

Infor Cloverleaf Integrated Patient Health Repository (CIPHR)

Technical Specification

User Version

Version 3.1.1

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**

**Section 2: Module Definitions 5**

**Section 3: System Architecture 11**

**Section 4: Data Sources 13**

**Section 5: Data Formats 15**

**Section 6: HIPAA, Privacy, & Security 17**



Section 1

Introduction 1 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 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 user perspective.

1. **Dashboard:** The Dashboard is a collection of every module within the CIPHR application. The dashboard is completely customizable for each user, in terms of layout, clustering, and displayed modules. The user can add or remove modules as they desire. Each of the individual modules that can be displayed on the dashboard are listed below:
   1. **Upcoming Appointments:** Users can see upcoming appointments that they have scheduled (and has been confirmed) with their provider. Users can also schedule appointments with their provider.
      1. **Schedule Appointments:** Users can schedule appointments with providers who have authorized this action to occur.
   2. **Prescriptions:** Users can see the current prescriptions they are taking and the prescriptions have been prescribed in the past. They can also request refills of prescriptions that are running low.
   3. **Medications:** Users can see the medications that they are currently taking. Users can also request refills of any medications that may be needed.
   4. **Profile Image:** A profile image is used to show the user which dashboard is being monitored, and different profiles (user, spouse, child, etc) can be displayed by the user.
   5. **Latest Vitals:** Users can see the most recent vital measurements that were captured in the last recorded care episode. Vitals can include blood pressure, cholesterol, body temperature, heart rate, blood glucose, height/weight, blood type, and respiratory rate, etc. Users can customize this display to see what is most relevant to themselves.
   6. **Financials:** Users can see the profile’s current insurance cards, deductible information, and costs. Each of these metrics can be expanded based on user input.
   7. **Message Center:** Users can securely message their providers, once properly authenticated. Unread messages, received messages, and sent messages can be seen here.
   8. **Fitness:** Data captured from wearable devices will be displayed here. Depending on the device, data such as BMI, calorie expenditure, steps taken, distance walked, sleep, activity level, flights climbed, and other activity metrics can be displayed.
2. **Records:** Records is a visual display of all records, either manually uploaded, captured in a picture, imported directly from the physician, or any other method of delivery. Users can see records related to all linked profiles to easily manage family records as well. Users can click on individual records to move into Record Details.
3. **Record Detail:** Record Detail shows users the details of the selected record. If multiple pages are stored, users can swipe/click to move from page to page. Users have the option to Zoom, Edit Record, Send Record, Download Record, and Print Record.
   1. Zoom: Shows an enlarged view of the selected record.
   2. Edit Record: Users can edit manually uploaded records.
   3. Send Record: Users can send the selected recorded to a provider (see section 8 for more detail).
   4. Download Record: User can download an electronic copy of the selected record.
   5. Print Record: User can print the selected record.
4. **User Profile:** Users can see specific information pertaining to the selected profile, including metrics relevant to CIPHR, Insurance Information, Allergies, Current Medication Tables, Emergency Contact, Primary Care Providers, Other Providers, and Advance Directives
   1. User Details: Shows the user the number of records for that profile, number of uploaded photographs, blood type, organ donor selection, phone number, and date of birth.
   2. Insurance Information: Shows the insurance information of the selected profile. Users can upload insurance card pictures and any relevant details to that insurance policy.
   3. Allergies: A list of all collected and manually entered allergic details. All allergic information entered by providers will be present, and details entered by the user will be passed to providers.
   4. Current Medications: A table list of all currently prescribed medications captured from providers. Users can also upload any externally prescribed medications or over the counter medications (e.g., vitamins or dietary supplements).
   5. Emergency Contact: Displays the emergency contact information for the selected profile. Users can add new contacts and manage existing contacts.
   6. Primary Care Provider: Displays the primary care provider for the selected profile. Users can also change the selected primary care provider.
   7. Other Providers: A list of other providers that have contributed to the user’s record list. Users can also manually add new providers, which could include dentists, OB/GYN, and other specialists.
   8. Advanced Directive: Displays to the user any advance directive that has been authorized by the user. Users can change this information and share with other profiles or providers.
5. **Add Profile:** Users have the ability to manage multiple profiles from a single login. This is aimed at the head of the household who need to manage the records of his/her spouse, children, or elderly parents. Profiles that the user can view/manage will be displayed on the left-hand toolbar. If the profile already exists, the requested profile will be required to approve sharing of the information, per HIPAA requirements.
6. **Add Record:** Users have several options to retrieve their clinical information. Rather than having a manila folder with printed paper records, users can now have an electronic copy, managed solely by the user. Users can retrieve records by scanning a barcode generated by a provider to directly import pending records, and they can manually upload paper records via an image.
   1. Scan Barcode: To expedite the process of collecting electronic copies of records, users can ask providers to generate a secure QR code that contains all relevant information needed to import the medical details of their latest visit. Users will scan the generated QR code, verify they are the record holder, and import the record directly into their record list.
   2. Import Record: If the provider has decided to automate the process of sharing electronic records, the user will see a list of pending records that have been shared with them. Users will select the profile to use, search for the provider name, clinic name, or other identifying details, and then users can select individual records to import into their record list, or import all linked records
   3. Manual Upload: If providers do not have the ability to electronically share the user’s records, the user still needs to generate an electronic copy of the record. This can be done by either uploading a PDF shared by the provider or a picture taken of a paper copy of the record.
7. **Request Record:** Users need to have the ability to import records from current or past appointments. Based on the selected profile, doctor/clinic name, fax number to send the request, and date of service, the user can generate a request to contact the provider directly. Users have the delivery options of email, fax, direct mail, picking up records in person, or BlueButton+. Once all fields have been properly filled out, a secure fax is generated and sent to the provider. Users are then notified of any HIPAA violations that may occur if the provider does not comply, and how to pursue those channels.
8. **Send Record:** Users will need to have the ability to send records to providers at a moments notice, regardless of how the provider needs that information. Patients will select the profile to use, which will dynamically generate and display the stored records. Users can then generate a QR code for the physician to scan, deliver manually, or securely send directly to the provider.
   1. Generate QR Code: If providers need immediate access to a record, patients can generate a QR code that can be scanned during an office visit or while in-person with the user.
   2. Delivery Manually: User can enter the name of the recipient and deliver the selected record via secure email, secure fax, or BlueButton+.
   3. Send to Provider: Users can send records directly to the provider without having to be present in-person. These records will be send to a “pending records” list, where the provider can approve, deny, or delete any records that have been sent to them.
9. **Search Records:** Users can perform a search on any existing records stored in the CIPHR data-store. Users can search by profile or record category.
10. **Device Center:** The device center is the primary location for all devices associated with the selected profile. All connected devices will be listed on screen, along with the status of the device and the last known update. Users can Add a New Device, Refresh Individual Devices, and Disconnect Individual Devices.
    1. Add New Device: Users can select from 200+ preconfigured device profiles, quickly and securely. The user will be presented with the list of device profiles, and they can select the preferred device. The user will then enter login credentials for the device API and authorize CIPHR to automatically collect the generated data.
    2. Refresh Device: If a device has gone offline, or a change is introduced by the device manufacturer, the user may need to refresh device connections periodically.
    3. Disconnect Device: If a device is no longer used, or the user simply doesn’t want to capture the generated data any longer, they can simply disconnect from the API and the device will be removed from the device store.
11. **Message Center:** Users will need to be able 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.



Section 3  
System Architecture3 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. Providers can also access patient information while using the Infor CIPHR provider version.

Patients will be able to access 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, 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. t 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 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 twenty years in the healthcare integration market. With Infor Cloverleaf being the backbone of Infor CIPHR, Infor CIPHR will be able to connect to any system in existence today.



Section 5

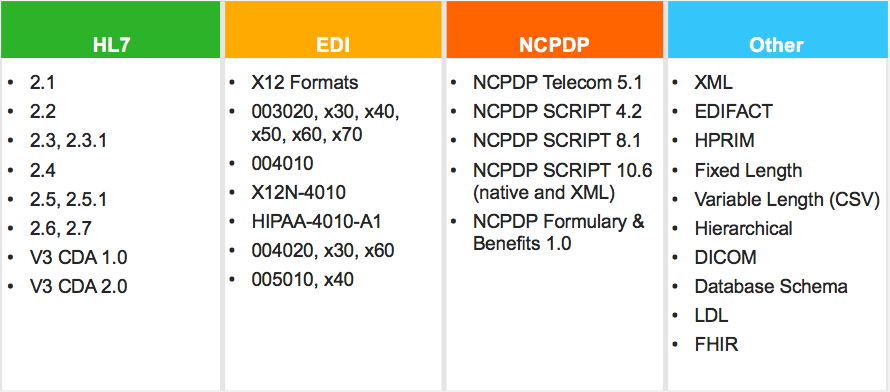
Data Formats 5

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 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.