

Infor Cloverleaf Integrated Patient Health Repository (CIPHR)

Technical Specification

Providers Version

Version 2.1.6

5/31/2016

Prepared by Todd Taylor

**Copyright © 2016 Infor**

**Important Notices**

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials ("Purpose").

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

**Trademark Acknowledgements**

The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All rights reserved. All other company, product, trade or service names referenced may be registered trademarks or trademarks of their respective owners.

**Publication Information**

Release: 1.0.0.0

Publication date: May 30/2016

**Disclaimer**

This document reflects the direction Infor may take with regard to the specific product(s) described in this document, all of which is subject to change by Infor in its sole discretion, with or without notice to you. This document is not a commitment to you in any way and you should not rely on this document or any of its content in making any decision. Infor is not committing to develop or deliver any specified enhancement, upgrade, product or functionality, even if such is described in this document.

Table of Contents

**Section 1: Introduction [4](#_gjdgxs)**

**Section 2: Module Definitions [5](#_30j0zll)**

**Section 3: System Architecture [9](#_1fob9te)**

**Section 4: Data Sources [11](#_3znysh7)**

**Section 5: Data Formats [13](#_2et92p0)**

**Section 6: HIPAA, Privacy & Security [15](#_tyjcwt)**



Section 1

Introduction 1

Infor Cloverleaf Integrated Patient Health Repository, or CIPHR, is an effort to put patients in the driver’s seat of their own clinical data. For far too long, clinical data has been only available to the physician that entered that information. Sharing data between physicians is a near impossible task when both use the same EMR system. Now imagine the challenges when the patient enters a new care setting. That legacy data is no longer with the patient and is stuck in a siloed system. CIPHR is an attempt to cure that problem, by putting the focus of care back on the patient and letting the patient be the core of all data and interactions. By utilizing the new FHIR API standards, HIPAA-compliant semantic data stores, an industry-leading integration software, and over twenty years of clinical integration experience, Infor CIPHR will revolutionize how patients access information about themselves and start a massive shift back towards patient-centric care.

Infor CIPHR also focuses on the new trends and technologies in the wearable space. New wearables are introduced and adopted daily, and patients have far too many dashboards to manage all these applications. From Apple Watch, FitBit, Garmin, Smart Scales, etc., each device has its own dashboard, login, password, and credentials to manage. This is confusing and overbearing for patients. Infor CIPHR will be a wearable data store (repository instead?) that can capture, aggregate, and display data from over two hundred wearable/smart devices. This will provide a single point of entry for patients, cutting down on the need to remember several different logins into a siloed data environment. And if the patient chooses to share this information, the provider can also access these insights into the patient’s daily life and activity. With Patient Generated Health Data trending exponentially upwards in a clinical setting, it is critical that patients and providers be given a tool that can manage the petabytes of data in a single application, and CIPHR aims to solve that problem.



Section 2

Module Definitions 2

Infor CIPHR has several core modules, sub modules, sub-sub modules, etc. This section is a general overview of what each module does, interactions it has with other modules and will provide a high-level synopsis of how CIPHR works from a provider perspective.

1. **Dashboard:** The Dashboard is a collection of every module within the CIPHR application. The dashboard is completely customizable for each provider, in terms of layout, clustering, and displayed modules. Providers can add or remove modules as they desire. Each of the individual modules that can be displayed on the dashboard are listed below
   1. **My Patients:** This shows providers a list of all patients that have authorized access to their information through the Infor CIPHR platform. Providers can click on any patient image to be taken to the Patient Details module (section 2.1). Providers can also search by patient name to narrow down the results shown onscreen.
   2. **Schedule & Appointment Requests:** The provider’s current schedule, gathered from their source EMR system, will be displayed onscreen. Appointment requests generated by users will be displayed as well. See Schedule (section 5) for more detail.
   3. **Message Center:** Any messages created by users will be displayed here for the provider to quickly view and respond.
   4. **Report Center:** Several stock reports will be available to every provider, which have yet to be defined. Providers can manage all reports from the Report module.
   5. **Document Center:** Documents that have been uploaded by users or other providers will be presented here. This shows providers a quick view of all the information that is available to them. Providers can quickly drill down into each document for a more detailed view.
2. **Patients:** All the users that have granted access to the provider user will be displayed on the screen. Each patient can be selected and taken to the patient detail view. Providers will also be able to search for users using the system that have not granted access to their information. Providers can search by generic information or by patient ID. Access requests can be presented to users, or providers can “break the glass” to gain immediate access, in the event of an emergency.
   1. **Patient Details:** Providers can now see a detailed view of all electronically captured user information. Data displayed includes latest captured vitals, appointment history, current medications and prescriptions, allergies, lab results & orders, quantitative results, problems, documents, device and wearable data, and all patient history.
   2. **Access Patient Records:** Providers will be presented with a list of all the records that the patient has either manually uploaded or that have been added electronically via other data sources.
      1. **Patient Record Details:** Providers may view a single record view. Providers can view either the uploaded image or electronic version of the data. Providers may also zoom into the record, download the record (either directly into their source system or a PDF image), or print the record. Notes related to the record are displayed onscreen.
   3. **Upload Patient Records:** Providers have the ability to manually upload an image of any medical records that they have for the selected patient. Providers simply upload the image and enter any relevant details into the correct fields. The record is then sent to the user for approval, linking, and storage.
3. **Prescriptions:** Providers are presented first with any refill requests that have been generated by users. Providers can quickly approve or deny each individual request or drill down into patient details to review the decision. All medications that have been prescribed by the physician will also be displayed for tracking purposes.
4. **Documents:** Any document that has been linked to the provider will be displayed on this screen, with an attached patient image for quick identification. Providers can sort by document type, patient, or any other relevant criteria. Providers can click on each document to open a more detailed view of the information.
5. **Schedule:** Provider schedules are presented onscreen in a calendar view, similar to all widely accepted formats, such as Outlook or iCal. Providers can click on each date, week, or month to update the appointment widget. The appointment widget displays all the appointments for the selected time-frame. Appointment requests are also shown in a lighter color, to show the provider how the new appointment will affect their schedule. Providers can approve or deny each request from this module.
6. **Import:** Providers have the ability to import records that have been shared with them by users or other data sources. Providers will be presented with records that are pending approval. Providers can also scan QR codes generated by users for immediate ingestion. Providers may also import records directly into their EMR.
   1. **Pending Records:** All pending records are displayed on screen. Providers will be required to review patient information, and verify that they are responsible for that patient. Providers can either import the records, deny the request, or simply delete the request.
   2. **Scan Patient QR Code:** Patients have the ability to generate

QR codes that contain the information needed to immediately import the records they wish to share with the provider. Providers will simply scan the QR code, which will start the process of collecting the requested information.

* 1. **Import into Your EMR:** This allows providers to automatically import any linked records directly into their EMR, so providers may continue using the current workflows that they are accustomed to. Records will only be imported if the records are associated with a matching patient in the data source.

1. **Export:** Providers, per HIPAA requirements, will need to share information directly with users. This can be accomplished by generating a QR code the patient can scan or by exporting results directly from their EMR. All records stored in Infor CIPHR will be displayed for the selected user.
   1. **Generate QR Code for Patient:** During an office visit, a user may wish to directly import their records without approving the action at a later date. Providers will select all the records for the user that they request, and generate a QR code. The user then scans the code and receives all the requested records.
   2. **Export from your EMR:** Providers can also configure any records that are generated by the EMR to be automatically exported into Infor CIPHR. When a new record is created, the data is sent to Infor CIPHR, which will handle linking the information to the user and waiting for approval to save.
2. **Message Center:** Users will need to securely communicate with their providers, and the message center will provide the ability to send and receive secure encryption to the selected provider. Users will NOT be able to use this feature without properly authorizing themselves with the provider. All message traffic is encrypted, and only interactions are logged, not the content of the messages.

3



Section 3

System Architecture 3

System Architecture is a critical component of any application and must be carefully planned and implemented, with a special emphasis on agility and scalability, all while maintaining reliability, ensuring trust in users and administrators. By utilizing Cloverleaf as the data transmission layer, Infor CIPHR will provide end-users with an application that can dynamically scale to handle enormous upticks in message volumes, while maintaining a unique guaranteed-message delivery structuring. This ensures that all data is securely transmitted through a HIPAA-certified application, is not affected by an increase in user traffic, and that all data is available at all points in time.



All endpoints in this diagram are bi-directional. Using Cloverleaf as the middleware offers several distinct competitive advantages. Cloverleaf can be utilized as a FHIR endpoint, capable of producing and consuming FHIR messages. Cloverleaf is also capable of connection to legacy applications that rely on older technologies, which are more prevalent in the marketspace today. Web service servers/clients, TCP/IP via TLS or SSL, and sFTP are a few of the more secure options that can be utilized to transmit data. Additionally, Cloverleaf Secure Courier can be used as an on premise VPN replacement technology. Amazon Web Services (AWS) is Infor’s selected partner for all cloud-based services, and AWS will be utilized to store all patient data securely, in a HIPAA certified, secure data store. Providers will need to configure their EMR systems to send/receive data electronically from the Infor CIPHR instance. Patients will be able to access all their relevant data through a single access point.

Providers will be able to access and share their data using either a web application, a native iOS application, or a native Android application. Native applications are much more user-friendly; however, the web application will be developed first to offer immediate access to all users & providers, regardless of mobile device.



Section 4

Data Sources 4

This application will not work well without data sources. EMR vendors are very difficult to deal with when asking for custom integrations or interfaces. Infor CIPHR can be utilized to speed-up this process by allowing whatever data is available to be sent into the ingestion engine, where translation and manipulation of the data can occur in order to process it correctly. EMR vendors are slowly adopting the new FHIR standard, but not all have done so fully, so other options of sending/receiving data are required

**Initial Data Sources & Methods**

|  |  |
| --- | --- |
| **Vendor** | **Source** |
| Epic | open.epic.com sandbox |
| Epic | Patient Portal – myChart |
| Cerner | fhir.cerner.com sandbox |
| Cerner | Patient Portal - HealtheLife |
| Athenahealth | API sandbox |
| Smart on FHIR | SMART on FHIR sandbox |

As a note, this initial version of the application will focus on solely retrieving FHIR data via a supported API. However, in the real-world, EMR vendors will be slow to rollout the FHIR standard to production systems. It would not be relevant to develop and application that only speaks FHIR. Doing so would significantly lower the amount of disparate systems that can be targeted. By being able to support legacy systems that support only VPN, sFTP, encrypted TCP/IP, or any other format, Infor CIPHR will be able to integrate with any EMR system on the market. This has been proven by Infor Cloverleaf over the last 20+ years in the healthcare integration market. With Infor Cloverleaf being the backbone of Infor CIPHR, it will be able to connect to any system in existence today.

Section 5

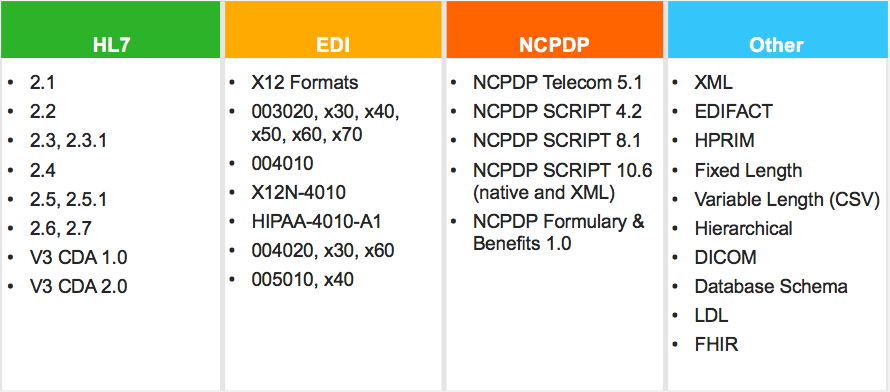
Data Formats 5

Infor CIPHR would be useless without data. It is critical that information flows through the system and that the information is in a format that can be understood by all end points. Infor CIPHR will communicate to end-users via a FHIR API, and it will target data sources that can currently produce FHIR messages. However, many data sources will not be able to talk FHIR for an extended period of time. Data content is more important than the format of the data. By utilizing Infor Cloverleaf as the ingestion engine, Infor CIPHR will be able to receive data in a number of widely accepted formats and convert that data into FHIR resources.

Infor CIPHR will have the ability to ingest and expose the required common data sets. This has been performed for over twenty years directly through Infor Cloverleaf, which will be used as the ingestion engine. Prebuilt content that is used in production systems currently will be imported into the Infor CIPHR instance and configured to receive and manipulate the following data sets, regardless of the format that is presented:

* Patient Name
* Sex
* Date of Birth
* Race
* Ethnicity
* Preferred Language
* Smoking Status
* Problems
* Medications
* Medication Allergies
* Laboratory Test(s)
* Laboratory Value(s)/Result(s)
* Vital Signs
* Care Plan Field(s), including Goals & Instructions
* Procedures
* Care Team Members
* Immunizations
* UDI(s)
* Assessment & Plan of Treatment
* Goals
* Health Concerns

All Supported Data Formats:





Section 6

HIPAA, Privacy, & Security 6

By adhering to HIPAA best practices and procedures, and using currently certified technology, Infor CIPHR will position itself as the market leader in security and privacy for patient information. These best practices and approaches have been tested in production settings for years, and will not require any software changes or potentially unknown breach points. Main areas of concern will be addressed in this section.

Several areas of potential security flaws exist in the Infor CIPHR application, including data transmission, data storage, patient identification, provider identification, sharing information between users, secure messaging, logging, and unauthorized access

**Data Transmission**

Moving PHI between endpoints over an unsecure, unencrypted connection is not acceptable, according to HIPAA and patient requirements. Infor CIPHR will use an encrypted communication protocol, depending on the data sources, that will securely ingest the PHI information directly from the source system. Data being sent downstream to the patient application will also be encrypted to a level well past the minimum HIPAA requirements. Infor CIPHR will not connect to or receive information from data sources that are unable to securely encrypt and transmit PHI.

**Data Storage**

Data at rest is required to be encrypted by HIPAA. By utilizing Amazon Web Services as the hardware partner, Infor CIPHR is able to achieve the necessary requirements set for by HIPAA in relation to secure data storage. Infor has used this approach in all cloud-based applications for years with no HIPAA violations to date.

**Patient Identification**

Users will be required to pass several forms of identification before accessing PHI information that may or may not belong to them. Users will have a login/password to access information, but they will also be required to authenticate using another form of identification, such as SSN lookup, secure text message, or other preferable methods.

**Provider Identification**

Users will have the ability to share information directly with their providers. It will be required that providers are also identified properly to prevent any unauthorized access into patient information. Providers will be required to be identified via NPI numbers and other characterizing traits that meet HIPAA requirements.

**Sharing Information Between Users**

Infor CIPHR will provide functionality to share information between end-users and providers. Both present unique challenges, but this functionality is needed in the healthcare industry. Without it, the application will not be successful

**Adding User Profiles and Sharing Records**: Users will be able to manage several profiles through a single login. This scenario relates to the head of the household managing records and data for spouses, children, and elderly parents. Profiles can be created by users and saved into the system. If the additional profile exists, then the newly added user profile must authorize sharing of the information to the newly linked profile. If the newly added profile does not exist in the Infor CIPHR platform, then the newly added user will have to authorize storing of their information via a secure messaging authorization process.

**Sharing Records Between Providers:** Users will need to transmit and receive information from linked providers. Users will be able to receive data from any provider within the Infor CIPHR platform. Users will be required to verify the information belongs solely to them before linking the information to their profile. Users will be presented with a de-identified view of the data to confirm. Once a user shares data to a provider, this transmitted data will be stored in a pending database that providers will need to review before accepting into their system or profile.

**Secure Messaging**

Users will have to ability to securely message any provider using Infor CIPHR. The provider will provide the user with an authorization code (generated for each user by Infor CIPHR) that the user will need to begin communication. Users will search by provider name and enter the authorization code before communication can begin. Once authorized, communication can begin. These messages are treated just like PHI data, and the messages are encrypted in transmission and at rest. Only the message endpoints will be logged; message content will not be logged or stored in any way.

**Logging**

Every interaction that takes place inside Infor CIPHR will be logged, per HIPAA requirements. Each connection, transmission, upload, and user interaction will be stored in a HIPAA compliant log store. Audit reports will be produced upon request.

**Unauthorized Access**

In the event that patient information is needed to be collected by a provider without prior approval from the patient, the provider will have the option to “break the glass” and collect the needed information. This is only needed in life/death situations to the patient, and will be reviewed manually by Infor staff before notifying any parties that may have legal actions available to them. This practice is common with Health Information Exchanges today, and is a necessary evil, in order to save patient lives.