

Digital Bridge Electronic Case Reporting (eCR)

Technical Specifications (8/29/2018)

Statement of Purpose

This document specifies or refers to additional documentation that collectively prescribe the data content, technical and security requirements to enable a participating organization (participant) to transmit electronic initial case reports (eICRs) to the Association of Public Health Laboratories (APHL) Informatics Messaging Services (AIMS) platform for evaluation by the Reportable Conditions Knowledge Management System (RCKMS) and subsequent return of a reportability response (RR) by the AIMS platform to the participant. When APHL transmits an eICR or RR to a public health authority for the permitted purpose on behalf of a participant that has elected to have APHL make such transmissions, APHL is responsible for doing so in compliance with applicable law and regulation, the Digital Bridge Pilot Participation Agreement and the following specifications. This document refers to additional implementation guidance, migration plans and other technical materials and resources that offer information to participants but do not themselves create compliance obligations.

For general background on the Digital Bridge collaborative or the electronic case reporting (eCR) use case, visit digitalbridge.us.

Audience

Any organization interested in using services on the AIMS platform to accomplish eCR as part of Digital Bridge should review this document in detail. Review of this document is a prerequisite to signing the Digital Bridge Pilot Participation Agreement or Joinder Agreement (as applicable). Participants may include health care provider organizations, health information exchanges, health departments that provide clinical services or other organizations.

Document Control Information

Document Name	Digital Bridge Electronic Case Reporting (eCR) Technical Specifications (Specifications)
Project Name	Digital Bridge: The Digital Intersection of Healthcare and Public Health, Electronic Case Reporting (eCR)
Initial Date	8/29/2018
Version	1.0

Change and Notice Log

The Digital Bridge eCR Implementation Workgroup adopted this document, and it is referenced in the Digital Bridge Pilot Participation Agreement. Changes or revisions to this document will result in notice in accordance with Section 7.3 of the Pilot Participation Agreement.

Date of Change	Change Description	Author	Date of Notice to Digital Bridge Pilot Participation Workgroup/Participants	Effective Date

Pre-Onboarding and Onboarding Guidance

- Additional documents are in development to guide all stakeholders participating in Digital Bridge eCR pilots through the pre-onboarding and onboarding processes and will be posted to digitalbridge.us once available.
- Select tasks for provider and vendor pre-onboarding are shown in Appendix A.

Data Content Requirements

- The eCR workflow uses a Health Level 7 (HL7) standard that provides one format, known as the eICR, for all reportable conditions to streamline reporting for providers and vendors. Participants will submit eICRs that comply with the *HL7 CDA® R2 Implementation Guide: Public Health Case Report, Release 2: the Electronic Initial Case Report (eICR), Release 1, STU Release 1.1 - US Realm*, available for download at http://www.hl7.org/implement/standards/product_brief.cfm?product_id=436.
 - Sample eICRs with synthetic patient data are available upon request.
- The Reportable Conditions Trigger Codes (RCTC) are a set of industry standard codes (e.g., ICD-10, LOINC, SNOMED) that are implemented in an electronic health record (EHR) system at the clinical care organization and matched against information in a patient encounter to initiate eICR generation. The RCTC provide a preliminary identification of which encounters, out of the millions of EHR encounters, may be of interest to public health. The codes are not jurisdiction-specific but represent any event that may be reportable to any public health agency in the United States. The RCTC are available at <https://phinivads.cdc.gov/vads/SearchVocab.action>.
 - The RCTC work in conjunction with the RCKMS is part of a two-step process to determine the reportability of an event. The RCKMS provides a second level of evaluation against jurisdiction-specific reporting regulations to confirm whether the triggered event is reportable and to which public health agency.
- The AIMS platform will return a RR to the appropriate participant and public health authorities that complies with the *HL7 CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.0 - US Realm* available for download at http://www.hl7.org/implement/standards/product_brief.cfm?product_id=470.
 - Sample RRs with synthetic patient data are available at https://gforge.hl7.org/gf/project/pher/scmsvn/?action=browse&path=%2Ftrunk%2FPHCASERPT-RR%2Fxml%2Fsamples%2FCDAR2_IG_PHCR_R2_RR_D1_2017DEC_SAMPLE.xml&view=log.

Technical Requirements

Supported Transport Protocols

- The AIMS platform supports a wide variety of transport mechanisms to support data trading partners. The AIMS platform can securely receive and send eICRs and RRs via:
 - Direct XDR
 - IHE XDR
 - NwHIN XDR
 - PHINMS
 - SFTP
 - AWS S3
 - Rhapsody comppoint and Mirth channel are available for sending eICRs and receiving RRs.
 - Web Services
- The AIMS platform also provides Virtual Private Network (VPN) connectivity for partners that require it.

Data Storage and Destruction

- eICR data received from participating organizations is stored by the AIMS platform for seven days to allow for any resubmission of data, if needed. Storing these data for this time period allows the AIMS and RCKMS support teams to investigate potential issues or questions related to an individual eICR or RR.
 - Both automated and manual processes for the AIMS environment ensure that eICR data are deleted after seven days.
 - Since eICR data are not stored past seven days, no service provided by AIMS or RCKMS makes any attempt at patient matching, eICR deduplication or electronic laboratory reporting (ELR) merging.
 - Audit logs containing metadata are retained by AWS storage options (e.g., Elasticsearch, S3, Glacier and EFS.)
 - The specific audit log data for the eCR use case will be defined following further exploration with the pilot sites. Audit log data may include date and time of receipt, sender, transport mechanism, and payload name.
- RCKMS does not retain any data once determination is made.

Security Practices

The following describe the security practices of the AIMS platform.

- The AIMS platform uses AWS for cloud web hosting and meets Federal Information Security Management Act (FISMA) moderate and HIPAA compliance. AIMS is compliant with the requirements of NIST 800-53 and undergoes third-party audits and penetration tests.
 - Executive summaries of A-LIGN or similar third party security audits are available from APHL upon request. An A-LIGN summary from 2016 is available in Appendix B.
 - The next audit and penetration test is planned for late 2018.

- Data received by the AIMS platform from participating organizations is encrypted at rest with Key Management Service (KMS) during its entire lifetime (i.e., from entry at AIMS to when an eICR or RR is sent out of AIMS) and logged every time the key is used. Additionally, all internal AIMS data transport between systems are encrypted and audited.
- The AIMS platform uses both a traditional and AWS Web Application Firewall (WAF).
- User access to applications housed and secured on the AIMS platform is very limited and is controlled using a stringent process requiring individuals to complete a robust Network Access Request Form (NARF). Depending on the use case, background checks (or confirmation of) may be required. For individuals requesting access to protected health information (PHI), the process is even more involved. See APHL's AIMS Security Practices FAQ document available at <https://aimsplatform.com/#/landing> for more information. However, neither participants nor public health authorities will have access to PHI within the AIMS or RCKMS environments for the eCR use case. Public health authority staff who access the RCKMS Authoring Interface must complete the NARF and, once approved, are then assigned login credentials that represent an additional layer of access and security.
 - Participants of Digital Bridge (as defined in the Pilot Participation Agreement) are not able to view data from other participants.
 - Participant data will be securely routed to public health authorities, as appropriate. See the *Use of eICR Data* section of this document for more details.
 - Limited AIMS and RCKMS technical staff will have access to PHI from eICRs and RRs for troubleshooting purposes.
- The AIMS platform maintains a Systems Security Plan (SSP) to provide security processes and procedures and to satisfy audit requirements. As use cases are added and the AIMS platform evolves, this SSP is revised and updated.
- eCR is one of approximately 20 use cases supported by the AIMS platform since its inception in 2008. Data from each use case are maintained separately on the AIMS platform.
- AIMS maintains a thorough Business Continuity Plan focused on a wide range of possible interruptions, including disasters.
- The AIMS platform supports both two-factor authentication and federated options for access control. For the eCR use case, this applies to public health authority staff who login to the RCKMS Authoring Interface. A white paper detailing two-factor authentication for the AIMS platform has been provided in Appendix C.
 - Additional information on federation capabilities is available at https://www.keycloak.org/docs/3.3/server_admin/topics/identity-broker.html.

Use of eICR Data

- The AIMS platform validates every eICR received from participants for structure and required data.
- Valid eICRs are sent to RCKMS for decision support (e.g., determination of reportability, determination of which public health authorities should receive the eICR/RR).
 - Prior to a site going live with the Digital Bridge eCR approach, public health jurisdictions input and manage their reporting criteria into a web portal, known as the RCKMS Authoring Interface. Initial reporting criteria are authored by a jurisdiction as part of each pilot site's onboarding process. Additional information on RCKMS is available at <https://www.cste.org/members/group.aspx?code=RCKMS>.

- The entered criteria get stored as machine-processable rules used by the RCKMS decision support. Reporting information can also be output as human-readable formats.
- The RCKMS decision support service processes information in the eICR (e.g., patient location, health care provider location, lab results, diagnoses) against authored reporting specifications to determine whether an eICR is reportable and to which public health authorities. This service drastically simplifies the complexity health care providers encounter in meeting multiple jurisdictions' reporting requirements.
- Based on RCKMS determination, AIMS creates an RR and routes the eICR and RR to the appropriate public health authorities. See Appendix D for visual representations of this process.

Support Contacts

AIMS: informatics.support@aphl.org

RCKMS: rckms@cste.org

Appendices

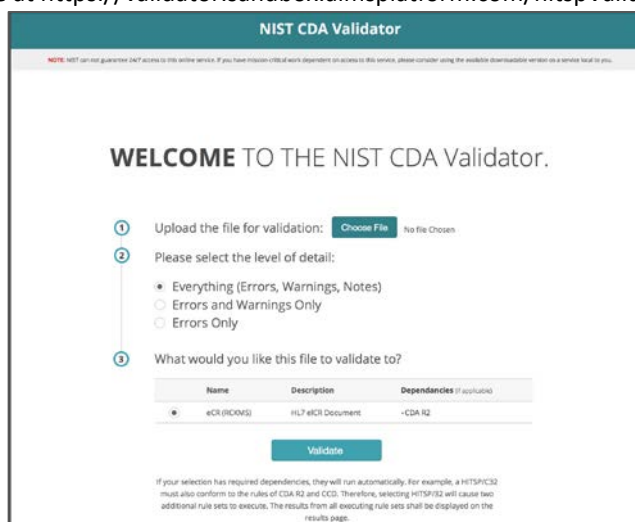
Appendix A. Pre-Onboarding Tasks

Provider Tasks

- Implement and update vendor software (i.e., EHR) capable of generating an eICR
- Map local codes to the Reportable Conditions Trigger Codes (RCTC) if using local codes
- Implement the RCTC and establish a process to maintain the most up-to-date version
- Ensure eICRs generated pass validation (without sending to the AIMS platform) using the AIMS Online Validator, available at <https://validator.sandbox.aimsplatform.com/hitspValidation2/>
- Test triggering and eICR generation during end-to-end testing (sending it to DSI)
- Use provided test scenarios to trigger and generate eICRs
- Add test package scenarios, if needed, to cover breadth and depth of testing scenarios
- Implement the ability to receive and attach the RR to the patient chart
- Provide POC for all technical work and communications

Vendor Tasks

- Implement functionality to support eICR 1.1 generation
 - Include the requirements for the eICR fields and the workflows
- Ensure eICRs generated pass validation (without sending to the AIMS platform) using the AIMS Online Validator, available at <https://validator.sandbox.aimsplatform.com/hitspValidation2/>



The screenshot shows the NIST CDA Validator web application. At the top, there is a teal header with the text "NIST CDA Validator". Below the header, a small red warning message states: "NIST: NIST cannot guarantee 24/7 access to this online service. If you have mission-critical work dependent on access to this service, please consider using the available downloadable version on a server local to you." The main content area has a heading "WELCOME TO THE NIST CDA Validator." followed by three numbered steps: 1. "Upload the file for validation:" with a "Choose File" button and "No file chosen" text; 2. "Please select the level of detail:" with three radio button options: "Everything (Errors, Warnings, Notes)" (selected), "Errors and Warnings Only", and "Errors Only"; 3. "What would you like this file to validate to?" with a table of options. The table has three columns: "Name", "Description", and "Dependencies (if applicable)". The first row shows "eICR (RCKMS)" with description "HL7 eICR Document" and dependency "-CDA R2". Below the table is a "Validate" button. At the bottom, a small disclaimer states: "If your selection has required dependencies, they will run automatically. For example, a HITSPIC32 must also conform to the rules of CDA R2 and CDS. Therefore, selecting HITSPIC32 will cause two additional rule sets to execute. The results from all executing rule sets shall be displayed on the results page."

- Share system generated eICR with the eCR Standards, AIMS, and RCKMS teams for content review and to test system generated eICRs with the AIMS test environment
 - Digital Bridge will provide a Standards team contact list for user convenience
 - The AIMS and RCKMS team will review validator output, decision support (RCKMS) and RR data
- Provide Point of Contact (POC) for all technical work and communications
- Add test package scenarios, if needed, to cover breadth and depth of testing scenarios



Patina Zarcone-Gagne
Director, Informatics
Association of Public Health Laboratories
Tallahassee, Florida 32312

June 20, 2016

Dear Ms. Zarcone-Gagne

Thank you for the opportunity to provide security services to Association of Public Health Laboratories. Summarized below are the scope, approach and results of the security assessment performed.

The Association of Public Health Laboratories (APHL), in association with the Centers for Disease Control (CDC) and many state and local Public Health Laboratories (PHLs) and Public Health Agencies (PHAs), has developed the APHL Informatics Messaging Services (AIMS) Platform focused on secure health information exchange. AIMS is a secure, cloud based environment that accelerates the implementation of health messaging by providing shared services to aid in the transport, storage, analysis, validation, translation and routing of electronic data.

PHLs and PHAs require a health information exchange network that focuses on the common tasks of message routing, translations/transformations and certificate management. Through AIMS, laboratories can be configured to send and receive messages with many different partners with minimal configuration per partner set-up. This reduces the burden of managing these tasks for individual laboratory and agency partners and facilitates more rapid implementation of secure electronic message exchange. The messages being routed via AIMS are encrypted and the payload is not decrypted or processed by AIMS, unless specified by the trading partners involved in the use case/project.

The PHINMS (Public Health Information Network Messaging System) is the technological foundation for the AIMS. It is the software messaging system provided by the CDC that features a secure and reliable way for information systems to exchange messages. The messages can be in text or binary formats and may use a standard specification, such as HL7, but the actual content is not important. The system securely sends and receives encrypted data over the Internet to public health information systems using Electronic Business Extensible Markup Language (ebXML) technology. In a typical configuration, a trading partner or laboratory will send messages directly to another partner using PHINMS. This is known as a direct send model, in which both partners must have complete PHINMS implementations and configurations. Although direct send is a feasible, secure method of exchanging data, the addition of each new partner to the community results in exponential growth of direct connections and maintenance. An alternative configuration is a hub model, in which multiple partners enter into an agreement to send messages by connecting to one or more central hubs, like the AIMS.

Demand from the public health space created momentum for APHL to begin offering additional services – services other than PHINMS message payload routing. Those services include:

Additional transport protocols:

- AWS S3
- VPN
- SFTP
- Web Services
- Direct

Additional services like:

- Translation/Transformation (Mirth and Rhapsody)
- Hosting
- Archiving/Backup
- Disaster Recovery/Business Continuity
- Transport Interoperability
- Remote Desktop (AWS Workspaces)
- Web Portals

A-LIGN performed an assessment to determine the Company's compliance with the relevant controls defined in the controls families in NIST 800-53 listed in the table below.

Access Controls	Media Protection
Awareness and Training	Physical and Environmental
Audit and Accountability	Planning
Security Assessment & Authorization	Personnel Security
Configuration Management	Risk Assessment
Contingency Planning	System and Service Acquisition
Identification and Authentication	System and Communications Protection
Incident Response	System and Information Integrity
Maintenance	Program Management

Based on A-LIGN's understanding of the Company's control environment and information provided by the Company, the information system is classified as a FISMA Moderate information system based on the Federal Information Processing Standards Publications 199 Standards for Security Categorization of Federal Information and Information Systems (**FIPS 199**). As such, the assessment activities performed by A-LIGN assessed the environment as a FISMA Moderate information system.

A-LIGN performed testing procedures based on the scope and locations defined in the Company's System Security Plan ("SSP") to determine if the controls listed in the SSP Baseline Security Controls and defined by NIST 800-53 revision 4 were implemented and operating as required. Testing procedures followed the guidance provided in NIST 800-53A revision 4 included interviewing Company personnel, inspecting evidence such as Company policies and procedures and system security setting, observing Company personnel and selecting samples of Company system components to ensure the Company's controls are in place.

Based on results of A-LIGN's testing procedures the information system was deemed compliant with the requirements of NIST 800-53.

If you have any questions or would like to discuss the assessment in detail please feel free to contact me at 888-702-5446 or Gene.Geiger@A-LIGN.com.

Sincerely,



Gene Geiger, Partner A-LIGN

Association Of Public Health Laboratories
(APHL)

AIMS 2-Factor Authentication Functionality

V2

APHL Association Of Public Health

AIMS 2-Factor Authentication

Functionality

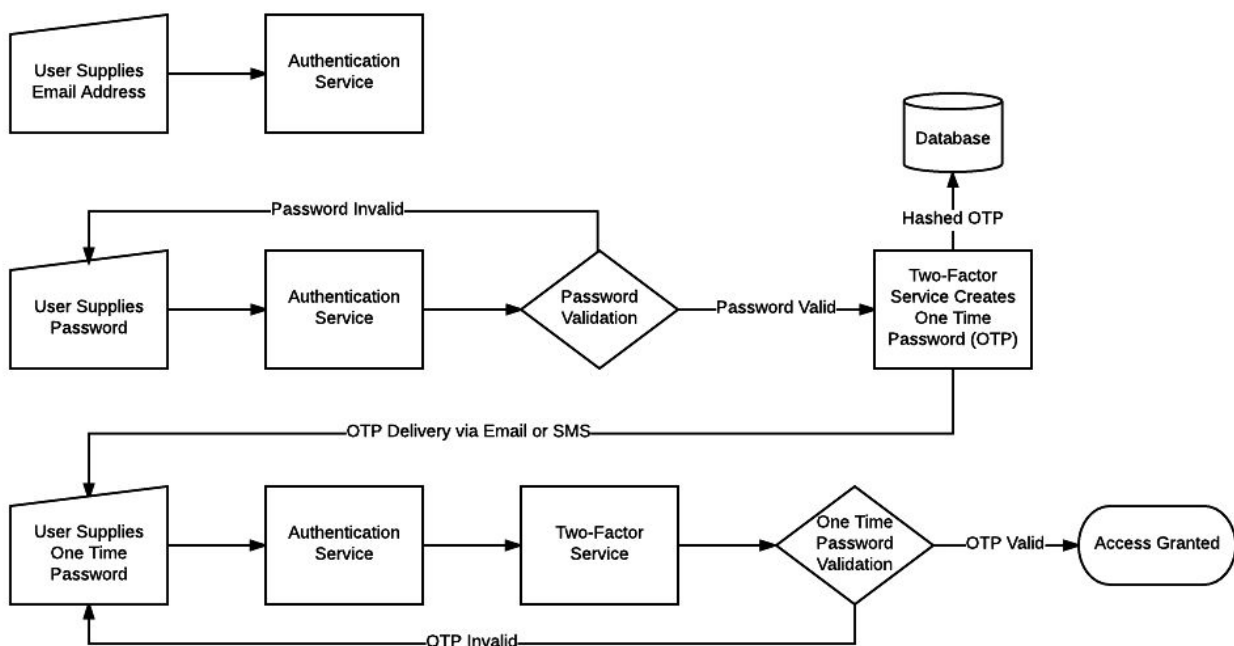
Overview

Our two factor authentication setup provides an added layer of security to the AIMS Platform. Users are required to provide both standard credentials (email and password) as well as a temporary one time use code. Successfully authenticated users will be remembered and allowed to only provide email and password when logging in from the same browser and IP for a 30 day period. This balances the needs of secure systems with convenience and usability.

Login and Authentication Process

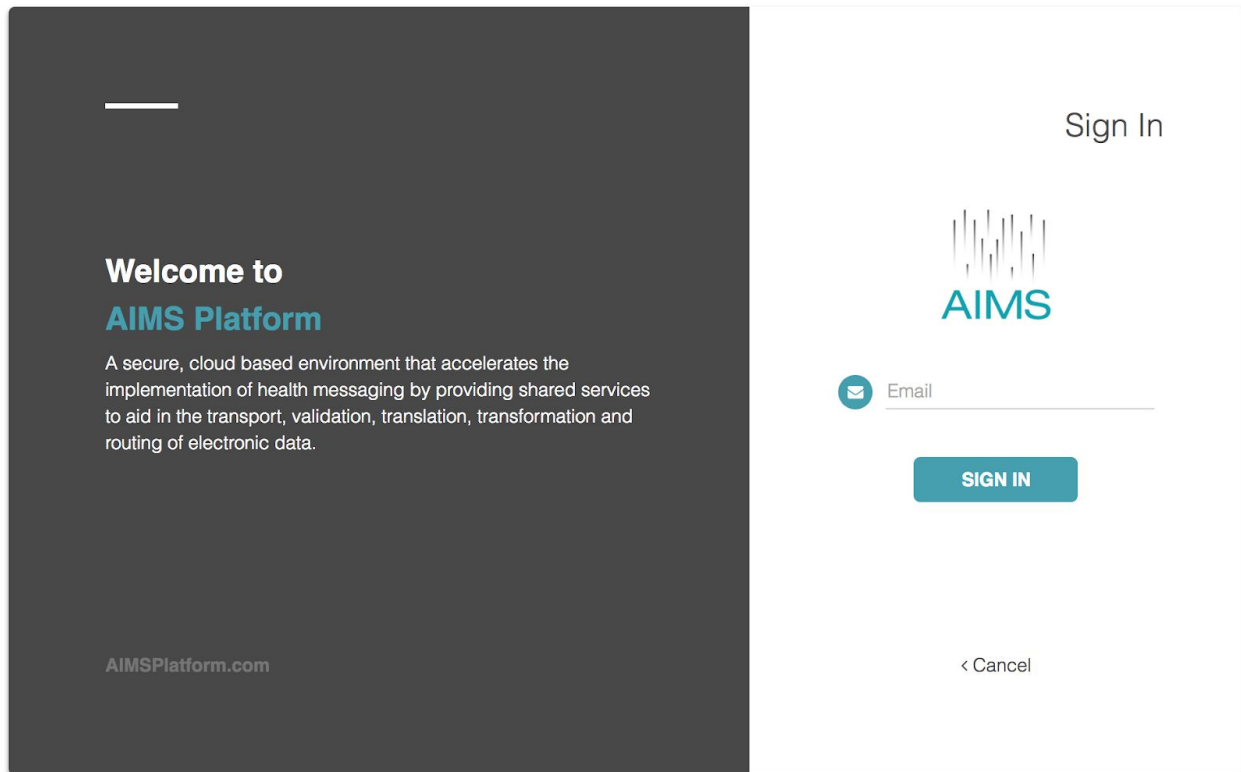
Flow Visualization

The complete login flow is shown in the diagram below and detailed on the next few pages with accompanying screenshots. Credentials supplied by the user are sent to the authentication service, which is responsible for validating them and communicating with the two-factor authentication service. When all steps are successful, the user receives a signed authentication token and is able to access AIMS Platform components.



Email Submission

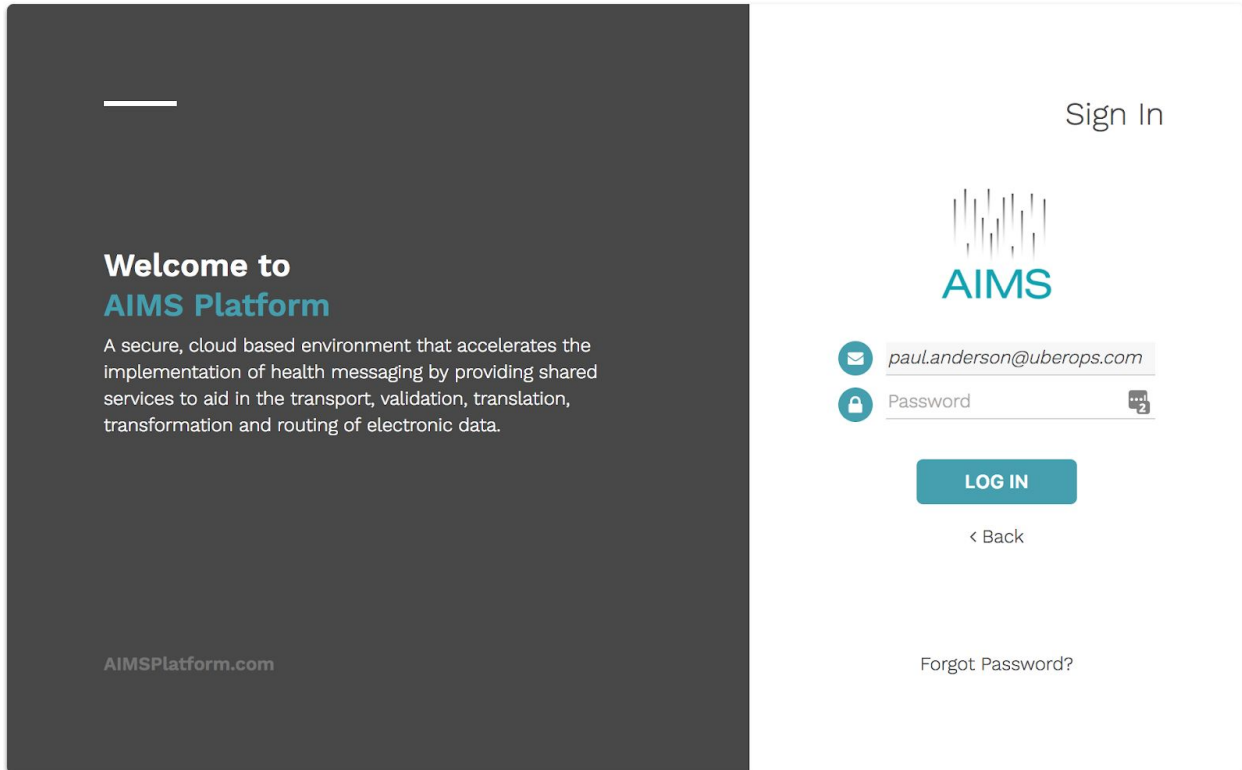
The AIMS Platform provides a login frontend, which first asks users to supply an email address.



The image shows a split-screen login interface for the AIMS Platform. The left side has a dark gray background with white text. It features a horizontal line, the heading "Welcome to AIMS Platform" (with "AIMS Platform" in teal), a paragraph describing the platform as a secure, cloud-based environment for health messaging, and the URL "AIMSPlatform.com" at the bottom. The right side has a white background. It includes the text "Sign In" at the top right, the AIMS logo (a stylized bar chart above the word "AIMS" in teal), an email input field with a teal envelope icon and the placeholder text "Email", a teal "SIGN IN" button, and a "< Cancel" link at the bottom.

Password Submission

A password is then submitted and verified via [Keycloak](#), which we use for identity management and most authentication services.




The screenshot shows a two-column layout. The left column has a dark grey background and contains a horizontal line, the text 'Welcome to AIMS Platform', a paragraph describing the platform as a secure, cloud-based environment for health messaging, and the URL 'AIMSPlatform.com' at the bottom. The right column has a white background and contains the 'Sign In' header, the 'AIMS' logo, an email input field with the placeholder 'paul.anderson@uberops.com', a password input field with a lock icon and a 'Show/Hide' toggle, a teal 'LOG IN' button, a '< Back' link, and a 'Forgot Password?' link.


Welcome to
AIMS Platform

A secure, cloud based environment that accelerates the implementation of health messaging by providing shared services to aid in the transport, validation, translation, transformation and routing of electronic data.


AIMSPlatform.com


Sign In





paul.anderson@uberops.com



Password 

LOG IN

< Back

Forgot Password?

Temporary One Time Password Submission


A temporary one time password is then generated and delivered via email or SMS depending on the user's preference. The password is valid for only 15 minutes and a single use.

Welcome to AIMS Platform

A secure, cloud based environment that accelerates the implementation of health messaging by providing shared services to aid in the transport, validation, translation, transformation and routing of electronic data.


AIMSPlatform.com

Log in to
aimsplatform



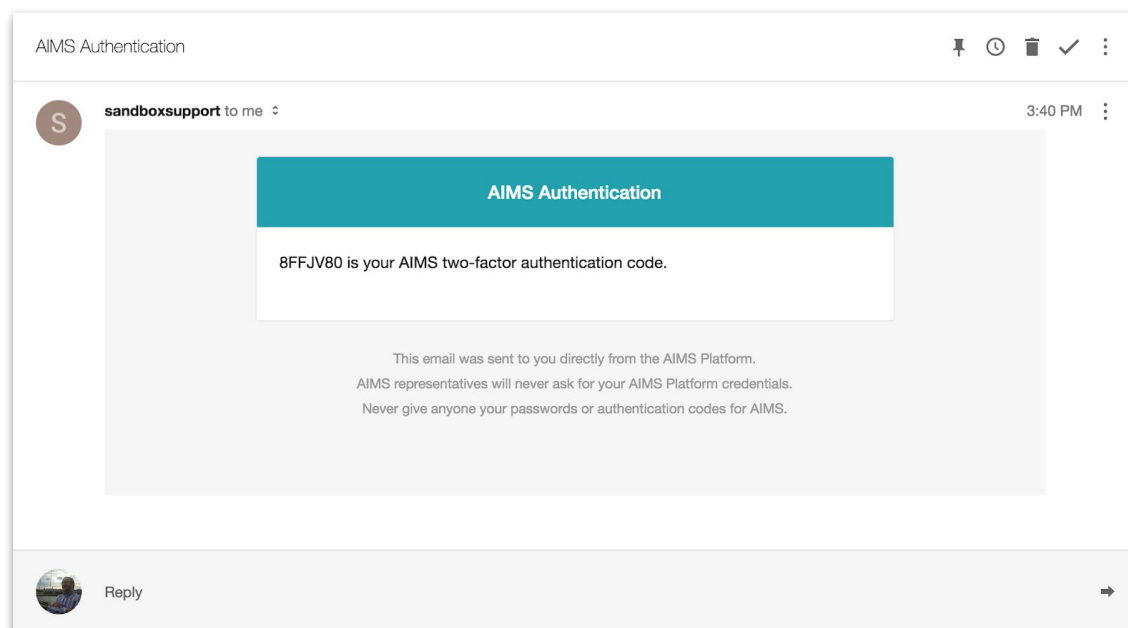
Authentication Code

A two factor authorization code has been delivered to your phone or email. Provide this code or a printed code to continue.



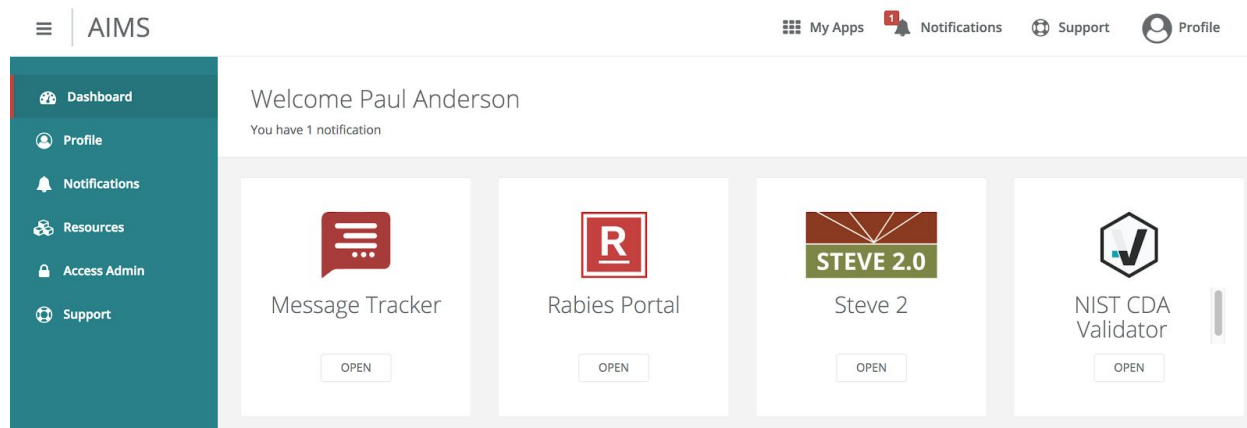
SUBMIT

CANCEL



Authentication Complete

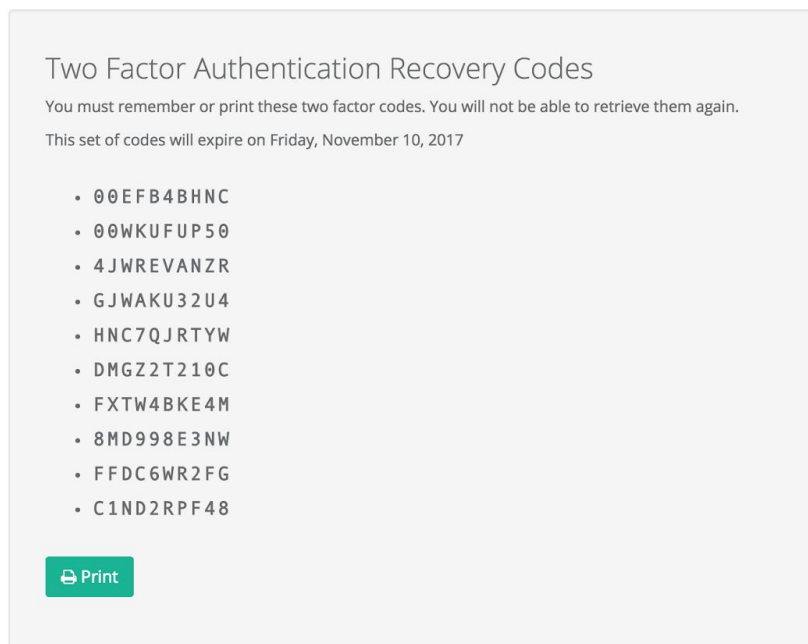
Users will be successfully authenticated and able to access AIMS applications after submitting a correct email, password, and temporary one time password.



Printable recovery codes may then be generated and saved from the User Profile page. These are particularly useful for users with limited email or SMS access and may be used in lieu of on-demand delivered codes.

Recovery codes

Two factor authentication recovery codes setup.



When requesting new printable codes, your old printable codes will be made invalid.

[Get recovery codes](#)

Generation and Storage of One Time Passwords

Temporary one time passwords are generated from cryptographically strong pseudo-random bytes. The bytes are encoded using base32 and uppercased for readability. Resulting passwords are a combination of letters and numbers that are both secure and human friendly. For example, the letter O and the number 0 are treated as equivalent and interchangeable.

Hashes of both user selected passwords and one time passwords are created using bcrypt and stored in an encrypted database. Validation of password logins and two-factor authentication attempts is completed without storing any plaintext passwords.

Expiration of One Time Passwords

The temporary nature of the one time passwords comes from expiration timestamps that are set when the password hashes are saved. On-demand delivery codes are set to expire in 15 minutes; printable authentication codes are set to expire in 3 months. In order to prevent anyone from unintentionally losing access to the AIMS Platform, users are notified both 5 days and 1 day before printable codes expire.

As a cleanup operation, expired codes are periodically removed, but it is important to note that they are treated as invalid regardless of removal from the database.

Appendix D. Digital Bridge eCR Process Diagrams

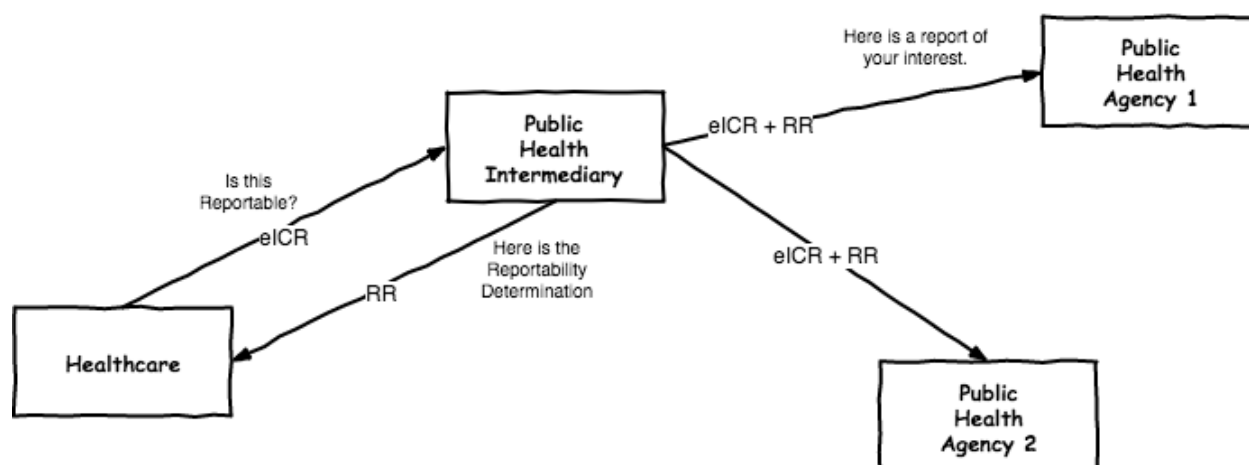


Figure 1. High-Level Overview of Public Health Intermediary Facilitation of eCR

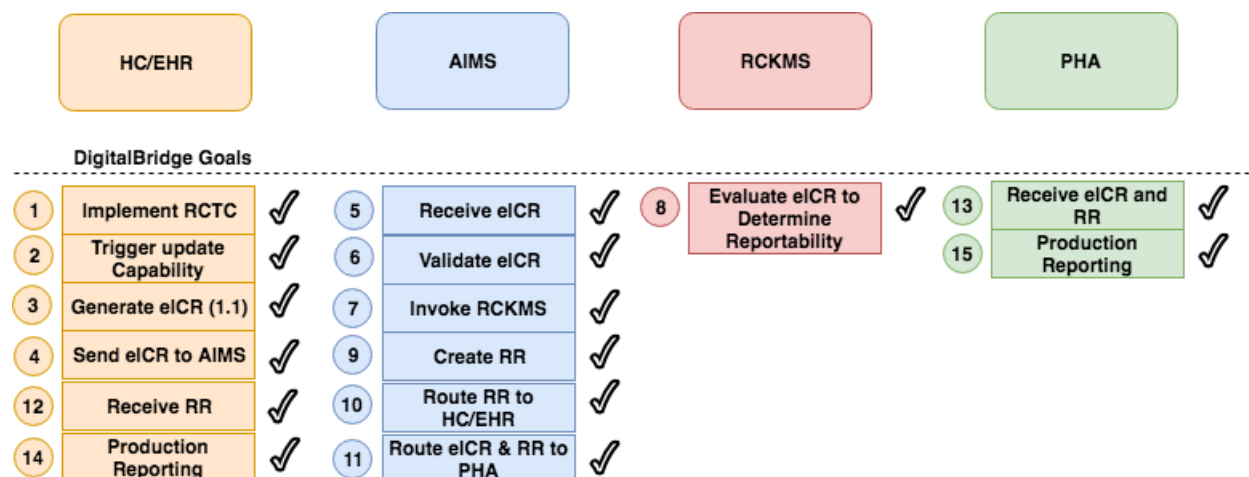


Figure 2. Goals of the Initial Implementations of the Digital Bridge eCR Approach

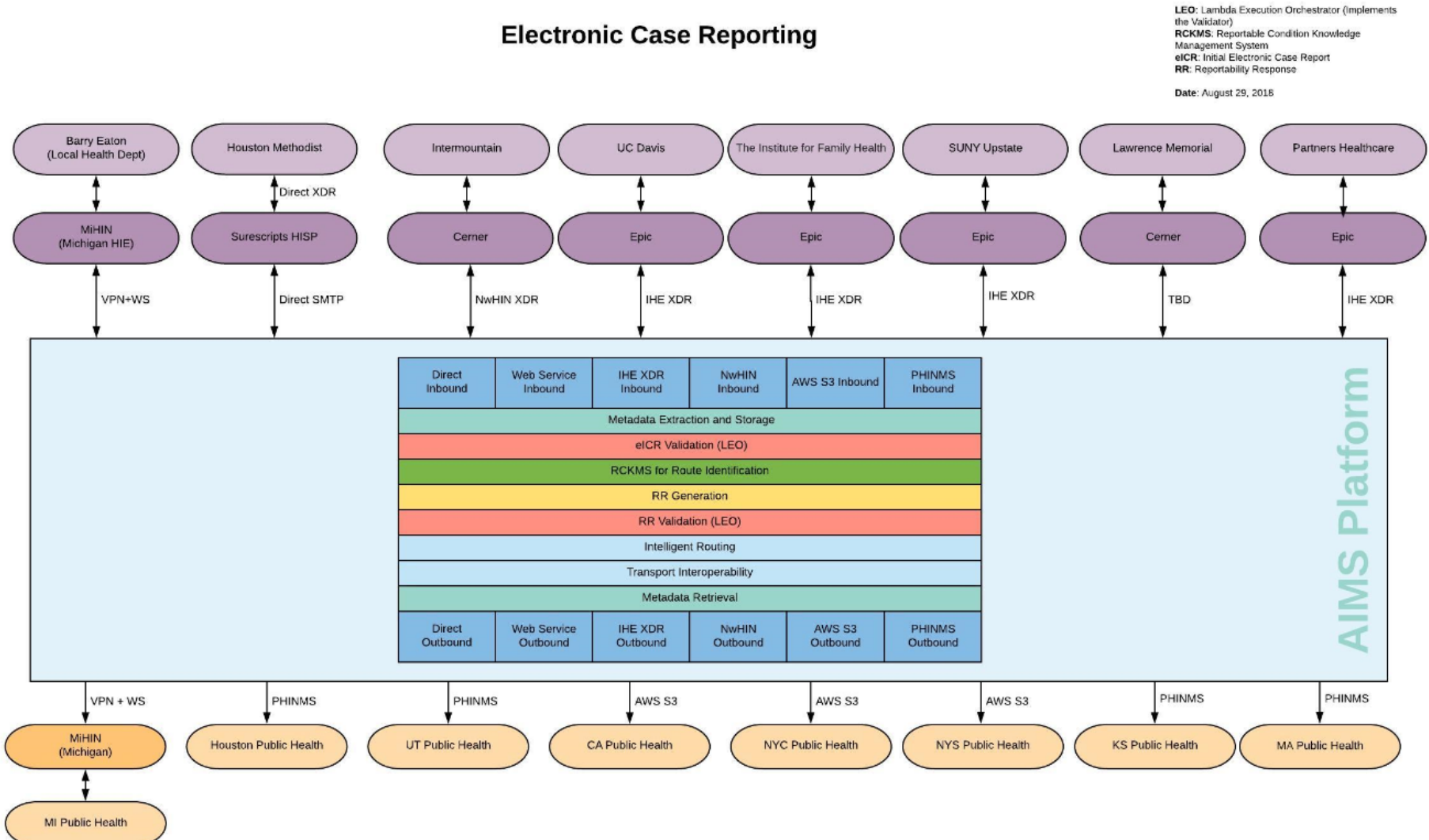


Figure 3. AIMS Platform Diagram for eCR Initial Implementations