Appendix F:
HISPC ASP Use Case Policy Requirements Templates

Table of Contents

List of Tables

HISPC ASP EHR Laboratory Results Use Case Policy Requirements Template for Participant Model States

Part 1. Introduction

Purpose

This document is intended for use as a guide to facilitate the systematic collection of information related to a specified range of health information organization business requirements in practice, policy, state regulation, and law for the authentication and audit of physicians and health care providers exchanging protected health information given defined scenarios.

Organization

The Policy and Information Requirements Use Case Collection Template is organized into six parts to allow responding states the flexibility to adapt the use of the instrument to a range of Health Information Organization (HIO) Models, business requirements, and modes of administration. This template may be administered in a group session, individual respondent mode, or other mode as defined by the user. Information may be captured and submitted in any combination of paper or electronic formats. The complete template includes the following:

- **Part 2:** Scenarios for Health Information Exchange
- **Part 3:** Requirements Worksheets A–E
  A. Authentication
  B. Audit
  C. Data
  D. System
  E. Policy

  The Requirement Worksheets A–E are to be completed by the state HIO model organization with help from the state HISPC staff. These documents are intended to capture the organizational policy and procedural requirements as well as any known statutory rules and/or regulations that may apply to the events and actions in the selected lab result scenario.
- **Part 4:** User Guide to Instrument Completion
- **Part 5:** State Business Actors
- **Part 6:** Supplemental Information. Defining roles; requirements crosswalk to HITSP defined standards.

Instrument Navigation

Please review these instructions and all parts of the complete instrument package prior to administration. Follow the steps as described to complete the instrument package.

1. Select an appropriate mode of administration based on the characteristics of the state environment in which the instrument is to be completed. This may include completing the instrument in a facilitated group discussion session, an individual respondent mode, or a combination of the two.
2. Go To Part 2: Scenarios for Health Information Exchange. Review the selected scenarios for your state. The selected scenarios will be noted by the State HISPC Project Manager.
3. Go To Part 3: Requirements Worksheets A–E. Complete Worksheets A through E as per the instructions. Responses on Worksheets A–E will be used to identify business requirements in the subsequent Part 4. One set of Requirements Worksheets for the HIO across scenarios is assumed unless otherwise noted by the state or HIO.
4. Go To Part 4: User Guide to Instrument Completion. Part 4 is to be completed with responses from Requirements Worksheets A–E. Select the state's first scenario for examination. Repeat Part 4 for each additional scenario selected by your state for review. If necessary complete additional Requirements Worksheets to note the change in requirements by scenario.
5. Go To Part 5: Local HIO Business Actors. Complete per instructions.

Part 2. Scenarios for Documenting Authentication and Audit Requirements

EHR Laboratory Test Results Use Case Summary

The Use Case includes two scenarios that cover typical interfaces involving an EHR system (or equivalent) and laboratory results. The HITSP EHR specifications describe both a laboratory message transaction and a document sharing paradigm. Ordering providers of care receive results as a laboratory message, nonordering providers of care access historical laboratory results as documents, and "copy-to" providers of care may receive document availability notifications to retrieve such lab report documents.

A summary of the scenarios is provided. Teams should be familiar with the contents of the scenario and supporting technical documents. This summary is not intended to provide the detail necessary to complete this template.

Scenario 1

Laboratory test results are transmitted as a result of the order. The specifics of the ordering process are outside the scope of this use case. The test results are sent directly to the clinician's EHR system (local or remote) and/or another clinical data system to provide laboratory results to ordering and non-ordering authorized recipients. Consideration is given to both message and document transactions: alternative scenario (1a), HL7 V2.5.1

messages are used and in the second alternative (1b), HL7 V3.0 CDA R2 documents are used.

Scenario 2

A provider of care accesses historical test results related to a specific patient by first querying for the laboratory report document and then retrieving or receiving the data. The provider may request the test results, possibly from separate data repositories, and after selection, they are sent to the provider's EHR.

This scenario extends the capabilities of Scenarios # 1a and # 1b by providing HL7 CDA laboratory reports to an authorized provider of care upon request. The provider queries a locator service for the location of a document and receives a pointer that is then used to retrieve the document. This allows for laboratory results to be stored in multiple repositories, but still requested from a single locator service.

Part 3. Policy and Information Exchange Requirements Worksheets for the Health Information Organization—EHR Laboratory Results Use Case

The following Requirements Worksheets A–E include tables that contain baseline identified business requirements in five areas: authentication, audit, data, systems, and policy (Tables F-1 through F-51). These requirements crosswalk to several selected specifications developed by the ONC Standards Harmonization initiative (HITSP) for the Electronic Health Record Laboratory Results Use Case (see Table F-56).

Each area of requirements is contained in a separate table. Each requirement has a unique text-numeric identifier and description. These requirements are not intended to capture all requirements that exist. The Requirements Worksheets are to be completed for the HIO model that is demonstrating the use case. These worksheets must be completed prior to work on Part 4 of this packet.

Instructions: Use the key concepts to indicate which of the following practices, policies, and/or procedures are either required, optional, under consideration, or the HIO considers not implementable at this time. If the HIO is not considering the practice, leave the item blank.

Key

R Required means the use of the indicated process, policy, or procedure is required by the HIO
O Optional means the use is in practice by some participants but not required by the HIO
U Under consideration for implementation by the HIO
N Not implementable at this time across all participants for multiple reasons (i.e., cost, technology, political)

A. Authentication Requirements

Table F-1. AUT-1a: User Authentication Requirement: Method(s) of User Identity Vetting at Time or Registration of HIO Members

Description	Key	Comment
In person	—	—
Notary	—	—
Demonstrate government-issued ID	—	—
Other: _____	—	—
Validate the provider license	—	—
Validate employees of licensed provider organization	—	—
HIO use of a specific naming convention as a primary identifier	—	—
Use of object identifier (OID): _____	—	—
Describe: _____	—	—

Em dash (—) is a placeholder for data.

Table F-2. AUT-1b: User Authentication Requirement: Assurance Level Used (Individual User)

Description	Key	Comment
Low (username/PIN)	—	—
Medium (knowledge/strong password)	—	—
High (PKI/digital ID)	—	—
Very high (token)	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-3. AUT-1c: User Authentication Requirement: Lab Results Context Restrictions Apply (see HITSP/C37[1])

Description	Key	Comment
Ordering clinician	—	—
Associated organization	—	—

Em dash (—) is a placeholder for data.

[1] HITSP lab report document component C37 description, HISPC Electronic Health Record Laboratory Result Reporting Use Case Policy Requirements and Standards Adoption V0.0.4. Working Draft, 20080625.

Table F-4. AUT-1d: User Authentication Requirement: Sensitivity Restrictions to Lab Results Apply

Description	Key	Comment
HIV	—	—
Mental health record	—	—
Substance abuse record	—	—
Sexual health record	—	—
Prison health record	—	—
Other: _____	—	—
Other restrictions: _____	—	—

Em dash (—) is a placeholder for data.

Table F-5. AUT-2: Subject of Care Identity

Description	Key	Comment
Collection and processing of patient demographics/identifiers required for matching	—	—
Collection of SSN	—	—
Collection of driver's license	—	—
Matching criteria policy (e.g., exact match on DOB, first name, last name, address)	—	—
Other: _____	—	—
Provider prove subject of care	—	—

Em dash (—) is a placeholder for data.

Table F-6. AUT-3a: System Authentication: System Identity Vetting

Note: Sharing laboratory results may be restricted by system type. Indicate which apply using key.

Description	Key	Comment
In-person—site visit	—	—
Assertion by authorized organization representative	—	—
Certification	—	—
FDA	—	—
CCHIT	—	—
Other: _____	—	—
System IP address	—	—
System domain name	—	—
Other: _____	—	—
Demonstrate association with licensed organization	—	—
HIO use of a naming convention as a primary identifier	—	—
Use of object identifier (OID): _____	—	—
Describe: _____	—	—

Em dash (—) is a placeholder for data.

Table F-7. AUT-3b: System Authentication: Assurance Levels (System to System)

Note: Sharing laboratory results may be restricted by system type. Indicate which apply using key.

Description	Key	Comment
Low (username/PIN)	—	—
Medium (knowledge/strong password/shared secret)	—	—
High (PKI/digital ID)	—	—
Very high (token)	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-8. AUT-3c: System Authentication: Lab Results Context Restrictions Apply (see HITSP C37[2])

Note: Sharing laboratory results may be restricted by system type. Indicate which apply using key.

Description	Key	Comment
Ordering system	—	—

Em dash (—) is a placeholder for data.

Table F-9. AUT-3d: System Authentication: Sensitivity Restrictions to Lab Results Apply

Note: Sharing laboratory results may be restricted by system type. Indicate which apply using key.

Description	Key	Comment
HIV	—	—
Mental health record	—	—
Substance abuse record	—	—
Sexual health record	—	—
Prison health record	—	—
Other: _____	—	—
Other restrictions: _____	—	—

Em dash (—) is a placeholder for data.

[2] HITSP Lab Report Document Component C37 description, HISPC Electronic Health Record Laboratory Result Reporting Use Case Policy Requirements and Standards Adoption V0.0.4. Working Draft, 20080625.

Table F-10. AUT-4: Data Authentication: Data Authentication Requirements Vary by Jurisdiction and Information Use

Description	Key	Comment
Use of time stamp	—	—
Signature purpose (ASTM E1762)	—	—

Em dash (—) is a placeholder for data.

Table F-11. AUT-5a: Organization Authentication: Organization Identity Vetting

Note: Laboratory results may be shared based upon organization type, leaving specific user authentication management and disclosures to the discretion of the organization.

Description	Key	Comment
In-person—site visit	—	—
Certification	—	—
Joint Commission	—	—
SAS-70 compliance	—	—
ENHAC compliance	—	—
Other: _____	—	—
Demonstrate articles of incorporation	—	—
Other: _____	—	—
Validation of organization health care licensure	—	—
HIO use of a specific naming convention as a primary identifier	—	—
Use of object identifier (OID): _____	—	—
Describe: _____	—	—

Em dash (—) is a placeholder for data.

Table F-12. AUT-5b: Organization Authentication: Assurance Levels (Organization to Organization)

Note: Laboratory results may be shared based upon organization type, leaving specific user authentication management and disclosures to the discretion of the organization.

Description	Key	Comment
Low (username/PIN)	—	—
Medium (knowledge/strong password/shared secret)	—	—
High (PKI/digital ID)	—	—
Very high (token)	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-13. AUT-5c: Organization Authentication: Lab Results Context Restrictions Apply

Note: Laboratory results may be shared based upon organization type, leaving specific user authentication management and disclosures to the discretion of the organization.

Description	Key		Comment
Ordering system	—	—	

Em dash (—) is a placeholder for data.

Table F-14. AUT-5d: Organization Authentication: Sensitivity Restrictions to Lab Results Apply

Note: Laboratory results may be shared based upon organization type, leaving specific user authentication management and disclosures to the discretion of the organization.

Description	Key		Comment
HIV	—	—	
Mental health record	—	—	
Substance abuse record	—	—	
Sexual health record	—	—	
Prison health record	—	—	
Other: _____	—	—	

Em dash (—) is a placeholder for data.

Table F-15. AUT-6: Authenticate Recipient Identity (User, Organization, System): Authenticate the Identity of Recipients of Communications by Any of the Following Means

Description	Key		Comment
Derived from ordering system communications	—	—	
Selected from a provider directory	—	—	
Derived from identifiers included in the request for information	—	—	

Em dash (—) is a placeholder for data.

B. Audit Requirements

Table F-16. AUD-1: Information Request—Requires Written Policy: Components Required in the Written Policy

Description	Key	Comment
Date/time of information request	—	—
Reason for information request	—	—
Description of information requested (to include):	—	—
Data accessed	—	—
Data transmission	—	—
Any data changes (adds, changes, deletes)	—	—
Whether data were transmitted to another party	—	—
Whether data were printed to another party	—	—
ID of person/system requesting disclosure	—	—
ID/verification of the party receiving the information	—	—
ID of the party disclosing the information	—	—
Verification method of requesting the party's ID	—	—
Authorization policy requires audit log identify	—	—
Whether release requires authorization	—	—
Whether authorization was obtained	—	—
Consent ID for audit purposes where applicable and as required	—	—

Em dash (—) is a placeholder for data.

Table F-17. AUD-2: Information Disclosure—Requires Written Policy: Components Required in the Written Policy

Description	Key	Comment
Date/time of request	—	—
Reason for request	—	—
Description of information requested (to include):	—	—
Data accessed	—	—
Data transmission	—	—
Any data changes (adds, changes, deletes)	—	—
Whether data were transmitted to another party	—	—
Whether data were printed to another party	—	—
ID of person/system requesting disclosure	—	—
ID/verification of the party receiving the information	—	—
ID of the party disclosing the information	—	—
Verification method of requesting the party's ID	—	—
Authorization policy requires audit log identify	—	—
Whether release requires authorization	—	—
Whether authorization was obtained	—	—
Consent ID for audit purposes where applicable and as required	—	—

Em dash (—) is a placeholder for data.

C. Data Requirements

Table F-18. DAT-1: Role: Establish a Defined Role Associated with the HIO Registered User Under Which the User Is Authenticated

Note: Allows for the defining of role-based access control using which of the following (see Part 6, Supplemental Material, for additional information on roles.)

Description	Key	Comment
Health care functional role	—	—
Structural role	—	—
Organization role	—	—

Em dash (—) is a placeholder for data.

Table F-19. DAT-2: Data Source

Description	Key	Comment
Directory of all National Health Bridge RHIOs	—	—
Directory of data sources within the target RHIO	—	—
Name of the RHIO	—	—
Data sources within that RHIO	—	—
Primary contact information (data in the directories):	—	—
Primary contact name	—	—
Contact phone numbers	—	—
Contact fax numbers	—	—
Master provider index to query by provider for a specific patient	—	—

Em dash (—) is a placeholder for data.

Table F-20. DAT-3: Assurance Levels: Assurance Levels Communicated

Description	Key	Comment
Low (username/PIN)	—	—
Medium (knowledge/strong password/shared secret)	—	—
High (PKI/digital ID)	—	—
Very high (token)	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-21. DAT-4: Requestor Type

Description	Key	Comment
Exchange (HIO)	—	—
Organization (institution)	—	—
User (individual)	—	—

Em dash (—) is a placeholder for data.

[There is no table for DAT-5.]

DAT-6 is an important part of this work but considered not within the strict limits of our project scope. ASP has defined DAT-6 as an optional requirement for data collection. If you choose to include this information, please indicate in the Comment field which, if any, of the following listed data elements are “not permitted to collect” and/or “not permitted to disclose” by state law, rule, or regulation in your state.

Table F-22. DAT-6: Data Elements/Identifiers the HIO Uses for Record Matching (Required Elements for Matching [Optional])

Description	Key	Comment
Identifiers (patient account number, SSN, driver license, mother's ID, MRN, alt patient ID)	—	—
Patient name (first, middle, last, family name, suffix, prefix/title, type)	—	—
Mother's maiden name (family name, surname)	—	—
Patient DOB	—	—
Gender	—	—
Patient previous names	—	—
Race	—	—
Patient home address (home street, street or mailing address, street name, dwelling number, other designation [second line of street address], city, state/province, zip, country, address type, county code)	—	—
Patient daytime phone (country code, area/city code, local number, extension, any other text)	—	—
Work telephone	—	—
Primary language	—	—
Marital status	—	—
Religion	—	—
Patient ethnicity	—	—
Birth place	—	—
Multiple birth indicator	—	—
Birth order	—	—
Citizenship	—	—
Veteran's military status	—	—
Nationality	—	—
Deceased (date/time, deceased indicator)	—	—

Em dash (—) is a placeholder for data.

Table F-23. DAT-7: Matching Criteria: Defined Required Minimum Number of Data Elements Required to Query Another System

Description	Key	Comment
Specify number: _____	—	Ex. CO requires 3

Em dash (—) is a placeholder for data.

Table F-24. DAT-8a: Persistence: Persistence of Source Signature

Description	Key	Comment
Persistent user signature	—	—
Persistent organization signature	—	—
Persistent system signature	—	—

Em dash (—) is a placeholder for data.

Table F-25. DAT-8b: Persistence: Nonrepudiation of Origin

Description	Key	Comment
User accountable	—	—
Organization accountable	—	—
System accountable	—	—
Source authentication	—	—
In transit	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-26. DAT-9: Demographics That May be Logged

Description	Key	Comment
HIO logs a subset of the subject identity attributes that have been used when a person is found.	—	—

Em dash (—) is a placeholder for data.

Table F-27. DAT-10: Provider Identity Attributes: User Attributes Included in Directory Entry

Note: HIO collects attributes needed for unique identification of recipient at HIO level.[3]

Description	Key	Comment
Profession	—	—
Specialization/specialty	—	—
Role	—	—
Name	—	—
E-mail	—	—
Address of physician's practice	—	—
Business/legal address	—	—
License/ID	—	—
License status	—	—
NPI	—	—
Digital identity	—	—
Identification service	—	—
Organization affiliation	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-28. DAT-11a: Organization Identity Attributes: Organization Attributes Required by HIO to Allow for Member Organization to Connect to HIO

Description	Key	Comment
Directory entry	—	—
Name	—	—
E-mail	—	—
Address	—	—
NPI	—	—
Digital identity	—	—
Organization affiliation	—	—
EDI administrative contact	—	—
Clinical information contact	—	—
Closure date	—	—
Successor name	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

[3] When a request comes in, look back at requesting HIO to identify provider and attributes in the registry (e.g., looking to send information to Dr. X—as a participant in HIO, roles, PCP).

Table F-29. DAT-11b: Organization Identity Attributes: Regulated Health Care Organization

Description	Key	Comment
All supporting organization attributes above	—	—
License/ID	—	—
License status	—	—
Registered name	—	—
Registered address	—	—
Service locations	—	—

Em dash (—) is a placeholder for data.

Table F-30. DAT-12a: System Identity Attributes: System Attributes Required by HIO for HIO Member Organization Systems to Connect

Description	Key	Comment
Directory entry	—	—
Name	—	—
Digital identity	—	—
Organization affiliation	—	—
System IP address	—	—
System domain name	—	—

Em dash (—) is a placeholder for data.

Table F-31. DAT-12b: System Identity Attributes: System Types (Check all Applicable Types Participating in the HIO)

Description	Key	Comment
Laboratory information system	—	—
Electronic health record system	—	—
Emergency medical system	—	—
Emergency department system	—	—
Personal health record	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

D. System Requirements

Table F-32. SYS-1: Preparing a Query Message: Specified by HITSP[4]

Description	Key	Comment
HIO generates a registry stored query—asking the registry or Record Locator Service if there are records for this patient (refer to HITSP IS01)	—	—
HIO generates an HL7 message	—	—

Em dash (—) is a placeholder for data.

Table F-33. SYS-2: Audit Log (HIPAA)

Description	Key	Comment
Audit log for use and disclosure and information systems activity exists[5]	—	—
Audit log for use and disclosure and information systems activity occurs at established periodic time frames	—	—
Audit log for use and disclosure of audit log has a set report constructed	—	—
Actions have been identified in the event of discovered anomalies/breaches	—	—
Log-in auditing is required audit criteria (security rule requirement)	—	—
Tracking of the state-specific consent policy[6] under which the data was disclosed exists; may be a global consent policy or a specific consent for each access (e.g., MA)	—	—

Em dash (—) is a placeholder for data.

Table F-34. SYS-3: Audit Log Content: Shared Specifics Include:

Note: Ability to share responsibilities for identifying what has been transmitted and which entities are responsible for tracking on specifics.

Description	Key	Comment
User ID	—	—
Date/time stamp	—	—
Data transmitted	—	—
Authorization needed to disclose	—	—
Whether data can be transmitted to another party	—	—

Em dash (—) is a placeholder for data.

[4] See HITSP IS01, Electronic Health Record Laboratory Results Reporting V:2.1.

[5] The audit log is intended for tracking use and disclosure of patient data when appropriate and/or information systems activity needs as required.

[6] Tracking of the state-specific consent policy under which the data was disclosed. May be a global consent policy (opt/in or opt/out) or a specific consent for each access (e.g., MA, tracking of the consent doc ID).

Table F-35. SYS-4: System Review

Description	Key	Comment
Automatic trigger exists for any out-of-state access; automated audit review to permit ready review of any interstate access exists	—	—
Information system review conducted on a regular and periodic basis	—	—

Em dash (—) is a placeholder for data.

Table F-36. SYS-5: Threshold Calculation

Description	Key	Comment
System ability to calculate some value that represents the quality of a match based on an algorithm	—	—

Em dash (—) is a placeholder for data.

Table F-37. SYS-6: Audit Trail and Node Authentication (ATNA)

Description	Key	Comment
Encryption is specified	—	—
Signing the data	—	—
Specified by policy	—	—

Em dash (—) is a placeholder for data.

[There is no table for SYS-7.]

Table F-38. SYS-8: Security Audit Practices[7]

Description	Key	Comment
HIO audits occur at a specified frequency	—	—
Periodic external audits of the HIO are conducted	—	—
Comprehensive audit procedures exist	—	—
Mitigation and remediation plans exist	—	—
Sharing of risk scores with other RHIOs exists	—	—

Em dash (—) is a placeholder for data.

[7] Based on Chris Apgar's *Identity Security Audit*.

Table F-39. SYS-9: Digital Signature

Description	Key	Comment
Ability for digital signature exists	—	—

Em dash (—) is a placeholder for data.

E. Policy Requirements

Table F-40. POL-1: Interim Reports

Description	Key	Comment
Interim reports of lab results are made available for sharing with persons that have appropriate access, once the ordering physician has signed off on the results and has discussed results with patient where required by policy	—	—

Em dash (—) is a placeholder for data.

Table F-41. POL-2: Restricted Data Sharing

Description	Key	Comment
Caveats to data completeness are transmitted	—	—

Em dash (—) is a placeholder for data.

[There are no tables for POL-3 through POL-7.]

Table F-42. POL-8: Returning More Demographics

Description	Key	Comment
Returning more demographic information to the end user than was initially entered	—	—

Em dash (—) is a placeholder for data.

Table F-43. POL-9: Audit Log Process

Description	Key	Comment
Minimum agreement on who is responsible for reconstitution and sharing audit log information during an investigation. Who is authorized to request this disclosure and to whom does this go? Where does or can a patient make the request to the RHIO?	—	—

Em dash (—) is a placeholder for data.

Table F-44. POL-10: Data Authentication

Description	Key	Comment
Methods for assurance that data have not been modified if a document is shared with a patient	—	—

Em dash (—) is a placeholder for data.

Table F-45. POL-11: Digital Signature

Description	Key	Comment
Policy allowing the organization to accept or express data without signature or with a caveat or some marker that no signature was received	—	—

Em dash (—) is a placeholder for data.

Table F-46. POL-12: Relationship to Patient

Description	Key	Comment
Gray area—for HIPAA-only regulated state—subject of care—provider needs to demonstrate they are the provider of the subject of care	—	—

Em dash (—) is a placeholder for data.

Table F-47. POL-13: Risk Assessment

Description	Key	Comment
Identification of risk issues (e.g., data authentication not a high risk in this scenario)	—	—

Em dash (—) is a placeholder for data.

[There is no table for POL-14.]

The HIPAA Security Rule and, by inference, the Privacy Rule require at a minimum four different types of audits. (State and other federal laws may specify additional requirements.) The following policies outline only the HIPAA Security Rule audit requirements. Each requirement definition includes the type of safeguard (administrative, physical, or technical), whether this impacts policy/system/data requirements, and the regulatory cite. This represents the bare minimum audit requirements for all covered entities and business associates. It includes RHIOs who are generally business associates of participating covered entities/providers.

Assumptions: Organizations have some variation of POL-17 Evaluation (a required administrative safeguard) in place, and, as such, this requirement is not identified on Part 4 of this template.

Table F-48. POL-15: Information System Activity Review (45 C.F.R. 164.308(a)(1): Administrative Safeguard; Policy, Data, and System Requirements

Description	Key	Comment
Software applications, network servers, firewalls, and other network hardware and software are configured to create audit logs that track activities involving electronic protected health information (ePHI) such as data modification, creation, deletion, etc.	—	—
The audit logs generated are reviewed on a regular basis based on audit criteria developed in advance, any anomalies documented, and mitigating action, if necessary.	—	—
Documentation is retained for a minimum of 6 years.	—	—

Em dash (—) is a placeholder for data.

Table F-49. POL-16: Log-in Monitoring (45 C.F.R. 164.308(a)(5): Administrative Safeguard; Policy, Data, and System Requirements

Description	Key	Comment
An audit log created to record when a workforce member or business associate logs onto the network or a software application, when log-in is attempted, and when the log-in attempt fails.	—	—
The audit logs generated are reviewed on a regular basis based on audit criteria developed in advance, any anomalies documented, and mitigating action, if necessary.	—	—
Documentation is retained for a minimum of 6 years.	—	—

Em dash (—) is a placeholder for data.

Table F-50. POL-17: Evaluation (45 C.F.R. 164.308(a)(8): Administrative Safeguard; Policy Requirements

Description	Key	Comment
Periodic technical and nontechnical evaluations are conducted to reasonably ensure the covered entity is compliant with the provisions of the HIPAA Security Rule; otherwise known as a compliance audit.	—	—
Audit criteria are to be developed in advance.	—	—
An evaluation occurs at least annually or when any major system or business changes occur.	—	—
Evaluation requires:	—	—
Generation of an audit findings report.	—	—
Associated mitigating action or documentation that an identified deficiency represents a risk the organization is willing to accept.	—	—
The organization is responsible for prioritizing mitigation and document mitigation plans (including documenting completion of mitigating activity).	—	—
All documentation must be retained for a minimum of 6 years.	—	—

Em dash (—) is a placeholder for data.

Table F-51. POL-18: Audit Controls (45 C.F.R. 164.312(b): Technical Safeguard; Policy, Data, System Requirements

Description	Key	Comment
Covered entities must implement technical processes that accurately record activity related to access, creation, modification, and deletion of ePHI.	—	—
Audit logs recording activity as it relates to ePHI and the periodic review of generated audit logs.	—	—
Review of audit logs is based on established audit criteria and includes documentation of any anomalies and mitigating action (including sanctions, security incident response team activation, etc., as appropriate), if necessary.	—	—
All documentation is retained for a minimum of 6 years.	—	—
Audit logs at a minimum must include:	—	—
Unique user name/ID	—	—
Date/time stamp	—	—
Action taken (view, add, change, delete)	—	—

Em dash (—) is a placeholder for data.

Part 4. User Guide to Instrument Completion

This part contains defined interactions and conditions described as events and actions in the Laboratory Results Use Case. In addition, it identifies authentication, audit, data, system, and policy requirements that may apply given the action as defined by the AHIC scenario. State health information organization models may differ in their responses to these given interactions and requirements. The provided actions in the AHIC comment section are to be used as a guide for states documenting specific processes associated with the use case.

Assumption: Requirements Worksheets A–E are complete with regard to the HIO policy and procedures for authentication and audit. Team members completing the template are familiar with the selected use case materials.

Instructions for completing this template.

- Review each event, associated action, and AHIC comment.
- For each identified event, describe the necessary action(s) that would need to follow according to the HIO business model in your state. For example, Code 3.2.1.0, Event: Integrate results and view in EHR, a sample question is included to guide the discussion "What action(s) or processes are necessary in order for a clinician to integrate a lab result into their EHR and be able to view the results given the HIO in your State?"

If the event is not applicable to the HIO business model, please indicate "not applicable to our HIO model" in the "State Model Comment" field.

- For each "State Model Comment" response where an action(s) is documented/supplied, circle which, if any, authentication, audit, data, system, and/or policy requirements are triggered at the HIO level. The details of these requirements are located in Part 3, Requirements Worksheets A–E. Circle those requirements specific to the given model being described that are necessary business processes, policies, and/or procedures in order for the action(s) to occur. (Each state demonstration model should have completed a summary list of requirements in each of these areas.) If the described actions have requirements that come into play other than those that are identified below for each action, write in the requirement name and number (as identified in worksheets from Part 3) in the appropriate column. If no requirement is needed, circle "No applicable requirements" in the appropriate requirement column.

EHR Laboratory Use Case

Code 3.2.1.0

Event: Integrate Results and View in EHR

Code: 3.2.1.1a

AHIC Description: Alternate action: Send request for historical lab test result content to data repository(ies).

AHIC Comment: The clinician selects data repository(ies) from which to retrieve lab test results and sends a request(s). The request may be sent from the EHR system or via Web application.

State Model Comment: Ex. What actions are needed for a participating clinician to send request for historical lab test result content data to repository(ies)?

ASP Business Requirements

Authentication

(AUT-1) User authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching
(DAT-10) Provider identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.2.1.7

AHIC Description: Action: Log receipt of lab test results

AHIC Comment: Include patient consent information in log

State Model Comment: What actions are needed to log receipt of lab results?

ASP Business Requirements

Authentication

Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-3) Consent disclosure
(POL-9) Audit log process
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

EHR Laboratory Use Case

Code 3.2.3.0

Event: Query for Laboratory (Historical) Test Results

The clinician queries the locator service for the availability and location of lab test results for a specified patient and receives the location of the results. Queries to the locator service could be accomplished either through the EHR user interface directly or through another clinical data system.

Code: 3.2.3.1

AHIC Description: Action: Submit authentication information to locator system.

AHIC Comment: Establish clinician's identity and verify whether clinician is a provider of care. Note that the clinician may be an individual, an organization, or system. The nature of the identification/authentication will be different in each case. One of many authentication methods could be used (biometrics, card, token, user ID and password, cryptographic techniques).

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-1) User authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-3) Assurance levels
(DAT-4) Requestor type
(DAT-10) Provider identity attributes
Other requirements (specify): _____
No applicable requirements

System

Other requirements (specify): _____
No applicable requirements

Policies

(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.2.3.2

AHIC Description: Action: Clinician and locator system agree on patient identity through patient trait matching.

AHIC Comment: The clinician and locator system must verify that they are interacting about the same patient. Patient identity may be agreed upon by a number of means including demographic information, agreed-to mapping of patient IDs, or shared patient ID. The means depend on whether the locator service is provided by a third party or part of available community or regional services. A set of traits (such as name, DOB, gender, etc.) may be used by a locator service to perform a probabilistic match. Business rules could be

established across a community or region to determine minimum acceptable combinations of traits (for example, name-only searches not allowed without a DOB).

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-2) Subject of care identity
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-6) Required elements for matching
(DAT-7) Matching criteria
(DAT-9) Demographics that may be logged
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-5) Threshold calculation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-8) Returning more demographics
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Alternate Actions 3.2.3.2a–b provide the functionality for a priori agreed-to identifiers by the clinician and locator service and lab data repository.

Code: 3.2.3.2a

AHIC Description: Alternate action: Clinician and locator system agree on patient identity based on shared MPI.

AHIC Comment: If the entity to which the clinician is affiliated (hospital, HMO, private physician practice, etc.) has already registered the patient internally and uploaded the entry into a shared MPI, the provider can capture and submit the entity's internal identifier for that patient (e.g., the patient's medical record number for that hospital) to a locator service. In this case, the provider would not need to manually enter demographic traits (name, date of birth [DOB], etc.) since that data are already present in the MPI.

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-2) Subject of care identity
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-6) Required elements for matching
(DAT-7) Matching criteria
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-5) Threshold calculation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-8) Returning more demographics
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.2.3.2b

AHIC Description: Alternate action: Clinician and locator system agree on patient identity based on patient identifier matching.

AHIC Comment: The locator system matches the patient identifiers supplied by the clinician with patient identifiers known within the locator service.

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-2) Subject of care identity
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-6) Required elements for matching
(DAT-7) Matching criteria
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-5) Threshold calculation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-8) Returning more demographics
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.2.3.5

AHIC Description: Action: Log interaction with locator service.

AHIC Comment: The locator system matches the patient identifiers supplied by the clinician with patient identifiers known within the locator service.

State Model Comment: —

ASP Business Requirements

Authentication

Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

EHR Laboratory Use Case

Code 3.2.4.0

Event: View Results Using Another Clinical Data System (Non-EHR System)

Not all clinicians will initially have an EHR to view lab test results. The clinician may view lab test results using a clinical data system (non-EHR).

Code: 3.2.4.2

AHIC Description: Action: Submit authentication information to data repository.

AHIC Comment: Establish clinician's identity and authorization. Note that clinician may be an individual, an organization, or system. The nature of the identification/ authentication will be different in each case. One of many authentication methods could be used (biometrics, card, token, user ID and password, cryptographic techniques).

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-1) User authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-3) Assurance levels
(DAT-6) Required elements for matching
(DAT-10) Provider identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.2.4.4

AHIC Description: Action: Verify correct patient identity and correctness of lab results and correct error if necessary.

AHIC Comment: Upon review of the result, a clinician may see suspect data (e.g., that should be confidential or may be erroneous).

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-2) Subject of care identity
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-6) Required elements for matching
(DAT-7) Matching criteria
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-5) Threshold calculation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-8) Returning more demographics
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.2.4.6

AHIC Description: Action: Log interaction with data repository

AHIC Comment: —

State Model Comment: —

ASP Business Requirements

Authentication

Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

EHR Laboratory Use Case

Code 3.3.1.0

Event: Process Laboratory Order

Laboratory creates the test results and sends the results to the data repository for availability to the ordering clinician and other providers of care, if appropriate.

Code: 3.3.1.2 (ONC priority flow)

AHIC Description: Action: Send results to data repository.

AHIC Comment: The laboratory transmits the results to the data repository with appropriate metadata necessary for indexing and browse/query response. Results update or error corrections should also be sent. The data repository may be within the laboratory, may be a separate entity, or may be part of a community or regional service provider.

State Model Comment: —

ASP Business Requirements

Authentication

Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

Other requirements (specify): _____
No applicable requirements

Policies

(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.3.1.3

AHIC Description: Action: Log creation of test results.

AHIC Comment: —

State Model Comment: —

ASP Business Requirements

Authentication

Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

EHR Laboratory Use Case

Code 3.4.1.0

Event: Store laboratory results

Code: 3.4.1.2

AHIC Description: Action: Verify authenticity of laboratory and lab test result file contents.

AHIC Comment: Verify integrity of test result (file) contents and that the results came from the identified source. The test results should contain appropriate patient information and other information per agreed-to standards and policies. Providers of care should be known.

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-4) Data authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-9) Digital signature
Other requirements (specify): _____
No applicable requirements

Policies

(POL-10) Data authentication
(POL-11) Digital signature
(POL-13) Risk assessment
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.4.1.6

AHIC Description: Action: Log receipt and storage of lab test results.

AHIC Comment: —

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-4) Data authentication
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
Other requirements (specify): _____
No applicable requirements

EHR Laboratory Use Case

Code 3.4.2.0

Event: Notify Locator Service of Laboratory Results

Code: 3.4.2.1

AHIC Description: Action: Authenticate to locator service.

AHIC Comment: —

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-1) User authentication
(AUT-3) System authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching
(DAT-10) Provider identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-9) Digital signature
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.4.2.3

AHIC Description: Action: Log interaction with locator system.

AHIC Comment: —

State Model Comment: —

ASP Business Requirements

Authentication

Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

EHR Laboratory Use Case

Code 3.4.3.0

Event: Process Request for Laboratory Test Results

The data repository receives a request for test result content and verifies the authenticity of the clinician, the integrity of the request, and any restrictions for use. The data repository either sends the test results for integration into the clinician's EHR, or sends the content to another clinical data system for viewing. The secrecy of the content is maintained during transmission.

Code: 3.4.3.2

AHIC Description: Action**:** Authenticate and verify as ordering clinician or provider of care.

AHIC Comment: May include provider identification and validation of credentials, privileges, and/or other authorization. Authentication and verification may be provided through community or regional services. This may include a trust relationship whereby the clinician is authenticated and authorized once by the community or regional service. The authentication and verification is then carried through the query/retrieval processes.

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-1) User authentication
(AUT-3) System authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching
(DAT-10) Provider identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.4.3.5

AHIC Description: Action: Log interaction.

AHIC Comment: —

State Model Comment: —

ASP Business Requirements

Authentication

Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

EHR Laboratory Use Case

Code 3.5.1.0

Event: Publish Availability of Laboratory Test Results

Code: 3.5.1.1

AHIC Description: Action: Receive test result (file) location information and related information.

AHIC Comment: Related information may include appropriate patient information and other information per agreed-to standards and policies. Providers of care or restrictions for use should also be provided by the data repository if not provided through supported community or regional services.

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-2) Subject of care identity
Other requirements (specify): _____
No applicable requirements

Audit:

Other requirements (specify): _____
No applicable requirements

Data

(DAT-6) Required elements for matching
(DAT-7) Matching criteria
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-5) Threshold calculation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-8) Returning more demographics
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.5.1.2

AHIC Description: Action: Verify authenticity of lab test result location and completeness of related information.

AHIC Comment: Verify that the location of the test results is accurate and that related information necessary for indexing is correct.

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-4) Data authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

Other requirements (specify): _____
No applicable requirements

Policies

(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

EHR Laboratory Use Case

Code 3.5.2.0

Event: Process query to provide laboratory test result location(s)

Code: 3.5.2.1

AHIC Description: Action: Authenticate clinician requesting laboratory test results.

AHIC Comment: Establish clinician's identity and verify status as ordering clinician or provider of care. Note that the clinician may be an individual, an organization, or system. The nature of the identification/authentication will be different in each case. One of many authentication methods could be used (biometrics, card, token, user ID and password, cryptographic techniques).

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-1) User authentication
(AUT-3) System authentication
(AUT-5) Organization authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching
(DAT-10) Provider identity attributes
(DAT-11) Organization identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.5.2.2

AHIC Description: Action: Clinician and locator system agree on patient identity.

AHIC Comment: The clinician and locator system must verify that they are interacting about the same patient. Patient identity may be agreed upon by a number of means including demographic information, agreed-to mapping of patient IDs, or shared patient ID. The means depend on whether the locator service is provided by a third party, or part of available community or regional services. A set of traits (such as name, DOB, gender, etc.) may be used by a locator service to perform a probabilistic match. Business rules could be established across a community or region to determine minimum acceptable combinations of traits (for example, name-only searches not allowed without a DOB).

State Model Comment: —

ASP Business Requirements

Authentication

(AUT-2) Subject of care identity
Other requirements (specify): _____
No applicable requirements
Other requirements (specify): _____
No applicable requirements

Data

(DAT-6) Required elements for matching
(DAT-7) Matching criteria
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-5) Threshold calculation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-8) Returning more demographics
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 3.5.2.5

AHIC Description: Action: Send lab result location (links) pointers to authorized clinician.

AHIC Comment: The location pointers will be used by the clinician to retrieve the lab test results for either viewing or integration into the EHR.

State Model Comment: —

ASP Business Requirements

Audit

Logged, not audited

Code: 3.5.2.6

AHIC Description: Action: Log interaction with clinician.

AHIC Comment: The location pointers will be used by the clinician to retrieve the lab test results for either viewing or integration into the EHR.

State Model Comment: —

ASP Business Requirements

Authentication

Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Part 5. Local HIO Business Actors

A business actor is the representation of a person, IT system, organization, or any combination that is engaged and benefits from the real world information interchange defined by a business use case. Table F-52 contains the HITSP business actors and description for the EHR Laboratory Results Use Case.

Instructions. In Table F-52, identify the name of the organization, the local business actor(s) participating in the HIO that align with the HITSP business actor, and description for this use case. Indicate in the "Availability" column which service options are provided by the local business actor. If the service options provided by your local business actor are not listed, please add the type of the service(s) provided to the appropriate category listing. For example, if XClinical Vendor provides document source, audit repository, secure node, and other, list XClinical Vendor in the "Local Business Actor" column; check each availability box next to the three identified service options, write in any additional service options provided, and check the corresponding availability box.

If other local business actors are part of your HIO model and are not included as part of the HITSP business actor grouping in this table, please add to the bottom of the table and add "Description" and "Service Options" for each additional actor supplied to the list.

Table F-52. Local HIO Business Actors

Local Business Actor	Mapping to HITSP Business Actor	Description	Availability	Service Options
—	Patient identifier service	An application that references a patient database to identify a particular patient based on one of many IDs or by matching patient demographics.	—	Enterprise master patient index
—	Provider identifier service	An application that references a provider database to retrieve data for treatment-related activities.	—	Enterprise master provider index
—	Locator service	Responds to queries for the test results by providing the list of available test results and their locations within data repositories.	—	eMPI repository Audit repository Common vocabulary services Aggregation services XDS registry XDS repository PIX manager Secure node CT client XUA Decision support services Presentation services
—	Laboratory system	Produces the laboratory results. Dedicated laboratory organizations, as well as laboratories operating as the provider of care perspective may be supported by the laboratory system business actor as laboratory testing services are performed by the organization.	—	Audit repository Secure node CT XUA
—	Data repository	The system that provides the laboratory test results.	—	HL7 query/response PIX manager Audit repository XDS registry XDS repository Secure node CT client XUA

Em dash (—) is a placeholder for data.

Part 6. Supplemental Material

The information in Tables F-53 through F-55 is for use in helping to answer Data Requirement DAT-1 role. [Table F-56 provides a crosswalk to several selected specifications developed by the ONC Standards Harmonization initiative (HITSP).] There are two parts to consider in review of the requirements:

1. Are HIO users established based on roles: structural, functional, organizational?
2. Are users/members/participants allowed access to data as defined by their user role?

Table F-53. Structural Roles

In this role, is the user expected to be able to access data?		Yes	No
1.	Physician (MD/allopath, osteopath, chiropractic, naturopath, homeopath)	—	—
2.	Advanced practice registered nurse (NP, NM, CAN, CNS)	—	—
3.	Physician assistant (PA)	—	—
4.	Midwives	—	—
5.	Registered nurse (RN)	—	—
6.	Licensed vocational nurse (LVN)	—	—
7.	Nonwestern medicine providers	—	—
8.	Ancillary service providers	—	—
8a.	Occupational therapy	—	—
8b.	Physical therapy	—	—
8c.	Cast technicians	—	—
8d.	Prosthetic technicians	—	—
8e.	Speech therapy	—	—
8f.	Respiratory therapy	—	—
9.	Technician	—	—
9a.	Technician: procedure-based (OR, cath lab, etc.)	—	—
9b.	Technician: departmental	—	—
9c.	Technician: specialty	—	—
9d.	Technician: general	—	—
10.	Nonlicensed care providers	—	—
10a.	Nurse's aide	—	—
10b.	Orderly	—	—
10c.	Phlebotomist	—	—
10d.	Bereavement counselor	—	—
10e.	Volunteer	—	—
10f.	Technician	—	—
10g.	Patient transportation personnel	—	—

(continued)

Table F-53. Structural Roles (continued)

In this role, is the user expected to be able to access data?	Yes	No
10h. Specimen transportation personnel	—	—
10i. Health record transportation personnel	—	—
11. Emergency services	—	—
11a. Paramedic	—	—
11b. EMT	—	—
11c. EMS	—	—
11d. Ambulance drivers	—	—
11e. Air transport pilots	—	—
12. Secular services (priest, rabbi, pastoral care, etc.)	—	—
13. Patient advocate	—	—
14. Interpreters	—	—
15. Clerical and administrative personnel	—	—
15a. Encounter registration clerk	—	—
15b. Admission clerk	—	—
15c. Ward/unit/clinic clerk	—	—
15d. Departmental clerk	—	—
15e. Clinical services	—	—
15f. Laboratory services	—	—
15g. Imaging services	—	—
15h. Pharmacy services	—	—
15i. Social services	—	—
15j. Ancillary services	—	—
16. Disposition/discharge clerks	—	—
17. Administrative support staff and services	—	—
17a. Physician office	—	—
17b. Nonphysician provider office	—	—
17c. Clinical department	—	—
17d. Administrative department	—	—
17e. Health records (medical records)/health information management department	—	—
17f. Quality assurance	—	—
18. Transcription personnel	—	—
18a. Coders/reimbursement specialists	—	—
18b. Transcriptionist	—	—

(continued)

Table F-53. Structural Roles (continued)

In this role, is the user expected to be able to access data?	Yes	No
18c. Claims personnel	—	—
18d. Proofreader	—	—
18e. QA personnel	—	—
18f. Clerks	—	—
18g. Students	—	—
18h. Supervisors/managers	—	—
18i. Vendors	—	—
18j. Maintenance and system support personnel	—	—
19. File clerk	—	—
19a. Clinical department	—	—
19b. Administrative department	—	—
19c. Health records (medical records)/health information management department	—	—
19d. Quality assurance	—	—
20. Supervisory personnel	—	—
20a. Clinical department	—	—
20b. Administrative department	—	—
20c. Health records (medical records)/health information management department	—	—
20d. Quality assurance	—	—
21. Health records (medical records)/health information management department	—	—
21a. Administration	—	—
21b. Administrative support	—	—
21c. File clerks	—	—
21d. Information management personnel	—	—
22. Information services	—	—
22a. Database administrator	—	—
22b. Network administrator	—	—
22c. Security administrator	—	—
22d. Trainer (of end users)	—	—
22e. Help desk	—	—
22f. Operations support	—	—
22g. System administrator	—	—
22h. Applications support	—	—
22i. Business analyst	—	—

(continued)

Table F-53. Structural Roles (continued)

In this role, is the user expected to be able to access data?	Yes	No
22j. Programmers	—	—
22k. Third-party support (vendors and consultants)	—	—
23. Financial services, billing, and claims	—	—
23a. Billing file clerk	—	—
23b. Billing personnel	—	—
23c. Administrative support personnel	—	—
23d. Collections personnel	—	—
23e. Cost and quality analysts	—	—
24. Quality assurance	—	—
25. Utilization review	—	—
26. Discharge planning	—	—
27. Infection control	—	—
28. Administrative support staff	—	—
29. Risk management	—	—
30. Health plan/insurer	—	—
30a. Claims file clerk	—	—
30b. Claims review personnel	—	—
30c. Claims adjudication personnel	—	—
30d. Internal quality assurance personnel	—	—
30e. Health care provision quality assurance personnel	—	—
30f. Internal utilization review personnel	—	—
30g. Health care provision utilization review personnel	—	—
30h. Administrative support personnel	—	—
31. Medical malpractice	—	—
31a. Health records file clerk	—	—
31b. Health records supervisor	—	—
31c. Lawyer/judge	—	—
31d. Legal aide	—	—
31e. Legal secretary	—	—
31f. Expert witness	—	—
31g. Governmental file clerk	—	—
32. Accrediting and regulatory agencies	—	—
32a. JCAHO auditors	—	—

(continued)

Table F-53. Structural Roles (continued)

In this role, is the user expected to be able to access data?	Yes	No
32b. NCQA auditors	—	—
32c. Local, state, and federal agencies	—	—
32d. Local, state, and federal surveyors	—	—
33. Administrative management	—	—
33a. Executive officers	—	—
33b. Board of trustees	—	—
33c. Medical staff administration	—	—
34. Pharmacist (DP)	—	—

Em dash (—) is a placeholder for data.

Table F-54. Health Care Functional Roles: In this Role, is the User Expected to be Able to Access Data?

Role Name	Description	Yes	No
Subject of care	Principal data subject of the electronic health record	—	—
Subject of care agent	E.g., parent, guardian, care provider, or other legal representative	—	—
Personal health care professional	Health care professional or professionals with the closest relationship to the patient, often the patient's general practitioner	—	—
Privileged health care professional	Nominated by the subject of care	—	—
Privileged health care professional	Nominated by the health care facility of care (if there is a nomination by regulation, practice, etc., such as an emergency override)	—	—
Health care professional	Party involved in providing direct care to the patient	—	—
Health-related professional	Party indirectly involved in patient care, teaching, research, etc.	—	—
Administrator	Any other parties supporting service provision to the patient	—	—

Em dash (—) is a placeholder for data.

Table F-55. Organization Roles: In this Role, is the User Expected to be Able to Access Data?

Roles (if more than one is listed, please specify those permitted)	Yes	No
Ambulance/aid-car	—	—
Ambulatory health care (ambulatory surgery facility, birthing center, clinic/health center (comp outpatient rehab, dental, free-standing, HMO, outpatient mental health, pain, rural, urgent care center (walk-in, free-standing), vision, private office (group, solo)	—	—
Hospital (acute care, acute care with psychiatric services, burn center, cancer, children's, emergency room, government, outpatient dept, psychiatric, rehabilitation, trauma center level 1, hospice)	—	—
Imaging services facility, free-standing	—	—
Independent laboratory	—	—
Mental health (multiservice organization, partial care organization, residential treatment center: emotionally disturbed children)	—	—
Nursing/custodial care facility (intermediate care facility, intermediate medicine, pulmonary-mentally retarded, skilled nursing facility/nursing home, hospice, industry health/occupational health center, end-stage renal disease treatment facility)	—	—
Residential (home health, retirement center, sheltered employment workshop)	—	—
School (day care center, residential, clinic/infirmary, special education program)	—	—
Substance abuse treatment facility, resident	—	—
Unlisted facility	—	—

Em dash (—) is a placeholder for data.

Table F-56. Crosswalk: Lab Authentication and Audit Requirements to HITSP Standards

Related Documents	Document Description	Lab Authentication Requirement(s)	Lab Audit Requirement(s)
HITSP/C19—Entity Identity Assertion Component	The Entity Identity Assertion Component provides the mechanisms to ensure that an entity is the person or application that claims the identity provided. An example of this component is the validation and assertion of a consumer logging on to a personal health record (PHR) system.	AUT-1 user authentication AUT-3 system authentication AUT-5 organization authentication	AUD-1 information request AUD-2 information disclosure
HITSP/C35—Lab Result Terminology Component	This document defines the vocabulary for either message-based or document-based laboratory results reporting.	—	—
HITSP/C36—Lab Result Message Component	This document describes the use of a constrained Health Level Seven (HL7) Version 2.5.1 ORU—Unsolicited Observation Message for electronic laboratory results reporting.	—	—
HITSP/C37—Lab Report Document Component	This component prescribes the use of the standard Clinical Document Architecture Release 2 (CDA R2), as in the HL7 V3 2006 normative edition for:	AUT-1 user authentication	—
HITSP/C37—Lab Report Document Component	Transmission of complete, preliminary, final, and updated laboratory results to the EHR system (local or remote) of the ordering clinician.	AUT-3 system authentication	—
HITSP/C37—Lab Report Document Component	Transmission of complete, preliminary, final, and updated (or notification) to the EHR system (local or remote) or other clinical data system of designated providers of care (with respect to a specific patient).	AUT-5 organization authentication	—
HITSP/C37—Lab Report Document Component	Transmit laboratory result data from electronically enabled health care delivery and public health systems in standardized and anonymized format to authorized public health agencies with less than 1-day lag time.	For context-based criteria—metadata	—
HITSP/C44—Secure Web Connection Component	This component provides the capability to access documents through a secure Web browser.	—	—
HITSP/T14—Send Laboratory Result Message Transaction	The functionality supported by this transaction is for sending laboratory result messages to the ordering clinicians and providers of care, and to receive acknowledgement from authorized recipients.	AUT-6 authenticate recipient identity (organization, user, system)	—
HITSP/T15—Collect and Communicate Security Audit Trail Transaction	The Collect and Communicate Security Audit Trail Transaction is a means to provide assurance that security policies are being followed or enforced and that risks are being mitigated. This document describes the mechanisms to define and identify security-relevant events and the data to be collected and communicated as determined by policy, regulation, or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed.	—	AUD-1 information request AUD-2 information disclosure

(continued)

Table F-56. Crosswalk: Lab Authentication and Audit Requirements to HITSP Standards (continued)

Related Documents	Document Description	Lab Authentication Requirement(s)	Lab Audit Requirement(s)
HITSP/T16—Consistent Time Transaction	The Consistent Time Transaction provides a mechanism to ensure that all of the entities that are communicating within the network have synchronized system clocks.	—	AUD-1 information request AUD-2 information disclosure
HITSP/T17—Secured Communication Channel Transaction	The Secured Communication Channel Transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of transactions and the mutual trust between communicating parties. It supports both application and machine credentials, and user machines (user nodes).	AUT—3 system authentication AUT—5 organization authentication	—
HITSP/T18—View Laboratory Results from a Web Application Transaction	This transaction allows a user to view a laboratory report through a secure browser. This transaction uses the HITSP/C44—secure Web connection component. It may not define all functions, constructs, and standards necessary to implement a conforming system in a real-world environment. In particular, an implementer must provide the technical infrastructure and security framework necessary to support operations in accordance with law, regulation, best practices, and business agreements (NOTE: Review for related policy—e.g., identity, node authentication).	—	—
HITSP/T23—Patient Demographics Query Transaction	This PDQ transaction is intended to provide a "list patients and their demographics" query/ "patient(s) and their demographics identified" response message pair (QBP^ Q22, RSP^ K22) for use wherever such needs exist. This transaction document extracts the Health Level Seven (HL7) Version 2.5 Query and Response data mapping. The underlying basis for this extraction can be found in the *Integrating the Healthcare Enterprise IT Infrastructure Technical Framework, Volume 2* (ITI TF-2), Revision 4.0: "Patient Demographics Query."	AUT-2 subject of care identity	—
HITSP/T29—Notification of Document Availability Transaction	The NAV Integration Profile introduces a mechanism allowing notifications to be sent point-to-point to systems within a Cross-Enterprise Document Sharing Affinity Domain (see "IHE IT Infrastructure Cross-Enterprise Document Sharing (XDS) Integration Profile"), eliminating the need for manual steps or polling mechanisms for a document consumer to be aware that documents of interest have been registered with an XDS document registry actor.	AUT-6 authenticate recipient identity (organization, user, system)	—

(continued)

Table F-56. Crosswalk: Lab Authentication and Audit Requirements to HITSP Standards (continued)

Related Documents	Document Description	Lab Authentication Requirement(s)	Lab Audit Requirement(s)
HITSP/TP13—Manage Sharing of Documents Transaction Package	This transaction package supports the sharing of patient records in the form of source attested objects called documents. A health care document is a composite of structured and coded health information, both narrative and tabular, that describes acts, observations, and services for the purpose of exchange. No assumption is made by this construct in terms of the format and structure of the content of documents shared. This interoperability specification, specifically references the IHE XDS.b option to support entity identity assertion (SAML support).	—	—
HITSP/TP20—Access Control Transaction Package	The Access Control Transaction Package provides the mechanism to administer security authorizations which control the enforcement of security policies including: role-based access control; entity-based access control; context-based access control; and the execution of consent directives. In an emergency, this construct supports the capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of nonemergency consents.	1 user authentication 3 system authentication 5 organization authentication	—
HITSP/TP22—Patient ID Cross-Referencing Transaction Package	This specification includes by reference the transactions and components that comprise the Patient ID Cross-Referencing Transaction Package. Source material is from the IHE IT Infrastructure (ITI) Technical Framework (TF), Volume 2 (ITI TF-2). The two transactions within this package are: The IHE Patient ID Cross-Referencing (PIX) transaction is described in IHE-ITI TF-2 §3.9.1 The IHE Patient Identity Feed transaction is described in IHE-ITI TF-2 §3.8.1	2 subject of care identity	—
HITSP/TP30—Manage Consent Directives Transaction Package	The Manage Consent Directives Transaction Package describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use, or disclose individually identifiable health information (IIHI), and also supports the delegation of the patient's right to consent. The transactions described in this construct are intended to be carried out by HITSP/TP13—Manage Sharing of Documents.	AUT—1 user authentication AUT—3 system authentication AUT- 5 organization authentication for consent restricted disclosures	AUD-1 information request AUD—2 information disclosure

HISPC ASP Medication Management Use Case Policy Requirements Template for Participant Model States

Part 1. Introduction

Purpose

This document is intended for use as a guide to facilitate the systematic collection of information related to a specified range of health information organization business requirements in practice, policy, state regulation, and law for the authentication and audit of physicians and health care providers exchanging protected health information given defined scenarios.

Organization

The Policy and Information Requirements Use Case Collection Template is organized into six parts to allow responding states the flexibility to adapt the use of the instrument to a range of Health Information Organization (HIO) Models, business requirements, and modes of administration. This template may be administered in a group session, individual respondent mode, or other mode as defined by the user. Information may be captured and submitted in any combination of paper or electronic formats. The complete template includes the following:

- Part 1: Introduction
- Part 2: Scenarios for Health Information Exchange
- Part 3: Requirements Worksheets A–E
  - A. Authentication
  - B. Audit
  - C. Data
  - D. System
  - E. Policy

    The Requirement Worksheets A–E are to be completed by the State HIO model organization with help from the state HISPC staff. These documents are intended to capture the organizational policy and procedural requirements as well as any known statutory rules and/or regulations that may apply to the events and actions in the selected lab result scenario.
- Part 4: User Guide to Instrument Completion
- Part 5: State Business Actors
- Part 6: Supplemental Information: Defining roles; requirements crosswalk to HITSP defined standards.

Instrument Navigation

Please review these instructions and all parts of the complete instrument package prior to administration. Follow the steps as described to complete the instrument package.

1. Select an appropriate mode of administration based on the characteristics of the state environment in which the instrument is to be completed. This may include completing the instrument in a facilitated group discussion session, an individual respondent mode, or a combination of the two.
2. Go To Part 2: Scenarios for Health Information Exchange. Review the selected scenarios for your state. The selected scenarios will be noted by the State HISPC Project Manager.
3. Go To Part 3: Requirements Worksheets A–E. Complete Worksheets A through E as per the instructions. Responses on Worksheets A–E will be used to identify business requirements in the subsequent Part 4. One set of Requirements Worksheets for the HIO across scenarios is assumed unless otherwise noted by the state or HIO.
4. Go To Part 4: User Guide to Instrument Completion. Part 4 is to be completed with responses from Requirements Worksheets A–E. Select the state's first scenario for examination. Repeat Part 4 for each additional scenario selected by your state for review. If necessary complete additional Requirements Worksheets to note the change in requirements by scenario.
5. Go To Part 5: Local HIO Business Actors. Complete per instructions.

Part 2. Scenarios for Documenting Authentication and Audit Requirements

Medication Management Use Case Summary

The Medication Management Use Case focuses on patient medication and allergies information exchange and the sharing of that information between consumers, clinicians (in multiple sites and settings of care), pharmacists, and organizations that provide health insurance and provide pharmacy benefits. This Use Case describes medication management in two scenarios. The first scenario, inpatient setting, includes medication reconciliation and ordering, along with other supporting interactions in the hospital. The second scenario, ambulatory setting, addresses access to current medication and allergy information, and support for electronic prescribing.

This Use Case assumes the developing presence of electronic systems such as Electronic Health Records (EHRs), ePrescribing tools, Personal Health Records (PHRs), and other local or Web-based solutions supporting consumers and clinicians, while recognizing the issues and obstacles associated with these assumptions.

Scenario 1: Inpatient Medication Reconciliation Overview

This scenario is focused on aspects of inpatient medication management including the formal process of medication reconciliation. Patients are at risk during transitions in care across settings, services, providers, or levels of care. Medication reconciliation documents

the efforts made to assemble and consider information on current medications and patient allergies during these transitions.

Briefly stated, medication reconciliation occurs at patient admission, discharge, and transfer (e.g., to another level of care in the hospital or to another hospital).

Scenario 2: Ambulatory Medication Management Overview

This scenario addresses access to current medication and allergy information and support for electronic prescribing in the ambulatory environment and includes

- gathering and documenting information on current medications;
- performing eligibility and benefits checking; and
- communicating the current medication list, prescriptions, allergy information, medication information, and care instructions to the patient.

Also included is prescription management, prescription writing, prescription transmittal to a pharmacy, and consumer-generated requests for prescription refills and renewals. This scenario focuses on providing clinicians and pharmacists with information about each patient's medications and allergies from local documentation; other ambulatory clinicians, hospitals, long-term care facilities, or other care settings from which the patient has been previously discharged; organizations that manage prescription- or insurance-related information; and patients, whose self-reported information may be recorded in PHRs or other electronic sources.

Part 3. Policy and Information Exchange Requirements Worksheets for the Health Information Organization—Medication Management Use Case

The following Requirements Worksheets A–E include tables that contain baseline identified business requirements in five areas: authentication, audit, data, systems, and policy (Tables F-57 through F-114). These requirements crosswalk to several selected specifications developed by the ONC Standards Harmonization Initiative (HITSP) for the Electronic Health Record Laboratory Results Use Case (see Table F-120).

Each area of requirements is contained in a separate table. Each requirement has a unique text-numeric identifier and description. These requirements are not intended to capture all requirements that exist. The Requirements Worksheets are to be completed for the HIO model that is demonstrating the use case. These worksheets must be completed prior to work on Part 4 of this packet.

Instructions. Use the KEY concepts to indicate which of the following practices, policies, and/or procedures are either required, optional, under consideration, or the HIO considers not implementable at this time. If the HIO is not considering the practice, leave the item blank.

Key
R Required means the use of the indicated process, policy, or procedure is required by the HIO
O Optional means the use is in practice by some participants but not required by the HIO
U Under consideration for implementation by the HIO
N Not implementable at this time across all participants for multiple reasons (i.e., cost, technology, political)

A. Authentication Requirements

Table F-57. AUT-1a: User Authentication Requirement: Method(s) of User Identity Vetting at Time or Registration of HIO Members

Description	Key		Comment
In person	—	—	
Notary	—	—	
Demonstrate government-issued ID	—	—	
Other: _____	—	—	
Validate the provider license	—	—	
Validate employees of licensed provider organization	—	—	
HIO use of a specific naming convention as a primary identifier	—	—	
Use of object identifier (OID): _____	—	—	
Describe: _____	—	—	

Em dash (—) is a placeholder for data.

Table F-58. AUT-1b: User Authentication Requirement: Assurance Level Used (Individual User)

Description	Key		Comment
Low (username/PIN)	—	—	
Medium (knowledge/strong password)	—	—	
High (PKI/digital ID)	—	—	
Very high (token)	—	—	
Other: _____	—	—	

Em dash (—) is a placeholder for data.

Table F-59. AUT-1c: User Authentication Requirement: Medication Processing Context Restrictions Apply

Description	Key	Comment
Ordering clinician	—	—
Associated organization	—	—

Em dash (—) is a placeholder for data.

Table F-60. AUT-1d: User Authentication Requirement: Sensitivity Restrictions for Medication Reconciliation Apply

Description	Key	Comment
HIV	—	—
Mental health record	—	—
Substance abuse record	—	—
Sexual health record	—	—
Prison health record	—	—
Other: _____	—	—
Other restrictions: _____	—	—

Em dash (—) is a placeholder for data.

Table F-61. AUT-2: Subject of Care Identity

Description	Key	Comment
Collection and processing of patient demographics/identifiers required for matching	—	—
Collection of SSN	—	—
Collection of driver's license	—	—
Matching criteria policy (e.g., exact match on DOB, first name, last name, address)	—	—
Other: _____	—	—
Provider prove subject of care	—	—

Em dash (—) is a placeholder for data.

Table F-62. AUT-3a: System Authentication: System Identity Vetting

Note: Sharing of medication information may be restricted by system type. Indicate which apply using key.

Description	Key	Comment
In-person—site visit	—	—
Assertion by authorized organization representative	—	—
Certification	—	—
FDA	—	—
CCHIT	—	—
Other: _____	—	—
System IP address	—	—
System domain name	—	—
Other: _____	—	—
Demonstrate association with licensed organization	—	—
HIO use of a naming convention as a primary identifier	—	—
Use of object identifier (OID): _____	—	—
Describe: _____	—	—

Em dash (—) is a placeholder for data.

Table F-63. AUT-3b: System Authentication: Assurance Levels (System to System)

Note: Sharing of medication information may be restricted by system type. Indicate which apply using key.

Description	Key	Comment
Low (username/PIN)	—	—
Medium (knowledge/strong password/shared secret)	—	—
High (PKI/digital ID)	—	—
Very high (token)	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-64. AUT-3c: System Authentication: Medication Processing Context Restrictions Apply (see HITSP C37[8])

Note: Sharing of medication information may be restricted by system type. Indicate which apply using key.

Description	Key	Comment
Ordering system	—	—

Em dash (—) is a placeholder for data.

Table F-65. AUT-3d: System Authentication: Sensitivity Restrictions for Medication Reconciliation Apply

Note: Sharing of medication information may be restricted by system type. Indicate which apply using key.

Description	Key	Comment
HIV	—	—
Mental health record	—	—
Substance abuse record	—	—
Sexual health record	—	—
Prison health record	—	—
Other: _____	—	—
Other restrictions: _____	—	—

Em dash (—) is a placeholder for data.

Table F-66. AUT-4: Data Authentication: Data Authentication Requirements Vary by Jurisdiction and Information Use

Description	Key	Comment
Use of time stamp	—	—
Signature purpose (ASTM E1762)	—	—

Em dash (—) is a placeholder for data.

[8] HITSP Lab Report Document Component C37 Description, HISPC Electronic Health Record Laboratory Result Reporting Use Case Policy Requirements and Standards Adoption V0.0.4. Working Draft, 20080625.

Table F-67. AUT-5a: Organization Authentication: Organization Identity Vetting

Note: Medication data may be shared based upon organization type, leaving specific user authentication management and disclosures to the discretion of the organization.

Description	Key	Comment
In-person—site visit	—	—
Certification	—	—
Joint commission	—	—
SAS-70 compliance	—	—
ENHAC compliance	—	—
Other: _____	—	—
Demonstrate articles of incorporation	—	—
Other: _____	—	—
Validation of organization health care licensure	—	—
HIO use of a specific naming convention as a primary identifier	—	—
Use of object identifier (OID): _____	—	—
Describe: _____	—	—

Em dash (—) is a placeholder for data.

Table F-68. AUT-5b: Organization Authentication: Assurance Levels (Organization to Organization)

Note: Medication data may be shared based upon organization type, leaving specific user authentication management and disclosures to the discretion of the organization.

Description	Key	Comment
Low (username/PIN)	—	—
Medium (knowledge/strong password/shared secret)	—	—
High (PKI/digital ID)	—	—
Very high (token)	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-69. AUT-5c: Organization Authentication: Medication Processing Context Restrictions Apply

Note: Medication data may be shared based upon organization type, leaving specific user authentication management and disclosures to the discretion of the organization.

Description	Key	Comment
Ordering system	—	—

Em dash (—) is a placeholder for data.

Table F-70. AUT-5d: Organization Authentication: Sensitivity Restrictions for Medication Reconciliation Apply

Note: Medication data may be shared based upon organization type, leaving specific user authentication management and disclosures to the discretion of the organization.

Description	Key	Comment
HIV	—	—
Mental health record	—	—
Substance abuse record	—	—
Sexual health record	—	—
Prison health record	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-71. AUT-6: Authenticate Recipient Identity (User, Organization, System): Authenticate the Identity of Recipients of Communications by Any of the Following Means

Description	Key	Comment
Derived from ordering system communications	—	—
Selected from a provider directory	—	—
Derived from identifiers included in the request for information	—	—

Em dash (—) is a placeholder for data.

Table F-72. AUT-7: Data Validation

Description	Key	Comment
Ensuring communication is valid	—	—
Signer credentials:	—	—
Credential issued by trusted authority	—	—
Credential is current	—	—
Credential is not suspended/revoked	—	—
Credential is of appropriate type (e.g., physician, pharmacist)	—	—
Data integrity:	—	—
Data has not been changed since signature	—	—
Time stamp	—	—

Em dash (—) is a placeholder for data.

B. Audit Requirements

Table F-73. AUD-1: Information Request—Requires Written Policy: Components Required in the Written Policy

Description	Key	Comment
Date/time of information request	—	—
Reason for information request	—	—
Description of information requested (to include):	—	—
Data accessed	—	—
Data transmission	—	—
Any data changes (adds, changes, deletes)	—	—
Whether data were transmitted to another party	—	—
Whether data were printed to another party	—	—
ID of person/system requesting disclosure	—	—
ID/verification of the party receiving the information	—	—
ID of the party disclosing the information	—	—
Verification method of requesting the party's ID	—	—
Authorization policy requires audit log identify	—	—
Whether release requires authorization	—	—
Whether authorization was obtained	—	—
Consent ID for audit purposes where applicable and as required	—	—

Em dash (—) is a placeholder for data.

Table F-74. AUD-2: Information Disclosure—Requires Written Policy: Components Required in the Written Policy

Description	Key	Comment
Date/time of request	—	—
Reason for request	—	—
Description of information requested (to include):	—	—
Data accessed	—	—
Data transmission	—	—
Any data changes (adds, changes, deletes)	—	—
Whether data were transmitted to another party	—	—
Whether data were printed to another party	—	—
ID of person/system requesting disclosure	—	—
ID/verification of the party receiving the information	—	—
ID of the party disclosing the information	—	—
Verification method of requesting the party's ID	—	—
Authorization policy requires audit log identify	—	—
Whether release requires authorization	—	—
Whether authorization was obtained	—	—
Consent ID for audit purposes where applicable and as required	—	—

Em dash (—) is a placeholder for data.

C. Data Requirements

Table F-75. DAT-1: Role: Establish a Defined Role Associated with the HIO Registered User Under Which the User is Authenticated

Note: Allows for the defining of role-based access control using which of the following (see Part 6, Supplemental Material, for additional information on roles.)

Description	Key	Comment
Health care functional role	—	—
Structural role	—	—
Organization role	—	—

Em dash (—) is a placeholder for data.

Table F-76. DAT-2: Data Source

Description	Key	Comment
Directory of all National Health Bridge RHIOs	—	—
Directory of data sources within the target RHIO	—	—
Name of the RHIO	—	—
Data sources within that RHIO	—	—
Primary contact information (data in the directories):	—	—
Primary contact name	—	—
Contact phone numbers	—	—
Contact fax numbers	—	—
Master provider index to query by provider for a specific patient	—	—

Em dash (—) is a placeholder for data.

Table F-77. DAT-3: Assurance Levels: Assurance Levels Communicated

Description	Key	Comment
Low (username/PIN)	—	—
Medium (knowledge/strong password/shared secret)	—	—
High (PKI/digital ID)	—	—
Very high (token)	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-78. DAT-4: Requestor Type

Description	Key	Comment
Exchange (HIO)	—	—
Organization (institution)	—	—
User (individual)	—	—

Em dash (—) is a placeholder for data.

[There is no table for DAT-5.]

DAT-6 is an important part of this work but considered not within the strict limits of our project scope. ASP has defined DAT-6 as an optional requirement for data collection. If you choose to include this information, please indicate in the Comment field which, if any, of the following listed data elements are "not permitted to collect" and/or "not permitted to disclose" by state law, rule, or regulation in your state.

Table F-79. DAT-6: Required Elements for Matching (Optional): Data Elements/Identifiers the HIO Uses for Record Matching

Description	Key	Comment
Identifiers (patient account number, SSN, driver license, mother's ID, MRN, alt patient ID)	—	—
Patient name (first, middle, last, family name, suffix, prefix/title, type)	—	—
Mother's maiden name (family name, surname)	—	—
Patient DOB	—	—
Gender	—	—
Patient previous names	—	—
Race	—	—
Patient home address (home street, street or mailing address, street name, dwelling number, other designation [second line of street address], city, state/province, zip, country, address type, county code)	—	—
Patient daytime phone (country code, area/city code, local number, extension, any other text)	—	—
Work telephone	—	—
Primary language	—	—
Marital status	—	—
Religion	—	—
Patient ethnicity	—	—
Birth place	—	—
Multiple birth indicator	—	—
Birth order	—	—
Citizenship	—	—
Veteran's military status	—	—
Nationality	—	—
Deceased (date/time, deceased indicator)	—	—

Em dash (—) is a placeholder for data.

Table F-80. DAT-7: Matching Criteria: Defined Required Minimum Number of Data Elements Required to Query Another System

Description	Key	Comment
Specify number: _____	—	Ex. CO requires 3

Em dash (—) is a placeholder for data.

Table F-81. DAT-8a: Persistence: Persistence of Source Signature

Description	Key	Comment
Persistent user signature	—	—
Persistent organization signature	—	—
Persistent system signature	—	—

Em dash (—) is a placeholder for data.

Table F-82. DAT-8b: Persistence: Nonrepudiation of Origin

Description	Key	Comment
User accountable	—	—
Organization accountable	—	—
System accountable	—	—
Source authentication	—	—
In transit	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-83. DAT-9: Demographics That May Be Logged

Description	Key	Comment
HIO logs a subset of the subject identity attributes that have been used when a person is found	—	—

Em dash (—) is a placeholder for data.

Table F-84. DAT-10: Provider Identity Attributes: User Attributes Included in Directory Entry

Note: HIO collects attributes needed for unique identification of recipient at HIO level.[9]

Description	Key	Comment
Profession	—	—
Specialization/specialty	—	—
Role	—	—
Name	—	—
E-mail	—	—
Address of physician's practice	—	—
Business/legal address	—	—
License/ID	—	—
License status	—	—
NPI	—	—
Digital identity	—	—
Identification service	—	—
Organization affiliation	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-85. DAT-11a: Organization Identity Attributes: Organization Attributes Required by HIO to Allow for Member Organization to Connect to HIO

Description	Key	Comment
Directory entry	—	—
Name	—	—
E-mail	—	—
Address	—	—
NPI	—	—
Digital identity	—	—
Organization affiliation	—	—
EDI administrative contact	—	—
Clinical information contact	—	—
Closure date	—	—
Successor name	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

[9] If getting a request in, look back at requesting HIO to identify provider and attributes in the registry (e.g., looking to send information to Dr. X—as a participant in HIO, roles, PCP).

Table F-86. DAT-11b: Organization Identity Attributes: Regulated Health Care Organization

Description	Key	Comment
All supporting organization attributes above	—	—
License/ID	—	—
License status	—	—
Registered name	—	—
Registered address	—	—
Service locations	—	—

Em dash (—) is a placeholder for data.

Table F-87. DAT-12a: System Identity Attributes: System Attributes Required by HIO for HIO Member Organization Systems to Connect

Description	Key	Comment
Directory entry	—	—
Name	—	—
Digital identity	—	—
Organization affiliation	—	—
System IP address	—	—
System domain name	—	—

Em dash (—) is a placeholder for data.

Table F-88. DAT-12b: System Identity Attributes: System Types: Check all Applicable Types Participating in the HIO

Description	Key	Comment
Laboratory information system	—	—
Electronic health record system	—	—
Emergency medical system	—	—
Emergency department system	—	—
Personal health record	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

Table F-89. DAT-13: Signature Purpose: Applicability and Captured Elements of Signature

Description	Key	Comment
"Author"—Author's signature	—	—
"Author.Co"—Coauthor's signature	—	—
"Participant"—Co-participant's signature	—	—
"Transcriptionist/Recorder"	—	—
"Verification"—Verification signature	—	—
"Validation"—Validation signature	—	—
"Consent"—Consent signature	—	—
"Witness"—Witness signature	—	—
"Witness.Event"—Event witness signature	—	—
"Witness.Identity"—Identity witness signature such as a Notary	—	—
"Witness.Consent"—Consent witness signature	—	—
"Interpreter"	—	—
"Review"—Review signature	—	—
"Source"—Source signature	—	—
"Addendum"—Addendum signature	—	—
Administrative	—	—
Time stamp	—	—
Modification	—	—
Authorization	—	—
Transformation	—	—
Recipient	—	—

Em dash (—) is a placeholder for data.

D. System Requirements

Table F-90. SYS-1: Preparing a Query Message: Specified by HITSP[10]

Description	Key	Comment
HIO generates a registry stored query—asking the registry or record locator service if there are records for this patient (Refer to HITSP IS01)	—	—
HIO generates an HL7 message	—	—

Em dash (—) is a placeholder for data.

[10] See HITSP IS01, Electronic Health Record Laboratory Results Reporting V:2.1.

Table F-91. SYS-2: Audit Log (HIPAA)

Description	Key	Comment
Audit log for use and disclosure and information systems activity exists[11]	—	—
Audit log for use and disclosure and information systems activity occurs at established periodic time frames	—	—
Audit log for use and disclosure of audit log has a set report constructed	—	—
Actions have been identified in the event of discovered anomalies/breaches	—	—
Log-in auditing is required audit criteria (security rule requirement)	—	—
Tracking of the state-specific consent policy[12] under which the data was disclosed exists; may be a global consent policy or a specific consent for each access (e.g., MA)	—	—

Em dash (—) is a placeholder for data.

Table F-92. SYS-3: Audit Log Content: Shared Specifics Include

Note: Ability to share responsibilities for identifying what has been transmitted and which entities are responsible for tracking on specifics.

Description	Key	Comment
User ID	—	—
Date/time stamp	—	—
Data transmitted	—	—
Authorization needed to disclose	—	—
Whether data can be transmitted to another party	—	—

Em dash (—) is a placeholder for data.

Table F-93. SYS-4: System Review

Description	Key	Comment
Automatic trigger exists for any out of state access; automated audit review to permit ready review of any interstate access exists	—	—
Information system review conducted on a regular and periodic basis	—	—

Em dash (—) is a placeholder for data.

[11] The purpose of the audit log is intended for tracking use and disclosure of patient data when appropriate and/or information systems activity needs as required.

[12] Tracking of the state-specific consent policy under which the data was disclosed. May be a global consent policy (opt/in or opt/out) or a specific consent for each access (e.g., MA, tracking of the consent doc ID).

Table F-94. SYS-5: Threshold Calculation

Description	Key	Comment
System ability to calculate some value that represents the quality of a match based on an algorithm	—	—

Em dash (—) is a placeholder for data.

Table F-95. SYS-6: Audit Trail and Node Authentication (ATNA)

Description	Key	Comment
Encryption is specified	—	—
Signing the data	—	—
Specified by policy	—	—

Em dash (—) is a placeholder for data.

[There is no table for SYS-7.]

Table F-96. SYS-8: Security Audit Practices[13]

Description	Key	Comment
HIO audits occur at a specified frequency	—	—
Periodic external audits of the HIO are conducted	—	—
Comprehensive audit procedures exist	—	—
Mitigation and remediation plans exist	—	—
Sharing of risk scores with other RHIOs exists	—	—

Em dash (—) is a placeholder for data.

Table F-97. SYS-9: Digital Signature

Description	Key	Comment
Ability for digital signature exists	—	—

Em dash (—) is a placeholder for data.

Table F-98. SYS-10: Electronic Signature

Description	Key	Comment
Ability for electronic signature (distinct from a digital signature)	—	—

Em dash (—) is a placeholder for data.

[13] Based on Chris Apgar's *Identity Security Audit.*

Table F-99. SYS-11: Signature Verification: Verification of Signer Credentials

Description	Key	Comment
Credential issued by trusted authority	—	—
Credential current	—	—
Credential not suspended/revoked	—	—
Appropriate credential type (e.g., physician, pharmacist)	—	—
Signed by person claimed (nonrepudiation)	—	—

Em dash (—) is a placeholder for data.

Table F-100. SYS-12: Information Integrity

Description	Key	Comment
No change since signature applied	—	—
Valid time stamp	—	—

Em dash (—) is a placeholder for data.

Table F-101. SYS-13: User Identity Verification

Description	Key	Comment
Revocation checking	—	—
Expiration checking	—	—
Authentication method checking	—	—
Challenge/response checking	—	—
Other: _____	—	—

Em dash (—) is a placeholder for data.

E. Policy Requirements

Table F-102. POL-1: Interim Reports

Description	Key	Comment
Interim reports of lab results are made available for sharing with persons that have appropriate access, once the ordering physician has signed off on the results and has discussed results with patient where required by policy	—	—

Em dash (—) is a placeholder for data.

Table F-103. POL-2: Restricted Data Sharing

Description	Key	Comment
Caveats to data completeness are transmitted	—	—

Em dash (—) is a placeholder for data.

[There are no tables for POL-3 through POL-7.]

Table F-104. POL-8: Returning More Demographics

Description	Key	Comment
Returning more demographic information to the end user than was initially entered	—	—

Em dash (—) is a placeholder for data.

Table F-105. POL-9: Audit Log Process

Description	Key	Comment
Minimum agreement on who is responsible for reconstitution and sharing audit log information during an investigation. Who is authorized to request this disclosure and to whom does this go? Where does or can a patient make the request to the RHIO?	—	—

Em dash (—) is a placeholder for data.

Table F-106. POL-10: Data Authentication

Description	Key	Comment
Methods for assurance that data have not been modified if a document is shared with a patient	—	—

Em dash (—) is a placeholder for data.

Table F-107. POL-11: Digital Signature

Description	Key	Comment
Policy allowing the organization to accept or express data without signature or with a caveat or some marker that no signature was received	—	—

Em dash (—) is a placeholder for data.

Table F-108. POL-12: Relationship to Patient

Description	Key	Comment
Gray area—for HIPAA-only regulated state—subject of care—provider needs to demonstrate they are the provider of the subject of care	—	—

Em dash (—) is a placeholder for data.

Table F-109. POL-13: Risk Assessment

Description	Key	Comment
Identification of risk issues (e.g., data authentication not a high risk in this scenario)	—	—

Em dash (—) is a placeholder for data.

Table F-110. POL-14: Signature/ Data Validation Checking: Signature and Data Integrity Conducted Prior to Allowing the Following Procedures

Description	Key	Comment
Using data communicated through secured methods (e.g., VPN)	—	—
Using data communicated through insecure methods (e.g., patient USB)	—	—
Storing data	—	—
Submitting data to shared resource	—	—

Em dash (—) is a placeholder for data.

The HIPAA Security Rule and by inference the Privacy Rule require at a minimum four different types of audits. (State and other federal laws may specify additional requirements.) The following policies outline only the HIPAA Security Rule audit requirements. Each requirement definition includes the type of safeguard (administrative, physical, or technical), whether this impacts policy/system/data requirements, and the regulatory cite. This represents the bare minimum audit requirements for all covered entities and business associates. It includes RHIOs who are generally business associates of participating covered entities/providers.

Assumptions. Organizations have some variation of POL-17 Evaluation (a required administrative safeguard) in place, and, as such, this requirement is not identified on Part 4 of this template.

Table F-111. POL-15: Information System Activity Review (45 C.F.R. 164.308(a)(1): Administrative Safeguard; Policy, Data, and System Requirements

Description	Key	Comment
Software applications, network servers, firewalls, and other network hardware and software are configured to create audit logs that track activities involving electronic protected health information (ePHI) such as data modification, creation, deletion, etc.	—	—
The audit logs generated are reviewed on a regular basis based on audit criteria developed in advance, any anomalies documented, and mitigating action, if necessary.	—	—
Documentation is retained for a minimum of 6 years.	—	—

Em dash (—) is a placeholder for data.

Table F-112. POL-16: Log-in Monitoring (45 C.F.R. 164.308(a)(5): Administrative Safeguard; Policy, Data, and System Requirements

Description	Key	Comment
An audit log created to record when a workforce member or business associate logs on to the network or a software application, when log-in is attempted, and when the log-in attempt fails.	—	—
The audit logs generated are reviewed on a regular basis based on audit criteria developed in advance, any anomalies documented, and mitigating action, if necessary.	—	—
Documentation is retained for a minimum of 6 years.	—	—

Em dash (—) is a placeholder for data.

Table F-113. POL-17: Evaluation (45 C.F.R. 164.308(a)(8): Administrative Safeguard; Policy Requirements

Description	Key	Comment
Periodic technical and nontechnical evaluations are conducted to reasonably ensure the covered entity is compliant with the provisions of the HIPAA Security Rule. Otherwise known as a compliance audit.	—	—
Audit criteria are to be developed in advance.	—	—
An evaluation occurs at least annually or when any major system or business changes occur.	—	—
Evaluation requires:	—	—
Generation of an audit findings report.	—	—
Associated mitigating action or documentation that an identified deficiency represents a risk the organization is willing to accept.	—	—
The organization is responsible for prioritizing mitigation and document mitigation plans (including documenting completion of mitigating activity).	—	—
All documentation must be retained for a minimum of 6 years.	—	—

Em dash (—) is a placeholder for data.

Table F-114. POL-18: Audit Controls (45 C.F.R. 164.312(b): Technical Safeguard; Policy, Data, System Requirements

Description	Key	Comment
Covered entities must implement technical processes that accurately record activity related to access, creation, modification, and deletion of ePHI.	—	—
Audit logs recording activity as it relates to ePHI and the periodic review of generated audit logs.	—	—
Review of audit logs is based on established audit criteria and includes documentation of any anomalies and mitigating action (including sanctions, security incident response team activation, etc. as appropriate), if necessary.	—	—
All documentation is retained for a minimum of 6 years.	—	—
Audit logs at a minimum must include:	—	—
Unique user name/ID	—	—
Date/time stamp	—	—
Action taken (view, add, change, delete)	—	—

Em dash (—) is a placeholder for data.

Part 4. User Guide to Instrument Completion

This part contains defined interactions and conditions described as events and actions in the Medication Management Use Case. In addition, it identifies authentication, audit, data, system, and policy requirements that may apply given the action as defined by the AHIC scenario. State health information organization models may differ in their responses to these given interactions and requirements. The following described actions under the AHIC comment section are to be used as a guide for states documenting their HIO-specific processes associated with the use case.

1. Review each Event, Associated Action, and AHIC Comment.
2. For each identified event, describe the necessary action(s) the state-specific HIO would follow given the HIO model in your state. For example, Code 6.1.1, Event: Configure medication decision support—Question: What action(s) or processes are necessary in order to receive information from drug knowledge suppliers via the HIO in your state? If the event is not applicable to your model, please indicate "not applicable to the HIO model" under the "State Model Comment" field.
3. For each "State Model Comment" response supplied, circle which, if any, authentication, audit, data, system, and/or policy requirements (see Part 3 for detailed specifics for these requirements: worksheets A–E) are triggered at the HIO level. The requirements are business processes, procedures, and/or policies that are specific to the given model being described that must occur in order for the action(s) to take place. (Each state demonstration model should have completed a summary list of requirements in each of these areas.) If the described actions have Requirements that come into play other than those that are identified below for each action, write in the requirement name and number (as identified in worksheets from Part 3) in the appropriate column. If no requirement is needed, circle "No applicable requirements" in the appropriate requirement column.

Medication Management Use Case

Code 6.1.1

Event: Configure Medication Decision Support

Code: 6.1.1.1

AHIC Description: Action: Receive information from drug knowledge suppliers.

AHIC Comment: Vendors and other sources provide data tables and reference information to support medication screening for contraindications and other decision support capabilities. These act in conjunction with, and are integrated into, the hospital EHR. These tools can also be used in a long-term care setting (re: provisioning for secondary use).

State Model Comment: What actions or process(es) are necessary to receive information from drug knowledge suppliers at the HIO level?

ASP Requirements

Authentication

(AUT-4) Data authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-9) Digital signature
Other requirements (specify): _____
No applicable requirements

Policies

(POL-10) Data authentication
(POL-13) Risk assessment
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Medication Management Use Case

Code 6.1.2

Event: Gather Medication and Allergy Information at Admission

Code: 6.1.2.1

AHIC Description: Action: Request available medication and allergy information in interoperable electronic form.

AHIC Comment: Upon admission to the emergency department or the hospital, the clinician gathers information about the patient's current medication and allergies from several sources. Consumer self-reported prescription, over-the-counter (OTC) medication, vitamins, implanted medication infusion devices, and herbal and other supplements may also be available from the patient's PHR, as well as information about allergies, intolerances, side effects, sensitivity responses, adverse effects, and similar reactions, in addition to accompanying information (e.g., nature of reaction, severity of reaction, and source of information). Additional available information could be gathered electronically via health information exchange, from hospital EHRs, ambulatory EHRs (such as from a primary care physician [PCP]), long-term care EHRs, and other sources (such as pharmacy systems, PNIs, PBMs, payors, etc.) that hold information about the patient. A generalized process for

matching patients is described in Appendix A: Arbitrating Identities. A generalized process for access control is described in Appendix A: Create and Maintain Access Control Lists. Ideally, this information should be provided in an integrated view without duplications that can be used during the stay and communicated at discharge. In each case, the information source (e.g., authoritative clinical source, administrative source, or patient) should also be captured.

State Model Comment: —

ASP Requirements

Authentication

(AUT-1) User authentication
(AUT-3) System authentication
(AUT-5) Organization authentication
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching (out of scope for HISPC Phase III)
(DAT-10) Provider identity attributes
(DAT-11) Organization identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-9) Audit log process
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Medication Management Use Case

Code 6.1.3

Event: Gather Medication and Allergy Information at Admission

Code: 6.1.3.3

AHIC Description: Action: Document medication reconciliation.

AHIC Comment: The clinician documents the decisions made regarding medications. In an EHR, once the decisions have been documented, the physician signs via electronic signature.

State Model Comment: —

ASP Requirements

Authentication

(AUT-4) Data authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-13) Signature purpose
Other requirements (specify): _____
No applicable requirements

System

(SYS-9) Digital signature
(SYS-10) Electronic signature
Other requirements (specify): _____
No applicable requirements

Policies

(POL-10) Data authentication
(POL-11) Digital signature
(POL-13) Risk assessment
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Medication Management Use Case

Code 6.1.4

Event: Write Medication Order

Code: 6.1.4.3

AHIC Description: Action: Sign medication order.

AHIC Comment: Once the clinician signs a new medication order, the patient's medication list is updated.

State Model Comment: —

ASP Requirements

Authentication

(AUT-4) Data authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-13) Signature purpose
Other requirements (specify): _____
No applicable requirements

System

(SYS-9) Digital signature
(SYS-10) Electronic signature
Other requirements (specify): _____
No applicable requirements

Policies

(POL-10) Data authentication
(POL-11) Digital signature
(POL-13) Risk assessment
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 6.1.4.4b

AHIC Description: Alternative action: Communicate medication order to external pharmacy system.

AHIC Comment: The medication order is communicated to an external pharmacy that is completely separate from the organization's EHR.

State Model Comment: —

ASP Requirements

Authentication

Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Medication Management Use Case

Code 6.1.5

Event: View Medication and Allergy Information

Code: 6.1.5.1

AHIC Description: During the hospital stay, clinicians and pharmacists involved in the patient's care need to be able to view information on the patient's current medications, including those that were documented during medication reconciliation at admission and other medications ordered during the stay. In order to be current, the information also includes pharmacist verification status and any order modifications made by the pharmacist.

AHIC Comment: Once the clinician signs a new medication order, the patient's medication list is updated.

State Model Comment: —

ASP Requirements

Authentication

(AUT-4) Data authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-13) Signature purpose
Other requirements (specify): _____
No applicable requirements

System

(SYS-9) Digital signature
(SYS-10) Electronic signature
Other requirements (specify): _____
No applicable requirements

Policies

(POL-10) Data authentication
(POL-11) Digital signature
(POL-13) Risk Assessment
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Medication Management Use Case

Code 6.1.6

Event: Perform Medication Reconciliation at Internal Transfer

Code: 6.1.6.3

AHIC Description: Action: Document medication reconciliation.

AHIC Comment: The clinician documents the decisions made during medication reconciliation. In an EHR, once the decisions have been documented, the physician signs via electronic signature.

State Model Comment: —

ASP Requirements

Authentication

(AUT-4) Data authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-13) Signature purpose
Other requirements (specify): _____
No applicable requirements

System

(SYS-9) Digital signature
(SYS-10) Electronic signature
Other requirements (specify): _____
No applicable requirements

Policies

(POL-10) Data authentication
(POL-11) Digital signature
(POL-13) Risk assessment
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Medication Management Use Case

Code 6.1.7

Event: Perform Medication Reconciliation Upon Discharge

Code: 6.1.7.3

AHIC Description: Action: Document medication reconciliation.

AHIC Comment: The clinician documents the decisions made about which outpatient medications to resume and any new prescriptions for discharge medications. In the EHR, this is documented electronically and signed via electronic signature.

State Model Comment: —

ASP Requirements

Authentication

(AUT-4) Data authentication
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-13) Signature purpose
Other requirements (specify): _____
No applicable requirements

System

(SYS-9) Digital signature
(SYS-10) Electronic signature
Other requirements (specify): _____
No applicable requirements

Policies

(POL-10) Data authentication
(POL-11) Digital signature
(POL-13) Risk assessment
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Medication Management Use Case

Code 6.1.8

Event: Write New Discharge Prescriptions

Code: 6.1.8.1

AHIC Description: Action: Prescribe new medications at discharge.

AHIC Comment: The clinician writes any new prescriptions required following the hospital stay. This process could be supported by clinical decision support for recommended indications, dosing, and access to reference information. The clinician could benefit from the ability to verify patient eligibility, formulary access, and pharmacy benefits coverage to minimize overall medication costs. Clinicians could use an electronic prescribing function (e.g., an e-Prescribing tool, an ambulatory EHR, or a hospital or long-term care EHR with ambulatory prescribing functionality) to write these prescriptions electronically. These prescriptions immediately update the information being compiled on discharge medications for medication reconciliation.

State Model Comment: —

ASP Requirements

Authentication

(AUT-4) Data Authentication
Other Requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-13) Signature purpose
Other requirements (specify): _____
No applicable requirements

System

(SYS-9) Digital signature
(SYS-10) Electronic signature
Other requirements (specify): _____
No applicable requirements

Policies

(POL-10) Data authentication
(POL-11) Digital signature
(POL-13) Risk assessment
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 6.1.8.3

AHIC Description: Action: Communicate information to pharmacy.

AHIC Comment: Discharge prescriptions may be communicated to an external pharmacy.

State Model Comment: —

ASP Requirements

Authentication

Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Medication Management Use Case

Code 6.1.9

Event: Provide Information to the Next Provider of Care and Patient

Code: 6.1.9.1

AHIC Description: Action: Communicate medication and allergy information to the next provider of care.

AHIC Comment: At the conclusion of the hospital stay, a patient could return to the care of their primary care physician (PCP) and/or medical specialist(s), be transferred from emergency department to hospital admission (if it is not handled as an internal transfer), or be transferred into the care of another health care facility (e.g., a long-term care facility). The information communicated includes current information on patient allergies (including new allergies documented during the hospital stay) and the outpatient medication list captured for the patient at admission, annotated as to which ones are to be resumed or discontinued, as well as any new discharge prescriptions.

State Model Comment: —

ASP Requirements

Authentication

(AUT-4) Data authentication
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
Other requirements (specify): _____
No applicable requirements

Data

(DAT-13) Signature purpose
Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
(SYS-9) Digital signature
(SYS-10) Electronic signature
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-10) Data authentication
(POL-11) Digital signature
(POL-13) Risk assessment
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

[Inpatient Medication Reconciliation, Pharmacist Perspective Events and Actions are out of project scope]

[Inpatient Medication Reconciliation, Consumer Perspective Events and Actions are out of project scope]

Ambulatory Medication Management, Clinician Perspective Events and Actions Use Case

Code 7.1.1

Event: Configure Medication Decision Support

Code: 7.1.1.1

AHIC Description: Action: Receive information from drug knowledge suppliers.

AHIC Comment: Vendors and other sources provide data tables and reference information to support medication screening for contraindications and other decision support capabilities. These act in conjunction with, and are integrated into, the ambulatory EHR. These tools may also support pharmacists in their roles. A generalized process is described in Appendix A: Provisioning for Secondary Use.

State Model Comment: —

ASP Requirements

Authentication

(AUT-4) Data authentication
(AUT-7) Data validation
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-13) Signature purpose
Other requirements (specify): _____
No applicable requirements

System

(SYS-9) Digital signature
(SYS-10) Electronic signature
(SYS-11) Signature verification
(SYS-12) Information integrity validation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-10) Data authentication
(POL-11) Digital signature
(POL-13) Risk assessment
(POL-14) Signature/data validation checking policy
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Ambulatory Medication Management, Clinician Perspective Events and Actions Use Case

Code 7.1.2

Event: Perform Eligibility and Benefits Checking

Code: 7.1.2.1

AHIC Description: Action: Check patient eligibility.

AHIC Comment: The patient's eligibility for services, including pharmacy benefits, needs to be confirmed. Direct query for eligibility and pharmacy benefits information from a pharmacy system, PBM, or payor directly and/or through health information exchange or a Medication Network Intermediary may exist. This event may also support the long-term

care setting. A generalized process for patient matching is described in Appendix A: Arbitrating Identities.

State Model Comment: —

ASP Requirements

Authentication

(AUT-1) User authentication
(AUT-2) Subject of care identity
(AUT-3) System authentication
(AUT-5) Organization authentication
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching (out of scope for HISPC Phase III)
(DAT-7) Matching criteria
(DAT-9) Demographics that may be logged
(DAT-10) Provider identity attributes
(DAT-11) Organization identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-5) Threshold calculation
(SYS-8) Security audit practices
(SYS-9) User identity verification
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-8) Returning more demographics
(POL-9) Audit log process
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Ambulatory Medication Management, Clinician Perspective Events and Actions Use Case

Code 7.1.3

Event: Gather Medication and Allergy Information

Code: 7.1.3.1

AHIC Description: Action: Request available medication and allergy information in interoperable electronic form.

AHIC Comment: To make decisions about care, the clinician would benefit from a complete view of the patient's current medications and allergies, as well as past access to a medication. A patient may have a PCP, as well as one or more specialists, all of whom may be writing medication prescriptions for the patient. Many external sources can supplement the information available locally on the medications and allergies: EHRs of other PCPs and specialists in the community, the EHR in a hospital from which the patient was recently discharged, PBMs, and organizations involved in communication of prescriptions and claims. Consumer self-reported prescription, over-the-counter (OTC) medication, vitamins, implanted medication infusion devices, and herbal and other supplements may be available from the patient's PHR, as well as information about allergies, intolerances, side effects, sensitivity responses, adverse effects, and similar reactions, in addition to accompanying information (e.g., nature of reaction, severity of reaction, and source of information). Ideally, information from these sources should be provided in an integrated view, without duplications, that can be easily incorporated into the EHR in codified form. In each case, the information source (e.g., authoritative clinical source, administrative source, or patient) should also be captured. A generalized process for patient matching is described in Appendix A: Arbitrating Identities. A generalized process for access control is described in Appendix A: Create and Maintain Access Control Lists.

State Model Comment: —

ASP Requirements

Authentication

(AUT-1) User authentication
(AUT-2) Subject of care identity
(AUT-3) System authentication
(AUT-5) Organization authentication
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching (out of scope for HISPC Phase III)
(DAT-7) Matching criteria
(DAT-9) Demographics that may be logged
(DAT-10) Provider identity attributes
(DAT-11) Organization identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-5) Threshold calculation
(SYS-9) User identity verification
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-8) Returning more demographics
(POL-9) Audit log process
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Ambulatory Medication Management, Clinician Perspective Events and Actions Use Case

Code 7.1.4

Event: Write Prescription

Code: 7.1.4.1

AHIC Description: Action: Consider formulary.

AHIC Comment: Clinicians would benefit from the ability to access and consider patient-specific pharmacy benefit information for pharmacy benefits, Medicare part D, and formulary information as they make prescribing decisions to minimize overall medication costs. [This information may have been obtained previously based on an earlier eligibility request.] This information may be provided by pharmacy systems, PBMs, or payors and may be provided directly or through the use of a Medication Network Intermediary. Formulary considerations are also relevant in the long-term care setting.

State Model Comment: —

ASP Requirements

Authentication

(AUT-1) User authentication
(AUT-2) Subject of care identity
(AUT-3) System authentication
(AUT-5) Organization authentication
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching (out of scope for HISPC Phase III)
(DAT-7) Matching criteria
(DAT-9) Demographics that may be logged
(DAT-10) Provider identity attributes
(DAT-11) Organization identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-5) Threshold calculation
(SYS-8) Security audit practices
(SYS-9) User identity verification
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-8) Returning more demographics
(POL-9) Audit log process
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 7.1.4.4

AHIC Description: Action: Sign prescription.

AHIC Comment: Once the clinician signs a new prescription, the patient's medication list is updated.

State Model Comment: —

ASP Requirements

Authentication

(AUT-4) Data authentication
(AUT-7) Data validation
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-13) Signature purpose
Other requirements (specify): _____
No applicable requirements

System

(SYS-9) User identity verification
(SYS-10) Electronic signature
(SYS-11) Signature verification
(SYS-12) Information integrity validation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-10) Data authentication
(POL-11) Digital signature
(POL-13) Risk assessment
(POL-14) Signature/data validation checking policy
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 7.1.4.5

AHIC Description: Action: Communicate information to pharmacy.

AHIC Comment: An e-Prescribing tool or an ambulatory EHR could communicate electronic prescriptions to the patient's preferred pharmacy. A pharmacy may also be affiliated with a clinician's ambulatory office (with integrated prescribing and pharmacy functions). Prescription changes and cancellations could also be transmitted to the pharmacy in a similar manner. Clinician prescribers (and clinics) may also give patients access to no-cost (free) medications that would need to be correctly captured in the EHR medication prescription record.

State Model Comment: —

ASP Requirements

Authentication

(AUT-4) Data authentication
(AUT-7) Data validation
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
Other requirements (specify): _____
No applicable requirements

Data

(DAT-13) Signature purpose
Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
(SYS-9) User Identity verification
(SYS-10) Electronic signature
(SYS-11) Signature verification
(SYS-12) Information integrity validation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-10) Data authentication
(POL-11) Digital signature
(POL-13) Risk assessment
(POL-14) Signature/data validation checking policy
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code: 7.1.4.5a

AHIC Description: Alternative action: Communicate information to pharmacy using paper or fax.

AHIC Comment: In cases where electronic communication to pharmacy is not offered, or if the system is currently unavailable, a traditional paper prescription, printed prescription, or fax could be used to communicate the prescription information.

State Model Comment: —

ASP Requirements

Authentication

(AUT-6) Authenticate recipient identity (organization, user, system)
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-13) Risk assessment
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Ambulatory Medication Management, Clinician Perspective Events and Actions Use Case

Code 7.1.6

Event: Provide Information to Patient

Code: 7.1.6.1

AHIC Description: Action: Communicate current medication list, prescriptions, allergy information, and care instructions to the patient.

AHIC Comment: The medication list, new prescriptions, allergy information, and instructions should be communicated to the patient. This information could also be communicated to their PHRs from the ambulatory EHR. The patient may also be provided with relevant medication guides or patient information sheets.

State Model Comment: —

ASP Requirements

Authentication

(AUT-1) User authentication
(AUT-3) System authentication
(AUT-5) Organization authentication
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching (out of scope for HISPC Phase III)
(DAT-10) Provider identity attributes
(DAT-11) Organization identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
(SYS-9) User identity verification
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-9) Audit log process
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Ambulatory Medication Management, Pharmacist Perspective Events and Actions Use Case

Code 7.2.1

Event: Verify Prescription

Code: 7.2.1.1

AHIC Description: Action: Verify prescription.

AHIC Comment: The prescription is processed in a series of steps including receipt of order, checking for possible contraindications using medication decision support tools, and prescription verification. The pharmacist may also communicate with the prescribing clinician where questions exist and prescription changes are appropriate. An electronic request for a prescription refill could also be initiated by a consumer via their PHR. **Note:** Pharmacist also might communicate with the consumer.

State Model Comment: —

ASP Requirements

Authentication

(AUT-1) User authentication
(AUT-3) System authentication
(AUT-5) Organization authentication
(AUT-7) Data validation
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching (out of scope for HISPC Phase III)
(DAT-10) Provider identity attributes
(DAT-11) Organization identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
(SYS-9) User identity verification
(SYS-11) Signature verification
(SYS-12) Information integrity validation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-9) Audit log process
(POL-14) Signature/data validation checking policy
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Ambulatory Medication Management, Pharmacist Perspective Events and Actions Use Case

Code 7.2.2

Event: Request and View Medication and Allergy Information

Code: 7.2.2.1

AHIC Description: Action: Request available medication and allergy information.

AHIC Comment: The pharmacist requests available medication and allergy information. This information may be derived from sources such as a PBM system, payor, and/or a pharmacy system.

State Model Comment: —

ASP Requirements

Authentication

(AUT-1) User authentication
(AUT-2) Subject of care identity
(AUT-3) System authentication
(AUT-5) Organization authentication
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching (out of scope for HISPC Phase III)
(DAT-7) Matching criteria
(DAT-9) Demographics that may be logged
(DAT-10) Provider identity attributes
(DAT-11) Organization identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
(SYS-9) User identity verification
(SYS-11) Signature verification
(SYS-12) Information integrity validation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-8) Returning more demographics
(POL-9) Audit log process
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Ambulatory Medication Management, Pharmacist Perspective Events and Actions Use Case

Code 7.2.4

Event: Dispense Prescription

Code: 7.2.4.2

AHIC Description: Action: Provide medication dispensing status.

AHIC Comment: The pharmacy system records the dispensing status (or "fill status notification") of each medication for future consideration. Clinicians would benefit from knowing the dispensing status as a partial indicator of patient compliance with the recommended treatment. The information communicated should include the dispensing date, the date the prescription was picked up from the pharmacy, medication lot number, expiration date and quantity dispensed.

State Model Comment: —

ASP Requirements

Authentication

(AUT-6) Authenticate recipient identity (organization, user, system)
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-13) Risk assessment
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Medication Management Use Case

Code 8

Event: Information Exchange

Code: 8.1

AHIC Description: Action: Identify subject.

AHIC Comment: Based on a query or the contents of a record, determine if an HIE subject registry has a record that matches the subject referenced in the query or record. Search for candidate subject matches within an HIE registry.

State Model Comment: —

ASP Requirements

Authentication

(AUT-2) Subject of care identity
Other requirements (specify): _____
No applicable requirements

Audit

Other requirements (specify): _____
No applicable requirements

Data

(DAT-6) Required elements for matching (out of scope for HISPC Phase III)
(DAT-7) Matching criteria
(DAT-9) Demographics that may be logged
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-5) Threshold calculation
Other requirements (specify): _____
No applicable requirements

Policies

(POL-8) Returning more demographics
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Medication Management Use Case

Code 8

Event: Information Exchange

Code: 8.2

AHIC Description: Action: Locate records.

AHIC Comment: Locate the records within an HIE or among several HIEs for a patient that has been identified. Retrieve any available locations that have records for the identified patient within an HIE and among several HIEs.

State Model Comment: —

ASP Requirements

Authentication

(AUT-1) User authentication
(AUT-3) System authentication
(AUT-5) Organization authentication
Other requirements (specify): _____
No applicable requirements

Audit

(AUD2) Information request
Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching (out of scope for HISPC Phase III)
(DAT-10) Provider identity attributes
(DAT-11) Organization identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-9) Audit log process
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Medication Management Use Case

Code 8

Event: Information Exchange

Code: 8.3

AHIC Description: Action: Retrieve data.

AHIC Comment: Enable providers and consumers to view or access patient records within and across HIEs. Provide the requested data from the identified record locations in response to the user request.

State Model Comment: —

ASP Requirements

Authentication

(AUT-1) User authentication
(AUT-3) System authentication
(AUT-5) Organization authentication
(AUT-7) Data validation
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
(AUD-2) Information request
Other requirements (specify): _____
No applicable requirements

Data

(DAT-1) Role
(DAT-2) Data source
(DAT-6) Required elements for matching (out of scope for HISPC Phase III)
(DAT-10) Provider identity attributes
(DAT-11) Organization identity attributes
(DAT-12) System identity attributes
Other requirements (specify): _____
No applicable requirements

System

(SYS-1) Preparing a query message
(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
(SYS-9) User identity verification
(SYS-11) Signature verification
Other requirements (specify): _____
No applicable requirements

Policies

(POL-2) Restricted data sharing
(POL-9) Audit log process
(POL-14) signature/data validation checking policy
(POL-15) Info sys review
(POL-16) Log-in monitoring
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Code 8

Event: Information Exchange

Code: 8.4

AHIC Description: Action: Route data based on content.

AHIC Comment: Some messages have content that indicates the providers and Care Delivery Organizations (CDOs) that should receive a message. Some consumers may seek to establish data delivery to their PHR or other providers of their care. The HIE reviews these contents and distributes the messages accordingly. The distribution may be within the HIE or across HIEs. Forward the message to the appropriate location based on the identified patient and/or provider referenced in the message.

State Model Comment: —

ASP Requirements

Authentication

(AUT-6) Authenticate recipient identity (organization, user, system)
Other requirements (specify): _____
No applicable requirements

Audit

(AUD-1) Information disclosure
Other requirements (specify): _____
No applicable requirements

Data

Other requirements (specify): _____
No applicable requirements

System

(SYS-2) Audit log
(SYS-3) Audit log content
(SYS-8) Security audit practices
Other requirements (specify): _____
No applicable requirements

Policies

(POL-9) Audit log process
(POL-13) Risk assessment
(POL-15) Info sys review
(POL-18) Audit controls
Other requirements (specify): _____
No applicable requirements

Part 5. Local HIO Business Actors

Instructions: In Table F-115, identify the name of the organization, the local business actor(s) participating in the HIO that align with the HITSP business actor, and description

for this use case. Indicate in the "Availability" column which service options are provided by the local business actor. If the service options provided by your local business actor are not listed, please add the type of the service(s) provided to the appropriate category listing. For example, if XClinical vendor provides document source, audit repository, secure node, and other, list XClinical vendor in the "Local Business Actor" column, check each availability box next to the three identified service options, write in the additional service options provided, and check the corresponding availability box.

If other local business actors are part of your HIO model and are not included as part of the HITSP business actor grouping in this table, please add to the bottom of the table and add "Description" and "Service Options" for the actor.

Table F-115. Local HIO Business Actors

Local Business Actor	Mapping to HITSP Business Actor	Description	Availability	Service Options
—	EHR	The electronic health record (EHR) is a longitudinal electronic record of patient health information generated in one or more encounters in any care delivery setting. This information may include patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory information, and radiology reports.	—	Document source Document consumer Audit repository XDS repository Secure node CT XUA
—	Pharmacy systems	Electronic systems that support pharmacists in their role for dispensing medications and performing professional services. This includes systems that may provide consumers' medication history.	—	Medication order filler Eligibility information receiver Medication formulary and benefits retriever Patient identity source PIX consumer Patient demographic consumer Audit record source CT client Secure node Service user Access control consumer
—	HIE (other clinical or administrative data sources)	An entity that enables the movement of health-related data within state, regional, or nonjurisdictional participant groups.	—	PIX manager Audit repository XDS registry XDS repository Secure node CT client XUA

(continued)

Table F-115. Local HIO Business Actors (continued)

Local Business Actor	Mapping to HITSP Business Actor	Description	Availability	Service Options
—	Clinical decision support/e-prescribing	Systems that help clinicians avoid adverse drug events through prompts and advisory messages about potential drug interactions, drug-diagnosis considerations, drug-renal function contraindications, patient allergies, potential errors in dosing, and other issues that may lead to adverse drug events. The clinician may also have access to relevant reference information.	—	Patient identity source PIX consumer Patient demographic Consumer Document source Audit record source CT client Secure node Service user Access control consumer
—	Pharmacy benefit managers	These entities manage pharmacy benefits on behalf of payors, interacting with pharmacies and providers via a medication network intermediary. As part of this role, they can provide information on pharmacy benefits available to an individual consumer and an individual consumer's medication history.	—	HL7 query/response PIX manager Audit XDS registry Repository XDS repository Secure node CT client XUA
—	Payers	Insurers, including health plans, self-insured employer plans, and third-party administrators, providing health care benefits to enrolled members and reimbursing provider organizations. As part of this role, they provide information on eligibility and coverage for individual consumers, as well as claims-based information on consumer medication history. Case management or disease management may also be supported.	—	Eligibility information Source Medication formulary and Benefits source Medication order filler PIX manager Patient demographic Supplier Document repository

* PHR determined out of scope.

Em dash (—) is a placeholder for data.

Part 6. Supplemental Material

The information in Tables F-116 through F-119 is for use in helping to answer Data Requirement DAT-1 Role. There are two parts to consider in review of the requirements:

1. Are HIO users established based on roles: structural, functional, organizational?
2. Are users/members/participants allowed access to data as defined by their user role?

Table F-116. Structural Roles

In this Role is the User Expected to be Able to Access Data?		Yes	No
1.	Physician (MD/allopath, osteopath, chiropractic, naturopath, homeopath)	—	—
2.	Advanced practice registered nurse (NP, NM, CAN, CNS)	—	—
3.	Physician assistant (PA)	—	—
4.	Midwives	—	—
5.	Registered nurse (RN)	—	—
6.	Licensed vocational nurse (LVN)	—	—
7.	Nonwestern medicine providers	—	—
8.	Ancillary service providers	—	—
8a.	Occupational therapy	—	—
8b.	Physical therapy	—	—
8c.	Cast technicians	—	—
8d.	Prosthetic technicians	—	—
8e.	Speech therapy	—	—
8f.	Respiratory therapy	—	—
9.	Technician	—	—
9a.	Technician: Procedure-based (OR, cath lab, etc.)	—	—
9b.	Technician: Departmental	—	—
9c.	Technician: Specialty	—	—
9d.	Technician: General	—	—
10.	Nonlicensed care providers	—	—
10a.	Nurse's aide	—	—
10b.	Orderly	—	—
10c.	Phlebotomist	—	—
10d.	Bereavement counselor	—	—
10e.	Volunteer	—	—
10f.	Technician	—	—
10g.	Patient transportation personnel	—	—

(continued)

Table F-116. Structural Roles (continued)

In this Role is the User Expected to be Able to Access Data?	Yes	No
10h. Specimen transportation personnel	—	—
10i. Health record transportation personnel	—	—
11. Emergency services	—	—
11a. Paramedic	—	—
11b. EMT	—	—
11c. EMS	—	—
11d. Ambulance drivers	—	—
11e. Air transport pilots	—	—
12. Secular services (priest, rabbi, pastoral care, etc.)	—	—
13. Patient advocate	—	—
14. Interpreters	—	—
15. Clerical and administrative personnel	—	—
15a. Encounter registration clerk	—	—
15b. Admission clerk	—	—
15c. Ward/unit/clinic clerk	—	—
15d. Departmental clerk	—	—
15e. Clinical services	—	—
15f. Laboratory services	—	—
15g. Imaging services	—	—
15h. Pharmacy services	—	—
15i. Social services	—	—
15j. Ancillary services	—	—
16. Disposition/discharge clerks	—	—
17. Administrative support staff and services	—	—
17a. Physician office	—	—
17b. Nonphysician provider office	—	—
17c. Clinical department	—	—
17d. Administrative department	—	—
17e. Health records (medical records)/health information management department	—	—
17f. Quality assurance	—	—
18. Transcription personnel	—	—
18a. Coders/reimbursement specialists	—	—

(continued)

Table F-116. Structural Roles (continued)

In this Role is the User Expected to be Able to Access Data?	Yes	No
18b. Transcriptionist	—	—
18c. Claims personnel	—	—
18d. Proofreader	—	—
18e. QA personnel	—	—
18f. Clerks	—	—
18g. Students	—	—
18h. Supervisors/managers	—	—
18i. Vendors	—	—
18j. Maintenance and system support personnel	—	—
19. File clerk	—	—
19a. Clinical department	—	—
19b. Administrative department	—	—
19c. Health records (medical records)/health information management department	—	—
19d. Quality assurance	—	—
20. Supervisory personnel	—	—
20a. Clinical department	—	—
20b. Administrative department	—	—
20c. Health records (medical records)/health information management department	—	—
20d. Quality assurance	—	—
21. Health records (medical records)/health information management department	—	—
21a. Administration	—	—
21b. Administrative support	—	—
21c. File clerks	—	—
21d. Information management personnel	—	—
22. Information services	—	—
22a. Database administrator	—	—
22b. Network administrator	—	—
22c. Security administrator	—	—
22d. Trainer (of end users)	—	—
22e. Help desk	—	—
22f. Operations support	—	—
22g. System administrator	—	—

(continued)

Table F-116. Structural Roles (continued)

In this Role is the User Expected to be Able to Access Data?	Yes	No
22h. Applications support	—	—
22i. Business analyst	—	—
22j. Programmers	—	—
22k. Third-party support (vendors and consultants)	—	—
23. Financial services, billing, and claims	—	—
23a. Billing file clerk	—	—
23b. Billing personnel	—	—
23c. Administrative support personnel	—	—
23d. Collections personnel	—	—
23e. Cost and quality analysts	—	—
24. Quality assurance	—	—
25. Utilization review	—	—
26. Discharge planning	—	—
27. Infection control	—	—
28. Administrative support staff	—	—
29. Risk management	—	—
30. Health plan/insurer	—	—
30a. Claims file clerk	—	—
30b. Claims review personnel	—	—
30c. Claims adjudication personnel	—	—
30d. Internal quality assurance personnel	—	—
30e. Health care provision quality assurance personnel	—	—
30f. Internal utilization review personnel	—	—
30g. Health care provision utilization review personnel	—	—
30h. Administrative support personnel	—	—
31. Medical malpractice	—	—
31a. Health records file clerk	—	—
31b. Health records supervisor	—	—
31c. Lawyer/judge	—	—
31d. Legal aide	—	—
31e. Legal secretary	—	—
31f. Expert witness	—	—

(continued)

Table F-116. Structural Roles (continued)

In this Role is the User Expected to be Able to Access Data?	Yes	No
31g. Governmental file clerk	—	—
32. Accrediting and regulatory agencies	—	—
32a. JCAHO auditors	—	—
32b. NCQA auditors	—	—
32c. Local, state, and federal agencies	—	—
32d. Local, state, and federal surveyors	—	—
33. Administrative management	—	—
33a. Executive officers	—	—
33b. Board of trustees	—	—
33c. Medical staff administration	—	—
34. Pharmacist (DP)	—	—

Em dash (—) is a placeholder for data.

Table F-117. Health Care Functional Roles: In this Role is the User Expected to be Able to Access Data?

Role Name	Description	Yes	No
Subject of care	Principal data subject of the electronic health record	—	—
Subject of care agent	E.g., parent, guardian, care provider, or other legal representative	—	—
Personal health care professional	Health care professional or professionals with the closest relationship to the patient, often the patient's GP	—	—
Privileged health care professional	Nominated by the subject of care	—	—
Privileged health care professional	Nominated by the health care facility of care (if there is a nomination by regulation, practice, etc., such as an emergency override)	—	—
Health care professional	Party involved in providing direct care to the patient	—	—
Health-related professional	Party indirectly involved in patient care, teaching, research, etc.)	—	—
Administrator	Any other parties supporting service provision to the patient	—	—

Em dash (—) is a placeholder for data.

Table F-118. Organization Roles: In this Role is the User Expected to be Able to Access Data?

Roles (if more than one is listed, please specify those permitted)	Yes	No
Ambulance/aid-car	—	—
Ambulatory health care (ambulatory surgery facility, birthing center, clinic/health center (comp outpatient rehab, dental, free-standing, HMO, outpatient mental health, pain, rural, urgent care center (walk-in, free-standing), vision, private office (group, solo)	—	—
Hospital (acute care, acute care w psych services, burn center, cancer, children's, emergency room, government, outpatient dept, psychiatric, rehab, trauma center level 1, hospice)	—	—
Imaging services facility, free-standing	—	—
Independent laboratory	—	—
Mental health (multiservice organization, partial care organization, residential treatment center: emotionally disturbed children)	—	—
Nursing/custodial care facility (intermediate care facility, intermediate medicine, pulmonary-mentally retarded, skilled nursing facility/nursing home, hospice, industry health/occupational health center, end-stage renal disease treatment facility)	—	—
Residential (home health, retirement center, sheltered employment workshop)	—	—
School (day care center, residential, clinic/infirmary, special education program)	—	—
Substance abuse treatment facility, resident	—	—
Unlisted facility	—	—

Em dash (—) is a placeholder for data.

Table F-119. Organization Roles: In this Role is the User Expected to be Able to Access Data?

Roles (if more than one is listed, please specify those permitted)	Yes	No
Ambulance/aid-car	—	—
Ambulatory health care (ambulatory surgery facility, birthing center, clinic/health center (comp outpatient rehab, dental, free-standing, HMO, outpatient mental health, pain, rural, urgent care center (walk-in, free-standing), vision, private office (group, solo)	—	—
Hospital (acute care, acute care w psych services, burn center, cancer, children's, emergency room, government, outpatient dept, psychiatric, rehab, trauma center level 1, hospice)	—	—
Imaging services facility, free-standing	—	—
Independent laboratory	—	—
Mental health (multiservice organization, partial care organization, residential treatment center: emotionally disturbed children)	—	—
Nursing/custodial care facility (intermediate care facility, intermediate medicine, pulmonary-mentally retarded, skilled nursing facility/nursing home, hospice, industry health/occupational health center, end-stage renal disease treatment facility)	—	—
Residential (home health, retirement center, sheltered employment workshop)	—	—
School (day care center, residential, clinic/infirmary, special education program)	—	—
Substance abuse treatment facility, resident	—	—
Unlisted facility	—	—

Em dash (—) is a placeholder for data.

Table F-120. Crosswalk: Medication Management Authentication and Audit Requirements to HITSP Standards

Related Documents	Document Description	Medication Management Authentication Requirement	Medication Management Audit Requirement
HITSP/C19—Entity Identity Assertion Component	The entity identity assertion component provides the mechanisms to ensure that an entity is the person or application that claims the identity provided. An example of this component is the validation and assertion of a consumer logging on to a personal health record (PHR) system.	AUT-1 user authentication AUT-3 system authentication AUT-5 organization authentication AUT-8 patient authentication AUT-9 PHR authentication	AUD-1 information request AUD-2 information disclosure
HITSP/C32	HITSP summary documents using HL7 continuity of care document (CCD) component	AUT-1 user authentication AUT-3 system authentication AUT-5 organization authentication AUT-8 patient authentication AUT-9 PHR authentication For context-based criteria—metadata	—
HITSP/T15—Collect and Communicate Security Audit Trail Transaction	The collect and communicate security audit trail transaction is a means to provide assurance that security policies are being followed or enforced and that risks are being mitigated. This document describes the mechanisms to define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation, or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed.	—	AUD-1 information request AUD-2 information disclosure
HITSP/T16—Consistent Time Transaction	The consistent time transaction provides a mechanism to ensure that all of the entities that are communicating within the network have synchronized system clocks.	—	AUD-1 information request AUD-2 information disclosure

(continued)

Table F-120. Crosswalk: Medication Management Authentication and Audit Requirements to HITSP Standards (continued)

Related Documents	Document Description	Medication Management Authentication Requirement	Medication Management Audit Requirement
HITSP/T17—Secured Communication Channel Transaction	The secured communication channel transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of transactions and the mutual trust between communicating parties. It supports both application and machine credentials, and user machines (user nodes).	AUT-3 system authentication AUT-5 organization authentication AUT-9 PHR authentication	—
HITSP/T23—Patient Demographics Query Transaction	This PDQ transaction is intended to provide a "list patients and their demographics" query/'patient(s) and their demographics identified' response message pair (QBP^ Q22, RSP^ K22) for use wherever such needs exist. This transaction document extracts the Health Level Seven (HL7) Version 2.5 Query and Response data mapping. The underlying basis for this extraction can be found in the Integrating the Healthcare Enterprise IT Infrastructure Technical Framework, Volume 2 (ITI TF-2), Revision 4.0: "Patient Demographics Query."	AUT-2 subject of care identity	—
HITSP/T29—Notification of Document Availability Transaction	The NAV integration profile introduces a mechanism allowing notifications to be sent point-to-point to systems within a cross-enterprise document sharing affinity domain (see "IHE IT Infrastructure Cross-Enterprise Document Sharing [XDS] Integration Profile"), eliminating the need for manual steps or polling mechanisms for a document consumer to be aware that documents of interest have been registered with an XDS document registry actor.	AUT-6 authenticate recipient identity (organization, user, system)	—

(continued)

Table F-120. Crosswalk: Medication Management Authentication and Audit Requirements to HITSP Standards (continued)

Related Documents	Document Description	Medication Management Authentication Requirement	Medication Management Audit Requirement
HITSP/TP13—Manage Sharing of Documents Transaction Package	This transaction package supports the sharing of patient records in the form of source attested objects called documents. A health care document is a composite of structured and coded health information, both narrative and tabular, that describes acts, observations, and services for the purpose of exchange. No assumption is made by this construct in terms of the format and structure of the content of documents shared. This interoperability specification specifically references the IHE XDS.b option to support entity identity assertion (SAML support).	AUT-1 user authentication AUT-3 system authentication AUT-5 organization authentication AUT-8 patient authentication AUT-9 PHR authentication Enabled by XDS.b option	—
HITSP/TP20—Access Control Transaction Package	The access control transaction package provides the mechanism to administer security authorizations that control the enforcement of security policies, including role-based access control, entity-based access control, context-based access control, and the execution of consent directives. In an emergency, this construct supports the capability to alter access privileges to the appropriate level (failsafe/ emergency access), which may include override of nonemergency consents.	AUT-1 user authentication AUT-3 system authentication AUT-5 organization authentication AUT-8 patient authentication AUT-9 PHR authentication	—
HITSP/TP22—Patient ID Cross-Referencing Transaction Package	This specification includes by reference the transactions and components that comprise the patient ID cross-referencing transaction package. Source material is from the IHE IT Infrastructure (ITI) Technical Framework (TF), Volume 2 (ITI TF-2). The two transactions within this package are (1) the IHE patient ID cross-referencing (PIX) transaction is described in IHE-ITI TF-2 §3.9.1, and (2) the IHE patient identity feed transaction is described in IHE-ITI TF-2 §3.8.1.	AUT-2 subject of care identity	—

(continued)

Table F-120. Crosswalk: Medication Management Authentication and Audit Requirements to HITSP Standards (continued)

Related Documents	Document Description	Medication Management Authentication Requirement	Medication Management Audit Requirement
HITSP/TP30—Manage Consent Directives Transaction Package	The manage consent directives transaction package describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use, or disclose individually identifiable health information (IIHI) and also supports the delegation of the patient's right to consent. The transactions described in this construct are intended to be carried out by HITSP/TP13—Manage Sharing of Documents.	AUT-1 user authentication	AUD-1 information request