
Identity.....	13
HIPAA.....	13
Trademarks and Intellectual Property.....	13
Appendix A: Changes history of CXP Protocol.....	15
Changes since 0.8.....	15
Changes since 0.9.....	15
Changes since 0.9.2.....	15
Changes since 0.9.3.....	15
Changes since 0.9.9.....	15
Appendix B – CXP SOAP WDSL.....	16
Appendix C: Example code.....	24
Example C# PUT call.....	24
Example C# GET Call.....	25
Appendix D: Normative Security/Identity Recommendations.....	25
Appendix E: Normative RegistryParameters Data Dictionary.....	27
Appendix F: Future directions.....	27



Overview

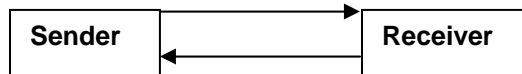
CXP is a TCP (SOAP) based end to end protocol allowing two parties to structure a spontaneous and reliable constrained exchange of standards-based, patient-focused healthcare information. It can be utilized over plain http or SSL, or preferably over locked-down certificate based TLS connections, with increasing levels of trust.

CXP may be used as a low-complexity, simple mechanism for document storage/retrieval with other types of registries and repositories. The use of multiple registry parameter blocks permits opt-in on the part of the call initiator to other repository models such as XDS.

The simplicity of the base protocol is intentional. Other services and protocols will be built on this foundation.

Protocol

CXP is a two party point to point protocol that moves CCRs and other documents across the Internet between co-operating Sending and Receiving systems from multiple vendors. It is designed to be a very lightweight protocol while being able to support different vendors and different system architectures.



All messages in CXP are synchronous and stateless. The Sender initiates the session; the Receiver responds. The protocol that the messages use is SOAP 1.1.

CXP contains three commands PUT, GET, and DELETE; while all of them need to be supported in the WDSL not all need to be supported by any particular implementation. The mechanism for this is described below.

PUT places a CCR into a Receiving system. There are no guarantees for what a system does with the document; it might be stored, digested, indexed depending on the policies and configuration of the Receiving server.

GET retrieves a document based on its identifier (which was returned by PUT) or optionally by metadata (subject to the configurations and policies of the Receiving system)

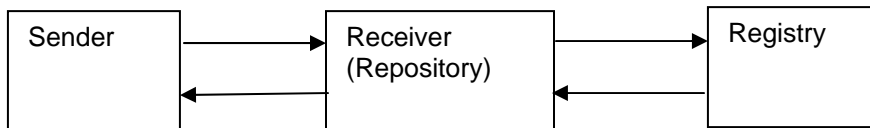
DELETE deletes a document based on its identifier (which was returned by PUT) or optionally by metadata (subject to the configurations and policies of the Receiving system).

A CXP service might support PUT but not GET or DELETE. For example – if the service was a desktop application that accepted the CCRs might parse them, use the contents, and then discard the CCR. In this case – the status code from any GET or DELETE messages would be 501 – Not Implemented (identical to HTTP).

Possible Architectures

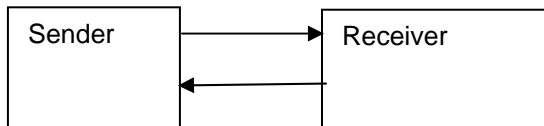
Although CXP does not mandate any type of architecture for the service endpoints, this section will describe three possibilities that could be implemented to illustrate how the protocol can be used.

Architecture A: System registry and repository



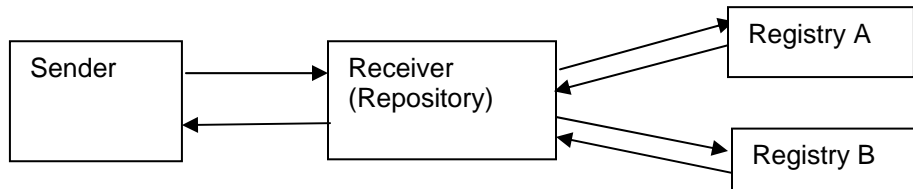
This model assumes that the sender wishes to store data on a repository with separate registry.

Architecture B: Simple End-to-End communication



The simplest architecture is a simple end-to-end message. This is especially appropriate for two devices sharing information without any need of a server or special registry.

Architecture C: System with multiple registries



Using CXP with multiple registries can be very useful for simple devices to interact with more complex repository models. For example – if the sender (the issuer of a PUT command) specified two registries with different structures (Registry A might use only opaque or voluntary identifiers with no patient metadata federation, Registry B might be an XDS registry which required ample metadata and federation across multiple MPIs) the sender can effectively ‘opt-in’ to both registries. This permits the sender to use a very simple protocol to interact with several registries with different policies.

The only differences in architectures A, B, and C is in the registry parameter blocks and the authentication layer; the core CXP commands remain the same.

API

All of the services have optional registry parameters. These registry parameters are always specified within an array.

Data Definitions

RegistryParameters object contains the following fields:

- String RegistryIdentifier
- String RegistryName
- String version – this is the version of CXP.
- List of name/value pairs.

RegistryParameters are used by several commands on input and output. Different implementations may have different sets of name/value pairs. The version number is the version of CXP; if there are versions of other software components they can be included in the name/value pairs.

The PutResponse object is defined to be

- String guid³
- Integer status
- String reason
- (optional) RegistryParameters parameters

The GetResponse object is defined to be

- String guid
- Integer status
- String reason
- String content-type
- String content
- (optional) RegistryParameters parameters

The Attachment object is defined to be

- String guid
- String content-type
- String content

³ A guid is a global document identifier. In CXP it is modeled as a string.

a. *Status code*

The status code is an integer. This table defines what the values mean; a future version of this specification will define specific codes. The meaning of any particular code should be obvious from the <Reason> text. The meanings of the codes should echo the W3C recommendations⁴ when possible. A short overview follows.

Code range	Meaning
200-299	Success. 200 means completely successful; other values in this range may have warning or informational messages in the reason field.
400-499	Bad request (client error)
500-599	Server error. Two special cases
	500 Internal Server Error
	501 Not supported

Any CXP implementation may define additional status codes within this broad framework.

b. *Content Types*

Table: Defined Content Types

Content type	Document type
application/pdf	PDF document
application/dicom	DICOM Series
Text/xml blah blah blah astm-ccr	CCR

⁴ see <http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html>

CXP Messages

PUT

Put places a CCR on the Receiving server. It returns success only after the document has been successfully received by the Receiver. There are three versions of PUT:

Response put(String ccr)

Response put(String ccr, RegistryParameters[] parameters)

Response put(String ccr, RegistryParameters[] parameters, Attachments[] attachments⁵)

GET

GetResponse get(String guid)

GetResponse get(RegistryParameters [] parameters)

GetResponse get(String guid, RegistryParameters[] parameters)

DELETE

DeleteResponse DELETE(String guid)

DeleteResponse DELETE(RegistryParameters [] parameters)

DeleteResponse DELETE(String guid, RegistryParameters [] parameters)

Note that there are no general query mechanisms in CXP for (say) all of the documents belonging to a patient or all of the documents belonging to a doctor. A query of this type could be supported by a registry – but that happens outside the scope of the CCR. By placing registry parameters in a second (optional) block we permit multiple business models.

⁵ This version of CXP places file attachments as base64 encoded entities; the next version will use MTOM.

Security

Data Encryption

There are two types of data encryption supported here. The first is session encryption. Session encryption takes place via SSL or TLS. It is recommended that all clinical data be transmitted over encrypted channels such as these.

The second type of encryption is data object encryption – such as a CCR with encrypted sections per the upcoming ASTM specification. This data can be handled via CXP but the storage and transmission of keys is outside of the CXP specification. Implementations may refuse encrypted CCRs or they may require additional registry parameter entries to process encrypted content.

Identity

Authentication happens outside of CXP. There are potentially two separate notions of identity that may be modeled in the future:

- Identity of the information system
- Identity of the sender (the human)

HIPAA

The CXP sender must accept responsibility for release of information to the recipient. Patient consent to information release is the responsibility of the sender.⁶. Consent and the key management are outside of CXP. Another example might be implied consent between two CXP systems that have a HIPAA covered entity or business associate relationship and that authenticate each other via TLS. The HIPAA relationship is beyond CXP. Other consent mechanisms may exist, all outside CXP.

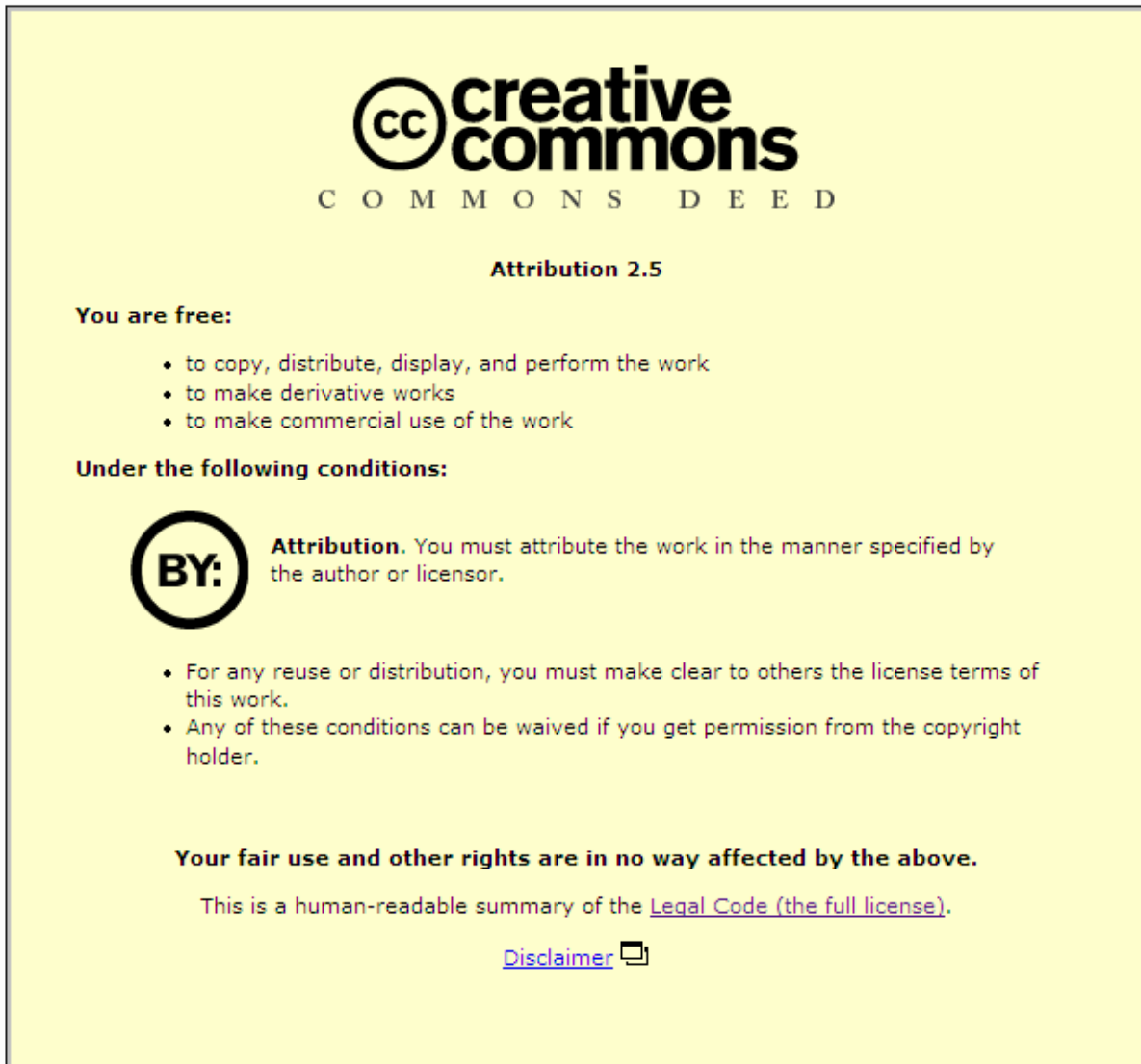
A CXP receiver is expected to manage its own security independent of the sender system or vendor. There is no defined responsibility for a recipient to publish general policies or to handle security for a particular transfer in a particular way. If the sender needs specific security information to manage its own policy, then the negotiation of these assertions is beyond the scope of CXP.

Apart from the use of SSL and TLS there is no authentication of the machine at the other end of the CXP connection. A Sender and Receiver can agree to use extra fields in the Registry Parameters to pass additional authentication data such as a shared secret in order to provide additional validation to the transaction.

Trademarks and Intellectual Property

CXP is licensed under the Creative Commons Attribution license. We request attribution to both MedCommons and the CCR Accelerator Group.

⁶ For example, use of a recipient's public key as derived from a consent form explicitly signed by the patient is one way to satisfy this legal mandate



This is a human-readable summary of the [Legal Code \(the full license\)](#).

[Disclaimer](#) 

Appendix A: Changes history of CXP Protocol

This appendix describes the changes in the different draft versions of the CXP protocol.

Changes since 0.8

- Status no longer a scalar value. There are status codes plus human-readable reasons that can be displayed.
- XML elements now consistently use the same convention for XML element naming as the CCR specification: upper case for abbreviations and upper CamelCase for other element names. So, <CXP> all capitals (like <URL>) and <opcode> is now <OperationCode>.
- Added explicit CXPVersion element in XML blob. This is used by the client to specify which version of CXP is being used. Servers can reject messages in versions of CXP that they do not support.
- Added <InformationSystem> identifiers to parameter block. This describes the vendor's product name and version number. This is mostly useful for error reporting.
- QUERY operation code has been replaced by QUERYTXID and QUERYUID for the two different types of queries.

Changes since 0.9

- Made consistent the specification of transaction numbers and PINS. QUERYTXID has been moved to Appendix C.
- Documented SOAP interface

Changes since 0.9.2

- Changed SOAP WDSL to work with .NET environment. The earlier WDSL worked well for a Java client but the resulting WDSL generated by Axis was not compatible with the .NET tools. The main difference is that the CCR is now encoded as a string instead of as an embedded XML document.
- There is now a working C# client.

Changes since 0.9.3

- Removed REST documentation
- Factored out all registry information (which may vary by vendor or by architecture) to separate objects.
- Made naming more consistent.
- Added section on future plans

Changes since 0.9.9

- Added support for multiple registries
- Made CXP specification a bit more generic; moved some policy constraints to a separate document.

Appendix B – CXP SOAP WDSL

The CXP WDSL is available on every server that implements CXP in a form such as:
<https://hostname/router/services/CXP?wsdl>

The current implementation of CXP uses SOAP 1.1.

The CXP 1.0 WDSL follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions targetNamespace="http://hostname:9080/router/services/CXP"
  xmlns:apacheSOAP="http://xml.apache.org/xml-soap" xmlns:impl="http://hostname:9080/router/services/CXP"
  xmlns:intf="http://hostname:9080/router/services/CXP" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:tns1="urn:BeanService" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <!--WSDL created by Apache Axis version: 1.2.1on Jun 14, 2005 (09:15:57 EDT)-->
  <wsdl:types>
    <schema targetNamespace="urn:BeanService" xmlns="http://www.w3.org/2001/XMLSchema">
      <import namespace="http://hostname:9080/router/services/CXP"/>
      <import namespace="http://schemas.xmlsoap.org/soap/encoding/" />
      <complexType name="Parameter">
        <sequence>
          <element name="name" nillable="true" type="xsd:string"/>
          <element name="value" nillable="true" type="xsd:string"/>
        </sequence>
      </complexType>
      <complexType name="RegistryParameters">
        <sequence>
          <element name="parameters" nillable="true" type="impl:ArrayOf_tns1_Parameter"/>
          <element name="registryId" nillable="true" type="xsd:string"/>
          <element name="registryName" nillable="true" type="xsd:string"/>
        </sequence>
      </complexType>
      <complexType name="PutResponse">
        <sequence>
          <element name="cxpVersion" nillable="true" type="xsd:string"/>
          <element name="guid" nillable="true" type="xsd:string"/>
          <element name="parameters" nillable="true" type="impl:ArrayOf_tns1_RegistryParameters"/>
          <element name="reason" nillable="true" type="xsd:string"/>
          <element name="registryParameters" nillable="true" type="impl:ArrayOf_tns1_RegistryParameters"/>
          <element name="status" type="xsd:int"/>
        </sequence>
      </complexType>
      <complexType name="CXPAttachment">
        <sequence/>
      </complexType>
      <complexType name="GetResponse">
        <sequence>
          <element name="content" nillable="true" type="xsd:string"/>
          <element name="contentType" nillable="true" type="xsd:string"/>
          <element name="cxpVersion" nillable="true" type="xsd:string"/>
          <element name="guid" nillable="true" type="xsd:string"/>
          <element name="parameters" nillable="true" type="impl:ArrayOf_tns1_RegistryParameters"/>
          <element name="reason" nillable="true" type="xsd:string"/>
          <element name="registryParameters" nillable="true" type="impl:ArrayOf_tns1_RegistryParameters"/>
          <element name="status" type="xsd:int"/>
        </sequence>
      </complexType>
      <complexType name="DeleteResponse">
        <sequence>
          <element name="cxpVersion" nillable="true" type="xsd:string"/>
          <element name="guid" nillable="true" type="xsd:string"/>
          <element name="parameters" nillable="true" type="impl:ArrayOf_tns1_RegistryParameters"/>
          <element name="reason" nillable="true" type="xsd:string"/>
          <element name="registryParameters" nillable="true" type="impl:ArrayOf_tns1_RegistryParameters"/>
          <element name="status" type="xsd:int"/>
        </sequence>
      </complexType>
    </schema>
  </wsdl:types>
```



```

<schema targetNamespace="http://hostname:9080/router/services/CXP" xmlns="http://www.w3.org/2001/XMLSchema">
  <import namespace="urn:BeanService"/>
  <import namespace="http://schemas.xmlsoap.org/soap/encoding"/>
  <complexType name="ArrayOf_tns1_Parameter">
    <complexContent>
      <restriction base="soapenc:Array">
        <attribute ref="soapenc:arrayType" wsdl:arrayType="tns1:Parameter[]"/>
      </restriction>
    </complexContent>
  </complexType>
  <complexType name="ArrayOf_tns1_RegistryParameters">
    <complexContent>
      <restriction base="soapenc:Array">
        <attribute ref="soapenc:arrayType" wsdl:arrayType="tns1:RegistryParameters[]"/>
      </restriction>
    </complexContent>
  </complexType>
  <complexType name="CXPEException">
    <sequence/>
  </complexType>
  <complexType name="ArrayOf_tns1_CXPAttachment">
    <complexContent>
      <restriction base="soapenc:Array">
        <attribute ref="soapenc:arrayType" wsdl:arrayType="tns1:CXPAttachment[]"/>
      </restriction>
    </complexContent>
  </complexType>
</schema>
</wsdl:types>

<wsdl:message name="getRequest">
  <wsdl:part name="xmlData" type="xsd:string"/>
</wsdl:message>

<wsdl:message name="getVersionResponse">
  <wsdl:part name="getVersionReturn" type="xsd:string"/>
</wsdl:message>

<wsdl:message name="putRequest">
  <wsdl:part name="ccrXml" type="xsd:string"/>
</wsdl:message>

<wsdl:message name="CXPEException">
  <wsdl:part name="fault" type="impl:CXPEException"/>
</wsdl:message>

<wsdl:message name="deleteRequest">
  <wsdl:part name="guid" type="xsd:string"/>
</wsdl:message>

<wsdl:message name="putResponse2">
  <wsdl:part name="putReturn" type="tns1:PutResponse"/>
</wsdl:message>

<wsdl:message name="getVersionRequest">
</wsdl:message>

<wsdl:message name="deleteRequest1">
  <wsdl:part name="parameters" type="impl:ArrayOf_tns1_RegistryParameters"/>

```

```
</wsdl:message>

<wsdl:message name="getRequest1">
  <wsdl:part name="inputRegistryParameters" type="impl:ArrayOf_tns1_RegistryParameters"/>
</wsdl:message>

<wsdl:message name="getResponse">
  <wsdl:part name="getReturn" type="tns1:GetResponse"/>
</wsdl:message>

<wsdl:message name="deleteResponse">
  <wsdl:part name="deleteReturn" type="tns1:DeleteResponse"/>
</wsdl:message>

<wsdl:message name="deleteResponse2">
  <wsdl:part name="deleteReturn" type="tns1:DeleteResponse"/>
</wsdl:message>

<wsdl:message name="putResponse">
  <wsdl:part name="putReturn" type="tns1:PutResponse"/>
</wsdl:message>

<wsdl:message name="putRequest2">
  <wsdl:part name="ccrXml" type="xsd:string"/>
  <wsdl:part name="inputRegistryParameters" type="impl:ArrayOf_tns1_RegistryParameters"/>
  <wsdl:part name="attachments" type="impl:ArrayOf_tns1_CXPAttachment"/>
</wsdl:message>

<wsdl:message name="deleteResponse1">
  <wsdl:part name="deleteReturn" type="tns1:DeleteResponse"/>
</wsdl:message>

<wsdl:message name="putRequest1">
  <wsdl:part name="ccrXml" type="xsd:string"/>
  <wsdl:part name="inputRegistryParameters" type="impl:ArrayOf_tns1_RegistryParameters"/>
</wsdl:message>

<wsdl:message name="deleteRequest2">
  <wsdl:part name="guid" type="xsd:string"/>
  <wsdl:part name="parameters" type="tns1:RegistryParameters"/>
</wsdl:message>

<wsdl:message name="putResponse1">
  <wsdl:part name="putReturn" type="tns1:PutResponse"/>
</wsdl:message>

<wsdl:message name="getResponse1">
```

```
<wsdl:part name="getReturn" type="tns1:GetResponse"/>
</wsdl:message>
<wsdl:portType name="CXP_10">
  <wsdl:operation name="put" parameterOrder="ccrXml">
    <wsdl:input message="impl:putRequest" name="putRequest"/>
    <wsdl:output message="impl:putResponse" name="putResponse"/>
    <wsdl:fault message="impl:CXPException" name="CXPException"/>
  </wsdl:operation>
  <wsdl:operation name="put" parameterOrder="ccrXml inputRegistryParameters">
    <wsdl:input message="impl:putRequest1" name="putRequest1"/>
    <wsdl:output message="impl:putResponse1" name="putResponse1"/>
    <wsdl:fault message="impl:CXPException" name="CXPException"/>
  </wsdl:operation>
  <wsdl:operation name="put" parameterOrder="ccrXml inputRegistryParameters attachments">
    <wsdl:input message="impl:putRequest2" name="putRequest2"/>
    <wsdl:output message="impl:putResponse2" name="putResponse2"/>
    <wsdl:fault message="impl:CXPException" name="CXPException"/>
  </wsdl:operation>
  <wsdl:operation name="get" parameterOrder="xmlData">
    <wsdl:input message="impl:getRequest" name="getRequest"/>
    <wsdl:output message="impl:getResponse" name="getResponse"/>
    <wsdl:fault message="impl:CXPException" name="CXPException"/>
  </wsdl:operation>
  <wsdl:operation name="get" parameterOrder="inputRegistryParameters">
    <wsdl:input message="impl:getRequest1" name="getRequest1"/>
    <wsdl:output message="impl:getResponse1" name="getResponse1"/>
    <wsdl:fault message="impl:CXPException" name="CXPException"/>
  </wsdl:operation>
  <wsdl:operation name="delete" parameterOrder="guid">
    <wsdl:input message="impl:deleteRequest" name="deleteRequest"/>
    <wsdl:output message="impl:deleteResponse" name="deleteResponse"/>
  </wsdl:operation>
  <wsdl:operation name="delete" parameterOrder="parameters">
    <wsdl:input message="impl:deleteRequest1" name="deleteRequest1"/>
    <wsdl:output message="impl:deleteResponse1" name="deleteResponse1"/>
  </wsdl:operation>
  <wsdl:operation name="delete" parameterOrder="guid parameters">
```

```

        <wsdl:input message="impl:deleteRequest2" name="deleteRequest2"/>
        <wsdl:output message="impl:deleteResponse2" name="deleteResponse2"/>
    </wsdl:operation>
    <wsdl:operation name="getVersion">
        <wsdl:input message="impl:getVersionRequest" name="getVersionRequest"/>
        <wsdl:output message="impl:getVersionResponse" name="getVersionResponse"/>
    </wsdl:operation>
</wsdl:portType>
<wsdl:binding name="CXPSoapBinding" type="impl:CXP_10">
    <wsdlsoap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="put">
        <wsdlsoap:operation soapAction=""/>
        <wsdl:input name="putRequest">
            <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://cxp.medcommons.net" use="encoded"/>
        </wsdl:input>
        <wsdl:output name="putResponse">
            <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>
        </wsdl:output>
        <wsdl:fault name="CXPEException">
            <wsdlsoap:fault encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" name="CXPEException"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>
        </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="put">
        <wsdlsoap:operation soapAction=""/>
        <wsdl:input name="putRequest1">
            <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://cxp.medcommons.net" use="encoded"/>
        </wsdl:input>
        <wsdl:output name="putResponse1">
            <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>
        </wsdl:output>
        <wsdl:fault name="CXPEException">
            <wsdlsoap:fault encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" name="CXPEException"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>
        </wsdl:fault>
    </wsdl:operation>

```

```
</wsdl:operation>

<wsdl:operation name="put">

  <wsdlsoap:operation soapAction=""/>

  <wsdl:input name="putRequest2">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://cxp.medcommons.net" use="encoded"/>

  </wsdl:input>

  <wsdl:output name="putResponse2">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>

  </wsdl:output>

  <wsdl:fault name="CXPEException">

    <wsdlsoap:fault encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" name="CXPEException"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>

  </wsdl:fault>

</wsdl:operation>

<wsdl:operation name="get">

  <wsdlsoap:operation soapAction=""/>

  <wsdl:input name="getRequest">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://cxp.medcommons.net" use="encoded"/>

  </wsdl:input>

  <wsdl:output name="getResponse">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>

  </wsdl:output>

  <wsdl:fault name="CXPEException">

    <wsdlsoap:fault encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" name="CXPEException"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>

  </wsdl:fault>

</wsdl:operation>

<wsdl:operation name="get">

  <wsdlsoap:operation soapAction=""/>

  <wsdl:input name="getRequest1">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://cxp.medcommons.net" use="encoded"/>

  </wsdl:input>

  <wsdl:output name="getResponse1">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>

  </wsdl:output>
```

```
<wsdl:fault name="CXPEException">

  <wsdlsoap:fault encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" name="CXPEException"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>

</wsdl:fault>

</wsdl:operation>

<wsdl:operation name="delete">

  <wsdlsoap:operation soapAction=""/>

  <wsdl:input name="deleteRequest">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://cyp.medcommons.net" use="encoded"/>

  </wsdl:input>

  <wsdl:output name="deleteResponse">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>

  </wsdl:output>

</wsdl:operation>

<wsdl:operation name="delete">

  <wsdlsoap:operation soapAction=""/>

  <wsdl:input name="deleteRequest1">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://cyp.medcommons.net" use="encoded"/>

  </wsdl:input>

  <wsdl:output name="deleteResponse1">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>

  </wsdl:output>

</wsdl:operation>

<wsdl:operation name="delete">

  <wsdlsoap:operation soapAction=""/>

  <wsdl:input name="deleteRequest2">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://cyp.medcommons.net" use="encoded"/>

  </wsdl:input>

  <wsdl:output name="deleteResponse2">

    <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>

  </wsdl:output>

</wsdl:operation>

<wsdl:operation name="getVersion">

  <wsdlsoap:operation soapAction=""/>
```

```
<wsdl:input name="getVersionRequest">

  <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://cxp.medcommons.net" use="encoded"/>

</wsdl:input>

<wsdl:output name="getVersionResponse">

  <wsdlsoap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
namespace="http://hostname:9080/router/services/CXP" use="encoded"/>

</wsdl:output>

</wsdl:operation>

</wsdl:binding>

<wsdl:service name="CXP_10Service">

  <wsdl:port binding="impl:CXPSoapBinding" name="CXP">

    <wsdlsoap:address location="http://hostname:9080/router/services/CXP"/>

  </wsdl:port>

</wsdl:service>

</wsdl:definitions>
```

Appendix C: Example code

Example C# PUT call

An example of PUT into a MedCommons Registry shows how to fill in the registry parameter block.

```

cxpsoap2.CXP.RegistryParameters[] inputParameters =
    new cxpsoap2.CXP.RegistryParameters[1];
cxpsoap2.CXP.RegistryParameters inputParameter =
    new cxpsoap2.CXP.RegistryParameters();
inputParameters[0] = inputParameter;
inputParameter.registryName = "MedCommons";
inputParameter.registryId = "medcommons.net";

cxpsoap2.CXP.Parameter []parameterList = new cxpsoap2.CXP.Parameter[4];
parameterList[0] = new cxpsoap2.CXP.Parameter();
parameterList[0].name = "CommonsID";
parameterList[0].value = this.CommonsID.Text;

parameterList[1] = new cxpsoap2.CXP.Parameter();
parameterList[1].name = "SenderID";
parameterList[1].value = this.SenderID.Text;

parameterList[2] = new cxpsoap2.CXP.Parameter();
parameterList[2].name = "RegistrySecret";
parameterList[2].value = this.RegistrySecret.Text;

parameterList[3] = new cxpsoap2.CXP.Parameter();
parameterList[3].name = "NotificationSubject";
parameterList[3].value = this.NotificationSubject.Text;

inputParameter.parameters = parameterList;

cxpsoap2.CXP.PutResponse response = null;

// Send the PUT message
try
{
    response = cxpServer.put(ccrData, inputParameters);
}
catch (Exception ex)
{
    MessageBox.Show("Unknown error communicating with server " +this.CXPServerWDSL.Text
        + "\n" + ex.ToString());
    return;
}
if (response.status == 200)
{
    handleOutputParameters(response.registryParameters);
    this.GUID.Text = response.guid;
    MessageBox.Show(this, "CXP Transfer Success!\nUUID:" + response.guid +
        "\nConfirmationCode:" + this.ConfirmationCode.Text +
        "\nRegistrySecret:" + this.RegistrySecret.Text
    );
}
else{
    // More code here
}

```


Example C# GET Call

```
cxpServer.Url = this.CXPServerWDSL.Text;
cxpsoap2.CXP.RegistryParameters []inputParameters = new
cxpsoap2.CXP.RegistryParameters[1];
cxpsoap2.CXP.RegistryParameters inputParameter = new cxpsoap2.CXP.RegistryParameters();
inputParameters[0] = inputParameter;
inputParameter.registryName = "MedCommons";
inputParameter.registryId = "medcommons.net";
```

```
cxpsoap2.CXP.Parameter []parameterList = new cxpsoap2.CXP.Parameter[5];
parameterList[0] = new cxpsoap2.CXP.Parameter();
parameterList[0].name = "CommonsId";
parameterList[0].value = this.CommonsID.Text;
```

```
parameterList[1] = new cxpsoap2.CXP.Parameter();
parameterList[1].name = "SenderId";
parameterList[1].value = this.SenderID.Text;
```

```
parameterList[2] = new cxpsoap2.CXP.Parameter();
parameterList[2].name = "RegistrySecret";
if (this.RegistrySecret.Text.Length == 0)
    parameterList[2].value = null;
else if (this.RegistrySecret.Text.Length == 5)
{
    parameterList[2].value = this.RegistrySecret.Text;
}
else
{
    MessageBox.Show(this, "Invalid RegistrySecret: Must be a 5 integer string or blank,
not '" + this.RegistrySecret.Text + "'");
    return;
}
```

```
parameterList[3] = new cxpsoap2.CXP.Parameter();
parameterList[3].name = "NotificationSubject";
parameterList[3].value = this.NotificationSubject.Text;
```

```
parameterList[4] = new cxpsoap2.CXP.Parameter();
parameterList[4].name = "ConfirmationCode";
parameterList[4].value = this.ConfirmationCode.Text;
```

```
inputParameter.parameters = parameterList;
```

```
cxpsoap2.CXP.GetResponse response = cxpServer.get(inputParameters);
String output = "GET Response:";
if (response.status == 200)
{
    output += "\n First 200 characters of CCR\n";
    output += response.content.Substring(0,200);
}
else
{
    output += "\n Status = " + response.status;
    output += "\n Reason = " + response.reason;
}
```

```
MessageBox.Show(this, output);
```

Appendix D: Normative Security/Identity Recommendations

The security goals of CXP are:

1. Permit a private/secure mechanism for messages.
2. Only actors with authorization to obtain a document can obtain a document.

How these goals are obtained is beyond the scope of this specification. This appendix discusses mechanisms for how these may be specified using the existing structure of CXP.

CXP is a simple wire protocol. It knows nothing about user identity, security, object identity, or auditing. However, all of these issues are critical to how CXP will be used.

Transaction/Audit logs

A CXP implementation may require that each party initiating a transaction supply an opaque Sender identity token and that both parties maintain an audit log of each CXP transaction so that the logs of each party can be conjoined for forensic problem and dispute resolution. These tokens may be hardwired shared secrets, or otherwise obtained dynamically via methods outside CXP.

The format of these logs is not yet specified. See the SenderID description in the data dictionary appendix below for what types of identifiers are expected.

Trust relationships

CXP can be used in conjunction with a Federated Identity Service such as Liberty Alliance. In this case, the two parties establish a static trust relationship using Liberty, and dynamically use SAML2.0 and SOAP based WSF2.0 to communicate CXP payloads. The initiator of a CXP transaction obtains an opaque Sender identity token from the Liberty IDP and passes it along to his counterpart (the Liberty Service Provider) as above. But instead of hard coded secrets, or cumbersome certificates, the Liberty services permit dynamic interconnection of CXP participants who have signed bilateral business agreements and achieved technical compliance.

When the CXP Receiver is a Document Repository, and there is a separate Document Registry, the CXP transaction initiator (the document source) may choose to have an initial conversation (WSF2.0) with the Registry (e.g. a Liberty Service Provider) to determine which Repository to contact. In this case there is an implied transfer of trust from the Registry to the Repository and the CXP protocol is then utilized as documented herein. When using a Federated Identity Service this initial conversation is mandatory and supplies the same opaque Sender identity token.

Additionally, TLS may be used to define trust relationships between nodes.

Appendix E: Normative RegistryParameters Data Dictionary

The RegistryParameters data structure contains an array of name-value pairs. While these values are currently unconstrained by the CXP specification it is hoped that common elements can be identified in practice and placed in future versions of the standard.

Name	Value	Description
CommonsID	A string containing an identifier	This is the identifier of the account or user that 'owns' the data. This is a portion of a mechanism that provides the ability for (say) User A to put a document into the system for User B.
SenderID	A string identifying the sender of the document.	<p>The SenderID format and semantics are still under development. A SAML assertion or artifact or a certificate are two candidates for inclusion.</p> <p>A SenderID can fall into three basic categories:</p> <ol style="list-style-type: none"> 1. It's unique to an individual 2. It's unique to an organization (and the organization in turn may internally be able to connect this token to a particular user) 3. It's a transaction identifier. From the point of view of CXP this means that the user is pseudonymous but potentially traceable via audit logs on other sites.

Appendix F: Future directions

- MTOM for streaming large binary files.
- Security; details on how SAML identifiers can be passed through.
- Support for non-CCR data validation schemas Such as CCD. .
- Handling encrypted document content (awaits to some degree the ASTM committees)

MedCommons C# CXP SOAP Client

CXP 1.0
3/2/2006

The C# CXP SOAP is a small sample program that demonstrates how to invoke the CXP 1.0 SOAP interface.

Currently only two SOAP calls are supported in this sample: PUT and GET.

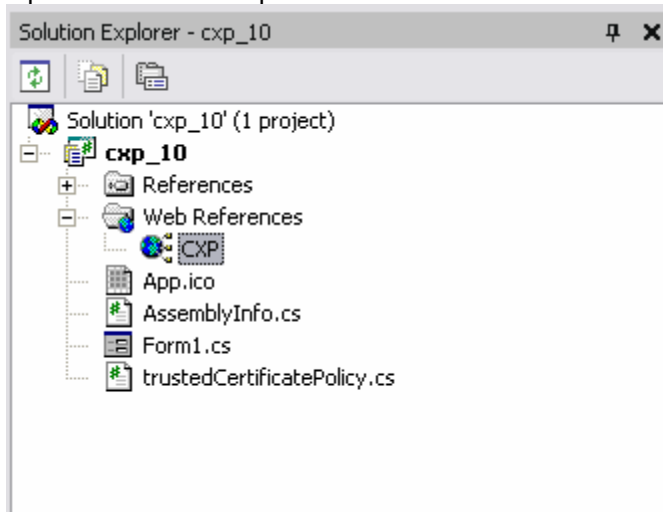
Installing the program

Unzip the file and open the cxp_10.csproj in Visual Studio.

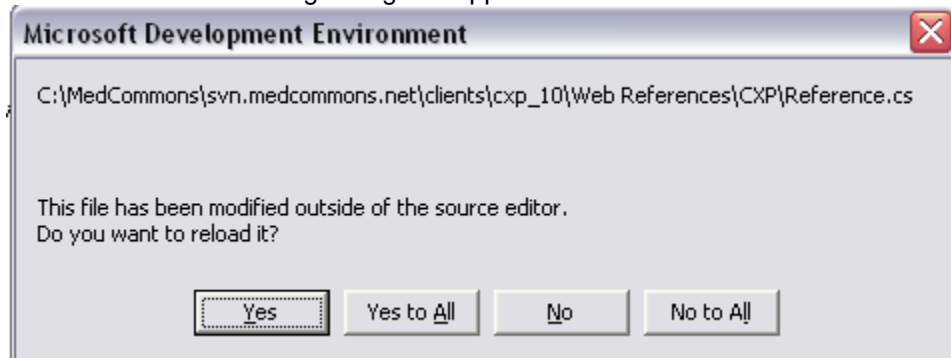
Configuring the program

Typically this program does not need to be configured. If you want to point at a host other than <https://gateway001.medcommons.net/router/services/CXP> then follow these steps:

1. Open the Solution Explorer and select CXP:

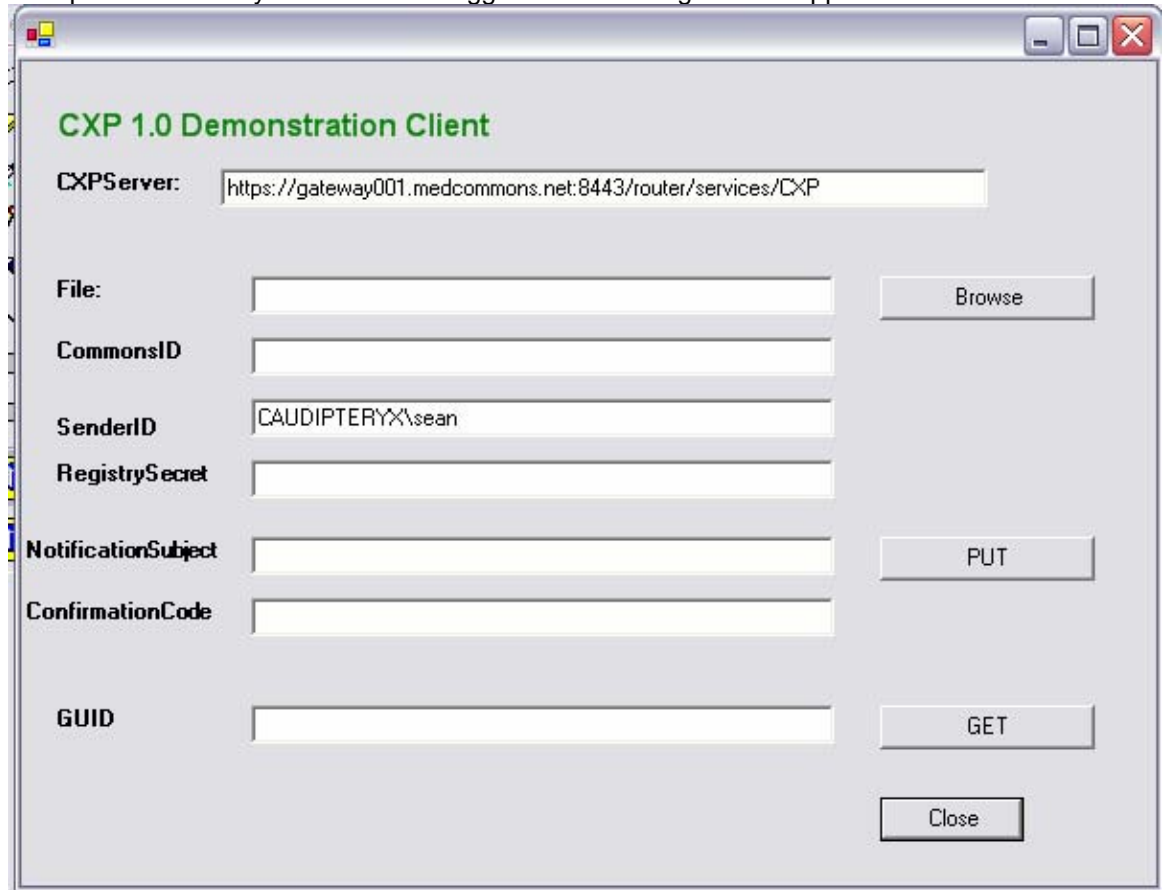


2. Right click and select Properties from the menu.
3. Enter the URL of the WDSL for the new SOAP endpoint.
4. Press Enter. The following dialog box appears:



Select "Yes to All".

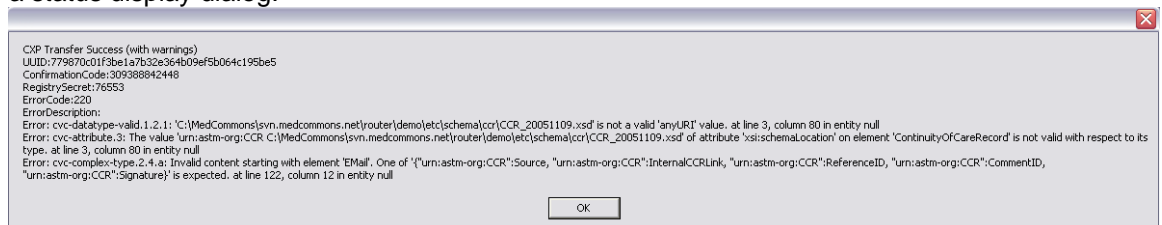
5. Now press the F5 key to start the debugger. The following window appears:



The image shows a window titled "CXP 1.0 Demonstration Client". It contains several input fields and buttons. The "CXP Server" field is pre-filled with "https://gateway001.medcommons.net:8443/router/services/CXP". The "SenderID" field is pre-filled with "CAUDIPTERYX\sean". There are buttons for "Browse", "PUT", "GET", and "Close".

Field	Value
CXP Server	https://gateway001.medcommons.net:8443/router/services/CXP
File	
CommonsID	
SenderID	CAUDIPTERYX\sean
RegistrySecret	
NotificationSubject	
ConfirmationCode	
GUID	

- The SenderID is automatically filled in with your user login information.
6. Click on the browse button to select a CCR, then click the PUT button. This transmits the CCR to the server. If the CCR contains validation errors then these will be enumerated in a status display dialog.



The image shows a status display dialog with the following text:

```
CXP Transfer Success (with warnings)
UUID: 779870c01f3be1a7b32e364b09ef5b064c195be5
ConfirmationCode: 309388842448
RegistrySecret: 76553
ErrorCode: 220
ErrorDescription:
Error: cvc-datatype-valid.1.2.1: 'C:\MedCommons\svn.medcommons.net\router\demo\etc\schemas\cor\CCR_20051109.xsd' is not a valid 'anyURI' value. at line 3, column 80 in entity null
Error: cvc-attribute.3: The value 'urn:astm-org:CCR C:\MedCommons\svn.medcommons.net\router\demo\etc\schemas\cor\CCR_20051109.xsd' of attribute 'xsi:schemaLocation' on element 'ContinuityOfCareRecord' is not valid with respect to its type. at line 3, column 80 in entity null
Error: cvc-complex-type.2.4.a: Invalid content starting with element 'EMail'. One of '{urn:astm-org:CCR':Source, 'urn:astm-org:CCR':InternalCCLink, 'urn:astm-org:CCR':ReferenceID, 'urn:astm-org:CCR':CommentID, 'urn:astm-org:CCR':Signature} is expected. at line 122, column 12 in entity null
```

OK

7. The application dialog box automatically has the ConfirmationCode and RegistrySecret filled in:

CXP 1.0 Demonstration Client

CXPServer:

File:

CommonsID

SenderID

RegistrySecret

NotificationSubject

ConfirmationCode

GUID

8. Clicking the “Get CCR” button will now retrieve the CCR for this ConfirmationCode and RegistrySecret.

Get returned:
<?xml version="1.0" encoding="UTF-8"?>
<ContinuityOfCareRecord xmlns="urn:astm-org:CCR" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:astm-org:CCR C:\MedCommons\svn.med...

- 9.

Only the first 200 characters of the CCR are displayed. In a real application the CCR would be saved to disk or would be imported into the application.



Healthcare Information Technology Standards Panel (HITSP)

Use Case #2

Consumer Empowerment: Registration and Medication History

Version 1.0

January 18, 2006

**Office of the National Coordinator
For Health Information Technology
(ONC)**

1. Use Case Revision History Table

Version	Description of Change	Name of Author	Date
----------------	------------------------------	-----------------------	-------------

Number			Published
V0.1	<i>Comments inserted prior to work group conference call on Dec 20</i>	<i>Alison Rein</i>	<i>Dec 16</i>
V0.11	Edits	Charles Parisot	Dec 19
V0.2	Edits	Charles Parisot	Dec 29
V0.3	Edits	Charles P. with comments from Alan Z., Kiang S., Lynne G., Noam A.	Jan 3, 2006
V0.3.1	Edits from Dec 5 th face to face meeting	Charles	Jan 5 th , 2006
V0.3.2A	Edits from e-mail feedback	Charles-Does not include the Events/Action section edited by Alan.	Jan 8 th , 2006
V0.3.3A	Edits from WG feedback	Charles-Only first part Comments from Noam, Lynn, Alan, Alison.	Jan 11 th , 2006
V0.3.4A	Edits from WG feedback	Entire UC WG distribution. Explicit OK from Lynne, Chantal, Input from Alison included. OK from Alan.	Jan 16 th , 2006
V1.0	Final Version	Ingram/Sensmeier	Jan 18 th , 2006

2. Description of Use Case

This use case establishes a framework for constructing two fundamental building blocks of a personal electronic health record– the registration summary and medication history. These initial building blocks, that are potentially a part of a broader set of personal health information, will allow consumers to share registration information and their list of medications with their health care providers and other authorized parties. Since consumers and their care providers have the potential to know the most about their core health information, such as medication use, it is essential that this use case puts the consumer (and authorized care providers) in control.

In addition to providing access to key health information, this approach of making the consumer be responsible for their health information will also improve consumers' awareness of their own health portrait, educate consumers about the importance of sharing this set of consistent information with their health care providers, and facilitate important communications between various health care providers.

3. Scope of Use Case

This use case establishes two building blocks for personal health records – registration and medication history. It is important to note that there are additional elements of health information that need to be defined in the future to have a complete picture about a consumer. This use case document defines the health information exchange services that will allow access to this information, by a variety of applications supporting consumers, providers and others. It is also not the intent of this document to spell out what a PHR application looks like on a screen to consumers and providers, rather what functions need to be in such an application and the interoperability needed with other health information systems.

- **Registration Summary:** In this use case, registration summary includes the demographic and financial information consumers generally need to provide when visiting a physician, hospital, or pharmacy, such as:
 - Identification information sufficient to help identify the consumer;
 - Financial information sufficient for eligibility checking and claims processing;
 - Emergency contact, advance directives, and donor information.
 - Typical demographic and financial data elements.

The summary may be expanded to include more clinically relevant information, such as allergies and health history. More complex clinical fields, such as chief complaints and current problem lists should be assessed but may be out of scope of a registration summary.

- **Medication History:** In this use case, medication history will contain sufficient information about the consumer's medications to enable the following functions:
 - Create and update medication history
 - Update medication history – medication history is updated by the following methods (This would include correcting errors, deleting redundant information, adding new medication, etc.)
 - View medication history - medication history is viewed by physician, pharmacist, consumer, etc. (distinguishes different sources of data and source of updates)
 - Review medication history with consumer - clinician and patient review medication history together
 - Analyze medication history for compliance
 - Utilize medication history for interaction checking with other drugs or allergies – clinician/system checks medications against other medications being taken or prescribed for interactions and allergies
 - Utilize medication history to trigger a renewal to the pharmacy
 - Differentiate current medications from relevant past medications –
 - Deliver patient education information (may be a future deliverable)
- **Populating the consumer electronic health record:** It can be assumed that registration and medication history can be made available to a PHR system through multiple sources, each with a different level of accuracy and completeness. To pre-populate the consumer electronic health record, consumers can choose their preferred source to build up the PHR. Over time, it is expected that additional sources will be available as a choice to the consumers. For example, the consumer's medication history may be available from:
 - Paid claims through their drug benefit program at a payer or Pharmacy Benefit Manager,
 - A Provider's Electronic Health Record system (EHR-S),
 - The consumer with or without assistance from other authorized parties such as health care providers (e.g., pharmacist or nurse) or a family member/caregiver.
- The source of the data (i.e., Provider, PBM, Payer) as well as a dated access log must be identifiable to consumers and their care providers. Inconsistencies between these sources will likely become apparent, and applications, institutions, and individuals will need to figure out how best to integrate and/or consolidate these data.
- **Data Access:** Consumers would have access to their own information, and could identify and authorize other parties to access some or all of their information. Access could be granted to other authorized users on a selective basis (i.e., physician offices or hospitals could be granted authority for a specific time period or content), or an "on-demand" basis (i.e., physician offices could be granted authority to query a consumer's information permanently or upon presence of the consumer in their care delivery facility), or some combination of the two. Regardless of frequency, upon initial creation consumers would establish the protocol for these permissions.
- **Privacy:** The issues of privacy, security and appropriate data use are well within the scope of this use case, and integration profiles/implementation guides should include the necessary interoperability security standards. However, setting policies that will apply to the broader system is not within scope of this use case. Privacy policies are needed to ensure secure and appropriate data usage, particularly in cases of sensitive information and special populations (e.g. adolescents and other for whom unintended disclosures to family members or other providers could be implied from medication lists). Specific scenarios for patients withholding information must be considered in a policy framework, and these scenarios must also be considered in the context of the HIPAA rule, which in some cases does not provide the intended baseline level of consumer privacy (e.g., consumers and many PHR Systems vendors are not covered entities). In addition, malpractice and/or state law implications of information non-disclosure need to be evaluated.
- **PHR Application Behavior:** As part of this use case, a minimum functional specification for PHR systems (*Consumer health record is the data, "PHR System" is a software application*) that will directly serve the consumer will be established in order to provide consistency and portability to consumers. It is not within the scope of this use case to define the detailed "PHR application behavior" that consumers will see: whether consumers could select to have prescription medication and/or other core health data "imported" into their application, or if the application could simply prompt consumer users to review their data on a regular basis to determine whether it is complete and current. Similar data elements could be imported from multiple data sources. Applications should be expected to

provide some support for achieving data harmonization across sources. But no solution should be expected in automatically providing a reconciled and complete medication history.

- **Assumptions:** This use case will not detail properties such as the means to ensure data consistency, audit trails, accountability, system integrity and management of patient consent. These will be addressed in further technical definition steps (standards selection/profiling/integration and architecture designs) that are beyond the use case definition.
- **Future Scope:** Although Public Health is mentioned in this use case as a stakeholder, it is recognized that it may initially play a small role, but could be expanded in the future.

4. Stakeholders for Use Case

Primary Actors:

Healthcare Consumers (including authorized family members/care givers)

- Clinicians/Medical institutions
- Ancillary service providers (Pharmacy, Lab, Imaging, etc.)
- PHR System Service Providers serving consumers
- Data Suppliers (e.g., pharmacy, payers, PBMs, providers)
- Public health agencies (Local, State, Federal)

Outside affected:

- Employers
- Emergency clinicians or others with whom the patient has no formal relationship⁷.
- Schools

5. Preconditions for Use Case

- Established network and policy infrastructures to enable consistent, appropriate, and accurate information exchange. This includes, but is not limited to:
 - Rules for identification of a consumer
 - Rules for identification of the health information sources of a consumer
 - Rules for establishing how data corrections do or do not get propagated back to the network.
- For providers with a Provider EHR system, these need to support appropriate interfaces to a standardized communication and policy infrastructure for communication with other systems, including PHR systems. It would not be acceptable to re-enter the same information twice for those care providers.
- PHR Systems offering their services to subscribing consumers with appropriate interfaces to a standardized communication and policy infrastructure.
- Pharmacy systems with appropriate interfaces to a standardized communication and policy infrastructure
- Data Supplier systems with appropriate interfaces to a standardized communication and policy infrastructure
- Consumer education and support for appreciating the essential concept of an electronic consumer health record
- Health care provider education and support for appreciating the essential concept of a consumer health record and associated protocols

6. Obstacles to Implementation of Use Case

- Establishment of harmonized and/or standard coding, functionality, and definitional requirements.
- Need to undertake a considerable education and outreach campaign targeting all relevant stakeholders, and informing them of their rights and responsibilities under the new paradigm.

⁷ In cases where patients (or authorized patient proxies) withhold important clinical information from emergency clinicians or others with whom the patient has no formal relationship, those clinicians and medical institutions may not have the complete information they need to deliver optimal care. It may not be known to them at the time, but they are considered stakeholders nonetheless.

- Posing a particular challenge will be the necessary outreach and education to disadvantaged, uninsured/underinsured, low tech, low health literacy and other hard-to-reach target populations.
- Need for high tech and low tech access means for consumer and care providers.
 - **Absent appropriate and proactive policy deliberations, people may be exposed to grave risks of employment or insurance discrimination, or other commercial exploitation if information is shared inappropriately. Specifically, the increased risks in a networked environment include:**
 - *Secondary use of data*, including the use of medical data for employment or welfare purposes; to restrict credit or other financial benefits; or in unsolicited marketing;
 - *Security breaches*, including hacking and other criminal activities that lead to “data leakage”;
 - *Criminal misuses of data*, including fraudulent acts or identity theft that result in financial or other harm; and
 - *Data quality issues*, including data corruption and loss.

- Protecting personal privacy – and engendering trust in the overall network – is not a matter of any single statutory, contractual, or technological provision. Technologies should be designed to provide security and privacy protections, and policies must both protect against any inappropriate disclosures and provide remedies for when they might occur. The public - all of us - must be confident that personal information will not be misused or disclosed inappropriately. Without such confidence, any identified breakthrough is likely to encounter significant opposition, both at its inception and throughout its existence.
- Current authentication and authorization technologies may be too expensive or cumbersome for widespread deployment.
 - Establishment of standard protocols to deal with tension arising due to potential conflict between consistent/accurate information and up to date information.
 - Lack of policies protecting consumers from denial of healthcare. Cost of service. Consequences with restriction of information to a given provider and impact to consumer care.
 - Consumer/provider frustration with variability of look, feel, interface for different PHR applications, inconsistent medication information
 - Providers will need to determine whether they are adequately comfortable with data quality/accuracy such that they would want to use data from electronic personal health records.

7. Post-conditions for Use Case

- Essential registration and medication history will be available electronically to participating consumers and designated health care providers.
- Consumers will have information needed to identify, reconcile, and use their health care data.
- PHR applications and data sources will need to ensure that the information shared is not misinterpreted or misused.
- Duplicate entries avoided, increases accuracy of information

8. Detail of Use Case Perspectives and Scenarios

8.1 Overview of Use Case Perspectives and Scenarios

The following entity-driven perspectives are part of the use case, which is organized around three scenarios:

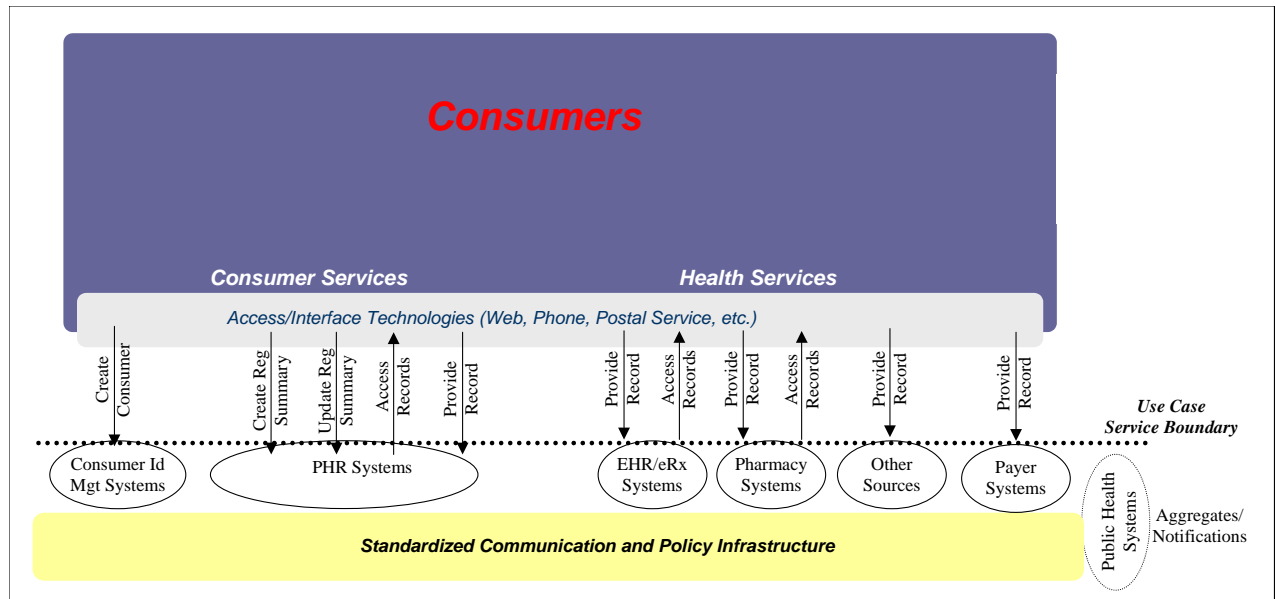
- Pre-encounter
- Encounter
- Post-encounter

Within these scenarios, a number of perspectives are defined to reflect the participation of the primary stakeholders. These primary four perspectives are used:

- Consumer
- Care Provider
- Pharmacy

d. Payer

Below is a visual illustration of the use case. Only the services provided are described at the “boundary” where the requirements for the use case are abstracted. A use case focuses on requirements, and these are introduced in terms of high-level services at the “service boundary” behind which all computers, application software, telephone, postal service, media, networks, security infrastructure exist. The definition of information flows, location of persistent information, network or interchange media transport, transactions among the various “elementary” systems will be defined once the use case requirements are stabilized. This is part of the solution design (including standards selection, profiling and integration).



The elementary systems (ovals) may be grouped as desired (e.g. an EHR application or a payer system may also offer a PHR application). Such combinations are implementation decisions and left open by the use case. The term EHR system should be understood in a broad sense. It includes systems maintained by hospitals, physicians, and other providers. It can also accommodate providers without a clinical application or a practice without an EHR system, accessing the services of this use case with the intent to simply print a medication history on paper and place it in the consumer’s chart.

The term “record” is used in a generic manner to designate a group of closely related health information produced by a single source (e.g. a consumer, payer, pharmacist, provider, etc.). In this use case, a record may be “the most recent consumer created registration summary”, or “medication history along with contextual information such as problems, allergies, etc.”. In the context of another use case, such a record may be a laboratory report.

The following types of high-level services have been identified (see figure above):

1. **Create Consumer**

The consumer opens a personal health record for its use. A display of a minimum set of demographic information used for identifying the owner of the record is shown (*consent designation may also be displayed if desired*). This results in an “empty” health record. This registration may have to be mediated by trusted entities. Permissions are established by the patient for a number of entities to provide and/or to access health information. This creation is a preliminary to selecting (or being assigned) a specific PHR system service provider. As consumers need to be empowered to change PHR system service providers, their identity has to be maintained independently from any PHR system.

2. **Consumer Creates and Updates Registration Summary**

The consumer using the services of his/her PHR service provider accesses an application allowing the creation and later any update of

the consumer registration summary. Once approved by the consumer this consumer registration summary is made available to the consumer and to the entities it authorizes.

3. *Consumer Provides and Accesses Records*

The consumer through a PHR system accesses his/her own records made available by authorized sources. In particular, medication lists made available by multiple sources are available to be viewed in an appropriate format with the status of the medication (prescribed, dispensed, claimed, administered, etc). The consumer may easily identify the source of entries in the medication list, “add, update or correct” by providing a new record.

4. *Care Provider Provides and Accesses Records*

The care provider provides and accesses records through his/her own EHR or Rx system when authorized by the consumer. In particular, medication lists made available by multiple sources, including consumer are available to be displayed along with the status of the medication (prescribed, dispensed, claimed, administered, etc). Care provider makes available pre-existing or new records through his/her own EHR or Rx system.

5. *Other Health Information Source Provides Record*

Other sources of medication records, including payer Systems permitted by the consumer makes available pre-existing medication records and new records as they become available, through their information systems (Pharmacy, Payers, etc.).

6. *Public Health Access and aggregate records*

This is a future service where public health at regular intervals (hour, day or week) may access the newly created records and extract information of interest and aggregate statistics for public health management, applying the appropriate policies.

It is beyond the scope of this use case to define the usage of the information collected (e.g. bio-surveillance notifications).

8.2 Detail of Use Case Perspectives and Scenarios

The following entity-driven perspectives will be part of the use case:

1. Consumer Perspective – includes patient, family members, and other authorized caregivers
2. Provider Perspective – includes physicians, hospitals, other clinicians, nurses, front desk, and other support staff. Also includes the front desk and support staff of laboratories, imaging centers, and other ancillary services that will use the registration summary and medication history from the same perspective as physicians and other health care providers. Includes EHR and e-prescribing systems used in health care delivery
3. Pharmacy Perspective – includes pharmacists and includes pharmacy information systems used in filling prescriptions
4. Payer Perspective – includes PBM and claims processing systems use to pay medication claims
5. PHR System Perspective – includes PHR information systems (as identified in the figure in section 8.1) owned and operated directly by any of the four perspectives listed above as well as stand alone commercial PHR systems, or services operated by employers, professional societies , or regional organizations when they act as certified PHR System providers. This perspective also includes the standardized communication and policy infrastructure (see section 8.1) that supports information exchange, including regional information networks and organizations.

The use case will be presented in three scenarios:

- a. Pre-Encounter and Pre-Population Scenario – All activities that must be completed before the first time the PHR is used.
- b. Encounter Use Scenario – Use of the consumer’s electronic health record during a physician visit,

- pharmacy visit, or interaction with a payer; includes patient providing registration and medication data, updates entered, and a new patient version generated for the next use.
- c. Post-Encounter and Home Use Scenario – Review of information in the consumer’s electronic health record at home following an encounter including entry of Patient information while the patient, family members or other caregivers are using the system on their own. This scenario also includes any use of the consumer’s electronic health record by a single perspective that is not part of an encounter between two or more parties centered around some type of health care event.

The PHR System perspective is somewhat of an artifact and mixture of alternatives that is included as a separate perspective to help visualize the events, actions, and information exchanges that take place as part of the use case. The PHR System is what the consumer sees when they use the system, but unlike the physician’s EHR, the pharmacist’s pharmacy information system, or the insurance company’s claims processing system; the consumer’s PHR System will typically not be owned and operated by the consumer themselves. When a provider, pharmacy, or payer; also provide the PHR system directly to their consumers, they will actually play two separate roles including their traditional role as well as the PHR system role.

The details of this use case are intended to be very inclusive and support very rapid deployment of the limited initial scope of the breakthrough using technologies ready for deployment to large numbers of people during 2006 using Katrina Health as a model of pre-population with existing digital data and ease of widely available access. The details include information flows for providers who use an EHR system or e-prescribing system and for those who do not. The approach should be compatible with EHR integrated PHR systems that present a patient view of the EHR data, as well as free-standing and dedicated PHR systems that import and export data to one or more EHR systems and other information systems. The details of the use case are intended to facilitate, encourage, and simplify adoption of e-prescribing and EHR systems among physicians who do not yet use these technologies. The details of the use case are intended to provide the framework for implementing the work and recommendations of the Office of the National Coordinator for HIT, the Commission on Systemic Interoperability, and the American Health Information Community.

The work group agreed to use the term “Access Media” to refer to a wide range of implementation options that a patient can present at home and at any health care location to gain access to their PHR and enable their current provider, pharmacy, or payer to interact with their PHR. Use of patient-controlled and patient-provided access media allows the patient carry their own virtual universal health identifier through their travels through the health care system. The details of the use case should thus be applicable to settings where an NHIN is available to provide authentication and identification services for patients, providers, and information systems including a record locator service that identifies the location of the patient’s information and the method for exchanging information between a provider’s EHR and the consumer’s electronic health record. The details will also work in regions where an NHIN is not available and these same services may be provided along side the PHR system giving access media tools directly to the consumer.

“Access Media” could be as simple as a web page printout with a URL and account number or username that is provided by the PHR system at the time of web-based registration; or it could be a sophisticated hardware token or smart card carrying digital certificates, automated login software, or even an extract of the consumer’s electronic health record with a digital signature and encryption to authenticate the source and affirm that modifications were made while the data was in the hands of the patient. Some form of access media is central to the use case and could be presented by the patient at each encounter either carrying a copy of the registration and medication data or enabling access to the information. This access media must be capable of use in emergency situations, and ideally should have both human readable and machine readable information necessary to establish a connection, but still require a password or other security method to gain full normal access to the consumer’s electronic health record.

In the following details, the consumer’s electronic health record is called a PHR. A PHR is the set of health related information that a number of care and service providers have released for sharing with the consumer and any other care or service providers. This includes information generated by care or service provider systems (e.g. Pharmacy information systems, physician and hospitals EHR Systems, etc.) as well

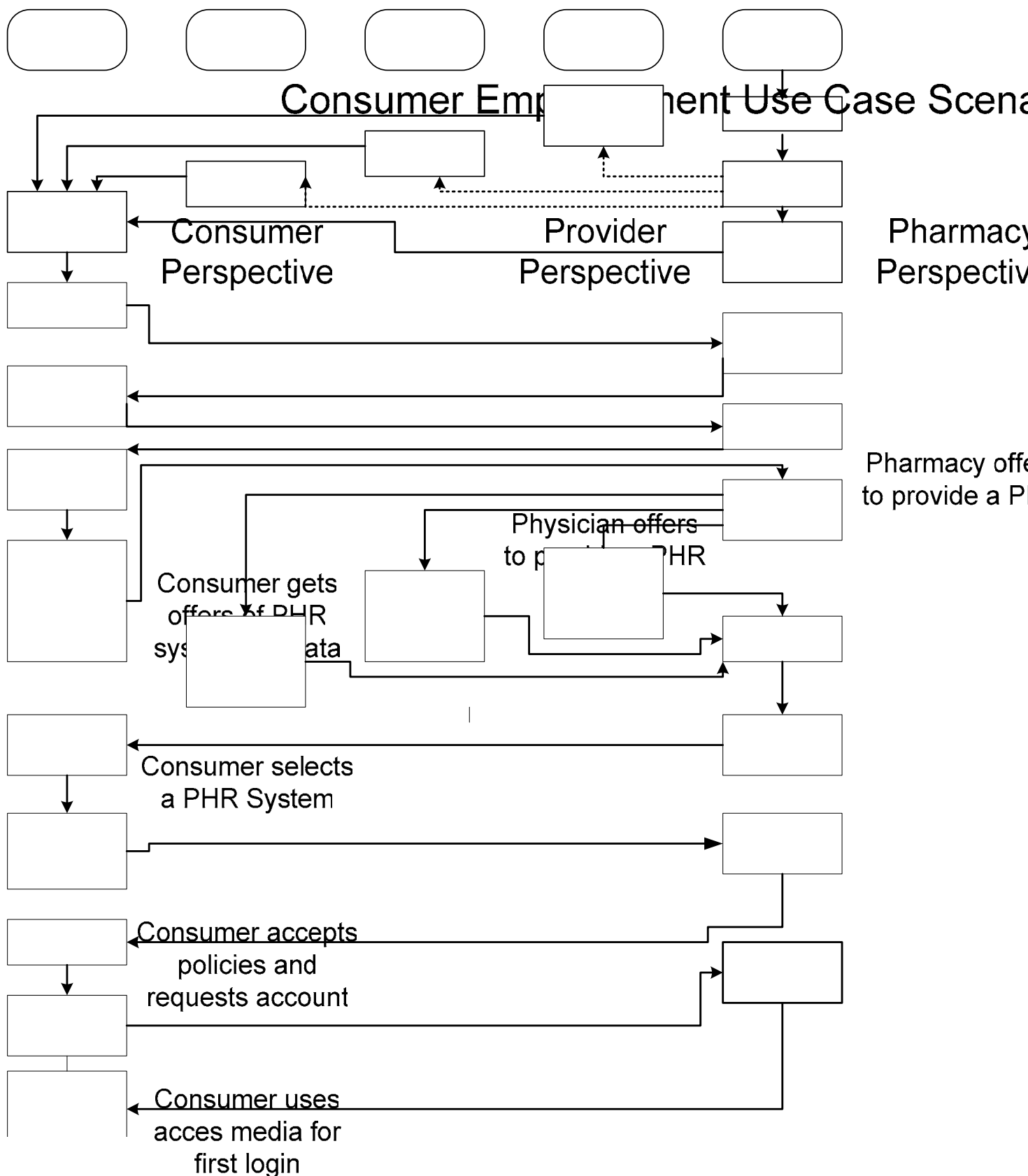
as patient generated information. The “PHR” is health information (e.g; medication, problems, allergies, etc.) and is not to be confused with the **PHR System** that supports the consumer’s access and contribution to the PHR. No assumption shall be made that the PHR information (in the sense defined in this use case) is stored in the PHR System.

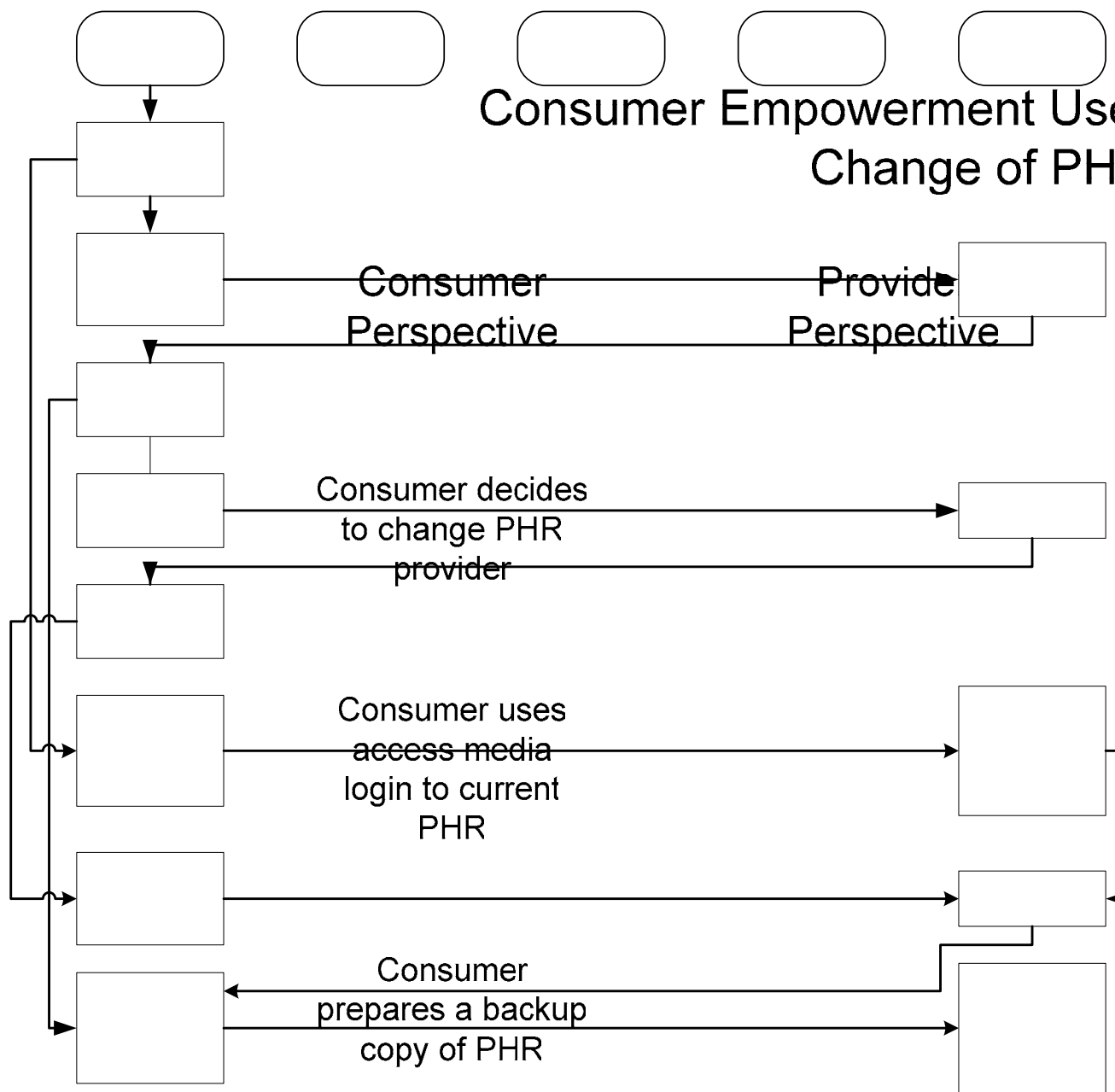
The level of detail included is intended to identify functional requirements and settings where interoperability will take place without specifying technologies, standards, and methods of implementation. In some cases, common Internet standards such as digital signature and XML are used to imply the required functionality of being able to authenticate the source of a document and detect changes to the content, or the ability to send data in both machine readable and human readable form. This level of detail is intended to ask questions and set an agenda rather than to provide definitive answers. Many of the details are included for illustration only.

When registration summaries or medication histories are implemented, it is important to preserve and protect the original sources of the data. A prescription or medication order actually has two sources including the physician or other clinician who prescribed or ordered the medication and the source of the information about the medication. Sometimes information about a prescription will come directly from the physician who wrote the prescription and sometimes it may come from the pharmacy, the PBM, or even the EHR of another physician who is aware of the medication. The identity of both sources (the prescriber and the information supplier) should be preserved wherever possible in this use case.

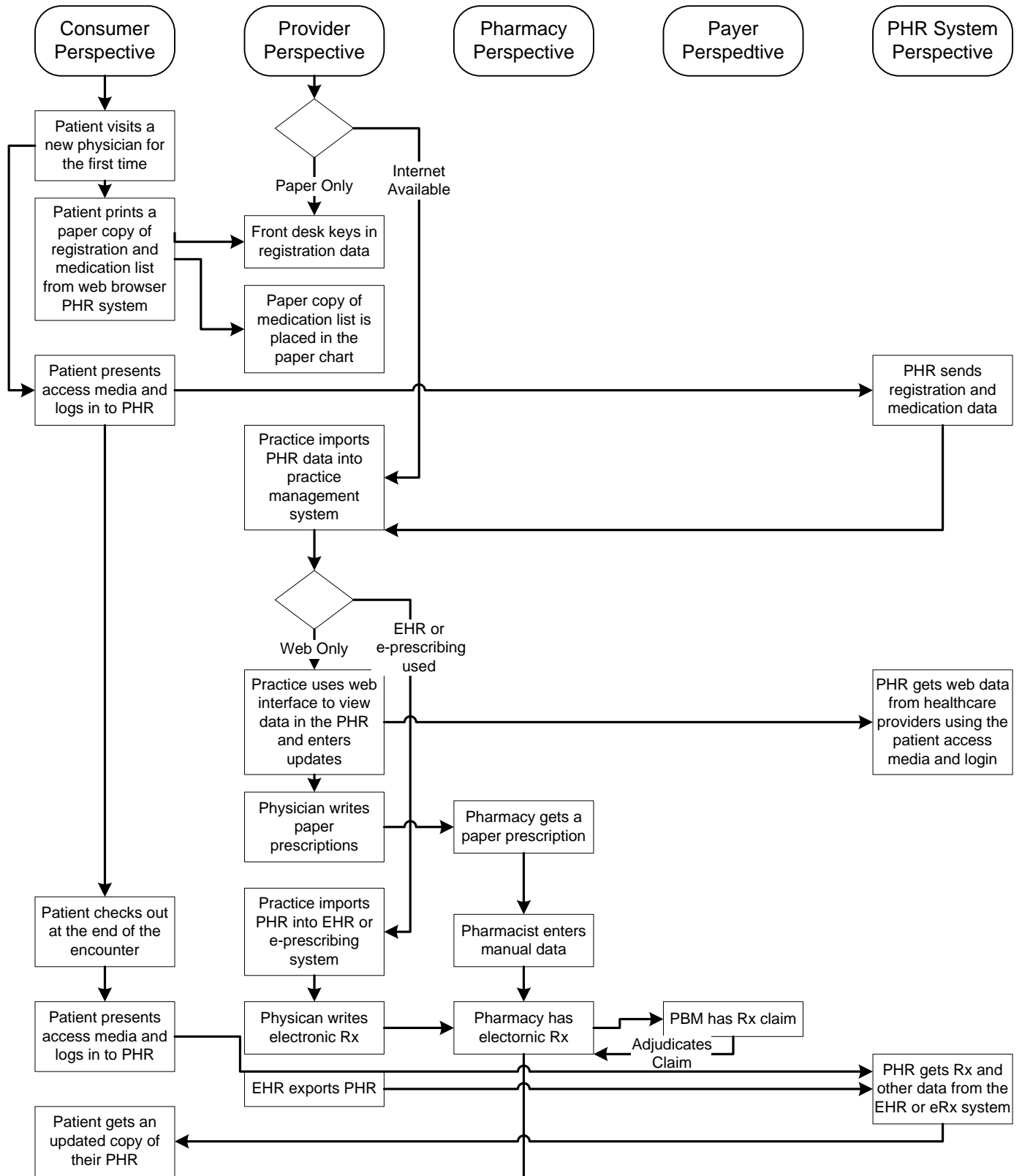
Not only is a PHR patient-centric combining data from all providers and other data sources, it will often need to be implemented in a family context where parents might create accounts for all of their children. A PHR is more than the sum of all information shared by providers’ from their EHR systems that all family members are represented in. On the other hand the information shared by each source EHR Systems or eRx System is intended to be used by a wide range of care and service providers directly, and thus the consistency of that information will have to be preserved. These are among the open issues that will need more study as the standards for this use case are harmonized and evolve into a common interoperability framework.

Close examination of the use case details will reveal many opportunities for the Federal Government to provide leadership by example in the marketplace. Medicare, Medicaid, and the Federal Employees Benefit Program; could become early adopters of an access media strategy that could help their deliver medication lists and linkages to formulary information for their beneficiaries. The Veterans Administration and Department of Defense already provide a consumer portal to their EHR systems and adding an access media could allow that information to be shared with community based providers and hospitals when their patients or beneficiaries are seen in facilities that are not part of their electronic medical records.

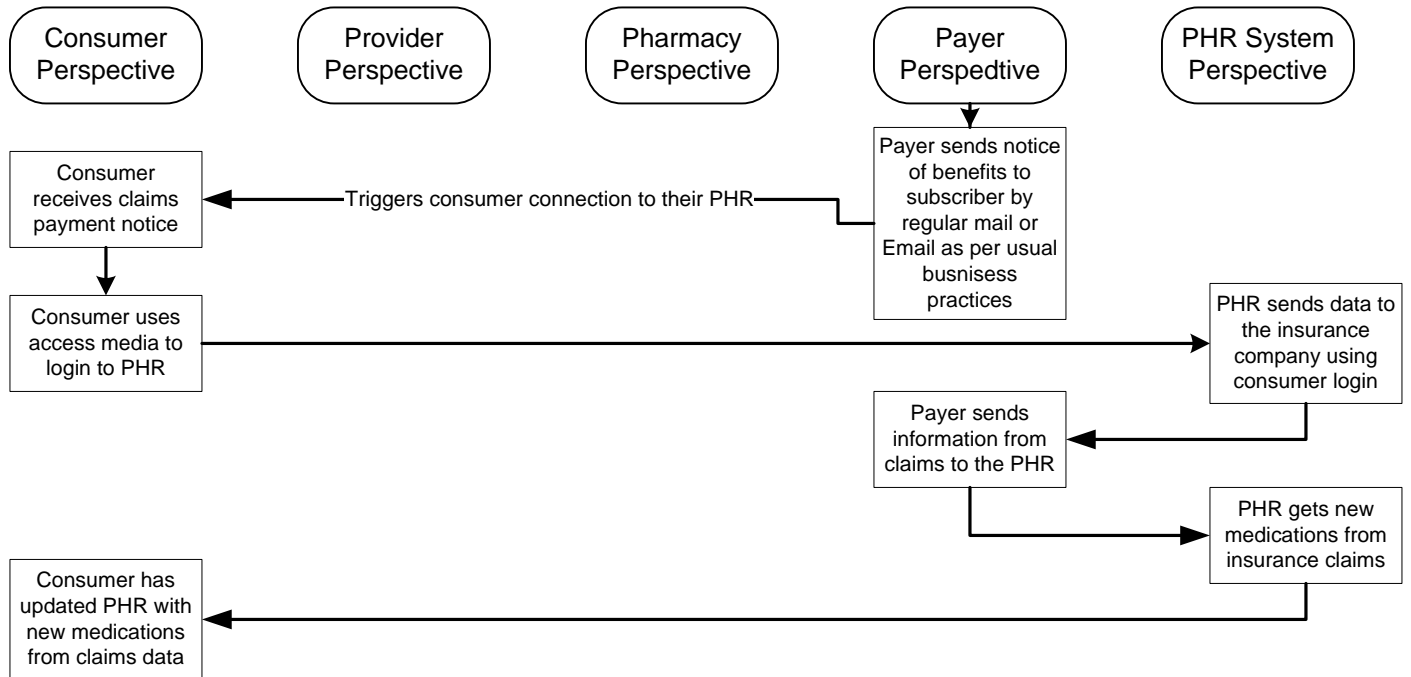




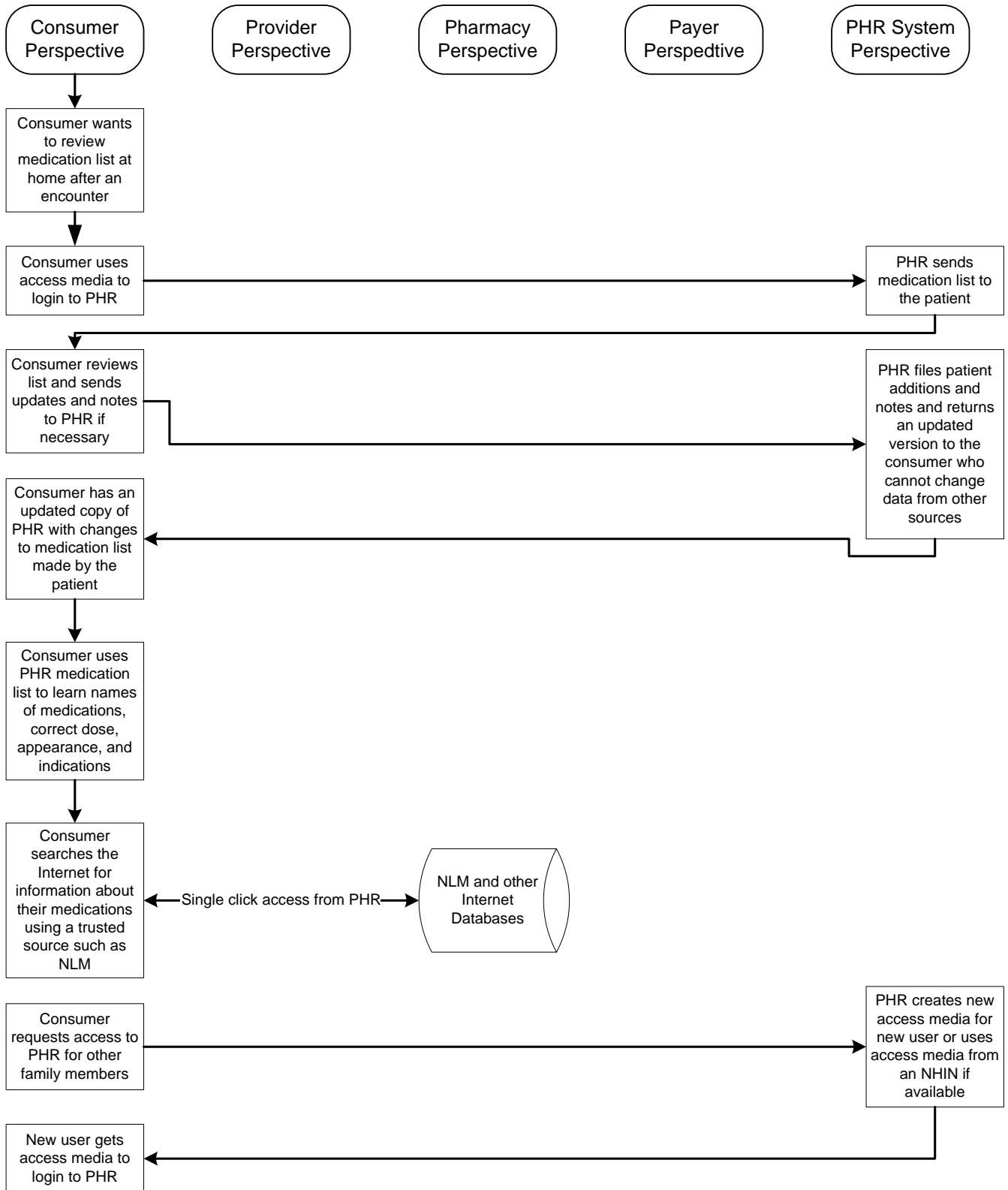
Consumer Empowerment Use Case Scenario b: Encounter Use Scenario



Consumer Empowerment Use Case Scenario b2: Encounter Use Scenario Using Claims Data to Update PHR



Consumer Empowerment Use Case Scenario c: Post-Encounter Use Scenario



2a.1 Consumer Perspective – Pre-Encounter and Pre-Population Scenario

Code	Description	Comment
2a.1.1.0	Event: Patient receives offers to provide or populate a PHR	Patients must be made aware of the option to have a PHR from a specific entity with which they have an existing relationship. The insurance company, health care provider, employer or other entity can offer to provide data, access to their own patient portal, or the full service access to all of the data from all sources including the patient.
2a.1.1.1	Action: Insurance company or PBM offers to provide a PHR or populate a record	
2a.1.1.2	Action: Pharmacy offers to provide a PHR or populate a medication list	
2a.1.1.3	Action: Physician or hospital offer to provide a PHR or populate a record	
2a.1.1.4	Action: A regional network, Employer, or private PHR vendor offer to provide a PHR	A national or regional service provider may be the preferred option. An employer who is not also acting directly as the payer fits this option but must respect appropriate privacy controls
2a.1.2.0	Event: Patient selects a PHR system provider	Patients should select one and only one primary PHR System provider that will link all of their information, but they still can use patient portals from other systems
2a.1.2.1	Action: Patient signs up with their chosen PHR provider and requests an account	May be as simple as answering an Email or going to a web site
2a.1.2.2	Action: Patient receives privacy and other policy information from the PHR System for review prior to finalizing the request for service	Informing and educating the patient about the privacy policies and potential disclosure of the information is an essential pre-requisite to obtaining patient consent to create and operate an account
2a.1.2.3	Action: Patient accepts policies and creates a username and password if required	The type of authentication will be determined by standards and business practices of the PHR system. Creating the login probably should include an explicit step such as clicking a box or radio button to indicate having read and agreed with the privacy policy and giving consent for everything implied. A reasonably uniform privacy policy should be required for all PHR systems so that patients will not be confused by assurances that other vendors may have made to their friends and associates and just in case patients do not read all of the information provided.
2a.1.2.3.a1	Alternative Action: If a local NHIN is available, the NHIN login methods and access media will be used	
2a.1.2.4	Action: Patient receives the access media	The access media has enough information to establish a connection and start authentication. Can be as simple as printing the web page confirming creation

Code	Description	Comment
		of the account and accepting the username and password
2a.1.3.0	Event: Patient authorizes pre-population from specific data sources	Patient authorization is required to access another information system
2a.1.3.1	Action: Patient requests that the PHR System obtains registration and medication data from specific sources using the patient provided access media	Ideally this will be linked to offers of information that originally came from the data source so that the right patient will be identified automatically. The request must include consent to release medical information.
2a.1.4.0	Event: Patient reviews pre-population data from existing sources, makes corrections and notes, and adds additional data	
2a.1.4.1	Action: Patient displays the data obtained from claims, EHR, e-prescribing, and pharmacy systems; and adds notes to medications that may be inactive or errors and adds additional notes. Patient never changes the original data.	
2a.1.4.2	Action: Patient enters additional medications or registration data including over the counter and alternative or herbal medications.	Resources for coding of medications or look-up from NDC codes on packages must be part of the PHR application. The patient might be the only source of registration and medication data if no other digital data is available.
2a.1.5.0	Event: Patient authorizes access by other family members and other caregivers or providers	This step is essential for parents of young children
2a.1.5.1	Action: Patient authorizes access by other users	Privacy policy for adolescents is complex and there are no fixed standards for when children gain access to their records and when they become the primary custodian and controller of who may use the record
2a.1.5.2	Action: PHR system provides access media for other users	Might be as simple as a family member entering a username and password in the presence of the patient. Authentication credentials should always be person specific and patients should not give their primary password to family members, but a parent could use the same login for all of their children. These credentials could come from an NHIN if one is available. If an NHIN is not available, it is not reasonable to expect all health care providers to create authentication credentials in all PHR systems for all patients. Until we have a common provider authentication systems as part of an NHIN, the patient can provide temporary authentication to each provider as needed at each encounter. Sometimes, special circumstances such as a home monitoring program for medication use might justify a provider login similar to a family member login.
2a.1.6.0	Event: Patient gets a first look at the ready to use PHR	
2a.1.6.1	Action: Patient displays the record on the screen and makes a paper and optional electronic copy to carry and use at all future encounters, perhaps using their access media to carry data	If the data sent to a web browser is in XML, it can be saved to electronic media, printed from a web browser, or used directly by an information system for interoperability because it will include standard tags to identify data fields. If the data contains a digital signature, it is possible to have third party

Code	Description	Comment
		authentication by the software certification agency that it comes from a specific certified PHR software and system provider, and data has not been modified since it was created by that PHR System. An XML digital signature will also specify the cryptographic methods used and identifying both the signer and the dates of valid PHR software certification.
2a.1.7.0	Event: Patient decides to change PHR System provider	This type of change may occur because of a patient move to another region or a change of job, insurance, or physician. This is an essential service and not always related to cost or satisfaction with service from the original vendor. If an NHIN with a patient locator service is available, this could be as simple as changing the PHR location in the Record Locator Service.
2a.1.7.1	Action: Patient prepares an electronic copy of their PHR	
2a.1.7.2	Action: Patient selects a new PHR system and opens an account and creates a login	Could use a login previously provided by NHIN if one exists
2a.1.7.3	Action: Patient notifies the old vendor of the change the new vendor and account so that data can be transferred, the old account closed, and any queries to the old account forwarded to the new vendor and account	Data transfers, but authentication may not be transferable so the new account must be created first before the old account is closed
2a.1.7.4	Action: Patient presents their copy of the old PHR to the new vendor to verify that the data transfer is complete and correct	This also provides a backup procedure in case the original vendor is unwilling or unable to transfer the data
2a.1.7.5	Action: Patient gets a copy of the PHR from the new vendor along with new access media	
2a.1.8.0	Event: PHR System decides to go out of business	
2a.1.8.1	Action: Patient receives notice of business termination and a list of alternate providers	Patients must be informed about this procedure when they open an account
2a.1.8.2	Action: Patient selects a new PHR System, opens an account, and informs the previous vendor or NHIN who will handle the new PHR and the data transfer	Data can be transferred, but authentication and permission data must be re-established at the new vendor
2a.1.8.3	Action: Patient receives a new copy of their PHR data from their new PHR system vendor along with new access media	The digital signature, if used, will be based on the new vendor's certificate
2a.1.9.0	Event: PHR System experiences a disaster that requires a change of URL	This refers only to the migration of the same system and same data to a new Internet hosting location, not a change of PHR system
2a.1.9.1	Action: Patient receives notice of a permanent or a temporary change in URL, and new access media that points to the new system location	The URL is the only thing that should change and all account numbers, usernames, and passwords should continue to work. The data should be identical to the original system and be validated with the same PHR software system certificate. This process could also be handled by the record locator

Code	Description	Comment
		service of an NHIN without any involvement of the patient.

2a.2 Provider Perspective – Pre-Encounter and Pre-Population Scenario

Code	Description	Comment
2a.2.1.0	Event: Physician offers to provide registration and medication data, a patient portal, or a full PHR	This will apply mainly to physicians who use an EHR or an e-prescribing system and it will be done in partnership with the EHR vendor or the e-prescribing vendor
2a.2.1.1	Action: Physician sends a message to patient or offers the service to the patient during a visit	If the patient accepts the offer and selects the PHR option, the physician now also functions under perspective 5 as the PHR system
2a.2.2.0	Event: Physician gets a request for pre-population data from a PHR System	
2a.2.2.1	Action: Physician gets a request for medication data that identifies and patient and includes consent from the patient to release the information using the patient's PHR access media	Ideally the patient provides the correct record linkage information to the physician's systems and the PHR System identifies the patient by their PHR access media that might send a time limited access token
2a.2.2.2	Action: Physician sends medication list and other information to the PHR	The source of the information could be the physician's EHR, an electronic prescribing system, or even manual entry from a paper record. If an electronic prescribing system is used, the request must be sent to the physician rather than the e-prescribing vendor because patients do not have a relationship with the e-prescribing provider and may have different e-prescribing records at the same vendor from different physician practices that do not share data. The medication information sent by the physician should include codes for the medications to facilitate standard terminology and patient friendly translations, future decision support, and identifying potential duplications of the medication. The information should ideally be sufficient to write a new prescription for the same medication and should include patient instructions

2a.3 Pharmacy Perspective – Pre-Encounter and Pre-Population Scenario

Code	Description	Comment
2a.3.1.0	Event: Pharmacy offers to provide a medication list, patient portal, or full PHR to a patient	
2a.3.1.1	Action: Pharmacy sends a notice to the patient or offers the service when the patient comes in to the pharmacy	If the patient accepts the offer to provide a PHR system, the pharmacy now also functions under perspective 5 as the PHR system
2a.3.2.0	Event: Pharmacy gets a request for a medication list from a PHR system	
2a.3.2.1	Action: Pharmacy gets a request from a PHR system that	A good source for accurate record linkage would be the prescription number

Code	Description	Comment
	identifies the patient, includes consent to release information based on the PHR access media provided by the patient	of a prescription the patient filled at that pharmacy
2a.3.2.2	Action: Pharmacy responds to request and sends the medication data to the PHR along with any additional insurance or registration data	Pharmacies have more data on refills and dates of filling prescriptions than might be found in physician's records or EHR. Pharmacies also have useful registration data that can be used if insurance and physician records are not available in electronic form

2a.4 Payer Perspective – Pre-Encounter and Pre-Population Scenario

Code	Description	Comment
2a.4.1.0	Event: Payer offers to provide PHR services to the patient	Sometimes the employer is the payer or may offer to play this role in close partnership with an insurance company
2a.4.1.1	Action: Payer sends a notice to the patient to offer the service, provide claims data to populate a PHR, or provide a patient portal to review claims data	If the patient accepts the offer to provide a PHR, the payer now functions under perspective 5 as the PHR system
2a.4.2.0	Event: Payer receives request to provide claims data to populate a PHR	
2a.4.2.1	Action: Payer gets a request from a PHR system that identifies the patient, includes consent to release information based on the PHR access media provided by the patient	
2a.4.2.2	Action: Payer sends the insurance information and medication claims to the PHR System using the time limited access media included in the request	

2a.5 PHR System Perspective – Pre-Encounter and Pre-Population Scenario

Code	Description	Comment
2a.5.1.0	Event: A PHR system applies for certification	Certification of PHR system software will be done by CCHIT using similar methods to those developed for ambulatory EHR. Certification of Functionality, Interoperability, and Security; are essential first steps before anyone can provide a PHR System that will be reliable and trustworthy. Lack of trust has been a key historical problem in the development of PHR and in the development of effective Health Information Exchange outside of a single enterprise.
2a.5.1.1	Action: PHR System software vendor or developer applies to the certification agency for certification	Certification must begin with an application for certification that provides information about the software system vendor or developer requesting

Code	Description	Comment
		certification. Certification will be done once for the software and the software vendor will then effectively extend that certification to all of their clients. Some PHR software developed for a national system or a large employer or insurance company may exist in only one instance. EHR software that includes PHR software will be sold to hundreds of physicians. PHR software that is marketed directly to consumers may have tens of thousands of instances but be certified only once.
2a.5.1.2	Action: Certification agency provides requirements and test scripts with sample patient information and test messages	Certification must be based on clear criteria and clear method for testing the PHR system software by using sample data and examining output based on hypothetical patients. Certification of HIPAA billing transactions has been assisted by use of a wibbler approach where random variations are inserted into a set of test patients to prevent gaming the system and simulating the output if the desired output is known in advance
2a.5.1.3	Action: PHR system completes demonstration that they meet all certification requirements and pass all live testing	The certification process will probably use a mixture of methods involving system assessment, demonstration of functions, and live laboratory testing of end to end interoperability
2a.5.1.4	Action: PHR system software vendor or developer generates a key pair and sends a certificate request to the certification agency. This is the essential first step in obtaining a digital certificate allowing only the requestor to possess the private key	The certification agency itself, or a single delegated contractor, will also serve as the root certificate authority to issue authentication certificates to PHR System software vendors and developers to prove that they have been certified. The same certificate can be used by all instances of the software since the identification of the practice that owns the EHR or the consumer that owns the PHR will be added to each message or data that the PHR system sends. PHR software should be designed so that the software vendor can effectively provide a moderate level of authentication of the identity of all of their customers. A certificate issued as part of the certification process makes sense even if digital signatures are not used when delivering or storing data, and even if there is an NHIN handling all other certificates and authentication. The digital certificate now becomes portable proof that a particular software system was actually certified by the certification agency for the time period indicated on the certificate. Any data produced by that system can carry proof of that certification as part of any digital signatures added to the data. This gives a digital signature a dual purpose of both protecting non-repudiation of the data and affirming a trustworthy source. Certificates can be revoked centrally after they are issued adding to the power of certification.

Code	Description	Comment
2a.5.1.5	Action: The certification agency provides a digital certificate to the PHR System	The certificate can be used for authentication and digital signature. This will enable PHR systems to provide reliable authentication and proof of certification to anyone who uses them, and also enable them to digitally sign any data and messages that they send if that technology is implemented or required. All instances of the same software can be signed by the same certificate if the software has been designed to give each instance some form of access to the private key and the identification of the instance owner is reasonably well controlled by the software vendor.
2a.5.1.5.a1	Alternative Action: If there is a local NHIN, PHR System certificates will not be used and instead the local NHIN provided certificates will be used by consumers and providers to sign PHR data from systems they own	Individual certificates for each practice or patient are clearly superior, but initial PHR systems will be a low stakes and low risk security activity where software vendors providing a sub-optimal solution will be adequate to introduce the use of sophisticated security technology.
2a.5.2.0	Event: A certified PHR offers its services to patients	Offers can be made directly by the PHR System provider or in partnership with another group such as a physician's EHR, a pharmacy, an insurance company, or an employer
2a.5.2.1	Action: A PHR System sends information directly to patients or makes information available at normal health care locations	Direct patient advertising or patient recruiting in shopping malls may or may not be an appropriate strategy. Aggressive and pervasive marketing may be necessary to drive rapid adoption, but has been a source of confusion with the Medicare Drug Program
2a.5.2.2	Action: A PHR System might offer its services jointly at the time of an encounter with another provider such as a physician	Recommendation from a trusted health care source such as the patient's physician, pharmacist, or hospital may be the preferred strategy.
2a.5.3.0	Event: PHR System receives a request from a patient to create an account	Accounts could be created in advance but not activated until the patient specifically issues a request, reviews privacy and other policies, and gives consent to create an account
2a.5.3.1	Action: Patient requests an account.	Group marketing might occur when an employer offers accounts to all employees, a doctor to all patients, or and insurance company to all family members of all policy holders. It may be helpful if whole families could request accounts for all families in one transaction. If accounts are created together for all family members, each family member requires their own account and their own login. A policy must be developed for families to create accounts for all children that are accessible to all custodial parents with a separate login for each custodial parent that allows access to their own account plus all children they are responsible for.
2a.5.3.2	Action: PHR system provides patient education about privacy and information sharing policies	A screen display, documents, videos, or live instruction are acceptable in accordance with local privacy policies

Code	Description	Comment
2a.5.3.3	Action: Patient accepts policies and gives consent to create an account and creates authentication credentials if they are required because there is no local NHIN	Consent and login creation can be done in one step
2a.5.3.4	Action: PHR System sends the access media to the patient	The PHR cannot be used until the patient has access media. Patients who have access to multiple PHR accounts, such as their own and their children's, should be able to use one access media and then identify the family member
2a.5.4.0	Event: PHR System receives requests, access media, and consent from the patient to populate the PHR	
2a.5.4.1	Action: PHR system sends requests for information to sources identified by the patient and for which the patient gives consent to release information. The request will be accompanied by a time limited access media that extends the patient's access media for one time use. If there is a local NHIN, the information source should have their own access media that can be used instead	Patient must identify the potential source of data and provide both consent and specific contact and account information to the PHR system. This will not normally be a general query to a Health Information Network or NHIN based on the patient's name and other identifiers (a general purpose query for all records would be another use case). A current personal medication history will have a simple starting place and grow over time with future encounters.
2a.5.4.2	Action: PHR system imports data and attempts to reconcile duplications	The coding of medications will be critical for detecting duplications. Free text data should be avoided for medication names and even patients can enter data from NDC codes on their medication bottle, or prescription numbers, to assist in correct linkage of even patient entered data
2a.5.5.0	Event: PHR System allows patient to review data and make annotations or additions	
2a.5.5.1	Action: PHR system displays data obtained from pre-population requests in a data entry mode after the patient presents their access media	Typical data entries might include adding a missing medication, adding over the counter medications, marking some medications inactive, indicating a change in dose from the original prescription, indicating how often some medications are used, and adding the last refill if not captured by pre-population requests.
2a.5.5.2	Action: PHR system receives updates from the patient and files patient notes and additions. Patients cannot change data from other sources	Patients should not be allowed to change data received from another primary source, but they can review and request changes in their record. Under HIPAA, patients can request review of their physician's medical record and request changes, but the physician is not required to make the changes. In the case of a PHR the patient is the owner of the data and they can mark and annotate any data that they believe is not true, and identify medications that are no longer active. The purpose of the PHR medication list is to identify the medications that the patient is actually currently taking as well as to note any relevant recent or past medication. The time relevance of previous

Code	Description	Comment
		medications varies, but some medications have long term significance hence PHR systems should never routinely drop medications that fall outside of the current date range.
2a.5.6.0	Event: PHR System receives request to allow additional consumer users	
2a.5.6.1	Action: PHR receives consumer request to add users	
2a.5.6.2	Action: PHR creates user access media for new users	
2a.5.7.0	Event: PHR System provides the patient a first look at the first ready to use version of the PHR	
2a.5.7.1	Action: PHR displays a copy of the PHR after the patient presents their access media	The patient now has the information to print a paper copy or save an electronic copy
2a.5.8.0	Event: Patient decides to change PHR System provider	Freedom of choice of system provider is essential
2.5.8.1	Action: Patient saves an electronic and paper copy of their PHR for backup from their current system	
2.5.8.2	Action: Patient opens an account with a new PHR system and creates new access media if required	An NHIN can provide patient authentication credentials that can be used with different vendors, but that is generally not available today.
2.5.8.3	Action: Patient notifies the current PHR system provider and provides information about the new PHR system provider	
2.5.8.4	Action: Current PHR transfers the data to the new PHR System	This can include a patient moving from a patient owned PHR system to one that is part of their physician's EHR
2.5.8.5	Action: Current provider closes the account and responds to future requests with forwarding information to reach the new PHR System provider	Current users and old copies of the access media and PHR will still point to the old PHR System but no information will be returned if the old access media is used unless it was provided by an NHIN
2.5.8.6	Action: New PHR system provides new access media and a current copy of the new PHR to the patient	
2.5.8.7	Action: If data transfer failed, the new PHR system can import the data from the backup copy of the old PHR and change the account information and digital signature to reflect the new PHR system provider	
2a.5.9.0	Event: PHR System decides to go out of business	Standards must be set for business operations and procedures when a vendor decides to cease operations voluntarily
2.5.9.1	Action: PHR System notifies all consumers and providers and offers options and assistance	Rules must be set for requirements for advance notice and providing alternative options
2.5.9.2	Action: PHR System migrates data to the new PHR system provider	Data can be migrated but authentication and permissions do not migrate unless they come from an NHIN. The patient may need to re-enroll, get new

Code	Description	Comment
		access media, and re-authorize other users.
2a.5.10.0	Event: PHR System experiences a disaster that requires a switch to a backup provider	Disaster could be natural (hurricane, flood, or earthquake), terrorist, or system failure. Normally backup systems should be transparent to the users and not require new connection information, but sometimes they will.
2a.5.10.1	Action: PHR system moves operations to a new location that requires a change in the URL for data access	
2a.5.10.2	Action: PHR system informs the patient, and other authorized users, of the new permanent or temporary URL and provides new access media	
2a.5.11.0	Event: PHR system experiences a disaster so sudden and so catastrophic that no continuity of operations is possible	This almost unimaginable event is included to affirm the robustness of the PHR system approach and the usefulness of standards that provide for continuity even when all disaster planning and preparation fails.
2a.5.11.1	Action: The patient takes their most recent electronic copy of their PHR that should be in their possession and takes it to another certified PHR system provider	This is identical to a change of PHR supplier under hostile conditions without the cooperation of the original PHR system provider. This approach depends on patients keeping their own personal electronic copy of the PHR, perhaps on a smart card also used for access media and login authentication. Because each electronic PHR has a digital signature, it is possible for the new PHR System to validate that the information is intact, unmodified, and comes from a trusted original source.

2b.1 Consumer Perspective – Encounter Use Scenario

Code	Description	Comment
2b.1.1.0	Event: Patient visits a new physician for the first time	Although not strictly part of the use case, this is a perfect time for the practice to share contact data with the patient and leave a brief record of the data and purpose of the encounter in the PHR
2b.1.1.1	Action: Patient presents their access media to the front desk and logs into the PHR System if Internet connection is available at the front desk	If a local NHIN is in operation the practice might be able to login themselves, but the usual procedure will be for the patient to do the login and grant the practice access for the duration of the encounter
2b.1.1.2	Action: The data in the PHR is imported into practice systems to create a new billing record, EHR record and/or electronic prescribing record	All PHR systems must use a uniform standard interface to decrease the burden on vendors
2b.1.1.3	Action: If the practice is not automated or the systems lack interoperability, a paper copy or a printout from a web page saves the patient the effort and potential errors of filling out a new registration form and also provides a personal medication list at the same time	
2b.1.1.4	Action: The patient reviews the new administrative records created by the practice and signs any necessary consent forms	Patient will get the final updated PHR at the time of checkout by presenting their access media again when they are ready to leave
2b.1.2.0	Event: Patient visits a physician they have seen previously for the first time with a PHR	The physician already knows the patient and has billing system records and EHR records already setup or has a paper chart with previous notes. This is still an important opportunity to add new information from a PHR that is not in the practice files
2b.1.2.1	Action: Patient presents their access media and logs in to the PHR system	The import and comparison of the data is transparent to the patient
2b.1.2.2	Action: Patient verifies comparison of PHR data with data already on file in the practice	Patient will get final updated PHR at the time of checkout when they present their access media for a second time
2b.1.3.0	Event: Patient visits a physician they have seen previously who has seen the patient before with a PHR	Each time the patient visits, the insurance must still be presented and checked, but now useful recent medication data is transferred at the same time
2b.1.3.1	Action: Patient presents access media and logs in to the PHR system	If there is a local NHIN, the practice might be able to do their own login, but patient presentation of access media at all encounters is a good practice with or without an NHIN to insure positive patient identification and linkage
2b.1.3.2	Action: New and changed data from the PHR including data from other practices is added to the practice records	Once data is imported at the front desk to an EHR, it can be used by all practice staff and all updates transferred back to the patient at the end of the encounter when the patient checks out and presents the access media a second time

Code	Description	Comment
2b.1.4.0	Event: Nurse or other health care provider reviews medications and allergies with the patient as part of a screening process prior to being seen by the physician	Nurse now has a copy of the medication list even if the practice does not use an EHR. This helps take a more accurate screening history.
2b.1.4.1	Action: Nurse receives a copy of the medications and allergies from the patient's PHR system	The copy could be the data imported into a practice EHR or e-prescribing system, a paper printout of the PHR, or an electronic web browser view of the PHR depending on the practice hardware and software availability
2b.1.4.2	Action: Nurse and patient make any appropriate notes or changes and patient may request refills	Updates are done in EHR if one exists or in the PHR depending on how the practice is operating
2b.1.4.a1	Alternative Event: The patient does not want to use a certified interoperable PHR system and instead maintains a personal medication list on a word processor or spreadsheet	True interoperability and security are impossible but valuable data is provided by the patient
2b.1.4.a1.1	Alternative Action: The patient gives their personal medication list to the physician or the nurse	The information will not have medication codes and may not be machines readable
2b.1.4.a1.2	Alternative Action: The physician or nurse enters the patient provided data into the EHR system or PHR system	The data will need to be re-keyed by the provider, but this activity is a very routine part of health care delivery and legible patient provided lists are usually appreciated by the provider if they are the only source of data. Paper bags of medications brought to a visit remain a common part of medical encounters where digital data does not exist.
2b.1.5.0	Event: Physician reviews medications and allergies with the patient and writes new prescriptions or refills as needed	Some of the prescriptions reviewed or refilled will have been written by another physician in another practice but the PHR will deliver the correct information to the current physician directly or through an NHIN
2b.1.5.1	Action: Physician displays the personal medication list presented at the front desk in the EHR, e-prescribing, or PHR system or examines a paper printout placed in the chart.	Even paper printouts of the PHR done from a web browser at the front desk and inserted into a manual chart will be an important change in workflow and patient safety. If the physician uses an EHR or e-prescribing system that can import the data from the PHR, the physician has immediate access to data from the patient that may be the only source of information from other physicians and recent emergency room visits
2b.1.5.2	Action: Physician and patient discuss changes to the current medication list	Changes can be entered directly by the physician if they have a web browser, an EHR, or electronic prescribing system available in the exam room.
2b.1.5.3	Action: Physician writes a new or refill prescription with the help of the insurance and personal medication list	Having access to a PHR system will make electronic prescribing easier by eliminating duplicate data entry by the physician and by saving the physician the work of asking and looking up the patient's pharmacy. Patient often cannot remember the phone number or address of the pharmacy they usually use and this wastes time and makes electronic prescribing difficult. EHR and e-prescribing saves time with refills only if you have a complete and accurate

Code	Description	Comment
		current medication list to eliminate the need to re-write each prescription
2b.1.5.4	Action: Physician sends the prescription to the pharmacy by electronic message or fax so that the filled prescription is waiting for the patient when they arrive at the pharmacy	Electronic prescribing or EHR use gets the data directly into the patient's personal medication list at checkout and saves time at the pharmacy because the prescription is ready and waiting.
2b.1.6.0	Event: Patient visits a pharmacy to pick up a new prescription written by the physician	Process is basically the same for mail order
2b.1.6.1	Action: Patient presents their access media and logs in to the PHR	If the patient is a new customer this saves time creating insurance records and also provides a current medication list.
2b.1.6.2	Action: Patient gets an updated copy of the PHR that includes the new medication and might include other medication data if this is the first time the patient used that pharmacy with a PHR	
2b.1.7.0	Event: Patient visits a pharmacy to pick up a refill of an existing prescription	Process is similar for mail order
2b.1.7.1	Action: Patient presents their access media and logs in to the PHR System	The patient should already be known to the pharmacy that has insurance and medication data on file
2b.1.7.2	Action: Patient gets an updated PHR with the refill date added	Pharmacist may inform the patient that no more refills remain and may offer to contact the physician to request more refills
2b.1.8.0	Event: Patient gets a coordination of benefits notice from payer that a visit claim and medication claim have been paid	Arrives by mail or Email as a routine business practice and may trigger a look at the PHR to add new data. Not necessary if the payer is the PHR system and could be a routine automatic data transfer in the presence of an NHIN
2b.1.8.1	Action: The patient presents their access media and logs in to the PHR system to review new claims for medications and other services	Sometime the claims data may be the only way to get accurate information into the PHR. Data entry by the patient should always be a last resort for prescription medications. Claims data is usually less complete than data obtained from the pharmacy or the physician
2b.1.9.0	Event: The patient is admitted to a hospital	A hospital admission is slightly different from an office visit because additional registration information might be required. Similar to ambulatory visits, data will be imported from the PHR into a hospital EHR. Data from old records is less useful, unless inpatient and ambulatory EHR are integrated and the same hospital is a major source of ambulatory care for the patient. JCAHO now requires that all hospitals get current medication lists at the time of admission and most are looking at the PBM as the source of that data
2b.1.9.1	Action: Patient presents their access media and logs in to PHR system	Registration for hospital admission is similar to ambulatory care and will be expedited by having a PHR
2b.1.9.2	Action: Patient completes any additional registration	Ideally a single registration would be adequate for all settings, but there is

Code	Description	Comment
	information including advance directives	some justification for some additional data during hospitalization
2b.1.9.3	Action: If patient does not provide a medication list, the hospital will launch some form of medication history query to a PBM clearing house.	Some form of medication history on admission is a requirement of JCAHO for certification of hospitals. If the data does not come from a PHR, it must come from someplace else. An NHIN might provide medication history to hospitals even for patients that do not have a PHR using methods similar to a PBM clearinghouse
2b.1.9.4	Action: At the time of discharge, the patient presents their access and media and logs in to the PHR to receive a new PHR with records of discharge medications and any relevant medications that were administered during the hospitalization	Discharge medications are similar to ordinary prescriptions written during ambulatory care, but significant antibiotics, chemotherapy, inhalation medications, and immune suppressive medications would not be entered on a personal medication list unless they are added by the hospital as medication administration data. A typical hospital discharge abstract would provide that data in narrative form as part of the hospital course and that data would never appear on a personal medication list. Adding hospital administered medications to a PHR is an important new function provided by this use case.
2b.1.10.0	Event: Patient visits laboratory, radiology, and other hospital departments for tests and procedures	Re-registration is not necessary for hospital inpatients, but most of these tests and procedures are done on an ambulatory basis and typically include starting with a new registration clipboard
2b.1.10.1	Action: Patient presents their access media and logs in to the PHR system for one time access.	Redundant clipboard registration is eliminated. This would be an excellent time for the patient's PHR to receive contact information for the lab or imaging department and a record of the date when the procedure was done.
2b.1.11.0	Event: Patient has an accident and is found on the street and cared for by Paramedics	
2b.11.1	Action: Paramedics find the access media the patient is carrying	The patient is unable to present the access media and login to the PHR system because of their injuries
2b.11.2	Event: The paramedics connect to the PHR using a "break glass" emergency login	The data on the access media must be sufficient for an emergency connection
2b.11.3	Event: The patient is informed of the emergency access and the justification for it, and is asked to give after the fact consent for that access	The most important part of "break glass" is the investigation, notification, and after the event obtaining of retroactive consent.
2b.1.12.0	Event: Patient visits an Emergency Room on their own	An Emergency Room visit is basically not different from an ordinary office visit except that more patients are new patients, old records are usually not available, and a different physician will see the patient for follow-up
2b.1.12.1	Action: same as for a routine office visit and additional tests or procedures starting with patient presentation of access media and log in to the PHR System	Medications administered in the emergency room as well as any new prescriptions should be transferred to the PHR system when the patient checks out of the ER and presents their access media a second time

2b.2 Provider Perspective – Encounter Use Scenario

Code	Description	Comment
2b.2.1.0	Event: Arrival of a new patient never seen before in the practice	The practice has little or no information about the patient and must start a complete new set of files
2b.2.1.1	Action: Patient presents their access media and logs in to PHR system for access during the encounter	Uniform data import interfaces from all PHR to all EHR systems is essential to this use case
2b.2.1.2	Action: New records are created with everything needed to bill the patient, start a new medical record, and do electronic prescribing from an EHR or standalone e-prescribing system	Having a medication list, allergies, and key chronic conditions is an important starting point for a new patient. Knowing the pharmacy information will make electronic prescribing easier. Linking registration information to electronic prescribing will help physicians find the right formulary for each patient.
2b.2.1.3	Action: If an NHIN is available, the practice may be able to login to the PHR System with permission from the patient using access media belonging to the practice or the physician	Usually the patient login will work and simplify operations until a full NHIN with universal common provider authentication is available
2b.2.2.0	Event: Arrival of an established patient seen previously in the practice with a new PHR	The patient is known and records and charts have been created previously, but there is still an opportunity to get new data from the PHR
2b.2.2.1	Action: Patient presents their access media and logs in to the PHR system for access during the encounter	Uniform data import interfaces from all PHR to all EHR systems is essential to this use case
2b.2.2.2	Action: Patient data is compared with data in the practice and corrections are made	Patients who have the wrong information about their medications may have safety risks and practices typically have incomplete data that does not include data from other providers and recent events such as an Emergency Room visit the night before where medications were administered or prescriptions written. The Physician also now has knowledge of whether previous prescriptions were actually filled and if chronic medication were refilled appropriately
2b.2.3.0	Event: Arrival of an established patient with an established PHR	All systems are in place and the PHR is used as a communication tool to link and collate data from multiple sources
2b.2.3.1	Action: Patient logs in to the PHR using their access media and data from the PHR system is used to update the practice EHR or paper charts	If an NHIN is available, the physician or practice staff may also have rights to login for the patient based on patient granted permissions
2b.2.4.0	Event: Nurse or other health care provider reviews medications and allergies with the patient as part of a screening history	Screening is an initial interview where vital signs are measured and medications and allergies are typically reviewed prior to the patient seeing the physician

Code	Description	Comment
2b.2.4.1	Action: nurse updates the PHR or EHR	Data can be entered directly into the PHR or entered into the EHR or e-prescribing system and transferred to the patient's PHR at the time of checkout. Whatever workflow is chosen, duplicate entry into two systems must always be avoided. Some updates may not happen until the patient reaches the pharmacy or gets home after the encounter in practices that are not automated and do not have Internet infrastructure available in all exam rooms.
2b.2.5.0	Event: Physician sees the patient, reviews medications, and changes dosage or other usage instructions	
2b.2.5.1	Event: Physician can change the patient dose instructions (called the prescription SIG) in the PHR system or in the EHR system, but does not need to send information to the pharmacy until the time of renewal because the original prescription remains unchanged while the patient may have changed to a new dose regimen.	Changes in medication use and plan of care that are made by the physician will now be available the next time the patient sees another physician or goes to the pharmacy for a refill. If the physician is making changes in an EHR or e-prescribing system, these changes will be transferred to the patient in one step at the time of checkout from the practice
2b.2.6.0	Event: Physician writes a new prescription or refills and existing one	The original prescription may have been written by another physician in another practice
2b.2.6.1	Action: New prescription is sent to the pharmacy	
2b.2.6.2	Action: The medication list in the PHR is updated with the new prescriptions and refills including any change in dosage or instructions	Depending on practice operations this might not happen until the time of patient checkout from the practice or on arrival at the pharmacy
2b.2.7.0	Event: The physician orders and the nurse administers a single dose medication in the office	There is no prescription at the pharmacy, but there might be a claim at the payer and refills might be required
2b.2.7.1	Action: Medications administered in the office are added to the PHR or EHR	This information may be very significant for future health care and also includes medications administered in the hospital. Data might be transferred to the PHR in one step at the time of office checkout or hospital discharge
2b.2.8.0	Event: Physician gives the patient sample medications	There is no prescription in the pharmacy and no claim at the payer
2b.2.8.1	Action: Sample medications are added to the PHR, EHR, or e-prescribing system	Sample medications are sometimes not recorded in the medical record and typically may need to be refilled and both the patient and other physicians should be aware of their use. Physicians are supposed to record dispensing of sample medication and this is a difficult task without information system support. Data in the EHR will reach the PHR on checkout after the visit when the patient presents access media for a second time, or through use of an NHIN if one is available

Code	Description	Comment
2b.2.9.0	Event: Physician sees an unknown patient in an emergency situation	
2b.2.9.1	Action: If physician can find the access media they can login to the PHR system with an emergency “break glass” login	Break glass functionality will require some form of reliable universal provider authentication and that is a challenge in the absence of an NHIN. Setting appropriate standards for this essential task is mandatory. Perhaps local enterprise credentials can be used such as a hospital login until all physicians have an NHIN login
2b.2.9.2	Action: After the encounter, the physician must submit a report justifying the action and if possible obtain consent from the patient or family	A simple web based procedure may be adequate for many cases if the patient can authenticate after the encounter. The Social Security Administration uses a bar coded web page printout to facilitate fax back of copies of medical records and consent forms for release of medical information to their Electronic Medical Evidence system.

2b.3 Pharmacy Perspective – Encounter Use Scenario

Code	Description	Comment
2b.3.1.0	Event: Pharmacist receives a new prescription or refill sent by the physician to the pharmacy	Prescriptions arrive hand carried by the patient, over the phone, by fax, and ideally as a electronic prescribing message, sometimes in response to a refill request message from the pharmacy
2b.3.1.1	Action: Pharmacist enters or imports the prescription data into the pharmacy information system before the patient arrives	With electronic prescribing, data does not have to be re-keyed
2b.3.1.2	Action: Pharmacist fills the medication bottle and sends claim information to the payer to verify coverage. The last step includes checking the physical form of the medication to be sure the right medication is in the bottle.	Pre-adjudication of the claim will determine how much the patient must pay when the prescription is picked up. It is not possible at this time to update the PHR because the medication has not actually been dispensed to the patient. The pharmacist will be the best source of information about the physical description of the medication if that information will be added to the PHR to provide a patient friendly method of referring to a medication
2b.3.1.3	Action: If there is a problem with coverage or formulary, the patient and the physician will need to be notified and the problem resolved before the prescription can be picked up	Patients are often willing to pay for non-formulary or premium cost medications
2b.3.2.0	Event: Patient picks up the medication at the pharmacy	
2b.3.2.1	Action: Patient presents their access media and logs in to the PHR system and the pharmacy can import the insurance data and current medication list. This will actually provide	A standard interface for all PHR systems is essential and should be exactly the same as the one used by EHR systems for data import and export to and from a PHR. Pharmacies do not require patient identification in all cases and

Code	Description	Comment
	positive identification of the patient on arrival at the pharmacy so that they cannot pick up another patient's medication without permission or by accident.	PHR systems will not be used in all cases, but patient identification does occur sometimes and there is already some discussion of more identification in the future.
2b.3.2.2	Action: The new medication is added to the PHR	The data transfer from the pharmacy to the PHR is done as one transaction using the patient provided access media that was used to provide insurance data and patient's medication list. Generally, only the new prescription needs to be added if pre-population took place before the encounter to avoid repeating the work of data clean-up and reconciliation of multiple existing data sources
2b.3.3.0	Event: Patient requests a refill of an existing prescription	
2b.3.3.1	Action: Patient makes the request by phone or web portal	
2b.3.3.2	Action: Pharmacist has the necessary information in their own system or from the patient's PHR	The PHR may be useful for transfer of prescriptions to a new pharmacy for refills subject to business policies and state law. The information in the PHR will help by accurately identifying the medication and the previous pharmacy. Data in a PHR is really a secondary source and may not be as trustworthy as primary sources such as the EHR or electronic prescribing, but it is always better than nothing. Controlled substances cannot be handled in this fashion so the potential for abuse is relatively small
2b.3.4.0	Event: Patient picks up a refill of an existing medication	
2b.3.4.1	Action: Patient presents their access media and the PHR is updated using patient login	Data transfer from pharmacy to PHR is done with a standard interface or document as a single step. Only the new refill is updated in the PHR to avoid adding noise to previously cleaned PHR data
2b.3.5.0	Event: Patient requests a consult from the Pharmacist to review the patient's personal medication list	Personal medication lists can be expected to increase patient interest in their medication list and the need for more education and corrections to the medication list
2b.3.5.1	Action: As a result of the consult, the PHR may be updated using the access media and login presented by the patient	Pharmacists can play a new and important role by assisting patient edits of their data and at the same time they can improve the data in their own information systems by doing the edit once and then importing or exporting the results

2b.4 Payer Perspective – Encounter Use Scenario

Code	Description	Comment
2b.4.1.0	Event: Payer receives claims for medications	Payers process claims from all physicians and all pharmacies so they may have the most complete information, including practices that do not use

Code	Description	Comment
		information systems. The main problem is that the data they require to pay claims is less than what is needed to write or fill prescriptions
2b.4.1.1	Action: Payer receives the medication claim, usually from the pharmacy	
2b.4.1.2	Action: Payer adjudicates the claim and identifies any problems in coverage or formulary and pays the claim	The date of the medication record may now be the date of adjudication and not the date the prescription was written or even the date when the prescription was filled and picked up at the pharmacy
2b.4.1.3	Action: Payer can update the PHR if the patient presents access media and logs in to a PHR while checking claims data. If an NHIN is available, and if the payer has been granted permission by the patient, the payer can access the PHR system directly and add the new medication if it is not already on the patient's personal medication list. The payer might even be the owner and operator of the patient's PHR system.	Duplicate entries for the same medication on the PHR medication list can be detected by preserving and using NDC medication codes for the package, mapping NDC to a more general code such as RxNorm, using the physician's prescription number for the electronic prescribing system, using the pharmacy prescription number, and using the payer claim number. Updates to the patient's PHR may require periodic patient login to the payer's web portal to have updates transferred to the PHR by a data import after web login and an immediate data export after update is complete. This type of insurance claim encounter will be a new experience for most patients but allows patients to get claims data into their PHR on an on-going basis when the insurance company is not the provider of the PHR System

2b.5 PHR System Perspective – Encounter Use Scenario

Code	Description	Comment
2b.5.1.0	Event: Patient, physician, pharmacy, or payer submit updates to the PHR at the time of an encounter	Typically based on a patient login and local system import at the start of the encounter and an export to the PHR in one step at the time of checkout at the end of the encounter
2b.5.1.1	Action: Patient presents their access media and logs in to the PHR system that files the updates	The PHR system may issue a time limited login ticket to the practice or hospital based on the patient's access media and login
2b.5.1.2	Action: PHR system displays a new updated version of the record with a new digital signature by the PHR system if digital signature is used assure non-repudiation and integrity	This usually occurs at the end of the encounter, typically as part of the checkout process from an office visit, ancillary service provider, or hospital discharge when the patient will present their access media for a second time

2c.1 Consumer Perspective – Post-Encounter and Home Use Scenario

Code	Description	Comment
2c.1.1.0	Event: Patient, family member, or care giver review current medication list	Home use of the PHR can be shared or delegated to others particularly for children or elderly patients
2c.1.1.1	Action: Patient uses their access media to login to the PHR and displays their current registration data and medication history	The standards probably should require the option of display in a standard web browser without installation of a special application so that the PHR will be maximally available including public web terminals in schools and libraries
2c.1.1.2	Action: Patient can print a paper copy directly from the web browser screen	If the PHR record is implemented as an XML document with a standard uniform XSLT formatting file, paper printouts will always be available from web browsers and look the same from all PHR system vendors
2c.1.1.3	Action: Patient can save an electronic copy for personal use, backup, and to give to other providers	Any media or local disks can be used including some types of access media used for login
2c.1.2.0	Event: Patient updates the PHR from home	Patients have limited rights to change only certain sections of their record and cannot make changes to data entered by others
2c.1.2.1	Action: Patient uses their access media to login to the PHR system and retrieves a copy in edit mode	
2c.1.2.2	Action: Patient enters changes to their PHR	Changes are filed directly to the PHR system and a new PHR display is generated. After all edits are complete, a new copy should be printed and saved
2c.1.3.0	Event: Patient modifies user permissions for family members, providers, and other users of their PHR	A clear set of roles and permissions needs to be developed for the PHR indicating who can view or enter specific types of data acting as a proxy for the patient
2c.1.3.1	Action: Patient uses their access media to login to the PHR system and views the current list of authorized consumer users and their current level of permissions	If an NHIN is available, it will provide services to manage access permissions
2c.1.3.2	Action: Patient changes the permissions either removing or adding permissions to existing consumer or provider users	In extreme situations, a family member or a parent may have custodial rights over a mentally ill, mentally incompetent, or non-independent minor and that non-patient consumer may have been delegated this control that has been removed from the patient. This situation must be anticipated and carefully articulated in the standard that will default to give the patient full control over permissions.
2c.1.3.3	Action: Patient requests access for a new user	This task cannot be done by the patient alone because the PHR System will need to create new access media and login for the new users unless this is done by an NHIN, hence it is normally part of scenario b, an encounter with the PHR System

Code	Description	Comment
2c.1.4.0	Event: Patient reviews who has seen their record	
2c.1.4.1	Action: Patient uses their access media to login to the PHR System and displays the access log of users who have viewed the record and when the access occurred	
2c.1.4.2	Action: The access log includes a record of all emergency or “break glass” access to the record without normal login and the results of investigations after the event to validate the justification and obtain after the fact patient consent	Patients need to provide after the fact consent for emergency access and they can do this while access the PHR System from home
2c.1.5.0	Event: Patient reviews changes to their record	
2c.1.5.1	Action: Patient uses their access media to login to the PHR system and requests a transaction log	
2c.1.6.0	Event: Patient wants to learn the various names of their medications and how to identify their specific medications	
2c.1.6.1	Action: The PHR can be designed to include generic names, brand names, physical descriptions (yellow liquid or small red pill with the number 512), or even indications such as blood pressure medicine, antibiotic for ear infection, cholesterol medicine, etc. as part of the data and routine display	It is probably best to include this supplemental information in the PHR System so that all patients and all providers share the same information and can communicate more effectively. All of this information may not be available for all medications but including brand name, generic name, and some form of patient friendly name will prevent errors in communication
2c.1.7.0	Event: Patient wants to search the Internet for information about their medications	
2c.1.7.1	Action: Patient uses the Internet to access database information about their medications	Perhaps the best source of information for patients will be the National Library of Medicine consumer database and this might be directly linked to PHR Systems for use with a single click. There are many other patient oriented medication data sources that could be integrated into a PHR system as well. General Internet searches on drug names require patient education on problems with data quality of unsupervised medical information on the Internet and are therefore less well suit for direct integration into the PHR systems.

2c.2 Provider Perspective – Post-Encounter and Home Use Scenario

Code	Description	Comment
2c.2.1.0	Event: Physician review of the PHR outside of a patient encounter or a specific request for information or services from a patient	Use of the PHR by a physician in the absence of the patient or a specific request for a service from a patient should be very rare and normally will occur through use of the Physician’s own EHR or e-prescribing system as in

Code	Description	Comment
		the case of drug recalls. Careful policies should be developed, but the patient's PHR, can with the patient's consent, become an extension of the physician's EHR and thus be appropriate for review. This might take the form of physician review of patient entered data on refilling chronic medications, use of "as needed" medications, and notes on medication actions and side effects. This is really an asynchronous home monitoring encounter usually for chronic disease management. A PHR that is not population based or practice based is typically not searchable across patients so population use is very limited. As use of PHR grows, and as potential public health uses are explored, population use may become important. The potential use of PHR for post-marketing medication surveillance has been suggested but will require data on vital signs, labs, and problems to detect unsuspected side effects or adverse effects of medications.
2c.2.1.1	Action: Physician logs in to the PHR and displays the PHR for a patient. This will probably require an NHIN as the patient will not be available to present the access media and do the login for the physician	The physician might use this to learn what another physician has prescribed for the patient. This normally should be part of a referral encounter and normally should be communicated physician to physician, but sometimes the patient may be the only available source of information
2c.2.1.2	Action: Physician might contact the patient with questions or suggestions	

2c.3 Pharmacy Perspective – Post-Encounter and Home Use Scenario

Code	Description	Comment
2c.3.1.0	Event: Pharmacist reviews the patient's medication list when the patient is not present and has not requested a pharmacy consult	This is a very unusual circumstance and has potential for abuse for marketing purposes. There must be rules governing medication review without a specific patient request. Clever pharmacy systems could use their information on where patients keep their PHR to make sequential automated queries to a PHR system for all patients in their files. This practice must be discouraged and systems might be designed to prevent this type of automated fishing for useful data. Normal pharmacy queries should be limited to their own systems and their own privacy rules and restrictions and use a PHR as a work around
2c.3.1.1	Action: Pharmacy logs in to the PHR and displays a patient's PHR for review. This will probably require an NHIN and special permission from the patient	In some situations this might be useful to avoid inappropriate attempts to contact a patient who now uses another pharmacy and may have already refilled a lapsed prescription or discontinued use of a recalled drug.
2c.3.1.2	Action: Pharmacy might inform the patient, physician, or even the insurance company of a recommended change in	

Code	Description	Comment
	medications	

2c.4 Payer Perspective – Post-Encounter and Home Use Scenario

Code	Description	Comment
2c.4.1.0	Event: Payer review of a Patient's PHR	This should be an unusual event because the payer will normally use their own claims based systems for this type of review. A PHR may include important information on OTC medication or alternative and herbal therapies and notes from the patient that might explain unusual patterns of medication claims. Other potential uses might include helping to administer a flexible spending account.
2c.4.1.1	Action: Payer logs in to the PHR System and reviews data in the patient's PHR without a request from the patient. This will probably require an NHIN and special patient permission.	When the payer is also the PHR system provider, this type of access will be more readily available to the payer.
2c.4.1.2	Action: Payer might make recommendations to the patient or the physician regarding formulary or coverage issues	

2c.5 PHR System Perspective – Post-Encounter and Home Use Scenario

Code	Description	Comment
2c.5.1.0	Event: PHR System receives requests for data display outside the context of a clinical encounter	
2c.5.1.1	Action: PHR receives a request to display data on a single patient	Queries across multiple patients will not be part of the initial use case. A family query for all family members with a single access media login of a user authorized to see all family member's PHR data should be offered as family-based use of the data can be very helpful to consumers as well as providers.
2c.5.1.2	Action: PHR System displays the current data.	Eventually the system must be enhanced to handle longitudinal data and include selected views of the data and historical data on demand. The initial version will be limited to the medication and registration data that is current or relevant past and recent data.
2c.5.2.0	Event: PHR System receives Updates to PHR data that are not part of a usual encounter	
2c.5.2.1	Action: Patient uses their access media to login to the PHR system and submit new data usually in the form of additions,	

Code	Description	Comment
	status changes, or annotations	
2c.5.2.2	Action: PHR system files the changes and displays a new copy of the PHR with a new digital signature	Patient can print the updated copy or save it to an electronic media
2c.5.3.0	Event: PHR System receives requests for changes in access permissions	
2c.5.3.1	Action: The PHR system makes the changes in access permission requested by the patient	
2c.5.3.2	Action: The PHR may need to provide new access media and create a new login for the new user.	This task is easier when performed in the context of an NHIN
2c.5.4.0	Event: PHR System receives requests for audit displays	
2c.5.4.1	Action: The PHR system verifies permissions and access media before displaying the access or transaction logs	
2c.5.5.0	Event: The PHR System conducts periodic scheduled, system maintenance and integrity checks	Good information system operation practices are too important to be left to the discretion of each software vendor and system provider. Standards must be set for appropriate best practices including continuity of operations and disaster recovery or back-up operation
2c.5.5.1	Action: The PHR conducts periodic operations to verify the internal integrity of the database, validate the database against transaction logs, maintain local backups, and prepare for disaster operations at a remote backup site in another region with periodic comparison of remote secondary data with data at the primary site.	The integrity of the data must be assured and the accuracy of secondary copies prepared at mirror sites for use in a disaster must be verified.
2c.5.5.2	Action: The PHR system conducts periodic tests of data recovery operations and periodic tests of continuity of operation from a remote standby site	Data backup and hot spare disaster operation sites are of no value unless they are regularly tested for their ability to be used without data loss.

March 2006

have **you** heard?

This monthly letter to subscribers from Consumers Union President Jim Guest highlights the critical consumer issues behind our current reports. [See archived letters.](#)

Your medical data, in bits & bytes

Hindsight is 20/20, and foresight can be, too. The latest example: the promise and peril of electronically storing all the data in your private medical records.

The federal government is working right now to convert bulging drawers of paper medical records into computer files, then linking those files to a central system (see our March 2006 report on [Electronic medical records](#)). Once this information network is established, your blood pressure and cholesterol levels, your bone and brain scans, will be accessible electronically, just as your banking and other financial records are now. That's precisely why consumer groups and patients must have a say in the development of the network and the standards that govern it. If we don't, we'll be scrambling to stop the same abuses and fix the same problems that we face in protecting our financial information.

There's widespread agreement on the need to accelerate the use of information technology in our otherwise high-tech health-care system. Most hospitals and doctors' offices still store patient records on paper, making the history of our medical care hard to transfer from one hospital or doctor to another. The inefficiencies of this system lead to medical errors and the loss or misplacement of vital information. As for the patients, we rarely see our own fragmented records or track our own health histories.

The federal Department of Health and Human Services has launched a program to speed up the adoption of electronic health records and to form a network linking them nationwide. The Senate passed legislation in November that includes a call for "uniform and consistent implementation of any standards for the electronic exchange of health information"; the House is expected to consider bills this year. Some hospitals and doctors' offices already use electronic records and stored MRIs, X-rays, and CAT scans.

Much more...



PROCEED WITH CAUTION
We need guarantees of control over our own health files before an information network is created.

We're awaiting permission from Consumers Union to reprint this editorial and the accompanying investigative report. Until then, please visit the links above and mind the fact that the Investigates Report is split into 7 sections.

<http://www.consumerreports.org/cro/aboutus/mission/haveyouheard/yourmedicaldatainbitsbytes0603.htm>
<http://www.consumerreports.org/cro/health-fitness/health-care/electronic-medical-records-306/overview.htm>