XDS Implementations Group on Security and Privacy

Affinity Domain Interoperability Policy

Working Draft
V1.0

State of Connecticut – Health Information Technology Exchange

September 8, 2011

For further details, contact:
lfourquet@ehealthsign.com

Affinity Domain Interoperability Policy Agreement

Revision History Table

Version Number	Description of Change	Name of Author	Date
V0.1	Initial Draft for discussion.	Lori L. Reed-Fourquet	March 16, 2011
V0.2	Draft for committee review	Lori L. Reed-Fourquet	September 1, 2011
V0.3	Draft for comment	Lori L. Reed-Fourquet	September 6, 2011
V1.0	Approved by HITE-CT Board for initial deployment	Lori L. Reed-Fourquet	November 21, 2011

Table of Contents

1 Introduction 7
2 Glossary 8
2.1 HITE-CT Glossary 8
2.1.1 HITE-CT Policy Terms 8
2.2 Abbreviations 23
3 Reference Documents 24
3.1 HITE-CT Reference Documents 24
3.2 Developer Resources Reference Documents 24
4 Organizational Rules 25
4.1 Organizational Structure 26
4.2 Organizational Roles 27
4.3 Funding 28
4.3.1 Fee Structure 28
4.3.2 Re-Imbursement Policies 29
4.3.3 Insurance Policies 29
4.3.4 Fiscal plan for System Operation, Maintenance, and Innovation 29
4.4 Enforcement and Remedies 29
4.5 Transparency 29
4.6 Legal Considerations 29
4.6.1 Legal Governance 29
4.6.2 Government Regulations 29
4.6.3 Liability and Risk Allocation 29
4.6.4 Indemnification 30
4.6.5 Intellectual Property Rights to Published Documents 30
5 Operational Rules 30
5.1 Service Level Agreements 30
5.2 Daily Governance 30
5.2.1 Policy Governance 30
5.2.2 Policy Change Procedures 30
5.2.3 Publication and Notification Policies 30
5.3 Management When Systems are Unavailable 31
5.4 Configuration Management 31
5.5 Addition of New Components 31
5.6 Data Retention, Archive, and Backup 32
5.7 Disaster Recovery 32
6 Membership Rules 33
6.1 Acceptance 33
6.2 Types of Membership 33
6.3 Membership Policies 34
6.3.1 Participation Agreements 34
6.3.2 Membership Lists 34

7 Connectivity to the XDS Affinity Domain from External Systems 34
7.1 Interoperability Strategy 34
7.1.1 External Connectivity Through Portals 35
8 System Architecture 35
8.1.1 Global Architecture 35
8.1.2 Affinity Domain Actors 36
8.1.2.1 Business Actors 36
8.1.3 Technical Actor Specifications 38
8.1.4 XDS Document Registry 38
8.1.5 XDS Document Repository 39
8.1.6 XDS Document Source 40
8.1.7 XDS-I Imaging Document Source 42
8.1.8 XDS Document Consumer 43
8.1.9 XDS-I Imaging Document Consumer 46
8.1.10 XDS Patient Identity Source 47
8.1.11 PIX Manager 48
8.1.12 PIX Consumer 49
8.1.13 PDQ Patient Demographics Supplier 49
8.1.14 PDQ Patient Demographics Consumer 50
8.1.15 ATNA Audit Record Repository 51
8.1.16 ATNA Secure Node 51
8.1.17 Secure Application 51
8.1.18 CT Time Server 52
8.1.19 CT Time Client 52
8.1.20 Any Additional IHE Actor Systems 52
8.1.21 Additional Affinity Domain Specific Recognized Technical Actors 52
8.1.22 XDS Affinity Domain Transaction Diagram 53
8.1.23 Cross XDS Affinity Domain Transaction Support 54
9 Terminology and Content 56
9.1 Introduction 56
9.1.1 Common Rules for Identifier Construction 56
9.1.1.1 Uniqueness 56
9.1.1.2 Namespace 56
9.1.1.2.1 Namespace - Connecticut Local Policy Extensions 57
9.1.1.3 Health care Organization Identifiers (Document Source Organization) 57
9.1.1.3.1 Connecticut Local Policy Extensions 58
9.1.1.4 Person Identifiers (Document Author, Authenticator, Provider, Patient) 61
9.1.1.4.1 Sponsored Health Care Provider Identities 73
9.1.1.4.1.1 Sponsored Health Care Provider Identities - Connecticut Local Policy Extensions 73
9.1.1.4.2 System Identifiers 74
9.1.1.4.2.1 System Identifiers- Connecticut Local Policy Extensions 74
9.1.1.4.3 Device Identities 74
9.1.1.4.4 License Restriction Classes 74
9.1.1.4.4.1 License Restriction Classes- Connecticut Local Policy Extensions 74

9.1.1.5 Validity 75
9.2 Data Content Rules and Restrictions 75
9.2.1 Example of Rules and Restrictions for Patient Demographic Data 75
9.3 XDS Registry Metadata 77
9.3.1 XDS Document Entry Metadata 77
9.3.1.1 Refinement of authorInstitution 82
9.3.1.1.1 Refinement of Organization Name component 83
9.3.1.1.2 Specification of Organization Type Code Component of authorInstitution 83
The authorInstitution organization type code shall be populated with the standard role code found in Table 9.1.1.3.1-1 “ Connecticut Regulated Healthcare Organization Types”. 83
9.3.1.1.3 Specification of ID Number Component of authorInstitution 83
9.3.1.1.4 Specification of Identifier Check Digit Component of authorInstitution ... 83
9.3.1.1.5 Specification of ID of Assigning Authority of authorInstitution 83
9.3.1.1.6 Specification of Identifier Type Code of authorInstitution 83
9.3.1.1.7 Specification of Assigning Facility of authorInstitution 84
9.3.1.1.8 Specification of Name Representation Code of authorInstitution 84
9.3.1.1.9 Specification of Organization Identifier of authorInstitution 84
9.3.1.2 authorPerson 84
9.3.1.3 authorRole 84
9.3.1.4 authorSpecialty 85
9.3.1.5 classCode and classCodeDisplayName 88
9.3.1.6 confidentialityCode 90
9.3.1.6.1 Derivation Rules for confidentialityCode 92
9.3.1.7 healthcareFacilityTypeCode and healthcareFacilityTypeCodeDisplayName .. 94
9.3.1.8 legalAuthenticator 96
practiceSettingCode and practiceSettingCodeDisplayName 96
9.3.2 XDS Submission Set Metadata 98
9.3.3 Folder Metadata 98
9.3.4 Supported Content 98
9.3.4.1 Document Content Specialization and Extensions 99
9.3.4.2 Connecticut Public Health Reporting 99
10 Patient Privacy and Consent 99
10.1 General Guidelines Regarding Document Access and Use 99
10.2 Patient consent 100
10.2.1 BPPC 100
10.2.2 Common Consent Agreements 100
10.2.3 Policy OIDs Supported for Patient Authorization 101
10.3 Privacy Override Guidelines 103
11 Technical Security 103
11.1 Authorization 103
11.1.1 Role Management 103
11.1.1.1 Functional and Structural Roles 103
11.1.1.2 Mapping of Structural Roles to Functional Roles 104
11.1.1.2.1 Subject of Care 104

11.1.1.2.2 Subject of Care Agent 104
11.1.1.2.3 Privileged health care professional 105
11.1.1.2.4 Healthcare Professional 105
11.1.1.2.5 Health-Related Professionals 106
11.1.1.2.6 Administrators 109
11.1.2 Authentication of Users/Role 115
11.1.2.1 User/Role Certificates Management 116
11.1.3 Attestation rights 116
11.1.4 Delegation rights 116
11.1.5 Validity time 117
11.2 Node Authentication 117
11.2.1 Node Certificates Management 117
11.3 Information Access 117
11.3.1 Security Audit Log Access 117
11.3.2 Network Communication Access Security Requirements 118
11.3.2.1 Node Access Security Requirements 118
11.3.2.2 Removable Media Access Security Requirements 118
11.4 Agreement validity period 118
11.5 Information Integrity 118
11.5.1 Network Communication Integrity Requirements 118
11.5.2 Document Digital Signature Requirements/Policy 118
11.5.3 Document Update and Maintenance Policies 119
11.5.4 Folder Update and Maintenance Policies 119
11.6 Ethics 119
11.7 Secure Audit Trail 119
11.8 Consistent Time 120
11.9 Audit Check 120
11.10 Risk Analysis 120
11.11 General Mitigations 120
11.11.1 Common Criteria (ISO/IEC 15408) 121
11.11.2 Identified Risks 121
11.12 Future system developments 153
Appendix X: HITE-CT Specification of Value Sets used to support the HITE-CT Affinity Domain Policy 153
A.1 HITE-CT Mental Health Role codes 153
A.1.1 Metadata 153
A.1.2 HITE-CT Mental Health Role Value Set Table 154
A.2 HITE-CT Substance Abuse Role codes 154
A.2.1 Metadata 154
A.2.2 HITE-CT Substance Abuse Role Value Set Table 155
A.3 HITE-CT Mental Health Role codes 155
A.3.1 Metadata 155
A.3.2 HITE-CT Mental Health Specialty Value Set Table 156
A.4 HITE-CT Substance Abuse Specialty codes 157
A.4.1 Metadata 157

A.4.2 HITE-CT Substance Abuse Specialty Value Set Table 157
A.5 HITE-CT Mental Health Facility Type codes 158
A.5.1 Metadata 158
A.5.2 HITE-CT Mental Health Facility Type Value Set Table 158
A.6 HITE-CT Substance Abuse Facility Type codes 159
A.6.1 Metadata 159
A.6.2 HITE-CT Substance Abuse Facility Type Value Set Table 159
B.1 HITE-CT Mental Health Practice Setting codes 160
B.1.1 Metadata 160
B.1.2 HITE-CT Mental Health Practice Setting Value Set Table 160
B.2 HITE-CT Substance Abuse Practice Setting codes 161
B.2.1 Metadata 161
B.2.2 HITE-CT Substance Abuse Practice Setting Value Set Table 162
1.1 HIV Findings (SNOMED-CT) 162
1.1.1 Metadata 162
1.1.2 HIV Findings Value Set 163

1 Introduction

HITE-CT is established pursuant to subsection (a) of section 19a-750 of the Connecticut General Statutes to carry out the purposes of the authority, as described in subsection (b) of this section. The purposes of the authority include, but are not limited to, "promoting, planning and designing, developing, assisting, acquiring, constructing, maintaining and equipping, reconstructing and improving of health care information technology." The HIE will connect physicians and other healthcare professionals in Connecticut. While initial HITE-CT efforts will be focused on supporting Meaningful Use Stage 1, the longer-term goals of the HIE initiative are to support a broad spectrum of clinical and population health services.

Through the Connecticut Department of Public Health, HITE-CT is participating in the Office of the National Coordinator for Health Information Technology (ONC) State Health Information (State HIE) Exchange Cooperative Agreement Program, and in conjunction therewith is looking to establish a hosted information exchange service to support HITE-CT area providers, for Meaningful Use Stage 1 exchanges within the state with initial goals including:

- Receipt of structured lab results
- Sharing patient care summaries (CCD/C32 as constrained for Meaningful Use) across unaffiliated organizations
- Support the exchange of immunization data between the State Immunization Registry and Meaningful Use Certified EMRs

These goals may evolve to include support for additional Meaningful Use stage I goals, and additional Meaningful Use and stakeholder requirements, including, but not limited to:

- providing patients with an electronic copy of their health information
- Reporting clinical quality measures to CMS or states
- Supporting Medication reconciliation between care settings
- Submitting of electronic syndromic surveillance data to public health agencies
- recording advanced directives for patients 65 years or older
- submitting of electronic data on reportable laboratory results to public health agencies
- Sending reminders to patients (per patient preference) for preventative and follow-up care
- Providing patients with timely electronic access to their health information (including laboratory results, problem list, medication list, medication allergies)
- Providing visit summaries

This document describes the statewide standard interoperability requirements and specifications including standard content, identification schemes, vocabularies, actors, and transactions to be supported by the Connecticut Health Information Exchange (HITE-CT). These Cross-Enterprise Document Sharing (XDS) profile extensions are

being defined statewide in Connecticut and are meant to be followed by all XDS affinity domains within the state.

(NOTE: The concept of an XDS affinity domain is defined in IHE ITI Technical Framework Volume-1 Section 10 and Appendix K.).

1.1 Copyright Statements

2 Glossary

2.1 HITE-CT Glossary

2.1.1 HITE-CT Policy Terms

The HITE-CT policy Terms are recaptured in the table below.

Table 2.1.2-1

Term	Definition	Reference
Access Control	A means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways	[ISO/IEC 2382-8]
Accountability	Property ensures that the actions of an entity may be traced to that entity.	[ISO 7498-2:1989]
Affinity Domain	A group of healthcare enterprises that have agreed to work together using a common set of policies and infrastructure	IHE IT Infrastructure Technical Framework-1:10
Applicant	A party undergoing the processes of	NIST 800-63-1 Draft

Term	Definition	Reference
	registration and identity proofing.	Electronic Authentication Guideline 2/20/08
Assertion	A statement from a Verifier to a Relying Party that contains identity information about a Subscriber. Assertions may also contain verified attributes.	NIST 800-63-1
Assurance	In the context of NIST SP 800-63, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.	NIST 800-63-1
Asymmetric keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.	NIST 800-63-1
Audit	systematic and independent examination of accesses, additions, or alterations to electronic health records to determine whether the activities were conducted, and the data were collected, used, retained or disclosed according to organizational standard operating procedures, policies, good clinical practice, and applicable regulatory requirement(s).	ISO DIS 27789 Health informatics — Audit trails for electronic health records
Audit Logs	chronological sequence of audit records, each of which contains data about a specific event	ISO DIS 27789 Health informatics — Audit trails for electronic health records
Audit Record	record of a single specific event in the life cycle of an electronic health record	ISO DIS 27789 Health informatics — Audit trails for electronic health records
Audit Trail	collection of audit records from one or more audit logs relating to a specific subject of care or a specific electronic health record	ISO DIS 27789 Health informatics — Audit trails for electronic health

Term	Definition	Reference
		records
Audit Trail and Node Authentication (ATNA)	Establishes the characteristics of a Basic Secure Node: 1. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. 2. It defines basic auditing requirements for the node 3. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. 4. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. The Radiology Audit Trail option in the IHE Radiology Technical Framework is an example of such an extension.	[Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 16)]
Authentication	The process of reliable security identification of subjects by incorporating an identifier and its authenticator. NOTE: See also data origin authentication and peer entity authentication.	[ISO 7498-2:1989]
Authorization	The granting of rights, which includes the granting of access based on access rights.	[ISO 7498-2:1989]
Availability	The property of being accessible and useable upon demand by an authorized entity.	[ISO 7498-2:1989]
Breach	A Reportable Event involving the unauthorized acquisition of, access to, use or disclosure of information managed by HITE-CT that compromises the security or privacy of the PHI. Such term does not include a Reportable	HITE-CT Breach Notification Policy

Term	Definition	Reference
	Event where an unauthorized person to whom such information is disclosed would not have reasonably been able to retain such information. An example of a Reportable Event is a clinician sharing his user name and password with another clinician in the practice who had forgotten his own user id or password.	
Certificate Revocation List	A list of revoked public key certificates created and digitally signed by a Certification Authority.	NIST 800-63-1
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates.	NIST 800-63-1
Challenge-response protocol	An authentication protocol where the Verifier sends the Claimant a challenge (usually a random value or a nonce) that the Claimant combines with a secret (such as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the Verifier. The Verifier can independently verify the response generated by the Claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the Claimant possesses and controls the secret.	NIST 800-63-1
Claimant	A party whose identity is to be verified using an authentication protocol.	NIST 800-63-1
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	ISO 7498-2:1989 45 CFR § 164.304 Definitions
Connecticut Health Information Exchange ("HITE-CT")	The health information exchange network operated by HITE-CT.	HITE-CT
Consent [data subject's]	Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.	ISO IS 22857
Consistent Time	Mechanisms to synchronize the time base between multiple actors and computers.	Vol. 1 (ITI TF-1): Integration Profiles,

Term	Definition	Reference
	Various infrastructure, security, and acquisition profiles require use of a consistent time base on multiple computers. The Consistent Time Profile provides a median synchronization error of less than 1 second.	Rev. 4.0 Final Text 2007-08-22 (p. 16)
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.	NIST 800-63-1
Credential Service Provider (CSP)	A trusted entity that issues or registers Subscriber tokens and issues electronic credentials to Subscribers. The CSP may encompass Registration Authorities and Verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.	NIST 800-63-1
Cryptographic Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, key requirements shall coincide with the minimum requirements stated in table 2 of NIST SP [800-57] part 1. See also Asymmetric keys, Symmetric key.	NIST 800-63-1
Cryptographic Token	A token where the secret is a cryptographic key.	NIST 800-63-1
Data Integrity	Property that data has not been altered or destroyed in an unauthorized manner.	[ISO 7498-2:1989]
Data Origin Authentication	Corroboration that the source of data received is as claimed.	[ISO 7498-2:1989]
De-identification	De-identification is the general term for any process of removing the association between a set of identifying data and the data subject.	[ISO TS25237]
Digital Signature	Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient.	[ISO 7498-2:1989]

Term	Definition	Reference
Electronic Authentication	The process of establishing confidence in user identities electronically presented to an information system.	NIST 800-63-1
Electronic Credentials	Digital documents used in authentication that bind an identity or an attribute to a Subscriber's token. Note that this document distinguishes between credentials, and tokens (see below) while other documents may interchange these terms.	NIST 800-63-1
Electronic Medical Record	An electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization.	National Alliance For Health Information Technology
Functional Roles	Functional roles reflect the essential business functions that need to be performed. Functional roles are defined by a set of standard healthcare tasks (e.g., Neurologist).	Neuman/Strembeck
Healthcare Consumer (Individual)	Person that is the receiver of health related services and that is a person in a health information system. Any person who uses or is a potential user of a health care service, subjects of care may also be referred to as patients, health care consumers or subject of cares. [ISO TS22220]. In the US, this may be referenced as an 'individual', which means the person who is the subject of protected health information.	ISO TS22220 HITE-CT
Health Information Exchange	The electronic movement of health-related information among organizations according to nationally recognized standards.	National Alliance For Health Information Technology
Health Information Organization	An organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards.	National Alliance For Health Information Technology
Health Care Operations	Activities of a Participating Health Care Provider providing treatment to an individual relating to quality assessment and improvement, evaluations relating to the competence of treating providers or	HITE-CT Policy on Patient Consent

Term	Definition	Reference
	necessary administrative and management activities all as defined in the HIPAA Privacy Regulations, 45 CFR $164.91.	
Healthcare Organization	Officially registered organization that has a main activity related to health care services or health promotion. EXAMPLES: Hospitals, Internet health care web site providers and health care research institutions. NOTE 1: The organization is recognized to be legally liable for its activities, but need not be registered for its specific role in health. NOTE 2: An internal part of an organization is called an organizational unit, as in X.91.	[ISO IS17090]
Individually Identifiable Health Information	Information that is a subset of health information including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearing house; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.	45 CFR 160.103.
Identification	Performance of tests to enable a data processing system to recognize entities.	[ISO/IEC 2382-8:1998]
Identifier	Piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator.	[ENV 13608-1]
Identity	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account	NIST 800-63-1

Term	Definition	Reference
	number) to make the complete name unique.	
Identity Proofing	The process by which a CSP and an RA validate sufficient information to uniquely identify a person.	NIST 800-63-1
IHE	Integrating the Healthcare Enterprise is an initiative by healthcare professionals and industry to improve the way the computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical need in support of optimal patient care.	Integrating the Healthcare Enterprise
Integrity	Proof that the message content has not been altered, deliberately or accidentally, in any way during transmission.	Adapted from ISO 7498-2:1989
Intentional violation	A deliberate violation of policies, procedures or law, conducted with planning or forethought.	HITE-CT Breach Notification Policy
May	Permits the action to happen, but does not require it.	HITE-CT
Member (Participating Health Care Subscriber)	Any healthcare institution or healthcare professional that has executed an effective Data Use and Reciprocal Support Agreement (DURSA) with HITE-CT. See Member List (www.hitect.org/members).	HITE-CT
Network	An open communications medium, typically the Internet, that is used to transport messages between the Claimant and other parties. Unless otherwise stated no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attack at any point between the parties (Claimant, Verifier, CSP or Relying Party).	NIST 800-63-1
NHIN	The Nationwide Health Information Network is being developed to provide a secure, nationwide interoperable health information infrastructure that will connect providers, consumers and others involved in supporting	The U.S. Department of Health and Human Services

Term	Definition	Reference
	health and healthcare.	
NIST	The National Institute of Standards and Technology is a non-regulatory agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.	The National Institute of Standards and Technology
Non-Regulated Health Professional	Person employed by a health care organization who is not a regulated health professional. EXAMPLES: Medical receptionist who organizes appointments or a nurse's aide who assists with patient care. NOTE: The fact that a body independent of the employer does not authorize the employee's professional capacity does not, of course, imply that the employee is not professional in conducting her/his services.	[ISO IS17090]
Non-Repudiation	Service providing proof of the integrity and origin of data (both in an un-forgeable relationship), which can be verified by any party.	Adapted from ASTM [31].
Object Identifier [OID]	A number assigned to devices in a network for identification purposes. OID numbering is hierarchical. Using a notation of digits and dots, OID resemble very long IP addresses, various registries such as ANSI assign high-level numbers to vendors and organizations. They, in turn, append digits to the number to identify individual devices or software processes.	PC Encyclopedia
ONC	Office of the National Coordinator for Health Information Technology; serves as the Secretary's principal advisor on the development, application, and use of health information technology in an effort to improve the quality, safety, and efficiency of the nation's health through the development of an interoperable harmonized health information infrastructure.	Department of Health and Human Services

Term	Definition	Reference
Organization Employee	Person employed by a health care organization or a supporting organization. EXAMPLES: Medical records transcriptionists, health care insurance claims adjudicator, and pharmaceutical order entry clerks.	ISO TS21091
Organizational Roles	This is the organization-defined job function of an individual employee or contractor.	Neumann/Strembeck
Participating Health Care Subscriber (PHCS)	Any healthcare institution or healthcare professional that has executed an effective Data Use and Reciprocal Support Agreement (DURSA) with HITE-CT. See Member List (www.hitect.org/members).	HITE-CT
Participant User	Individual personnel of each Participating Health Care Subscriber who is authorized, pursuant to the policies of, and agreements with, HITE to access and use the HIE through such Participating Health Care Subscriber's subscription to the HIE	HITE-CT
Password	A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.	NIST 800-63-1
Patient Identifier Cross-referencing (PIX)	Provides cross-referencing of patient identifiers from multiple Patient Identifier Domains. These patient identifiers can then be used by identity consumer systems to correlate information about a single patient from sources that know the patient by different identifiers.	Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 15)
Patient/Consumer	Person who is the receiver of health related services and who is an actor in a health information system.	[ISO IS17090]
Persistence	In computer science, persistence refers to the characteristic of data that outlives the execution of the program that created it. Without this capability, data only exists in RAM.	Programming persistence in chi Authors: Sajeev, A.S.M.; Hurst, A.J. Description: Computer Start Page: 57 End Page: 66 ISSN: 0018-9162

Term	Definition	Reference
		ISBN: Volume: 25 Issue: 9
Personal Health Record	An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.	National Alliance For Health Information Technology
Personal Identification Number (PIN)	A password consisting only of decimal digits.	NIST 800-63-1
Possession and Control of a Token	The ability to activate and use the token in an authentication protocol.	NIST 800-63-1
Privacy	Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.	[ISO/IEC 2382-8:1998]
Private Key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.	NIST 800-63-1
Proof of Possession (PoP) protocol	A protocol where a Claimant proves to a Verifier that he/she possesses and controls a token (e.g., a key or password)	NIST 800-63-1
Protected Health information" ("PHI")	Individually identifiable personal information in any form or medium about the past, present or future physical or mental health or condition of an individual, or the past, present or future payment for the provision of healthcare to an individual, [pursuant to federal and state law]. 45 CFR 160.103 .	HITE-CT Policies
Pseudonymization	Pseudonymization is a process by which identifying information of a data subject is removed while retaining a link between multiple records pertaining to the data subject.	[ISO TS25237]
Public Key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.	NIST 800-63-1
Public Key Certificate	A digital document issued and digitally	NIST 800-63-1

Term	Definition	Reference
	signed by the private key of a Certification Authority that binds the name of a Subscriber to a public key. The certificate indicates that the Subscriber identified in the certificate has sole control and access to the private key	
Regional Health Information Organization	A health information organization that brings together health care stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and care in that community.	National Alliance For Health Information Technology
Registration	The process through which a party applies to become a Subscriber of a CSP and an RA validates the identity of that party on behalf of the CSP.	NIST 800-63-1
Registration Authority (RA)	A trusted entity that establishes and vouches for the identity of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).	NIST 800-63-1
Registry Stored Query	An ad-hoc query invoked by a transaction issued on behalf of a care provider to a Document Registry. A search of the registry locates documents that meet the provider's specified query criteria and returns registry metadata containing a list of document entries found to meet the specified criteria including the locations and identifier of each corresponding document in one or more Document Repositories.	IHE ITI-18
Regulated Health Professional	Person who is authorized by a nationally recognized body and qualified to perform certain health services. EXAMPLES: Physicians, registered nurses, and pharmacists. NOTE 1: The types of registering or accrediting bodies differ in different countries and for different professions. Nationally recognized bodies include local or regional governmental agencies, independent	[ISO IS17090]

Term	Definition	Reference
	professional associations, and other formally and nationally recognized organizations. They MAY be exclusive or non-exclusive in their territory. NOTE 2: A nationally recognized body in this definition does not imply one nationally controlled system of professional registration but, in order to facilitate international communication, it would be preferable for one nationwide directory of recognized health professional registration bodies to exist.	
Reportable Event	An action (or lack of action) that violates HITE-CT policies and procedures for accessing or using protected health information managed by the HITE-CT systems. Such violations may be unintentional or intentional.	HITE-CT
Role	Set of competences and/or performances that are associated with a task	[ISO TS21298]
Secure Node	The secure node is responsible for providing reasonable access controls. This typically includes user authentication and authorization. The secure node is also responsible for providing security audit logging to track security events. The difference between the Secure Node and the Secure Application is the extent to which the underlying operating system and other environment are secured. A Secure Node includes all aspects of user authentication, file system protections, and operating environment security. The Secure Application is a product that does not include the operating environment.	IHE Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 64)
Security	Combination of availability, confidentiality, integrity, and accountability.	[ENV 13608-1]
Security Policy [primary – internal]	Plan or course of action adopted for providing computer security.	[ISO/IEC 2382-8:1998]
Security Policy [secondary - external]	Service, provided by a layer of communicating open systems, which ensures adequate security of the systems or	[ISO 7498-2:1989]

Term	Definition	Reference
	of data transfers	
Sensitivity	Measure of importance assigned to information to denote its need for protection	ISO 13606-4
Shall	The action must be taken	HITE-CT
Should	It is a recommendation that an action ought to be done, but it is not required.	HITE-CT
Shared Secret	A secret used in authentication that is known to the Claimant and the Verifier.	NIST 800-63-1
Signer	Entity generating a digital signature.	ISO/IEC 1st CD 13888-1: 2007-11-12
Sponsored Health Care Provider	Health services provider who is not a regulated professional in the jurisdiction of his/her practice, but who is active in his/her health care community and sponsored by a regulated health care organization EXAMPLES: A drug and alcohol education officer who is working with a particular ethnic group, or a health care aid worker in a developing country.	[ISO IS17090]
Subscriber	A party who receives a credential or token from a CSP.	NIST 800-63-1
Structural Role	A structural role is a type of healthcare personnel warranting differing levels of access control. Also known as “basic role,” “organizational role,” or “role group.” For a listing of healthcare structural roles see ASTM E 1986-98 (e.g., Attending Physician)	ASTM E 1986-98
Symmetric Key	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.	NIST 800-63-1
Supporting Organization	Officially registered organization which is providing services to a health care organization, but which is not providing health care services. EXAMPLES: Health care financing bodies such as insurance institutions, suppliers of pharmaceuticals and other goods.	[ISO IS17090]

Term	Definition	Reference
Target	A resource being accessed by a claimant.	[ISO TS26000]
Technical safeguards	The technology and the policy and procedures for its use that protect electronic PHI and control access to it.	HITE-CT Information Security Policy
Token	Something that the Claimant possesses and controls (typically a key or password) used to authenticate the Claimant's identity.	NIST 800-63-1
Token Authenticator	The value that is provided to the protocol stack to prove that the Claimant possesses and controls the token. Protocol messages sent to the Verifier are dependent upon the token authenticator, but they may or may not explicitly contain it.	NIST 800-63-1
Trading Partners	Entities that exchange (submit or receive) data electronically with each other. Examples include any pairing of physicians, providers, billing services, clearinghouses, health plans or third-party administrators.	45 CFR 160.103 Trading Partner Agreements
Treatment	The provision, coordination, or management of health care and related services by one or more health care providers.	HITE-CT
Unintentional Violation	A violation of policies, procedures or law without planning or forethought. The violation MAY have been accidental in nature or due to a lack of training or understanding of requirements.	HITE-CT
Verified Name	A Subscriber name that has been verified by identity proofing.	NIST 800-63-1
Verifier	An entity that verifies the Claimant's identity by verifying the Claimant's possession of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status.	NIST 800-63-1
(XDS) Cross-Enterprise Document Sharing	Enables a number of healthcare delivery organizations belonging to an XDS Affinity Domain (e.g. a community of care) to cooperate in the care of a patient by sharing clinical records in the form of documents as they proceed with their patients' care delivery	Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 16)

Term	Definition	Reference
	activities. This profile is based upon ebXML Registry standards, SOAP, HTTP and SMTP. It describes the configuration of an ebXML Registry in sufficient detail to support Cross Enterprise Document Sharing.	
XDS Document	An XDS Document is the smallest unit of information that may be provided to a Document Repository and registered in a Document Registry. An XDS Document may contain simple text, formatted text (e.g. HL7 CDA Release 1), images (e.g. DICOM) or structured and vocabulary coded clinical information (e.g. CDA Release 2, CCR), or may be made up of a mixture of the above types of content.	Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 156)
(XUA) Cross-Enterprise User Assertion Profile	Provides a means to communicate claims about the identity of an authenticated principal (user, application, system...) in transactions that cross enterprise boundaries. To provide accountability in these cross enterprise transactions there is a need to identify the requesting principal in a way that the receiver can make access decisions and generate the proper audit entries. The XUA Profile supports enterprises that have chosen to have their own user directory with their own unique method of authenticating the users, as well as others that may have chosen to use a third party to perform the authentication.	[http://wiki.ihe.net/index.php?title=Cross-Enterprise_User_Assertion_Profile]
Zero-knowledge Password Protocol	A password based authentication protocol that allows a claimant to authenticate to a Verifier without revealing the password to the Verifier. Examples of such protocols are EKE, SPEKE and SRP.	NIST 800-63-1

2.2 Abbreviations

XDS Cross-Enterprise Document Sharing (IHE profile, see IHE below)

EHR Electronic Health Record

HIE Health Information Exchange

HITSP	Health Information Technology Standards Panel
IHE	Integrating the Healthcare Enterprise
PHI	Protected Health Information
PHCS	Participating Health Care Subscriber
PHR	Personal Health Record
HITE-CT	State of Connecticut – Health Information Technology Exchange

3 Reference Documents

3.1 HITE-CT Reference Documents

The following infromation reference provide additional background on HITE-CT initiatives and associated resources, all available at www.HITECT.net:

- Connecticut Public Act No. 10-117
- The Connecticut Health Information Technology and Exchange Strategic and Operational Plan
- Privacy and security policies adopted by the HITE-CT Board of Directors (see www.hitect.org/policies)

3.2 Developer Resources Reference Documents

The ITI Technical Framework specifies the following ITI Profiles. Where available, the titles below link to expanded brief descriptions of the profile. Implementers SHOULD refer to the Technical Frameworks page for details.

- Consistent Time [CT] ensures system clocks and time stamps of computers in a network are well synchronized (median error less than 1 second).
- Audit Trail and Node Authentication [ATNA] authenticates systems using certificates and sends PHI-related audit events to a repository to help implement confidentiality policies.
- Basic Patient Privacy Consents records patient privacy consents, notes consent on electronically published documents and enforces privacy appropriate to the use.
- Cross-Community Access [XCA] allows members to query and retrieve patient relevant health data held by other communities. Such communities MAY be XDS Affinity Domains which define document sharing using the XDS profile or any other communities, no matter what their internal sharing structure.
- Cross-Community Patient Discovery supports the means to locate communities which hold patient relevant health data and the translation of patient identifiers across communities holding the same patient's data.

- Cross Enterprise Document Sharing [XDS] registers and shares electronic health record documents between healthcare enterprises, ranging from physician offices to clinics to acute care in-patient facilities and personal health records.
- Cross-Enterprise Sharing of Scanned Documents [XDS-SD] defines how to couple legacy paper, film, electronic and scanner outputted formats, represented within a structured HL7 CDA R2 header, with a PDF or plaintext formatted document containing clinical information.
- Cross-Enterprise User Assertion communicates claims about the identity of an authenticated principal (user, application, system...) across enterprise boundaries.
- Document Metadata Subscription [DSUB] describes the use of subscription and notification mechanism for use within an XDS Affinity Domain and across communities
- Healthcare Provider Directory [HPD] supports management of healthcare provider information, both individual and organizational, in a directory structure.
- Multi-Patient Queries [MPQ] The Multi-Patient Queries profile defines a mechanism to enable aggregated queries to a Document Registry based on certain criteria needed by areas related to data analysis, such as quality accreditation of health care practitioners or health care facilities, clinical research trial data collection or population health monitoring.
- Patient Identifier Cross Referencing [PIX] cross-references patient identifiers between hospitals, sites, health information exchange networks, etc.
- Patient Demographics Query [PDQ] lets applications query a central patient information server and retrieve a patient's demographic and visit information.
- Retrieve Form for Data Capture [RFD] enables EHR applications to directly request forms from clinical trial sponsors and public health reporting.

Source: http://www.ihe.net/IT_infra/committees/index.cfm. Accessed March 22, 2011.

4 Organizational Rules

A health inforation exchange (HIE) is a cooperative venture among different stakeholder and interested parties. To ensure an orderly and equitable approach to the planning and operation of the HIE and related activities, a clear system of governance and accountability needs to be implemented in advance of any technical implementation. This section reviews the current legal backdrop for HITE-CT as well as the foundation for its ongoing organization. As HIT/HIE activities grow and mature, HITE-CT will continue to evolve to meet the emerging and changing needs of the state.

4.1 Organizational Structure

HITE-CT is established pursuant to subsection (a) of section 19a-750 of the Connecticut General Statutes to carry out the purposes of the authority, as described in subsection (b) of this section. The purposes of the authority include, but are not limited to, "promoting, planning and designing, developing, assisting, acquiring, constructing, maintaining and equipping, reconstructing and improving of health care information technology."

As of January 1, 2011, the HITE-CT, a quasi-public agency will be the State Designate Entity (SDE) for HIE in Connecticut. Governance for the HITE-CT will be provided by its legislatively appointed Board of Directors responsible for implementing and sustaining a private, secure and robust statewide HIE in Connecticut.

With respect to direct and specific oversight of a health information exchange, it is important to note that the HITE-CT Board, in consultation with its Committees, other stakeholders, and the public will oversee the development of policies for privacy and security. In particular, the HITE-CT Board will establish policies regarding consumer authorization and consent, user access and control, provider access, financing, and secondary uses of that data. The HITE-CT Board will develop policies that ensure a high level of protections for the statewide HIE.

As described in the Strategic Plan, HITE-CT will build a comprehensive governance model to:

- Advocate for shared governance mechanisms and encouraging public participation;
- Encourage stakeholder participation in HITE-CT, including individuals, enterprises and stakeholder representative bodies such as association;
- Promote health information technology adoption across all health care providers, payers, and patients to provide the structured health information that will be the key to achieving improvement goals;
- Oversee the HIE utilities by managing technical operations to ensure availability, adaptability, and usability;
- Conduct business operations, including financing and accountability mechanisms;
- Provide accountability and oversight of the exchange of health information to ensure legal and policy requirements are satisfied; and
- Foster intrastate and interstate collaboration on health information exchange and related standards development.

4.2 Organizational Roles

The Board consists of the following members as defined by the HITE-CT Board of Directors Bylaws:

- The Leutenant Governor, or his or her designee;
- The Commissioners of Public Health, Social Services and Consumer Protection, or their designees;
- The Chief Information Officer of the Department of Information Technology, or his or her designee;
- three appointed by the Governor,
    - one of whom shall be a representative of a medical research organization,
    - one of whom shall be an insurer or representative of a health plan and
    - one of whom shall be an attorney with background and experience in the field of privacy health data security or patient rights;
- three appointed by the president pro tempre of the Senate,
    - one of whom shall have background and experience with a private sector health information exchange or health information technolgy entity,
    - one of whom shall have expertise in public health and
    - one of whom shall be a physician licensed under chapter 370 of the general statues who works in a practice of not more than ten physicians and who is not employed by a hospital, health network, health plan, health system, academic institution or university;
- three appointed by the speaker of the House of Representatives,
    - one of whom shall be a representative of hospitals, and integrated delivery network or a hospital association,
    - one of whom shall have expertise with federally qualified health centers, and
    - one of whom shall be a consumer or consumer advocate;
- one appointed by the majority leader of the Senate, who shall be a primary care physician whose practice utilizes electronic health records;
- one appointed by the majority leader of the House of Representatives, who shall be a consumer or consumer advocate;
- one appointed by the minority leader of the Senate, who shall be a pharmacist or a health care provider utilizing electronic health information exchange;
- and one appointed by te minority leader of the House of Representatitves, who shall be a large employer or a prepresentative of a business group

The Secretary of the Office of Policy and Mangement and Healthcare Advocate or their esignees, shall be ex-officio, nonvoting members of the Board. The Commissioner of Public Health or his or her designee, shall serve as the chairperson of the Board.

HITE-CT's by-laws futher stipulate the member and term limits of board members. While other board members MAY represent the perspective of major organizations within the Connecticut health care landscape, they serve on the board as appointed individuals rather than as official representatives of those organization.

The board meets on a monthly basis to discuss current business to review the work of its committees, and to analyze the strategic direction of the organization. All contractual relationships and significant operational decisions are reviewed and finalized by the board.

HITE-CT's organizational structure includes several committees. These are formed by the board as described in the by-laws and currently incude:

- Governance/Executive Committee
- Legal and Policy Committee
- Business and Technical Operations Committee
- Technical Infrastructure Committee and
- Finance Committee

to manage ongoing business issues and are comprised of board members and advisory board members. Committees make recommendations to the board but do not have independent decision-making authority.

4.3 Funding

HITE-Connecticut has developed a proposed multi-phsed approach to ensure funding. The State plans to leverage the ARRA ONC funding as the foundation and funds from fees levied on potnetial for-profit and non-profit HIE users or contributors to sustain the HIE in the short term. For long-term sustainability, Connecticut has developed a multi-phased methodology for funding with each phase aligned to the products and services provided by the HITE, the value provided, the extent of participation and the overal level of HIE maturity. This model will seek contributed income from various stakehoders in the form of universaal assessment fees, subscription fees and transaction fees (based on services provided) to support HITE-CT's financial needs and growth of its HIE capabilities.

4.3.1 Fee Structure

HITE-CT offers several different services. Interested parties SHOULD contact HITE-CT's [Administrator (administrator@hitect.org] for fees and contract terms.

4.3.2 Re-Imbursement Policies

HITE-CT does not offer reimbursement of fees.

4.3.3 Insurance Policies

HITE-CT carries liability insurance. For details, please contact the HITE-CT administrator, administrator@hitect.org.

4.3.4 Fiscal plan for System Operation, Maintenance, and Innovation

HITE-CT maintains a multi-year contract with a leading technology firm to operate and maintain the HITE-CT. HITE-CT budgets for its core services and will seek additional resources as new service requirements surface.

4.4 Enforcement and Remedies

Where there is a breach identified in patient confidentiality or non-conformance to this policy identified, the HIE participant is subject to removal of access privileges until the source has mitigated the issue locally, or possibly permanently as considered on a case-by-case basis.

4.5 Transparency

HITE-CT promotes transparency of its operations by holding open meetings, publishing materials on its web site, enacting policies that require it to disclose information to outside entities, and by coordinating communication with and among members of the health care community.

4.6 Legal Considerations

4.6.1 Legal Governance

HITE-CT's board of directors and legal counsel provide direction to the organization for legal decisions. HITE-CT MAY from time to time convene an interest group of outside entities to make recommendations.

4.6.2 Government Regulations

The HITE-CT is governed by and enforced in accordance with the laws of the State of Connecticut. In particular, HITE-CT participating Health Care Organizations are subject to the following:

4.6.3 Liability and Risk Allocation

Refer to the HITE-CT Data Use and Reciprocal Support Agreement (DURSA) (www.hitect.org/policies/DURSA).

4.6.4 Indemnification

Refer to HITE-CT Data Use and Reciprocal Support Agreement (DURSA) (www.hitect.org/policies/DURSA).

4.6.5 Intellectual Property Rights to Published Documents

HITE-CT participants who publish documents to the Health Information Exchange agree to share them, including allowing other participants to retrieve, download and save copies of the documents. They also reserve the right to withdraw their documents from the Health Information Exchange, thereby preventing any further access to them.

5 Operational Rules

5.1 Service Level Agreements

For the operation of the Health Information Exchange, HITE-CT maintains a service level agreement with its contractor. This agreement governs the contractor's responsibilities in regards to the XDS' security, availability, and response time; and in regards to customer support and maintenance. HITE-CT in turn maintains service level agreements with its customers that mirror the terms of HITE-CT's agreement with its contractor.

5.2 Daily Governance

5.2.1 Policy Governance

All of HITE-CT's policies require board approval prior to publication or modification. HITE-CT has divided its policies by topic area (security, consent, reportable events, etc.). HITE-CT maintains documents that describe procedures that HITE-CT will follow to adhere with each policy.

5.2.2 Policy Change Procedures

All change proposals SHOULD go to HITE-CT's administrator (administrator@hitect.org). The HITE-CT CEO will manage change with HITE-CT's legal counsel and board of directors.

Prior to making any changes to a policy, the governing body SHALL notify all HITE-CT members that operate under the policy. The policy change SHALL be approved by the HITE-CT board of directors. If policies defined in this document are assigned an Object Identifier (OID), and the policy change is determined by the governing body to have a material impact on a significant number of users of the policy, the HITE-CT Privacy Officer (privacy_officer@HITECT.org) MAY, at its sole discretion, assign a new object identifier to the modified policy.

5.2.3 Publication and Notification Policies

Policies are posted on the HITE-CT website http://www.HITECT.org/policies under the 'Policy' tab. Notifications of policy updates are sent via email to the primary business

contact of HITE-CT members. The [TITLE AND CONTACT] will maintain the list of business contacts.

5.3 Management When Systems are Unavailable

Members are responsible for providing HITE-CT with email addresses to which notifications should be sent. HITE-CT notifies members via email of planned downtime one week in advance. HITE-CT notifies members of unplanned downtime immediately upon its discovery. For both types of downtime, HITE-CT sends periodic explanations of progress and a notification of resolution.

Members should have contingency plans in place for extended downtime periods.

All system actors shall be managed in an environment conformant to ISO IS27799, JCAHO, SSAE 16, ENHAC, or other conformance criteria recognized by CT Department of Information Technology (DOIT).

5.4 Configuration Management

When a configuration change is required of participants, HITE-CT will notify technical contacts via email and will schedule testing and verification with each participant prior to applying the configuration change to production systems.

When the HITE-CT hardware or software requires a configuration change, upgrade or replacement, HITE-CT will schedule the work in such a manner as to impact the smallest number of members possible.

Authorization to make changes. Authorizations for changes to the configuration are subject to affirmation by the HITE-CT Technical Committee.

DNS management: HITE-CT has secured rights to hitect.org and hitect.net. hitect.org wi be used primarily for process management of HITE-CT functions (e.g. committee meeting notifications, minutes, policy publication, etc). hitect.net will be used primarily for HIE functions (e.g. services access such as provider directory).

Dissemination of configuration settings among systems in the Affinity Domain will be don through this Affinity Domain Policy. The latest version of this document can be found at https://www.hitect.org/policies/AffinityDomainPolicy.

5.5 Addition of New Components

All new components SHALL be approved by HITE-CT. Requests for the addition of new components SHALL be directed to administrator@hitect.org.

- Speification for new components not already offered by HITE-CT SHALL be reviewed by the HITE-CT Technical Committee. Recommendations for new services SHALL be approved by the HITE-CT Board of Directors. Any associated configuration and security information SHALL be incorporated into an updated release of this Affinity Domain Policy as a means to communicate to the

managers of components that will need to communicate with a new component. Notification of new components and offerings will be disseminated to the technical and business contacts provide to HITE-CT as part of the DURSA.

- Where an additional XDS Repository is added to an XDS Affinity Domain and a subset of the data in existing Repository(s) is to be migrated to the new system, an export of data MAY be requested subject to mutually agreed-upon terms and formats.

5.6 Data Retention, Archive, and Backup

All security audit logs, both electronic and non-electronic, will be retained and made available for compliance audits and legal review if required by law officials. The security audit logs for each auditable event defined in this section shall be maintained for a period of 10 years. Detailed procedures for data retention, archive, and backup are specified in the HITE-CT Audit Policy (see http://www.hitect.org/policies).

5.7 Disaster Recovery

The following disaster recovery procedures apply to all HITE-CT infrastructure services (Patient Identity Cross Reference Manage, Document Registry, Document Repository, Healthcare Provider Directory, HITE-CT portal, Direct communications portal, etc):

- *How to recover:* Required application and critical data files are securely synchronized between production application environments and the DR facility. File replication processes are monitored and validated at each replication cycle. In the event of disaster at the primary hosting site, the services will be engaged from the recovery location.
- *What process/workflow to invoke:* Processes will entail notification of HITE-CT PHCSs of the disaster event, applicable plans that are to be invoked for recovery, anticipated impact on the users, limitations on data availability, and instructions for any associated configuration requirements.
- *Where to recover:* Infrastructure service recovery SHALL be supported through a tier 4 data center facility in a region of the US physically distant from the primary facility. Recovery location for the infrastructure services will have no physical location recovery services for HITE-CT PHCSs systems given the nature of the services offered.
- *Expectations:* Infrastructure Service will have minimal unplanned downtime. HITE-CT managed health records will be available in accordance with agreed-upon operational SLAs.
- *Service Level Agreement (SLA) for recovery:* Disaster Recovery time objects are 24 hours with 24 hour point in time recovery objective.
- *Notifications/Communications:* HITE-CT management within 1 hour of a disaster declaration that services are being switched to the fail-over site. Notice SHALL include impact on operational configuration, data availability, and service

availability. HITE-CT SHALL notify PHCSs of such expectations and with any associated instructions.

- *Business impact analysis:* Disaster incidents impact the ability of Connecticut practitioners to share clinical information electronically. This will impact efficiency and patient care delivery for those that have adopted electronic workflow methods for this information exchange.
- *Emergency procedures for lack of access:* Lack of access to HITE-CT infrastructure services SHALL revert to traditional paper-based communications or to secure direct electronic communications.

6 Membership Rules

6.1 Acceptance

HIE membership is restricted to regulated clinical care providers within the state of Connecticut, their staff, and service providers acting on behalf of a clinical care provider. State of Connecticut restrictions are imposed to better align the HIE affinity domain policy with legal policies imposed by state-level health related legislation. For interstate communications and other external communications, this domain will leverage the IHE XCA profile. If the remote node is not able to connect via XCA, the remote node MAY be validated and allowed to join the HIE.

6.2 Types of Membership

HITE-CT supports the following participation types:

- Fully Integrated EMR Participant Level: This membership type supports native EMR interoperability for publishing and retrieving documents. This type of member MAY be configured with transformation or portal services to supplement required functionality or interoperability not supported natively by the participant EMR product.
- Temporary Read-Only: HITE-CT participation is intended to support bi-directional exchanges with members. Practitioners that retrieve information from the health information exchange are expected to also contribute information to the exchange. Temporary Read-only access MAY be supported in cases where source practitioner systems are not available to publish if publishing is not otherwise possible. This provision will be supported on a case-by-case basis with the expectation that there is a plan to achieve Full Participant Level within a mutually agreed-upon timeframe.
- Public Health Level: Public health systems MAY engage in read-only access to support public health purposes, including provisions to support multi-patient queries. HITE-CT is actively working with public health authorities to support bi-directional exchanges as an integral value-added offering of the health information exchange.
- HITE-CT members MAY engage in Direct-only communications.

6.3 Membership Policies

HITE-CT PHCSs SHALL execute a Data Use and Reciprocal Support Agreement (DURSA) that outlines responsibilities of membership. The HITE-CT DURSA will be posted on http://www.hitect.org/agreements.

The list of HITE-CT members will be posted at http://www.hitect.org/members.

Prospective PHCSs may contact HITE-CT to discuss membership at administrator@hitect.org.

Current HITE-CT PHCSs that wish to apply to no longer be a member may contact HITE-CT at administrator@hitect.org.

Members leaving the affinity domain MAY request that their data be removed from the XDS or to have it locked down.

6.3.1 Participation Agreements

HITE-CT membership requires executing the HITE-CT Data Service and Participation Agreement.

HITE-CT participation agreements SHALL automatically renew for consecutive one year terms until terminated by mutual agreement or by either party during the ninety (90) days prior to renewal date.

Either HITE-CT or the HITE-CT member party MAY suspend services or terminate the HITE-CT participation Agreement at any time for material failure of the other party to comply with the terms and conditions thereof, if such material failure is not corrected within a period of sixty (60) days after receipt of written notice from the orther party specifiying such failure.

6.3.2 Membership Lists

The list of member is maintained and published on the HITE-CT website www.HITECT.org/members. This is a publically available web site location. Participation of the HITE-CT with other Health Information Exchange is also published and is accessible from this location

7 Connectivity to the XDS Affinity Domain from External Systems

7.1 Interoperability Strategy

The policy agreement SHALL identify the procedure for how to reach the data over the domain borders. There are many ways to bring this about and it is therefore very important that this is specified in the agreement. HITE-CT MAY offer interoperability through the IHE Cross-Community Access (XCA) profile to enable communications with other health information exchanges. For interoperability with federal agencies, NwHIN Direct MAY be used. NwHIN Direct is available for point-to-point communications.

7.1.1 External Connectivity Through Portals

Access by 'portal' is permitted. Remote access requires strong authentication. The Portal user SHALL be contractually bound to abide by HITE-CT security and privacy policies and this Affinity Domain Policy. Agreements with portal user SHALL be executed either with HITE-CT or with a HITE-CT Participating Health Care Subscriber that is already bound to these policies. (see HITE-CT Access Control Policy http://www.hitect.org/policies).

8 System Architecture

In order to secure both information retrieval and publishing, the system architecture of the applications has to be specified and understood by all parties. This policy agreement therefore contains detailed information regarding the architectural expectation of systems supporting the various actor/profiles, and the supported document types and publication policies for Connecticut implementations of this policy.

8.1.1 Global Architecture

The HITE-CT global architecture is depicted in Figure 1. Each of the providers will be configured with a document source and document consumer. This MAY be done through a web portal or through the native EMR product. The patient identity source is supplied by each provider source either through the interface engine or through data extract processing. The HITE-CT supports a hybrid model whereby a participating organization MAY utilize the HITE-CT managed repository or the participating organization MAY utilize a document repository under the management of that organization. This hybrid model allowing for practitioner organizations to access the HIE and publish to the HIE leveraging multiple implementation approaches to better enable local autonomy. Where the provider EMR is able to natively publish conformant document types, the EMR MAY be configured directly as a document source. Those that are operating in a legacy EMR environment MAY leverage transformation services provided by the HITE-CT to transform the content to a conformant document for HIE sharing. Where the provider EMR is able to natively consume the HIE documents, the EMR MAY be configured directly as a document consumer. Those that are operating in a legacy EMR environment MAY leverage a portal to enable conformant HIE document access. The patient identity source is supplied by each provider source either through the interface engine or through data extract processing.

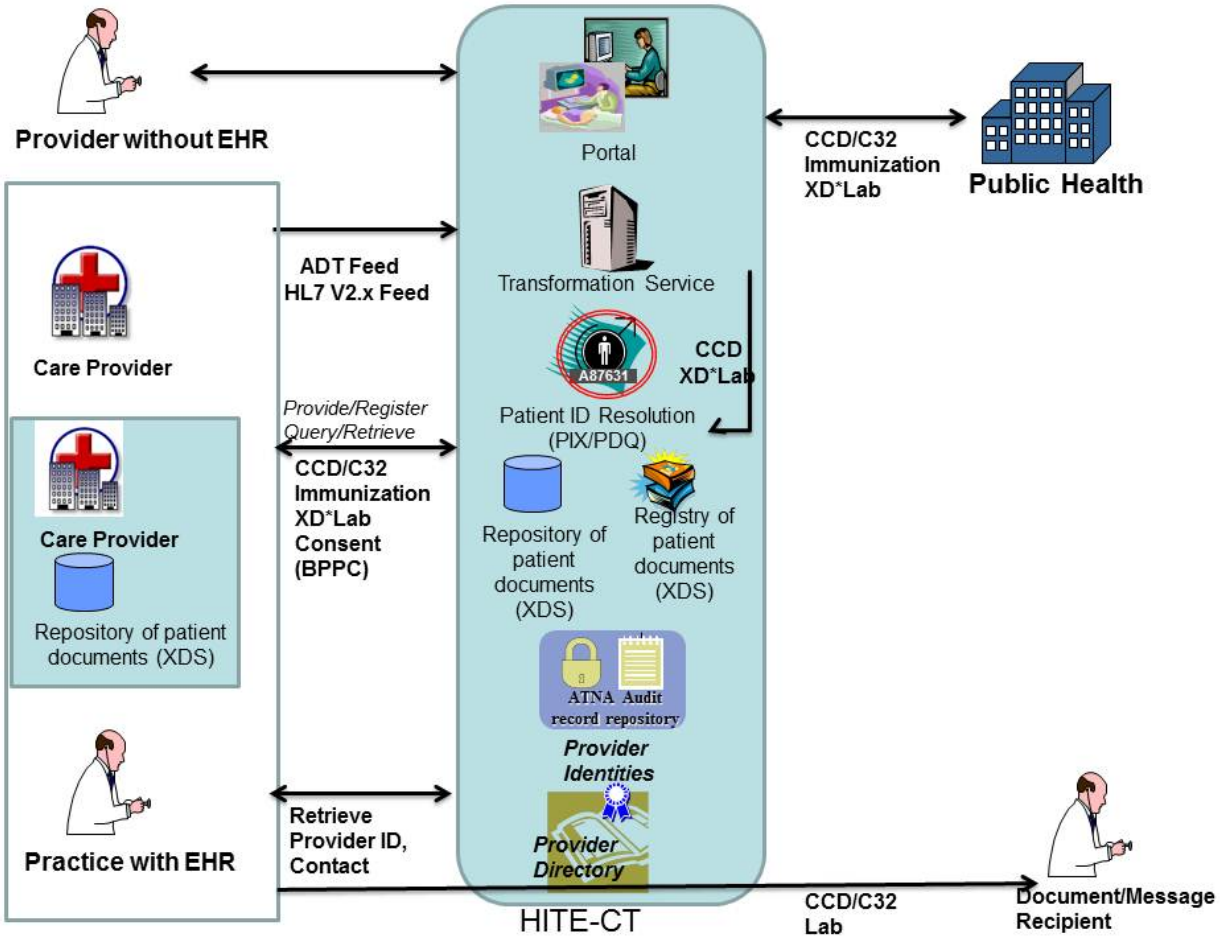


Figure 1: HITE-CT Global Architecture

8.1.2 Affinity Domain Actors

A number of systems implementing IHE Actors defined in the XDS integration profile need to be identified and configured to communicate. This includes defining addressing information and ATNA secured node certificate.

8.1.2.1 Business Actors

The following business actors and the technical actor required support are identified within the HIE:

Table 8.1.2.1-1.Business Actors

Business Actor	Definition	Technical Actors	Actor Optionality	Comments
HITE-CT Infrastructure Service Provider	Shared service provider for Patient ID Cross-Referencing Manager, Consent Repository, Audit Repository, and	PIX Manager	R	
		PDQ Supplier	R	
		ATNA Audit Repository	R	
		XDS Registry	R	

Business Actor	Definition	Technical Actors	Actor Optionality	Comments
	Document Registry: HITE-CT (Services provided by infrastructure vendor)	XUA X-Service Provider	C	Pending operational deployment
Health care Providers Retrieving Records (Document Consumer)	HIE member health care providers and public heath autorities that are authorized to query and retrieve documentss: See Member List for Document Consumers Providers (www.hitect.org/members) HITE-CT Portal	XDS Document Consumer	C	May use HITE-CT portal for access to HITE-CT documents
		XDS-I Imaging Document Consumer	O	
		Consistent Time Client	R	Uses NIST time server
		ATNA Secure Node	R	Where XDS Document Consumer, XDS-I document Consumer is implemented. Where portal access is used, portal SHALL provide ATNA Secure Node
		PIX Consumer	C	Either PIX Consumer or PDQ Consumer is Required retrieval of documents from the HITE-CT
		PDQ Consumer	C	Either PIX Consumer or PDQ Consumer is Required retrieval of documents from the HITE-CT
		PIX Feed	C	Required for Dcoument Consumers using PIX
Health care Providers Publishing Records (Document Source)	HIE member health care providers and public heath autorities that are authorized to publish documents: See Member List for Document Consumers Providers (www.hitect.org/members)	XDS Document Source	C	May use HITE-CT transformation service for submission of documents
		XDS-I Imaging Document Source	O	
		Consistent Time Client	R	Uses NIST time server
		ATNA Secure Node	R	Where XDS Document Consumer, XDS-I document Consumer is implemented. Where portal access is used, portal SHALL provide ATNA Secure Node
		Patient Identity Source	R	

8.1.3 Technical Actor Specifications

This section provides the details for the transactions/messaging that need to be supported by the technical actors required by the listed business actors. For the most part these technical actors will correspond to particular IHE Profile Actors. A number of systems implementing IHE Actors defined in the XDS Integration Profile need to be identified and configured to communicate. In addition, there will be systems in the XDS Affinity Domain that MUST conform to other IHE Actor Profiles. This section identifies the requirements for all IHE Actor/Profiles that are not fully specified or mandated by the IHE Technical Framework.

8.1.4 XDS Document Registry

This section identifies specific requirements for a registry actor in the XDS affinity domain that are not fully specified or mandated by the IHE technical framework. The registry SHALL support XDS.b transactions. Where the registry is intended for data repurposing, the repurposing registry SHALL be installed as a separate service from the clinical care registry, and the registry SHALL support Multi-Patient Queries (MPQ) and/or DSUB.

When the registry receives registration requests, containing terminology it does not understand it SHALL reject those requests and SHALL notify the HIE to contact the non-conformant system owner for additional conformance testing.

Table 8.1.4-1. XDS.b Document Registry Transactions

Actor	Transactions	Optionality	Comments
Document Registry	Register Document Set-b [ITI-42]	R	Shall support multiple Document Repositories to support HITE-CT members that choose to maintain a federated repository
	Registry Stored Query [ITI-18]	R	
	Patient Identity Feed [ITI-8]	R	
	Patient Identity Feed HL7v3 [ITI-44]	R	
	Multi-Patient Stored Query [ITI-51]	C	Either MPQ or DSUB SHALL be supported
	Document Metadata Subscribe [ITI-52]	C	Either MPQ or DSUB SHALL be supported (NOTE: subject to document consumer capability)
	Document Metadata Notify [ITI-53]	C	Either MPQ or DSUB SHALL be supported (NOTE: subject to document consumer capability)

Table 8.1.4-2 defines any additional messaging that MUST be supported that is not defined as a Transaction for this Profile Actor in the IHE Technical Framework, such as additional HL7 messaging

Table 8.1.4-2. Additional XDS Document Registry Messaging

Actor	Messaging	Optionality	Comments

Actor	Messaging	Optionality	Comments
Document Registry	HL7 V2.x Transformation	R	Registry SHALL provide a transformation interface to support a provide and register capability for those HITE-CT members unable to support directly the Provide and Register Transaction from the native EHR installed system
Document Registry	Portal Interface	R	Registry SHALL provide a portal interface to support query registry functionality for those HITE-CT members unable to support directly the Query Registry and Registry Stored Query Transaction from the native EHR installed system
Document Registry	Patient Identity Feed Transformation	R	Registry SHALL provide a transformation interface to support a provide and register capability for those HITE-CT members unable to support directly the Patient Identity Feed Transaction from the native EHR installed system. The specific implementation details of the receipt, conversion, and registration of registry content are negotiated between the HITE-CT member and the HITE-CT infrastructure service provider on a case-by-case basis. The members SHALL use the ADT specification provided by HITE-CT.

8.1.5 XDS Document Repository

This section identifies specific requirements for a repository actor in the XDS affinity domain that are not fully specified or mandated by the IHE technical framework. The repository SHALL support XDS.b transactions. All federated repository implementations SHALL conform to the policies of the HITE-CT and this Affinity Domain Policy as applicable.

Table 8.1.5-1. XDS.b Document Repository Transactions

Actor	Transactions	Optionality	Comments
Document Repository	Provide and Register Document Set-b [ITI-41]	R	
	Register Document Set-b [ITI-42]	R	
	Retrieve Document [ITI-17]	R	

The table below defines any additional messaging that MUST be supported that is not defined as a Transaction for this Profile Actor in the IHE Technical Framework, such as additional HL7 messaging

Table 8.1.5-3. Additional XDS Document Repository Messaging

Actor	Messaging	Optionality	Comments

Actor	Messaging	Optionality	Comments
Document Repository	HL7 V2.x Transformation	R	XDS Document Repository SHALL support acting as a gateway for receiving HL7 v2.x messages for encounter and laboroatory content that it transforms and registers. To support a provide and register document capability for those HITE-CT members unable to support directly the Provide and Register Transaction from the native EHR installed system. The specific implementation details of the receipt, conversion, and registration of repository content are negotiated between the HITE-CT member and the HITE-CT infrastructure service provider on a case-by-case basis. The member SHALL use the HL7 specification(s) provided by HITE-CT.

8.1.6 XDS Document Source

XDS document source is used to provide clinical data for both clinical care and quality reporting purposes. C32 as contrained for Meaningful Use is the preferred document for conveying quality data from the ambulatory setting; XDS-MS is the preferred document from the inpatient setting.

This section identifies specific requirements for a document source actor in the XDS affinity domain that are not fully specified or mandated by the IHE technical framework.

The document source SHALL support XDS.b transactions. See also metadata constraints. The document source SHOULD digitally sign the documents provided and registered for sharing, or upon negotiation, MAY be omitted with a transition plan for addition of machine signatures. The document source SHALL support Basic Patient Privacy Consents (BPPC)[1], or upon negotiation, SHALL populate the published document's ConfidentialityCode using the routine default Policy: [1.3.6.1.4.1. 38571.1.1000] If the document source does not support BPPC, then the document source SHALL NOT publish restricted content, or the document source SHALL submit documents using the transformation services so that any restricted data may be appropriately flagged according to the BPPC specifications.

Table 8.1.6-1. XDS.b Document Source Transactions

Actor	Transactions	Optionality	Comments
Document Source	Provide and Register Document Set-b [ITI-41]	R	At least one of the content optionsbelow SHALL be supported

[1] "The Basic Patient Privacy Consents profile provides a mechanism to record the patient privacy consent(s), a method to mark documents published to XDS with the patient privacy consent that was used to authorize the publication, and a method for XDS Consumers to use to enforce the privacy consent appropriate to the use." Available: http://wiki.ihe.net/index.php?title=Basic_Patient_Privacy_Consents.

795 **Table 8.1.6-2. Provide and Register Document Transaction Options**

Option	Optionality	Comments
Document Replace Option	R	The Document Consumer SHALL support the Document Replace Option. Where this option is not supported by the HITE-CT member installed system, requests for document deprecation or deletion SHALL be submitted in writing to HITE-CT with the reasons for the requested deprecation or deletion clearly documented.
Document Addendum Option	O	The Document Consumer SHOULD support the Document Addendum Option.
Document Transformation Option	O	The Document Consumer SHOULD support the Document Transformation Option.
Folder Management Option	O	
Asynchronous Web Services Exchange	O	
Basic Patient Privacy Enforcement	R	The Document Source SHALL support the Basic Patient Privacy Enforcement. Transformation services may be offered on a case-by-case basis for those source systems unable to perform this function. The Document Source actor shall be able to be configured with the Patient Privacy Policies, Patient Privacy Policy Identifiers (OIDs) and associated information necessary to understand and enforce the HITE-CT Affinity Domain Policy Sensitivity Classification defined in section 9.3.1.6.

Table 8.1.6-3. Provide and Register Document Set Content Options

Content Options	Optionality	Comments
Meaningfur Use constrainted HITSP/C32 CCD document	C	SHALL conform to HITSP/C32 v2.5 HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component as constrained for Meaningful Use. HITE-CT member systems SHALL support at least one of HITSP/C32 v2.5 CCD, XDS-MS or XPHR. .
Medical Summary in HL7 CDA Format [XDS-MS]	C	HITE-CT member systems SHALL support at least one of HITSP/C32 v2.5 CCD, XDS-MS or C32.
Exchange of Personal Health Record Content [XPHR]	C	SHALL conform to HITSP/C32 v2.5 HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component. HITE-CT member systems SHALL support at least one of HITSP/C32 v2.5 CCD, XDS-MS or XPHR.
Scanned Document as HL7 CDA with PDF or plain text content [XDS-SD]	O	
Document Digital Signature [DSG]	C	Where not supported, upon negotiation, MAY be omitted with a transition plan for addition of machine signatures.
Sharing Laboratory Results [XD*Lab]	O	
Emergency Department Encounter Summary [EDES]	O	
Immunization Content [IC]	O	

Content Options	Optionality	Comments
Emergency Department Referral [EDR]	O	
Labor and Delivery Record [LDR]	O	
Antepartum Record [APR]	O	
Basic Patient Privacy Consents [BPPC]	R	Where BPPC is not supported, upon negotiation, transformation or portal option may be offered.

Table 8.1.6-3 defines any additional messaging that MUST be supported that is not defined as a Transaction for this Profile Actor in the IHE Technical Framework, such as additional HL7 messaging

Table 8.1.6-3. Additional XDS Document Source Messaging

Actor	Messaging	Optionality	Comments
Document Source	HL7 v2.x	O	HITE-CT information sources MAY negotiate a transformation interface whereby and HL7 v2.x message is provided from the organization supplying the clinical data, including quality data, for the document source. This serves to support a provide and register document capability for those HITE-CT members unable to support directly the Provide and Register Transaction from the native EHR installed system. The specific implementation details of the receipt, conversion, and registration of repository content are negotiated between the HITE-CT member and the HITE-CT infrastructure service provider on a case-by-case basis.

8.1.7 XDS-I Imaging Document Source

This section identifies specific requirements for an Imaging Document Source Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework. XDS-I is not required of document sources or document consumers in the HITE-CT. Where implemented, the associated XDS-I Imaging Document Source SHALL conform to the following:

Table 8.1.7-1. XDS-I Imaging Document Source Transactions

Actor	Transactions	Optionality	Comments
Imaging Document Source	Provide and Register Imaging Document Set [RAD-54]	R	No document content stipulation applied by this policy at this time. At least one of the options below SHALL be supported
	Retrieve Images [RAD-16]	R	
	Retrieve Presentation States [RAD-17]	R	
	Retrieve Reports [RAD-27]	R	
	Retrieve Key Image Note [RAD-31],	R	

Actor	Transactions	Optionality	Comments
	Retrieve Evidence Documents [RAD-45]	R	
	WADO Retrieve [RAD-55]	R	

No stipulations are specified at this time regarding options for the Content in the following table.

Table 8.1.7-2. Provide and Register Imaging Document Set Content Options

Content Options	Optionality	FComments
Set of DICOM Instances [RAD-18.2.1]	O	At least one of these SHALL be supported where XDS-I is implemented
PDF Report [RAD-18.2.2]	O	At least one of these SHALL be supported where XDS-I is implemented
Text Report [CDA]	O	At least one of these SHALL be supported where XDS-I is implemented

The table below defines any additional messaging that MUST be supported that is not defined as a Transaction for this Profile Actor in the IHE Technical Framework, such as additional HL7 messaging

Table 8.1.7-3. Additional XDS-I Imaging Document Source Messaging

Actor	Messaging	Optionality	Comments
Imaging Document Source		O/R	HITE-CT information sources MAY negotiate a transformation interface whereby and HL7 v2.x message is provided from the organization supplying the imaging data for the imaging document source. This serves to support a provide and register document capability for those HITE-CT members unable to support directly the Provide and Register Transaction from the native EHR installed system. The specific implementation details of the receipt, conversion, and registration of repository content are negotiated between the HITE-CT member and the HITE-CT infrastructure service provider on a case-by-case basis.

8.1.8 XDS Document Consumer

This section identifies specific requirements for a Document Consumer Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework. The document source SHALL support XDS.b transactions, or, upon negotiation, MAY support XDS.a with a transition plan for migration to XDS.b. The document consumer SHOULD support verification of a digitally signed document retrieved from the registry, or upon negotiation, MAY be omitted with a transition plan for addition of signatures verifications. The document consumer SHALL support BPPC, or negotiate HITE-CT server-side enforcement of BPPC and document access or other method to assure that BPPC policies SHALL be supported. Providers who retrieve a document are responsible for retaining a copy in case the document source has

deprecated, replaced or created an addendum to the document. Documents SHALL be retrieved from the document repository for each use to support the ability for document update/corrections.

Table 8.1.8-1. XDS.b Document Consumer Transactions

Actor	Transactions	Optionality	Comments
Document Consumer	Retrieve Document Set [ITI-43]	R	At least one of the content options below SHALL be supported
	Registry Stored Query [ITI-18]	R	At least one of the content options below SHALL be supported
document consumer implemented by public health, quality, research	Multi-Patient Stored Query [ITI-51]	C	Where the document consumer is authorized to issue population-level queiries then either MPQ or DSUB SHALL be supported
	Document Metadata Subscribe [ITI-52]	C	Where the document consumer is authorized to issue population-level queiries then either MPQ or DSUB SHALL be supported
	Document Metadata Notify [ITI-53]	C	Where the document consumer is authorized to issue population-level queiries then either MPQ or DSUB SHALL be supported

It is the responsibility of the member to retain documents upon which it has made medical decisions. In order to support this policy requirement, the document consumer SHALL support document import option for all documents retrieved from the HITE-CT or demonstrate to HITE-CT that secondary methods are in place to retain all retrieved documents. No constraints are placed at this time regarding support for document discrete data import, but HITE-CT members are encouraged to require this support from their vendors for optimum benefit from HITE-CT participation.

Table 8.1.8-2. XDS.b Document Consumer Options

Option	Optionality	Comments
Basic Patient Privacy Enforcement	R	The Document Consumer SHALL support the Basic Patient Privacy Enforcement. Augmented Registry services may be offered on a case-by-case basis for those source systems unable to perform this function. The Document Consumer actor shall be able to be configured with the Patient Privacy Policies, Patient Privacy Policy Identifiers (OIDs) and associated information necessary to understand and enforce the HITE-CT Affinity Domain Policy Sensitivity Classification defined in section 9.3.1.6.
Basic Patient Privacy Proof	R	The Document Consumer actor shall be capable of querying for HITE-CT 'Approved' Patient Privacy Acknowledgement Documents in HITE-CT defined in section 10.2.3 Table 10.2.3-1 Patient Privacy Policies. The Document Consumer actor shall be capable of

		recognizing the eventCodeList from the resulting XDS Metadata. There is no required handling of Patient Privacy Consent Acknowledgement Document XDS Metadata**.**
Asynchronous Web Services Exchange	O	

Table 8.1.8-3. Document Consumer Content Support

Content Options	Optionality	Comments
Medical Summary in HL7 CDA Format [XDS-MS]	C	SHALL conform to HITSP/C32 v2.5 HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component as constrained for Meaningful Use. HITE-CT member systems SHALL support at least one of HITSP/C32 v2.5 CCD, XDS-MS or XPHR. Where this content is used, document import option and discrete data import option SHOULD be supported.
Continuity of Care Document (CCD/C32)	C	HITE-CT member systems SHALL support at least one of HITSP/C32 v2.5 CCD, XDS-MS or C32. Where this content is used, document import option and discrete data import option SHOULD be supported.
Scanned Document as HL7 CDA with PDF or plain text content [XDS-SD]	O	HITE-CT meber systems SHOULD support XDS-SD.
Document Digital Signature [DSG]	C	Where not supported, upon negotiation, MAY be omitted with a transition plan for addition of machine signatures. Where this content is used, document import option SHOULD be supported.
Sharing Laboratory Results [XD*Lab]	O	HITE-CT meber systems SHOULD support XD*Lab.. Where this content is used, document import option and discrete data import option SHOULD be supported.
Emergency Department Encounter Summary [EDES]	O	HITE-CT meber systems SHOULD support EDES. Where this content is used, document import option and discrete data import option SHOULD be supported.
Immunization Content [IC]	O	HITE-CT meber systems SHOULD support IC. Where this content is used, document import option and discrete data import option SHOULD be supported.
Emergency Department Referral [EDR]	O	HITE-CT meber systems SHOULD support EDR. Where this content is used, document import option and discrete data import option SHOULD be supported.
Labor and Delivery Summary [LDS]	O	HITE-CT meber systems SHOULD support LDS. Where this content is used, document import option and discrete data import option SHOULD be supported.
Antepartum Summary [APS]	O	HITE-CT meber systems SHOULD support APS.Where this content is used, document import option and discrete data import option SHOULD be supported.
Basic Patient Privacy Consents [BPPC]	C	SHALL support BPPC or MAY negotiate an alternative method with HITE-CT. Where this content is used, document import option SHOULD be supported.

C=Consumer MUST support either XDS-MS or XPHR or both.
O=Optional
R=Required

The table below defines any additional messaging that MUST be supported that is not defined as a Transaction for this Profile Actor in the IHE Technical Framework, such as additional HL7 messaging.

Table 8.1.8-4. Additional XDS Document Consumer Messaging

Actor	Messaging	Optionality	Comments
Document Consumer		O	HITE-CT members MAY access the Documents via the HITE-CT portal. No additional non-IHE interfaces are currently supported. Requests for a new non-standard interface SHALL be directed to the HITE-CT administrator (administrator@hitect.org)

8.1.9 XDS-I Imaging Document Consumer

This section identifies specific requirements for an Imaging Document Consumer Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework. XDS-I is not required of document sources or document consumers in the HITE-CT. Where implemented, the associated XDS-I Imaging Document Source SHALL conform to the following:

Table 8.1.9-1. XDS-I Imaging Document Consumer Transactions

Actor	Transactions	Optionality	Comments
Imaging Document Consumer	Retrieve Images [RAD-16]	O	No document content stipulation applied by this policy at this time. At least one of these SHALL be supported where XDS-I is implemented
	Retrieve Presentation States [RAD-17]	O	No document content stipulation applied by this policy at this time. At least one of these SHALL be supported where XDS-I is implemented
	Retrieve Reports [RAD-27]	O	No document content stipulation applied by this policy at this time. At least one of these SHALL be supported where XDS-I is implemented
	Retrieve Key Image Note [RAD-31]	O	No document content stipulation applied by this policy at this time. At least one of these SHALL be supported where XDS-I is implemented
	Retrieve Evidence Documents [RAD-45]	O	No document content stipulation applied by this policy at this time. At least one of these SHALL be supported where XDS-I is implemented
	WADO Retrieve [RAD-55]	O	No document content stipulation applied by this policy at this time. At least one of these SHALL be supported where XDS-I is implemented

No stipulations are specified at this time regarding display, integration in application, content options, and workflow context management for the types of retrieved Content in the following table.

Table 8.1.9-2. XDS-I Imaging Document Consumer Content Support

Content Options	Optionality	Comments
Set of DICOM Instances [RAD-18.2.1]	O	At least one of these SHALL be supported where XDS-I is implemented
PDF Report [RAD-18.2.2]	O	At least one of these SHALL be supported where XDS-I is implemented
Text Report [CDA]	O	At least one of these SHALL be supported where XDS-I is implemented

The table below defines any additional messaging that MUST be supported that is not defined as a Transaction for this Profile Actor in the IHE Technical Framework, such as additional HL7 messaging.

Table 8.1.9-3. Additional XDS-I Imaging Document Consumer Messaging

Actor	Messaging	Optionality	Comments
Imaging Document Consumer		O	HITE-CT members MAY access the Documents via the HITE-CT portal. No additional non-IHE interfaces are currently supported. Requests for a new non-standard interface SHALL be directed to Lauri Scharf at info@HITE-CT.net..

8.1.10 XDS Patient Identity Source

HL7 v2.3.1 is supported by the HITE-CT. Patient Identity Feed HL7v3 MAY be supported under individual negotiation with HITE-CT.

Table 8.1.10-1. XDS Patient Identity Source Transactions

Actor	Transactions	Optionality	Comments
Patient Identity Source	Patient Identity Feed [ITI-8]	R	Patient Identity Feed HL7v3 MAY be supported under individual negotiation with HITE-CT if ITI-8 is not supported by the HITE-CT member system vendor

Table 8.1.10-2. XDS HL7v3 Patient Identity Source Transactions

Actor	Transactions	Optionality	Comments
Patient Identity Source	Patient Identity Feed HL7v3 [ITI-44]	O	Patient Identity Feed HL7v3 MAY be supported under individual negotiation with HITE-CT

Table 8.1.10-3. Additional XDS Patient Identity Source Messaging

Actor	Messaging	Optionality	Comments

Actor	Messaging	Optionality	Comments
Patient Identity Source		O	HITE-CT information sources MAY negotiate a transformation interface whereby alternate approaches of delivering patient identity information provided from the organization supplying the patient identity data. This serves to support a patient identity feed capability for those HITE-CT members unable to support directly the standard patient identity feed transactions from the native EHR installed system. The specific implementation details of the receipt, conversion, and registration of patient identity content are negotiated between the HITE-CT member and the HITE-CT infrastructure service provider on a case-by-case basis.

8.1.11 PIX Manager

Patient Identity Feed HL7v3 MAY be supported under individual negotiation with HITE-CT..

890 **Table 8.1.11-1. PIX Manager Transactions**

Actor	Transactions	Optionality	Comments
Patient Identifier Cross-reference Manager	Patient Identity Feed [ITI-8]	R	
	PIX Query [ITI-9]	R	
	PIX Update Notification [ITI-10]	R	

Table 8.1.11-2. PIX HL7v3 Manager Transactions

Actor	Transactions	Optionality	Comments
Patient Identifier Cross-reference Manager	Patient Identity Feed HL7v3 [ITI-44]	R	Patient Identity Feed HL7v3 SHALL be supported by the PIX Manager. Patient Identity Feed using HL7v3 SHALL be subject to individual negotiation between HITE-CT and the HIE member
	PIXV3 Query[ITI-45]	R	Patient Identity Feed HL7v3 SHALL be supported by the PIX Manager. Patient Identity Feed using HL7v3 SHALL be subject to individual negotiation between HITE-CT and the HIE member
	PIXV3 Update Notification[ITI-46]	R	Patient Identity Feed HL7v3 SHALL be supported by the PIX Manager. Patient Identity Feed using HL7v3 SHALL be subject to individual negotiation between HITE-CT and the HIE member

Table 8.1.11-3. Additional PIX Manager Messaging

Actor	Messaging	Optionality	Comments

Actor	Messaging	Optionality	Comments
Patient Identifier Cross-reference Manager		R	HITE-CT PIX Manager SHALL support a transformation interface supporting alternate approaches of delivering patient identity information provided from the organization supplying the patient identity data. This serves to support a patient identity feed capability for those HITE-CT members unable to support directly the standard patient identity feed transactions from the native EHR installed system. The specific implementation details of the receipt, conversion, and registration of patient identity content are negotiated between the HITE-CT member and the HITE-CT infrastructure service provider on a case-by-case basis.

8.1.12 PIX Consumer

This section identifies specific requirements for the PIX Consumer Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework. At least one of PIX Query or Patient Demographic Query SHALL be supported. PIX V3 Query MAY be used upon negitionation.

Table 8.1.12-1. PIX Consumer Transactions

Actor	Transactions	Optionality	Comments
Patient Identifier Cross-reference Consumer	PIX Query [ITI-9]	C	The PIX consumer SHALL support either ITI-9 or PDQ (ITI-21) or both.
	PIX Update Notification [ITI-10]	C	If ITI-9 is used, the PIX consumer SHALL support ITI-10, or MAY negotiate a migration plan to ITI-10 with HITE-CT.

Table 8.1.12-2. PIX HL7v3 Consumer Transactions

Actor	Transactions	Optionality	Comments
Patient Identifier Cross-reference Consumer	PIXV3 Query [ITI-45]	C	PIXv3 Query MAY be used by the PIX Consumer. PIXv3 Query support SHALL be subject to individual negotiation between HITE-CT and the HIE member
	PIXV3 Update Notification [ITI-46]	C	PIXv3 Update Notification MAY be used by the PIX Consumer. PIXv3 Update Notification support SHALL be subject to individual negotiation between HITE-CT and the HIE member

8.1.13 PDQ Patient Demographics Supplier

This section identifies specific requirements for the PDQ Patient Demographics Supplier Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework. PDQ transactions are required and PIX V3 Query MAY be supported upon negotiation.

Table 8.1.13-1. PDQ Patient Demographics Supplier Transactions

Actor	Transactions	Optionality	Comments

Actor	Transactions	Optionality	Comments
Patient Demographics Supplier	Patient Demographics Query [ITI-21]	R	
	Patient Demographics and Visit Query [ITI-22]	R	

Table 8.1.13-2. PDQ HL7v3 Patient Demographics Supplier Transactions

Actor	Transactions	Optionality	Comments
Patient Demographics Supplier	Patient Demographics Query HL7 V3[ITI-47]	O	

Table 8.1.13-3. Additional PDQ Patient Demographics Supplier Messaging

Actor	Messaging	Optionality	Comments
Patient Demographics Supplier		O	None at this time.

8.1.14 PDQ Patient Demographics Consumer

This section identifies specific requirements for the Patient Demographics Consumer Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework. At least one of PIX Query or Patient Demographic Query SHALL be supported. PDQ V3 Query MAY be used upon negotiation.

Table 8.1.14-1. PDQ Patient Demographics Consumer Transactions

Actor	Transactions	Optionality	Comments
Patient Demographics Consumer	Patient Demographics Query [ITI-21]	C	The Patient Demographics consumer SHALL support either ITI-9 or PDQ (ITI-21 and ITI-22) or both.
	Patient Demographics and Visit Query [ITI-22]	C	The Patient Demographics consumer SHALL support either ITI-9 or PDQ (ITI-21 and ITI-22) or both.

Table 8.1.14-2. PDQ HL7v3 Patient Demographics Consumer Transactions

Actor	Transactions	Optionality	Comments
Patient Demographics Consumer	Patient Demographics Query HL7 V3[ITI-47]	O	PDQ HL7 V3 MAY be supported upon negotiation.

Table 8.1.14-3. Additional PDQ Patient Demographics Consumer Messaging

Actor	Messaging	Optionality	Comments
Patient Demographics Consumer		O	None at this time.

8.1.15 ATNA Audit Record Repository

No additional stipulations beyond XDS audit events are required.

Table 8.1.15-1. ATNA Audit Record Repository Transactions

Actor	Transactions	Optionality	Comments
Audit Record Repository	Record Audit Event [ITI-20]	R	ITI-20 is required for both the HITE-CT member's system and the HITE-CT infrastructure.

8.1.16 ATNA Secure Node

The organization responsible for a new node MUST make a request for participation in the HITE-CT. Upon approval, the organization will generate a PKCS10 request and send it to the HITE-CT technical contact. In response, the HITE-CT will generate a digital identity and deliver it to the member's technical contact. Secure Node and Secure Application SHALL both be supported; the HITE-CT member SHALL support one or the other or both (see HITE-CT Identity Management Policy http://www.hitect.org/policies).

Table 8.1.16-1. ATNA Secure Node Transactions

Actor	Transactions	Optionality	Comments
Secure Node	Authenticate Node [ITI-19]	C	The HITE-CT member SHALL support either Secure Node or Secure Application or both.
	Maintain Time [ITI-1]	R	

8.1.17 Secure Application

The organization responsible for a new node MUST make a request for participation in the HITE-CT. Upon approval, the organization will generate a PKCS10 request and send it to the HITE-CT technical contact. In response, the HITE-CT will generate a digital identity and deliver it to the member's technical contact. The member's system SHALL support Secure Node or Secure Application or both (see HITE-CT Identity Management Policy http://www.hitect.org/policies).

Table 8.1.17-1. ATNA Secure Application Transactions

Actor	Transactions	Optionality	Comments

Actor	Transactions	Optionality	Comments
Secure Application	Authenticate Node [ITI-19]	C	The HITE-CT member SHALL support either Secure Node or Secure Application or both.
	Maintain Time [ITI-1]	R	
	Record Audit Event [ITI-20]	R	

8.1.18 CT Time Server

No further stipulation on the transaction (ITI-1). All systems SHALL use the NIST time server.

Table 8.1.18-1 CT Time Server Transactions

Actor	Transactions	Optionality	Comments
Time Server	Maintain Time [ITI-1]	R	

8.1.19 CT Time Client

No further stipulation on the transaction (ITI-1). All systems SHALL use the NIST time server.

Table 8.1.19-1. CT Time Client Transactions

Actor	Transactions	Optionality	Comments
Time Client	Maintain Time [ITI-1]	R	

8.1.20 Any Additional IHE Actor Systems

The Healthcare Provider Directory support for the following transactions is available:

Table 7.2.20-1. <Profile Actor>Transactions

Actor	Transactions	Optionality	Comments
Provider Information Directory	Provider Information Query	R	SHALL be supported by the infrastructure service provider
	Provider Information Feed	O	MAY be supported by the infrastructure service provider
Provider Information Consumer	Provider Information Query	O	MAY be implemented by participating health care subscribers
Provider Information Source	Provider Information Feed	O	MAY be implemented by CT source licensing authority

8.1.21 Additional Affinity Domain Specific Recognized Technical Actors

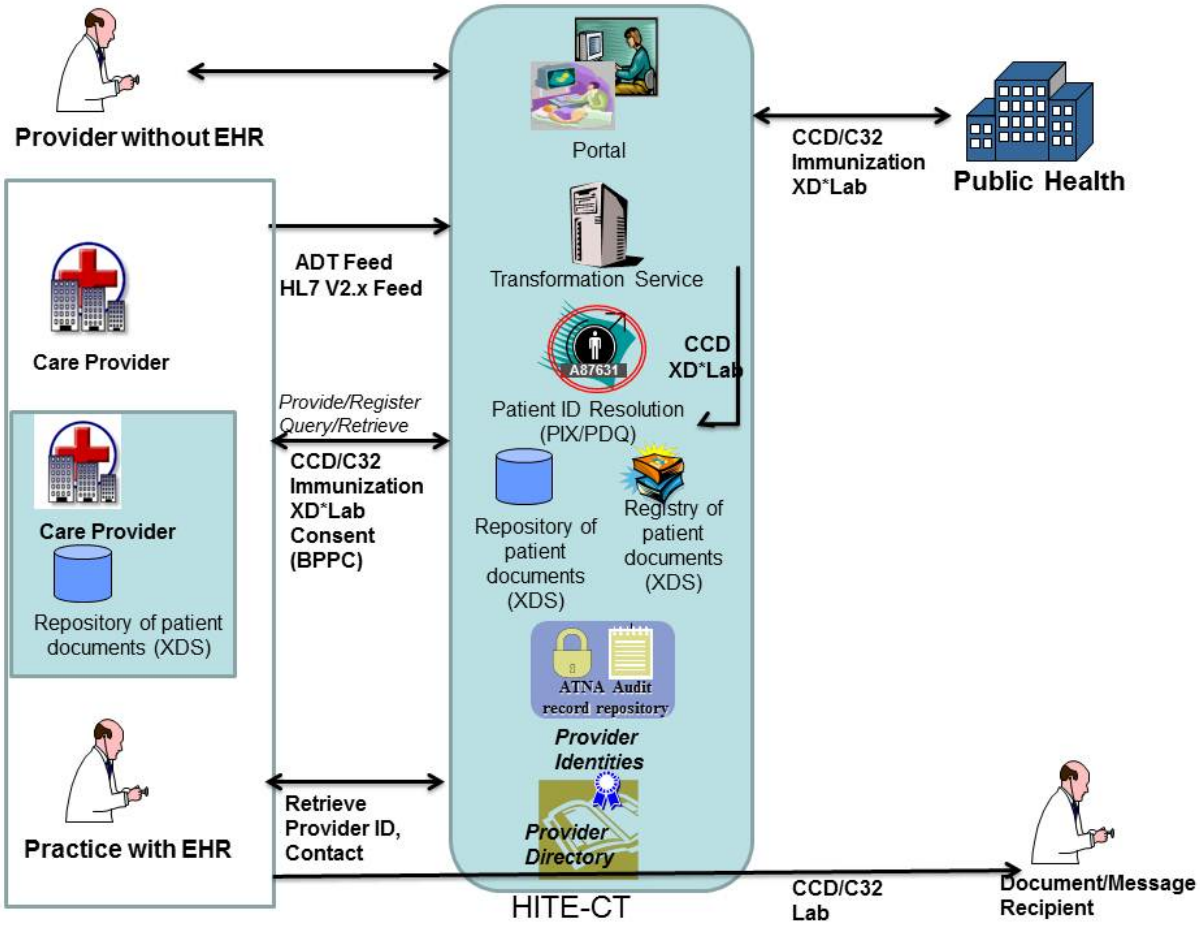
HITE-CT provides transformation interface to public health using a member ADT message or document source (CCD). Organizations MAY choose to subscribe to this transformation service or in addition to other HITE-CT interfaces.

Table 7.2.21-1. Additional Technical Actor Messaging

Actor	Transactions	Optionality	Comments
Immunization Report Source	HL7 VXU 2.5.1	C	Refer to HITE-CT Implementation Guide based on CDC implementation guide.
Laboratory Report	HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1	C	MAY be transformed for document sharing in the Health Information Exchange

8.1.22 XDS Affinity Domain Transaction Diagram

The following transaction diagram is offered in this section indicating the stakeholders, business actors, system actors and transactions.



Glossary:

ADT HL7 message containing Admit/Discharge/Transfer information about a patient

BPPC Consent Document as described by the IHE Basic Patient Privacy Consents

CCD Continuity of Care Document, containing key information about a patient; a type of CDA document

C32 CCD as constrained by HITSP/C32 v2.5 and further constrained by Meaningful Use

CDA HL7 Clinical Document Architecture: a system of XML structured electronic documents to capture information about individual patients

EMPI Enterprise Master Person Index: Stores and manages patient identities from many different external systems

HITE-CT Connecticut Health Information Technology Exchange: The state's system for sharing and routing health data

Connecticut HIE components:

1. Transformation services: The HITE-CT can translate from one code set to another (e.g., from a local laboratory observation code to LOINC); transform a message from one format to another (e.g., from HL7 v. 2.3 MDM to HL7 CCD); and perform various processes to ensure interoperability between disparate systems.
2. Enterprise Master Person Index (EMPI): A core component of HIE sharing, the EMPI keeps track of all patient identities and cross-references them as the HITE-CT receives new identity information from participants. HIE sharing relies upon proper identification of a patient before the HITE-CT associates any clinical data with that patient and shares the data.
3. XDS Registry: Another HIE sharing core component, the Registry is an index of all health information documents available through the HIE. Participants requesting information about a patient first receive metadata from the Registry describing the available documents.
4. XDS Repository: The XDS Registry's metadata points to the XDS Repository, where the actual documents reside. Participants "publish" (save, or store) documents to and "retrieve" them from the Repository. Participants MAY choose to use the Repository in the HITE-CT Infrastructure Service Provider, host their own, or host with another party. In all cases, the HITE-CT Registry maintains pointers to the available documents.
5. Cross Community Access (XCA) is provided for interoperability with Connecticut Regional HIEs and with other HIEs outside of Connecticut.
6. Additional: HITE-CT will continue to add components to the HITE-CT as needs and technology solutions arise.

Connecticut HIE services:

1. Provider Directory Services: The HITE-CT supports a directory of providers and trusted identities for those providers to support direct communications
2. HIE Sharing: Participants share clinical data with one another through the XDS system. Participants MAY "publish" their clinical documents to the HITE-CT-hosted XDS Repository, or they MAY host their own. In either case, each published document is registered with the HITE-CT's XDS Registry, thereby making the document known and accessible to participants. HIE sharing addresses myriad use cases from hospital transfers to specialty referrals.

8.1.23 Cross XDS Affinity Domain Transaction Support

For interstate communications, communications with CT Regional HIEs, and other external communications, this domain will leverage the IHE XCA profile. The remote

node MAY be validated and allowed to join the HITE-CT or the organization MAY be granted remote access via an existing HITE-CT member's system. Transactions across domains with federal entities will be supported with XCA via the "NHIN Connect gateway."

1025

9 Terminology and Content

9.1 Introduction

This introductory section explains any principle areas that the affinity domain specifies for XDS terminology and content, and lists any overall philosophy in defining these.

This HIE interoperability policy defines the identification methods used in the domains including identification of persons (patient, health care professionals, health professionals, etc.), organizations, systems, devices, applications, components, etc. Regional and local HIE's do not have region-specific identification needs that cannot be expressed at the state, national, or international levels to attain community-wide interoperability.

9.1.1 Common Rules for Identifier Construction

This terminology sub-section specifies general rules for constructing identifiers for this XDS affinity domain.

9.1.1.1 Uniqueness

The number must be unique to the name assigning authority. Because the National Provider ID (NPI) does not have a bi-directional 1:1 mapping, in order to retain accountability and consistency, the identifier shall be specified by the jurisdiction under which healthcare privileges are regulated. For the US, this is typically the State or territory.

9.1.1.2 Namespace

HL7 has assigned the following OID root for healthcare provider identities: 2.16.840.1.113883.4.61. HL7 further specifies the next position for each state or territory. Each state or territory conforming to this policy shall register with HL7 the OID subsets for healthcare persons and organizations including organization trading partners. A jurisdiction may choose to recognize an existing OID for a given organization. Such recognized OIDs shall be published under the Local Policy Extensions. Where the practitioner holds multiple medical licenses, the identifier associated with the license under which the electronic information is being capture shall be used.

9.1.1.2.1 Namespace - Connecticut Local Policy Extensions

HL7 has assigned the following OID root for healthcare provider identities in Connecticut: 2.16.840.1.113883.4.61.9. HITE-CT has further sub-divided this root as follows:

2.16.840.1.113883.4.61.9.0 – Reserved for vocabularies

2.16.840.1.113883.4.61.9.0.1 – License Status

2.16.840.1.113883.4.61.9.1 – CT DPH Licensees

2.16.840.1.113883.4.61.9.1.1.1 – CT DPH Licensed Practitioners

2.16.840.1.113883.4.61.9.1.2.1 – CT DPH Licensed Organizations

2.16.840.1.113883.4.61.9.2 – CT DCP Licensees

2.16.840.1.113883.4.61.9.2.1.1 – CT DCP Licensed Practitioners

2.16.840.1.113883.4.61.9.2.2.1 – CT DCP Licensed Organizations

2.16.840.1.113883.4.61.9.3 – CT SOTS Registrants

2.16.840.1.113883.4.61.9.3.1 – Reserved

2.16.840.1.113883.4.61.9.3.2.1 – CT SOTS Registered Organization (Health Care Trading Partners) and CT Provider Organizations not licensed by DPH with EIN number

2.16.840.1.113883.4.61.9.4 – State of Connecticut Insurance Department Licensees

2.16.840.1.113883.4.61.9.4.1.1 – State of CT Insurance Department Licensed Persons

2.16.840.1.113883.4.61.9.4.2.1 – State of CT Insurance Department Licensed Organizations

2.16.840.1.113883.4.61.9.5.2.1 – CT Provider Organizations not licensed by DPH with NPI number

Healthcare Organizations licensed by other agencies (e.g. Department of Children and Families) will be assigned identifiers through CT DPH.

9.1.1.3 Health care Organization Identifiers (Document Source Organization)

Health care organizations shall be identified as follows:

The unique identifier for the healthcare organizations can be expressed as an HL7 OID subset to be specified by the jurisdiction responsible for regulating healthcare professions and registered with HL7. Organization OIDs may have an additional suffix to reflect practice location where a single license is issued to an organization with multiple locations in order to assure uniqueness.

9.1.1.3.1 Connecticut Local Policy Extensions

Given that there is uniqueness across the licensure categories, and that each Connecticut credential type has a numeric definition (expressed as the License prefix), the provider identities shall be constructed from the Connecticut State Department of Public Health (CT DPH) (2.16.840.1.113883.4.61.9.1.2.1) , the version (1), appended by the organization license-class, then by license number:

Table 9.1.1.3.1-1 Connecticut Regulated Healthcare Organization Types

CT DPH Organization License Class Code (PENDING)	CT DPH Organization License Class Code	healthcareFacility TypeCode	healthcareFacility TypeCode DisplayName
0		NA	Unlicensed.
1	**CCNH**	**311ZA0620X**	Chronic and Convalescent Nursing Home
2	**RHNS**	**10400000X**	Rest Home with Nursing Supervision
3	**CCRH**	**313M00000X**	Chronic and Convalescent Nursing Home and Rest Home with Nursing Supervision
4	**RCH**	**311Z00000X**	Residential Care Home
5	**GH**	**282N00000X**	General Hospital.
6	**CH**	**282NC2000X**	Children's Hospital
7	**CDH**	**281P00000X**	Chronic Disease Hospital
8	**PSY**	**283Q00000X**	Hospital for Mentally Ill Persons
9	**OPC**	**261Q00000X**	Outpatient Clinic
10	**ASC**	**261QA1903X**	Outpatient Surgical Facility
11	**----**	**302F00000X**	Outpatient HMO
12	**HEMO**	**261QE0700X**	Outpatient Dialysis Unit
13	**MATH**	**311Z00000X**	Maternity Home
14	**MHDT**	**261QM0801X**	Mental Health Day Treatment Facility
15	**MHIT**	**320800000X**	Mental Health Intermediate Treatment Facility
16	**POCA**	**261QM0801X**	Psychiatric Outpatient Clinic for Adults
17	**MHRL**	**3104A0625X**	Mental Health Residential Living Center
18	**ALSA**	**310400000X**	Assisted Living Services Agency
19	**MHCR**	**320800000X**	Mental Health Community Residence
20	**SA**	**324500000X**	Facility for the Care or Treatment of

CT DPH Organization License Class Code (PENDING)	CT DPH Organization License Class Code	healthcareFacility TypeCode	healthcareFacility TypeCode DisplayName
			Substance Abusive or Dependent Persons
21	**HHC**	**251E00000X**	Home Health Care Agency
22	**HHHA**	**251E00000X**	Homemaker-Home Health Aide Agency
23	**RCC**	**261QR0800X**	Recovery Care Center
24	**FP**	**261QF0050X**	Family Planning Clinic
25	**INF**	**261QS1000X**	Infirmary Operated by an Educational Institution
26	**MAT**	**282NW0100X**	Maternity Hospital
27	**WCC**	**261QC1500X**	Well Child Clinic
28	**CLAB, RLAB**	**291U00000X**	Laboratory
29	**NA**	**322D00000X**	Family Care Group Homes
30	**HSPC**	**315D00000X**	Inpatient Hospice
31	**NHMG**	**PENDING**	Nursing Home Management Company
32		**NA**	Funeral Home
33	C	**261QE0002X**	Certified EMS Organization
34	VEH	**3416L0300X**	Emergency Ambulance
35	VEH	**3416S0300X**	Emergency Boat
36	VEH	**3416A0800X**	Emergency Helicopters
37	VEH	**3416L0300X**	Emergency Coach
38	VEH	**261QE0002X**	Non-Transporting Emergency Medical Service
39	L	**261QE0002X**	Licensed EMS Organization
40	FR	**261QE0002X**	First Responder EMS Organization
41	SR	**261QE0002X**	Supplemental Responder EMS Organization
42	SH	**NA**	Sponsor Hospital

Example

For health care organizations licensed by the CT DPH, where hospital A is licensed as 12345, the OID would be: 2.16.840.1.113883.4.61.9.1.2.1.7.12345

For DCP-regulated organizations: 2.16.840.1.113883.4.61.9.2.2.BB.YY

Where BB reflects the category of license in accordance with the following table:

Table 9.1.1.3.1- 2 Connecticut DCP Regulated Organizations

DCP License Code	Standard Role Code	State Role Description
PENDING		controlled substance laboratory
PENDING		manufacturer of drugs, cosmetics, or medical-devices
PENDING		nonresident pharmacy
PENDING		Pharmacy
PENDING		temporary permit to practice pharmacy
PENDING		wholesaler of drugs, cosmetics, or medical-devices

Where YY reflects the assigned medical license number.

Example

For health care organizations licensed by the department of consumer protection, the HIE OID for the Connecticut State Department of Consumer Protection Licensed Organizations appended by the license-class, then by license number.

2.16.840.1.113883.4.61.9.2.2.xx.yy – CT DCP Licensed Organizations where xx is the code for the license class and yy is the license number.

For Connecticut insurance-regulated organizations: 2.16.840.1.113883.4.61.9.4.2. BB.YY

Where BB reflects the category of license in accordance with the following table:

Table 9.1.1.3.1- 3 Connecticut Insurance Department Regulated Organizations

CT Insurance Department Facility Type Code	Standard role code	State Regulated Organization Type
PENDING		Life, Accident, and Health

CT Insurance Department Facility Type Code	Standard role code	State Regulated Organization Type
PENDING		Fraternal Benefit Society
PENDING		Health Care Centers
PENDING		Reinsurance (life-health)
PENDING		Limited Health Service Organization

Where YY reflects the assigned License number.

Example

For insurance organizations licensed by the State of CT Insurance Department, the HIE OID for the State of CT Insurance Department Licensed Organizations appended by the license-class, then by license number.

2.16.840.1.113883.4.61.9.4.2.xx.yy – State of CT Insurance Department Licensed Organizations where xx is the code for the license class and yy is the license number.

Example

If the health care organization is not licensed as a health care organization, insurance organization or an organization licensed by the Department of Consumer Protection, the HIE OID for the Connecticut Secretary of State Registered Organizations appended by the organization-class, then by registration number.

2.16.840.1.113883.4.61.9.3.2.xx.yy – CT DCP Licensed Organizations CT SOC Registered Organization (Health Care Trading Partners) where xx is the code for the registration class and yy is the registration number.

9.1.1.4 Person Identifiers (Document Author, Authenticator, Provider, Patient)

Health care providers shall be identified as follows:

The unique identifier for the regulated health care providers can be expressed as an OID:

For CT DPH-issued licenses: 2.16.840.1.113883.4.61.9.1.1.AA.YY

Where AA reflects the category of license in accordance with the following table:

Table 9.1.1.4-1 Connecticut CT DPH Regulated Professions

CT License Code	Standard Role code (SNOMED)	State Role (standard role concept – ASTM E1986)	Description
PENDING	46255001	Pharmacist	An individual licensed by the appropriate state regulatory agency to engage in the practice of pharmacy. The practice of pharmacy includes, but is not limited to, assessment, interpretation, evaluation, and implementation, initiation, monitoring or modification of medication and or medical orders; the compounding or dispensing of medication and or medical orders; participation in drug and device procurement, storage, and selection; drug administration; drug regimen reviews; drug or drug-related research; provision of patient education and the provision of those acts or services necessary to provide medication therapy management services in all areas of patient care. Source: Adapted from National Association of Boards of Pharmacy Model State Pharmacy Act, Article 1, Section 104. [1/1/2006: definition modified, source modified]
PENDING		Nuclear Pharmacist	A licensed pharmacist who has demonstrated specialized knowledge and skill in procurement, compounding, quality control testing, dispensing, distribution, and monitoring of radiopharmaceuticals. Source: Specialty certification and recertification program administered by Board of Pharmaceutical Specialties, www.bpsweb.org [7/1/2006: modified title, added definition]
1	112247003	Medical Doctor	Parent entry: A broad category grouping state licensed providers in allopathic or osteopathic medicine whose scope of practice is determined by education.
1	80584001	Medical Doctor Psychiatry	A Psychiatrist specializes in the prevention, diagnosis, and treatment of mental disorders, emotional disorders, psychotic disorders, mood disorders, anxiety disorders, substance-related disorders, sexual and gender identity disorders and adjustment disorders. Biologic, psychological, and social components of illnesses are explored and understood in treatment of the whole person. Tools used may include diagnostic laboratory tests, prescribed medications, evaluation and treatment of psychological and interpersonal problems with individuals and families, and intervention for coping with stress, crises, and other problems. Source: The American Board of Psychiatry and Neurology, Inc. [1/1/2007: new definition]
1	56466003	Medical Doctor Public Health	Public health and general preventive medicine focuses on promoting health, preventing disease, and managing the health of communities and defined populations. These practitioners combine population-based public health skills with knowledge of primary, secondary, and tertiary prevention-oriented clinical practice in a wide variety of settings. Source: American Board of Medical Specialties, 2007. www.abms.org [7/1/2007: definition added, source added] Additional Resources: American Board of Preventive Medicine, 2007.

CT License Code	Standard Role code (SNOMED)	State Role (standard role concept – ASTM E1986)	Description
			http://www.abprevmed.org/. American Osteopathic Board of Preventive Medicine, 2007. https://www.do-online.org/index.cfm?PageID=edu_main&au=D&SubSubPageID=crt_speclist&SubPageID=crt_main
1	76231001	Osteopathic Physician	A broad category grouping state licensed providers in allopathic or osteopathic medicine whose scope of practice is determined by education.
2	106289002	Dentist	A dentist is a person qualified by a doctorate in dental surgery (D.D.S.) or dental medicine (D.M.D.), licensed by the state to practice dentistry, and practicing within the scope of that license. There is no difference between the two degrees: dentists who have a DMD or DDS have the same education. Universities have the prerogative to determine what degree is awarded. Both degrees use the same curriculum requirements set by the American Dental Association's Commission on Dental Accreditation. Generally, three or more years of undergraduate education plus four years of dental school is required to graduate and become a general dentist. State licensing boards accept either degree as equivalent, and both degrees allow licensed individuals to practice the same scope of general dentistry. Additional post-graduate training is required to become a dental specialist. Source: Council on Dental Education and Licensure, American Dental Association A dentist is a person qualified by a doctorate in dental surgery (D.D.S.) or dental medicine (D.M.D.), licensed by the state to practice dentistry, and practicing within the scope of that license. There is no difference between the two degrees: dentists who have a DMD or DDS have the same education. Universities have the prerogative to determine what degree is awarded. Both degrees use the same curriculum requirements set by the American Dental Association's Commission on Dental Accreditation. Generally, three or more years of undergraduate education plus four years of dental school is required to graduate and become a general dentist. State licensing boards accept either degree as equivalent, and both degrees allow licensed individuals to practice the same scope of general dentistry. Additional post-graduate training is required to become a dental specialist. Source: Council on Dental Education and Licensure, American Dental Association
3	28229004	Optometrist	Doctors of optometry (Ods) are the primary health care professionals for the eye. Optometrists examine, diagnose, treat, and manage diseases, injuries, and disorders of the visual system, the eye, and associated structures as well as identify related systemic conditions affecting the eye. An optometrist has completed pre-professional undergraduate education in a college or university and four years of professional education at a college of optometry, leading to the doctor of

CT License Code	Standard Role code (SNOMED)	State Role (standard role concept – ASTM E1986)	Description
			optometry (O.D.) degree. Some optometrists complete an optional residency in a specific area of practice. Optometrists are eye health care professionals state-licensed to diagnose and treat diseases and disorders of the eye and visual system. Source: American Optometric Association (AOA), approved by the AOA's Board of Trustees, June 21, 2005. [7/1/2006: definition modified]
5		Naturopathic Physician	Diagnoses, treats, and cares for patients, using system of practice that bases treatment of physiological functions and abnormal conditions on natural laws governing human body: Utilizes physiological, psychological, and mechanical methods, such as air, water, light, heat, earth, phototherapy, food and herb therapy, psychotherapy, electrotherapy, physiotherapy, minor and orificial surgery, mechanotherapy, naturopathic corrections and manipulation, and natural methods or modalities, together with natural medicines, natural processed foods, and herbs and nature's remedies. Excludes major surgery, therapeutic use of x ray and radium, and use of drugs, except those assimilable substances containing elements or compounds which are components of body tissues and are physiologically compatible to body processes for maintenance of life. Source: The Federal Dictionary of Occupational Titles, U.S. Department of Labor, Washington, D.C., section #079, 101-014 [7/1/2007: definition changed, source added]
7	3842006	Chiropractic Physician	A provider qualified by a Doctor of Chiropractic (D.C.), licensed by the State and who practices chiropractic medicine –that discipline within the healing arts which deals with the nervous system and its relationship to the spinal column and its interrelationship with other body systems.
8	59944000	Psychologist	psychologist is an individual who is licensed to practice psychology which is defined as the observation, description, evaluation, interpretation, and modification of human behavior by the application of psychological principles, methods, and procedures, for the purpose of preventing or eliminating symptomatic, maladaptive, or undesired behavior and of enhancing interpersonal relationships, work and life adjustment, personal effectiveness, behavioral health, and mental health. The practice of psychology includes, but is not limited to, psychological testing and the evaluation or assessment of personal characteristics, such as intelligence, personality, abilities, interests, aptitudes, and neuropsychological functioning; counseling, psychoanalysis, psychotherapy, hypnosis, biofeedback, and behavior analysis and therapy; diagnosis and treatment of mental and emotional disorder or disability, alcoholism and substance abuse, disorders of habit or conduct, as well as of the psychological aspects of physical illness, accident, injury, or disability; and psychoeducational evaluation, therapy, remediation, and consultation. Psychological services may be rendered to individuals, families, groups and the public. Source: American Psychological Association [1/1/2007:

CT License Code	Standard Role code (SNOMED)	State Role (standard role concept – ASTM E1986)	Description
			modified definition]
9	224609002	Homeopath	A provider who is educated and trained in a system of therapeutics in which diseases are treated by drugs which are capable of producing in healthy persons symptoms like those of the disease to be treated. Treatment requires administering a drug in minute doses. Source: Dorland's Illustrated Medical Dictionary. 26th edition. Philadelphia: W.B. Saunders Company, 1981.
10	224535009	Registered Nurse	(1) A registered nurse is a person qualified by graduation from an accredited nursing school (depending upon schooling, a registered nurse may receive either a diploma from a hospital program, an associate degree in nursing (A.D.N.) or a Bachelor of Science degree in nursing (B.S.N.), who is licensed or certified by the state, and is practicing within the scope of that license or certification. R.N.'s assist patient in recovering and maintaining their physical or mental health. They assist physicians during treatments and examinations and administer medications. (2) A provider who is trained and educated in a formal nursing education program at an accredited school of nursing, passes a national certification examination, and is licensed by the state to practice nursing. The individual provides nursing services to patients or clients in areas such as health promotion, disease prevention, acute and chronic care and restoration and maintenance of health across the life span. Sources: (2) American Nurses Association, American Nurses Credentialing Center, 1996 Certification Catalogue, and Rhea, Ott, and Shafritz, The Facts On File Dictionary of Health Care Management, New York: Facts On File Publications, 1988.
11	159002008	Licensed Practical Nurse	An individual with post-high school vocational training and practical experience in the provision of nursing care at a level less than that required for certification as a Registered Nurse. Requirements for education, experience, licensure, and job responsibilities vary among the states. Source: Rhea, Ott, and Shafritz, The Facts On File Dictionary of Health Care Management, New York: Facts On File Publications, 1988.
12	224571005	Advanced Registered Nurse Practitioner	(1) A registered nurse provider with a graduate degree in nursing prepared for advanced practice involving independent and interdependent decision making and direct accountability for clinical judgment across the health care continuum or in a certified specialty. (2) A registered nurse who has completed additional training beyond basic nursing education and who provides primary health care services in accordance with state nurse practice laws or statutes. Tasks performed by nurse practitioners vary with practice requirements mandated by geographic, political, economic, and social factors. Nurse practitioner specialists include, but are not limited to, family nurse practitioners, gerontological nurse practitioners, pediatric nurse practitioners, obstetric-gynecologic nurse practitioners, and school nurse practitioners. Source: (1) American Nurses' Association, American Nurses Credentialing Center, 1996 Certification Catalogue. (2) Lexicon: Dictionary of Health Care Terms, Organizations and Acronyms for the Era of

CT License Code	Standard Role code (SNOMED)	State Role (standard role concept – ASTM E1986)	Description
			Reform, The Joint Commission on Accreditation of Healthcare Organizations, Oakbrook Terrace, Illinois: 1994, p. 549.
12	224571005	Advanced Practice Registered Nurse (NP, NM, CAN, CNS)	(1) A registered nurse provider with a graduate degree in nursing prepared for advanced practice involving independent and interdependent decision making and direct accountability for clinical judgment across the health care continuum or in a certified specialty. (2) A registered nurse who has completed additional training beyond basic nursing education and who provides primary health care services in accordance with state nurse practice laws or statutes. Tasks performed by nurse practitioners vary with practice requirements mandated by geographic, political, economic, and social factors. Nurse practitioner specialists include, but are not limited to, family nurse practitioners, gerontological nurse practitioners, pediatric nurse practitioners, obstetric-gynecologic nurse practitioners, and school nurse practitioners. Source: (1) American Nurses' Association, American Nurses Credentialing Center, 1996 Certification Catalogue. (2) Lexicon: Dictionary of Health Care Terms, Organizations and Acronyms for the Era of Reform, The Joint Commission on Accreditation of Healthcare Organizations, Oakbrook Terrace, Illinois: 1994, p. 549.
13	26042002	Dental Hygienist	An individual who has completed an accredited dental hygiene education program, and an individual who has been licensed by a state board of dental examiners to provide preventive care services under the supervision of a dentist. Functions that may be legally delegated to the dental hygienist vary based on the needs of the dentist, the educational preparation of the dental hygienist and state dental practice acts and regulations, but always include, at a minimum, scaling and polishing the teeth. To avoid misleading the public, no occupational title other than dental hygienist should be used to describe this dental auxiliary. Source: Comprehensive Policy Statement on Dental Auxiliaries, American Dental Association.
14	36682004	Ancillary Service Providers – Physical Therapist	1) Physical therapists are health care professionals who evaluate and treat people with health problems resulting from injury or disease. PT's assess joint motion, muscle strength and endurance, function of heart and lungs, and performance of activities required in daily living, among other responsibilities. Treatment includes therapeutic exercises, cardiovascular endurance training, and training in activities of daily living. (2) A physical therapist is a person qualified by an accredited program in physical therapy, licensed by the state, and practicing within the scope of that license. Physical therapists treat disease, injury, or loss of a bodily part by physical means, such as the application of light, heat, cold, water, electricity, massage and exercise. They develop treatment plans based upon each patient's strengths, weaknesses, range of motion and ability to function. (3) A health professional who specializes in physical therapy- the health care field concerned primarily with the treatment of disorders with physical agents and methods, such as massage, manipulation, therapeutic exercises, cold, heat (including short-wave, microwave, and ultrasonic diathermy), hydrotherapy, electric stimulation and light

CT License Code	Standard Role code (SNOMED)	State Role (standard role concept – ASTM E1986)	Description
			to assist in rehabilitating patients and in restoring normal function after an illness or injury.
15	NA	Electrologist	
16	106294002	Midwife	A Midwife is a trained professional with special expertise in supporting women to maintain a healthy pregnancy birth, offering expert individualized care, education, counseling, and support to a woman and her newborn throughout the childbearing cycle. A Midwife is a skilled and independent practitioner who has undergone formalized training. Midwives are not required to be nurses and may be trained via multiple routes of education (apprenticeship, workshop, formal classes, or programs, etc., usually a combination). The educational background requirements and licensing requirements vary by state. The Midwife may or may not be certified by a state or national organization. Source: The National Uniform Claim Committee [7/1/2007: title changed, definition changed, source changed]
17	309418004	Audiologist	A specialist in evaluation, habilitation and rehabilitation of those whose communication disorders center in whole or in part in hearing function. Audiologists are autonomous professionals who identify, assess, and manage disorders of the auditory, balance and other neural systems. Audiologists provide audiological (aural) rehabilitation to children and adults across the entire age span. Audiologists select, fit and dispense amplification systems such as hearing aids and related devices. (2) An audiologist is a person qualified by a master's degree in audiology, licensed by the state, where applicable, and practicing within the scope of that license. Audiologists evaluate and treat patients with impaired hearing. They plan, direct and conduct rehabilitative programs with audiotry substitutional devises (hearing aids) and other therapy. Source: (1) American Speech-Language-Hearing Association, (1996, Spring) Scope of practice in Audiology, p. 2
17	309418004	Audiologist	(1) A specialist in evaluation, habilitation and rehabilitation of those whose communication disorders center in whole or in part in hearing function. Audiologists are autonomous professionals who identify, assess, and manage disorders of the auditory, balance and other neural systems. Audiologists provide audiological (aural) rehabilitation to children and adults across the entire age span. Audiologists select, fit and dispense amplification systems such as hearing aids and related devices. (2) An audiologist is a person qualified by a master's degree in audiology, licensed by the state, where applicable, and practicing within the scope of that license. Audiologists evaluate and treat patients with impaired hearing. They plan, direct and conduct rehabilitative programs with audiotry substitutional devises (hearing aids) and other therapy. Source: (1) American Speech-Language-Hearing Association, (1996, Spring) Scope of practice in Audiology, p. 2
18	159026005	Speech-Language	A speech pathologist is a person qualified by a master's degree in speech-language pathology, and where applicable, licensed by the

CT License Code	Standard Role code (SNOMED)	State Role (standard role concept – ASTM E1986)	Description
		Pathology	state and practicing within the scope of the license. Also, known as speech therapist, a speech pathologist evaluates patients with language and speech impairments or disorders, whether arising from physiological and neurological disturbances, defective articulation or foreign dialects, and conducts remedial programs designed to restore or improve their communication efficacy. Speech pathologists assess and treat persons with speech, language, voice, and fluency disorders.
19	159034004	Podiatric Physician	A podiatrist is a person qualified by a Doctor of Podiatric Medicine (D.P.M.) degree, licensed by the state, and practicing within the scope of that license. Podiatrists diagnose and treat foot diseases and deformities. They perform medical, surgical and other operative procedures, prescribe corrective devices and prescribe and administer drugs and physical therapy.
21	158970007	Dental Conscious Sedation Permit	
22	158970007	Dental Anesthesia/Conscious Sedation Permit	
23	22515006	Physician Assistant	A physician assistant is a person who has successfully completed an accredited education program for physician assistant, is licensed by the state and is practicing within the scope of that license. Physician assistants are formally trained to perform many of the routine, time-consuming tasks a physician can do. In some states, they may prescribe medications. They take medical histories, perform physical exams, order lab tests and x-rays, and give inoculations. Most states require that they work under the supervision of a physician.
26	442867008	Respiratory Care	A Registered Respiratory Therapist (RRT) is an advanced therapist who has passed standardized written and clinical simulation examinations administered by the National Board for Respiratory Care (NBRC). In addition, to the certified therapist (CRT) entry level skills, RRTs have advanced education and training in patient assessment, in the development and modification of patient care plans, and in assuring the appropriate utilization of respiratory care resources. An RRT is a graduate of an associate or baccalaureate degree producing educational programs approved by the Commission on Accreditation of Allied Health Education Programs (CAAHEP) and where applicable, is licensed by the state and is practicing within the scope of that license.
27	224596008	Marital and Family Therapist	
28	159017007	Diagnostic Radiological Physicist	A radiological physicist deals with the diagnostic and therapeutic applications of roentgen rays, gamma rays from sealed sources, ultrasonic radiation and radio-frequency radiation, as well as the equipment associated with their production and use, including

CT License Code	Standard Role code (SNOMED)	State Role (standard role concept – ASTM E1986)	Description
			radiation safety. Source: American Board of Medical Specialties, 2007. www.abms.org [7/1/2007: definition added, source added] Additional Resources: American Board of Radiology, 2007. http://www.theabr.org/. Board certification for Medical Doctors (MDs) is provided by the American Board of Radiology.
28	159018002	Therapeutic Radiological Physicist	
28	159016003	Medical Nuclear Radio Physicist	A radiologist who is involved in the analysis and imaging of radionuclides and radiolabeled substances in vitro and in vivo for diagnosis and the administration of radionuclides and radiolabeled substances for the treatment of disease. Source: American Board of Medical Specialties, 2007. www.abms.org [7/1/2007: definition added, source added] Additional Resources: American Board of Radiology, 2007. http://www.theabr.org/. American Osteopathic Board of Radiology, 2007. https://www.do-online.org/index.cfm?PageID=edu_main&au=D&SubSubPageID=crt_speclist&SubPageID=crt_main Board certification for Medical Doctors (MDs) is provided by the American Board of Radiology. Board certification for Doctors of Osteopathy is provided by the American Osteopathic Board of Radiology.
29	45419001	Massage Therapist	An individual trained in the manipulation of tissues (as by rubbing, stroking, kneading, or tapping) with the hand or an instrument for remedial or hygienic purposes.
36	159741001	Nursing Home Administrator	An individual, often licensed by the state, who is responsible for the management of a nursing home. Source: Lexikon: Dictionary of Health Care Terms, Organizations, and Acronyms for the Era of Reform, Joint Commission on Accreditation of Healthcare Organizations, Oakbrook Terrace, IL, 1994, p. 552.
37	309421002	Hearing Aid Specialists	Individuals who test hearing for the selection, adaptation, fitting, adjusting, servicing, and sale of hearing aids. Hearing Instrument Specialist is a designation provided individuals who qualify by the National Hearing Aid Society
38	159023002	Optician	parent definition: A broad category grouping different kinds of technologists and technicians. See individual definitions.

CT License Code	Standard Role code (SNOMED)	State Role (standard role concept – ASTM E1986)	Description
43	171100000X	Acupuncturist	An acupuncturist is a person who performs ancient therapy for alleviation of pain, anesthesia and treatment of some diseases. Acupuncturists use long, fine needles inserted into specific points in order to treat painful conditions or produce anesthesia.
44	446701002	Licensed Alcohol and Drug Counselor	
45	446701002	Certified Alcohol and Drug Counselor	
46	310190000	Mental Health Counselor	parent definition: A provider who is trained and educated in the performance of behavior health services through interpersonal communications and analysis. Training and education at the specialty level usually requires a master's degree and clinical experience and supervision for licensure or certification.
47	106290006	Veterinarian	
48	80546007	Ancillary Service Providers – Occupational Therapy	An occupational therapist is a person qualified by completion of an approved program in occupational therapy, licensed by the state and practicing within the scope of that license, or where licensure does not exist, certified by the American Occupational Therapy Certification Board. An occupational therapist evaluates the self-care, work and leisure performance skills of well and disabled clients and plans and implements programs to restore, develop or maintain the task performance skills necessary for daily living and for the client's particular occupational role.
49	224587008	Occupational Therapy Assistant	An Occupational Therapy assistant: provides medically prescribed occupational therapy services under the supervision of a registered occupational therapist to promote rehabilitation of patients in the hospital, home, schools and other settings; has completed a 2-year associate degree or one of the limited number of certificate programs; has met the qualifications as determined by the representative assembly and thus is entitled to use the term Certified occupational therapy assistant. Source: Valerie Walker, COTA Program Specialist, Practice Dept., Chronicle Guidance publications, American Occupational Therapy Association
54	2255A2300X	Athletic Trainer	Athletic trainers are allied health care professionals who work in consultation with or under the direction of physicians, and specialize in the prevention, assessment, treatment and rehabilitation of injuries and illnesses. Currently, the entry-level employment requirements are a bachelor's degree with a major in athletic training from an accredited university or college. A majority of athletic trainers hold advanced degrees. National board certification is generally required as a condition of state licensure and employment. Most states regulate athletic trainers, and they practice within the scope of that license or regulation. Clinical practice includes emergency care, rehabilitation, reconditioning, therapeutic exercise, wellness

CT License Code	Standard Role code (SNOMED)	State Role (standard role concept – ASTM E1986)	Description
			programs, exercise physiology, kinesiology, biomechanics, nutrition, psychology and health care administration.
58	106328005	Clinical Social Worker	Parent definition: A clinical social worker is a person who is qualified by a master of Social Work (M.S.W.) degree, licensed, certified or registered by the state as a social worker and practicing within the scope of that license. A social worker provides assistance and counseling to patients and their families and dealing with social, emotional and environmental problems.
59	159033005	Dietetics/Nutritionist	A registered dietician (RD) is a food and nutrition expert who has successfully completed a minimum of a bachelor's degree at a US regionally accredited university or college and course work approved by The American Dietetic Association (ADA); an ADA-accredited or approved, supervised practice program, typically 6 to 12 months in length; a national examination administered by the Commission on Dietetic Registration; and continuing professional educational requirements to maintain registration.
62	73265009	Nurses Aide	
63	309404006	Physical Therapist Assistant	(1)Physical therapist assistants are skilled health care providers who are graduates of a physical therapist assistant associate degree program accredited by an agency recognized by the Secretary of the U.S. Department of Education or Council on Postsecondary Accreditation, who assists the physical therapist in providing physical therapy. The supervising physical therapist is directly responsible for the actions of the physical therapist assistant. The PTA performs physical therapy procedures and related tasks that have been selected and delegated by the supervising physical therapist. Duties of the PTA include assisting the physical therapist in implementing treatment programs, training patients in exercised and activities of daily living, conducting treatments, and reporting to the physical therapist on the patient's responses. In addition to direct patient care, the PTA may also perform such functions as patient transport, and clinic or equipment preparation and maintenance. Currently more than half of all states require PTAs to be licensed, registered or certified. (2) An individual who works under the supervision of a physical therapist to assist him or her in providing physical therapy services. A physical therapy assistant may, for instance, help patients follow an appropriate exercise program that will increase their strength, endurance, coordination, and range of motion and train patients to perform activities of daily life. Source: (1) American Physical Therapy Association, P.O. Box 37257, Washington, D.C. 20013. (2) Lexikon: Dictionary of Health Care Terms, Organizations and Acronyms for the Era of Reform, Joint Commission on Accreditation of Healthcare Organizations, Oakbrook Terrace, IL: 1994, p. 612
69	397897005	Medical Response Technician	DESCRIPTION PENDING

CT License Code	Standard Role code (SNOMED)	State Role (standard role concept – ASTM E1986)	Description
70	397897005	Emergency Medical Technician	DESCRIPTION PENDING
71	397897005	Emergency Medical Technician-Intermediate	DESCRIPTION PENDING
72	397897005	Paramedic	DESCRIPTION PENDING
73	397897005	Emergency Medical Services - Instructor	DESCRIPTION PENDING
78	159022007	Optician Apprentice	DESCRIPTION PENDING
83	265939002	Perfusionist	DESCRIPTION PENDING
86	397897005	Medical Response Technician - CSP	DESCRIPTION PENDING

For DCP-issued licenses: 2.16.840.1.113883.4.61.9.2.1.BB.YY

Where BB reflects the category of license in accordance with the following table:

Table 9.1.1.4- 2 Connecticut DCP Regulated Professions

License Code	Standard Role	State Role Description
PENDING	46255001	Pharmacist
PENDING	159014000	pharmacy intern
PENDING	159040006	pharmacy technician

Where YY reflects the assigned medical license number.

Example: For health care providers licensed by the department of consumer protection, the HIE OID for the Connecticut State Department of Consumer Protection appended by the license-class, then by license number.

9.1.1.4.1 Sponsored Health Care Provider Identities

The unique identifier for the sponsored health care providers can be expressed as an HL7 OID subset to be specified by the jurisdiction responsible for regulating healthcare professions and registered with HL7.

9.1.1.4.1.1 Sponsored Health Care Provider Identities - Connecticut Local Policy Extensions

For CT DPH-issued licensed sponsors: 2.16.840.1.113883.4.61.9.1.2.CC.DD.ZZ

Where CC indicates the license category of the organization sponsoring the individual in accordance with table 9.1.1.3.1-1. Where DD indicates the license number of the organization sponsoring the individual, and where ZZ is the unique ID assigned by the sponsoring organization to the sponsored individual. If the sponsored person is an employee, then the health care organization ID employee id

For DCP-issued licensed sponsors: 2.16.840.1.113883.4.61.9.2.2.CC.DD.ZZ

Where CC indicates the license category of the organization sponsoring the individual in accordance with table 9.1.1.3.1-2. Where DD indicates the license number of the organization sponsoring the individual, and where ZZ is the unique ID assigned by the sponsoring organization to the sponsored individual. If the sponsored person is an employee, then the health care organization ID employee id

For CT Insurance Department -issued licensed sponsors: 2.16.840.1.113883.4.61.9.4.2.CC.DD.ZZ

Where CC indicates the license category of the organization sponsoring the individual in accordance with table 9.1.1.3.1-3. Where DD indicates the license number of the organization sponsoring the individual, and where ZZ is the unique ID assigned by the sponsoring organization to the sponsored individual. If the sponsored person is an employee, then the health care organization ID employee id

Example: For consumers, health care consumer or patient shall be identified as follows:

A sponsored/affiliated identity will be issued to consumers with a designated health care-related identification number (e.g. insurance number, provider-issued number). A non-affiliated identity may be issued to a consumer in the absence of a designated identification number. HITE-CT policy will recognize a designated health care-related

identification number for a sponsored/affiliated identity with an application and subscriber agreement authorized by the Local Registration Authority. The identification for the consumer shall be constructed as indicated above based upon the type of sponsoring organization.

9.1.1.4.2 System Identifiers

The unique identifier for systems can be expressed as an HL7 OID subset to be specified by the jurisdiction responsible for regulating healthcare professions and registered with HL7.

9.1.1.4.2.1 System Identifiers- Connecticut Local Policy Extensions

System identifiers are constructed using, the organization identifier as indicated above followed by their certificate issuing authority/MD5. Not currently required in Connecticut.

9.1.1.4.3 Device Identities

Devices shall be identified by either the assigned external IP address or by the DNS name.

9.1.1.4.4 License Restriction Classes

The coded values shall be used to indicate license restriction classes where this information is maintained in directory or certificate attributes as part of the practitioner identity attributes.

9.1.1.4.4.1 License Restriction Classes- Connecticut Local Policy Extensions

This coded value set is identified by OID: 2.16.840.1.113883.4.61.9.0.1

Table 9.1.1.4.4.1-1 Connecticut License Restriction Classes

CodeDataValue	codeDataFreeText	Description
01	active	PENDING
02	denied	PENDING
03	disciplined	PENDING
04	inactive	PENDING
05	lapsed	PENDING
06	pending	PENDING
07	revoked	PENDING

08	surrendered	PENDING

9.1.1.5 Validity

Validity of the digital identity shall be the date of license expiration + 90 days reflecting the 90-day grace period (or grace period permitte by licensing authority if not DPH) for renewal permissible by state practitioner licensing before the license “lapses.”

9.2 Data Content Rules and Restrictions

This section define general rules and restrictions regarding the usage of certain general types of data, such as patient demographic information. Match thresholds shall be optimized accoring to the demographic make-up of the patients managed by the PIX manager and/or other analytical computations informing the demogrphic make-up of the Connecticut patient population. Match exception resolution processes will be specified by standard operating procedures that offer distributed management options to allow patient identity sources to resolve match exceptions.

9.2.1 Example of Rules and Restrictions for Patient Demographic Data

The following table describes restrictions on the usage of patient demographic attributes for the patient identity feed transaction and corresponding PIX Manager attributes. Some patient demographic attributes MAY be required for matching and thus specified as required, whereas the collection and processing of others MAY be prohibited by jurisdiction, law, or policy.

Table 8.3.1-1. Example of Patient Demographic Data Restrictions

Data Element	Transactions	
	Patient Identity Feed (Regulatory Restrictions – i.e. HITSP)	**Patient Identity Feed (XDS Affinity Domain - HIE)**
Set ID - Patient ID	R (‘1’)	R (‘1’)
Patient ID	O	O
Patient Identifier List	R	R
Medical Record Number/Patient_ID Assigning Authority	R	R
Medical Record Number/Patient_ID Assigning Authority Universal ID	R	R
Medical Record Number/Patient_ID Assigning Authority Universal ID Type	R (‘ISO’)	R (‘ISO’)
Medical Record Number/Patient_ID	R	R
Alternate Patient ID	O	O

Data Element	Transactions	
	Patient Identity Feed (Regulatory Restrictions – i.e. HITSP)	**Patient Identity Feed (XDS Affinity Domain - HIE)**
Patient Name	R	R (Must use Full Legal Name)
Patient First Name	C (Required if known)	R (Must use Full legal name)
Patient Middle Name	C (Required if known)	C (Required if known) (Must use Full Legal Name)
Patient Last Name	R	R (Must use Full legal name)
Patient Family Name	R	R (Must use Ful Legal Name)
Patient Suffix	C (Required if known)	C (Required if known) (Must use Full legal name)
Name Prefix/Title	C (Required if known)	C (Required if known) (Must use Full legal name)
Name Type Code	R	R
Mother's Maiden Name	C (Required if known)	C (Required if known)
Mother's Maiden Name Family Name	C (Required if known)	C (Required if known)
Mother's Maiden Name Surname	C (Required if known)	C (Required if known)
Patient DOB	R	R
Gender	C (Required if known)	C (Required if known)
Patient Previous Names	O	O
Race	O	N (Not Permitted) PENDING REVIEW
Patient Address	O	C (Required if known)
Patient Home Street Address	O	C (Required if known)
Patient home Street or mailing Address	O	C (Required if known)
Street Name	O	C (Required if known)
Dwelling Number	O	C (Required if known)
Other Designation (second line of street address)	O	C (Required if known)
Patient Home City	O	C (Required if known)
Patient Home State/Province	O	C (Required if known)
Patient Zip	O	C (Required if known)
Country	O	C (Required if known)
Address type	O	O
County Code	O	O
Patient Daytime Phone	O	O
Patient Daytime Phone country code	O	O
Patient Daytime Phone Area/City Code	O	O
Patient Daytime Phone Local Number	O	O

Data Element	Transactions	
	Patient Identity Feed (Regulatory Restrictions – i.e. HITSP)	**Patient Identity Feed (XDS Affinity Domain - HIE)**
Patient Daytime Phone Extension	O	O
Patient Daytime Phone Any other text	O	O
Work Telephone	R2	R2
Primary Language[l1]	O	C (Required if known)
Marital Status	O	O
Religion	O	O
Patient Account Number	O	O
Patient SSN[l2]	O	N (Not Permitted) PENDING REVIEW
Patient Driver License	O	O
Mother's Identifier	O	O
Patient Ethnicity	O	N (Not Permitted) PENDING REVIEW
Birth Place	O	O
Multiple Birth Indicator	O	O
Birth Order	O	O
Citizenship	O	O
Veteran's Military Status[l3]	O	O
Nationality	O	O
Deceased Data/Time	O	O
Deceased Indicator	O	O

9.3 XDS Registry Metadata

This section defines all ways in which the XDS affinity domain refines metadata attributes of an XDS submission set or an XDS Folder.

9.3.1 XDS Document Entry Metadata

The following table lists all of the submission set metadata attributes from ITI TF-2: Table 3.14.4.1-6 whose use is refined in any way.

Submission Set Metadata Attribute Definitions

XDSDocumentEntry Attribute	Refinement of Attribute	Source/Query (Bold and Underline if refined)	Data Type

XDSDocumentEntry Attribute	Refinement of Attribute	Source/Query (Bold and Underline if refined)	Data Type
authorInstitution	Represents a specific health care facility under which the human and/or machines authored the document. A specific case is that of homecare.	R2/R	XON Refer to 9.3.1.1 for the specification of this attribute.
authorPerson	Represents the humans and/or machines that authored the document within the authorInstitution. The document author may be the patient itself. This attribute may be multi-valued.	R2/R	XCN Refer to 9.3.1.2 for the specification of this ttribute
authorRole	A code that represents the role of the author with respect to the patient when the document was created. This specification references ISO TS21298	R2/O	Refer to 9.3.1.3 Table 9.3.1.3-1, 9.3.1.3-2 Standard Role Codes for the specification of this ttribute
authorSpecialty	Represents a specific specialty within a health care facility under which the human and/or machines authored the document. This specification references ISO TS21298 specialty codes.	R2/O	Refer to 9.3.1.4 for the specification of this attribute.
classCode	The code specifying the particular kind of document (e.g. prescription, discharge summary, report). It is suggested that the XDS affinity domain draws these values from a coding scheme.	R/R	Refer to 9.3.1.5 for the specification of this attribute.
classCode DisplayName	The name to be displayed for communicating to a human the meaning of the class code. See class code for example.	R/P	Refer to 9.3.1.5 for the specification of this attribute.

XDSDocumentEntry Attribute	Refinement of Attribute	Source/Query (Bold and Underline if refined)	Data Type
confidentialityCode	The code specifying the level of confidentiality of the XDS document. These codes are specific to an affinity domain. Enforcement and issues related to highly sensitive documents are beyond the scope of XDS (see security section). These issues are expected to be addressed, in later years. Confidentiality code is part of a codification scheme and value set enforced by the document registry.	R/P	Refer to 9.3.1.6 for the specification of this attribute.
creationTime	Represents the time the author created the document in the document source. No specialization.	R/R	DTM
healthcareFacility TypeCode	This code represents the type of organizational setting of the clinical encounter during which the documented act occurred. In some cases, the setting of the encounter is inherent in the typeCode, such as "Diabetes Clinic Progress Note". Health careFacility typeCode shall be equivalent to or further specialize the value inherent in the typeCode; for example, where the typeCode is simply "Clinic Progress Note" and the value of health careFacility typeCode is "private clinic". The value shall not conflict with the value inherent in the typeCode, as such a conflict would create an ambiguous situation.	R/R	Refer to 9.3.1.7 for the specification
health careFacility TypeCodeDisplay Name	The name to be displayed for communicating to a human the meaning of the health careFacility typeCode See health careFacilityTypeCode for an example.	R/P	Refer to 9.3.1.7 for the specification

XDSDocumentEntry Attribute	Refinement of Attribute	Source/Query (Bold and Underline if refined)	Data Type
legalAuthenticator	Represents a participant who has legally authenticated or attested the document within the authorInstitution. Legal authentication implies that a document has been signed manually or electronically by the legalAuthenticator. This attribute may be absent if not applicable.	O/O	XCN Refer to 9.3.1.8 for the specification.
patientId	The patient Id represents the subject of care medical record identifier as selected by the document source. This identifier shall be from the assigning authority domain supporting the affinity domain in which the document registry operates. It shall contain two parts: Authority domain Id (enforced by the registry) . An Id in the above domain. The value of the patientId shall be the same for all new documents of a submission set.	R/R	CX No specialization.
practiceSettingCode	The code specifying the clinical specialty where the act that resulted in the document was performed (e.g. familly practice, laboratory, radiology). It is suggested that the XDS affinity domain draws these values from a coding scheme providing a coarse level of granularity (about 10 to 100 entries).	R/R	Refer to 9.3.1.9 for the specification.

XDSDocumentEntry Attribute	Refinement of Attribute	Source/Query (Bold and Underline if refined)	Data Type
practiceSettingCode DisplayName	The name to be displayed for communicating to a human the meaning of the practiceettingode. See practiceettingode for an example.	R/P	Refer to 9.3.1.9 for the specification
sourcePatientId	The source patient Id represents the subject of care medical record Identifier (e.g. Patient Id) in the local patient Identifier Domain of the Document Source. It shall contain two parts: Authority Domain Id. An Id in the above domain (e.g. Patient Id). This source patient Id is not intended to be updated once the document is registered (just as the document content and metadata itself will not be updated without replacing the previous document). As this source patient Id may have been merged by the source actor, it may no longer be in use within the document source (EHR-CR). It is only intended as an audit/checking mechanism and has occasional use for document consumer actors.	R/P	CX No specialization.

XDSDocumentEntry Attribute	Refinement of Attribute	Source/Query (Bold and Underline if refined)	Data Type
sourcePatientInfo	This attribute contains demographics information of the patient to whose medical record this document belongs, as the document source knew it at the time of submission. This information typically includes: the patient first and last name, sex, and birth date. The clinical affinity domain policies may require more specific information and format. This patient information is not intended to be updated, once the document is registered (just as the document content and metadata itself will not be updated without replacing the previous document). As source patient info may have been updated by the source actor, it may no longer be in use within the document source (EHR-CR). It is only intended as an audit/checking mechanism and has occasional use for document consumer actors.	R2/P	No specialization.

9.3.1.1 Refinement of authorInstitution

This sub-section for the authorInstitution Metadata Attribute should state how the values for this attribute are specified for this XDS Affinity Domain.

This sub-section for the authorInstitution Metadata attribute states how the values for this attribute are specified for this affinity domain.

HL7 Component Table - XON – for authorInstitution

SEQ	DT	OPT	COMPONENT NAME	COMMENTS
1	ST	O	Organization name	See section 9.1.1.3 for details
2	IS	O	Organization name type code	See section 9.1.1.3 for details
3	NM	R	ID number	See section 9.1.1.3 for details

[2] Certain segments are required, see definition.

SEQ	DT	OPT	COMPONENT NAME	COMMENTS
4	NM	O	Identifier check digit	
5	ID	O	Check digit scheme	
6	HD	O	Assigning authority	
7	ID	O	Identifier type code	
8	HD	O	Assigning facility	
9	ID	O	Name representation code	
10	ST	O	Organization identifier	

9.3.1.1.1 Refinement of Organization Name component

The authorInstitution shall be populated with the organization name as they are known by the licensing authority (see section 9.1.1.2 for the state licensing authorities associated with health care entities and supporting organizations). This attribute shall be populated so as to distinguish location where the organization has multiple locations.

9.3.1.1.2 Specification of Organization Type Code Component of authorInstitution

The authorInstitution organization type code shall be populated with the standard role code found in Table 9.1.1.3.1-1 " Connecticut Regulated Healthcare Organization Types".

9.3.1.1.3 Specification of ID Number Component of authorInstitution

The authorInstitution shall be populated with the unique OID of the organization as specified in section 9.1.1.3.1.

9.3.1.1.4 Specification of Identifier Check Digit Component of authorInstitution

NA (PENDING VERIFICATION FROM DCP whether license numbers include a check digit)

9.3.1.1.5 Specification of ID of Assigning Authority of authorInstitution

Where the NPI is the referenced identifier then this shall be (Find NPI OID). Where the state identifier is used, then this shall be the OID of the state licensing authority responsible for this organization type (see section 9.1.1.2 for the state licensing authorities associated with health care entities and supporting organizations).

9.3.1.1.6 Specification of Identifier Type Code of authorInstitution

No further stipulation.

9.3.1.1.7 Specification of Assigning Facility of authorInstitution

No further stipulation.

9.3.1.1.8 Specification of Name Representation Code of authorInstitution

No further stipulation.

9.3.1.1.9 Specification of Organization Identifier of authorInstitution

No further stipulation.

9.3.1.2 authorPerson

The authorPerson shall be populated with the OID for the author of the document as they are known by the licensing authority (see section 9.1.1.2 for the state licensing authorities associated with health care entities and supporting organizations).

9.3.1.3 authorRole

A code that represents the role of the individual author when the document was created. This shall use the structural role vocabulary in section 9.1.1.4 Table 9.1.1.4-1, 9.1.1.4-2.

Where the authorRole is available only at the granularity of the institution, Functional roles coded values MAY be drawn from vocabulary Identification: iso (1) standard (0) functional and structural roles (21298) functional role vocabulary (4)

role_identifier	role_name	Description
01	Subject of care	principal data subject of the electronic health record
02	Subject of care agent	e.g. parent, guardian, carer, or other legal representative
03	Personal healthcare professional	healthcare professional or professionals with the closest relationship to the patient, often the patient's GP
04	Privileged healthcare professional	nominated by the subject of care OR nominated by the healthcare facility of care (if there is a nomination by regulation, practice, etc. such as an emergency over-ride)
05	Healthcare professional	party involved in providing direct care to the patient
06	Health-related professional	party indirectly involved in patient care, teaching, research, etc.)
07	Administrator	any other parties supporting service provision to the patient

9.3.1.4 authorSpecialty

Represents a specific specialty within a health care facility under which the human and/or machines authored the document. This SHALL use the specialty codes specified in table 9.3.1.4-1 below with preference to those that correspond to CT recognized specialties as indicated by the mapping table/value set below:

Table 9.3.1.4-1 authorSpecialty Value Set Definition

CT Specialty Code	SNOMED CT ® Concept ID	Concept Name Specialty Area
	408467006	Adult mental illness
20, 75, 113	394577000	Anesthetics
	394578005	Audiological medicine
	421661004	Blood banking and transfusion medicine
	408462000	Burns care
	394579002	Cardiology
	394804000	Clinical cytogenetics and molecular genetics
35, 88, 126	394580004	Clinical genetics
	394803006	Clinical hematology
17, 73, 111	408480009	Clinical immunology
	408454008	Clinical microbiology
	394809005	Clinical neuro-physiology
22, 77, 115	394592004	Clinical oncology
	394600006	Clinical pharmacology
	394601005	Clinical physiology
	394581000	Community medicine
26, 81, 119	408478003	Critical care medicine
64, 69	394812008	Dental medicine specialties
	408444009	Dental-General dental practice
25, 80, 118	394582007	Dermatology
	408475000	Diabetic medicine
	410005002	Dive medicine
	394583002	Endocrinology
21, 27, 76, 82, 114, 120	419772000	Family practice (including Bariatric Medicine)
	394584008	Gastroenterology
	408443003	General medical practice
	394802001	General medicine

CT Specialty Code	SNOMED CT ® Concept ID	Concept Name Specialty Area
18, 19, 23, 51, 74, 78, 101, 112, 116, 138, 154, 155	394915009	General pathology
65	394814009	General practice
	394808002	Genito-urinary medicine
	394811001	Geriatric medicine
	408446006	Gynecological oncology
	394586005	Gynecology
	394916005	Hematopathology
	408472002	Hepatology
	394597005	Histopathology
	394598000	Immunopathology
	394807007	Infectious diseases
32, 86, 124	419192003	Internal medicine
	408468001	Learning disability
	394593009	Medical oncology
	394813003	Medical ophthalmology
	410001006	Military medicine
	394589003	Nephrology
37, 90, 91, 128, 129, 38, 39, 151	394591006	Neurology
	394599008	Neuropathology
41, 93, 131	394649004	Nuclear medicine
	408470005	Obstetrics
42, 94, 132	394585009	Obstetrics and gynecology
31, 43, 85, 95, 123, 133	394821009	Occupational medicine
	422191005	Ophthalmic surgery
44, 96, 134	394594003	Ophthalmology
47, 48, 152, 153	416304004	Osteopathic manipulative medicine
49, 99, 137	418960008	Otolaryngology
	394882004	Pain management
50, 100, 139	394806003	Palliative medicine
141	394588006	Pediatric (Child and adolescent) psychiatry
52, 102, 140	408459003	Pediatric cardiology
52, 102, 140	394607009	Pediatric dentistry
52, 102, 140	419610006	Pediatric endocrinology

CT Specialty Code	SNOMED CT ® Concept ID	Concept Name Specialty Area
52, 102, 140	418058008	Pediatric gastroenterology
52, 102, 140	420208008	Pediatric genetics
52, 102, 140	418652005	Pediatric hematology
52, 102, 140	418535003	Pediatric immunology
52, 102, 140	418862001	Pediatric infectious diseases
52, 102, 140	419365004	Pediatric nephrology
52, 102, 140	418002000	Pediatric oncology
52, 102, 140	419983000	Pediatric ophthalmology
52, 102, 140	419170002	Pediatric pulmonology
52, 102, 140	419472004	Pediatric rheumatology
52, 102, 140	394539006	Pediatric surgery
52, 102, 140	420112009	Pediatric surgery-bone marrow transplantation
55, 105, 140, 144, 16, 72, 110	409968004	Preventive medicine
56, 106,145	394587001	Psychiatry
	394913002	Psychotherapy
	408440000	Public health medicine
57, 158	418112009	Pulmonary medicine
	419815003	Radiation oncology
58, 107, 146, 63	394914008	Radiology
	408455009	Radiology-Interventional radiology
53, 103, 142	394602003	Rehabilitation
	408447002	Respite care
	394810000	Rheumatology
	408450004	Sleep studies
	408476004	Surgery-Bone and marrow transplantation
	408469009	Surgery-Breast surgery
	408466002	Surgery-Cardiac surgery
	408471009	Surgery-Cardiothoracic transplantation
24, 79, 117	408464004	Surgery-Colorectal surgery
	408441001	Surgery-Dental-Endodontics
45, 97, 135	408465003	Surgery-Dental-Oral and maxillofacial surgery
67	394605001	Surgery-Dental-Oral surgery
68	394608004	Surgery-Dental-Orthodontics
70	408461007	Surgery-Dental-Periodontal surgery
71	408460008	Surgery-Dental-Prosthetic dentistry (Prosthodontics)
	408460008	Surgery-Dental-surgical-Prosthodontics
	394606000	Surgery-Dentistry-Restorative dentistry

CT Specialty Code	SNOMED CT ® Concept ID	Concept Name Specialty Area
	408449004	Surgery-Dentistry--surgical
	394608004	Surgery-Dentistry-surgical-Orthodontics
	418018006	Surgery-Dermatologic surgery
	394604002	Surgery-Ear, nose and throat surgery
28, 59, 83, 121, 60, 108, 147, 156	394609007	Surgery-general
	408474001	Surgery-Hepatobiliary and pancreatic surgery
40, 89, 92, 127, 130, 36	394610002	Surgery-Neurosurgery
54, 104, 143	394611003	Surgery-Plastic surgery
	408477008	Surgery-Transplantation surgery
46, 98, 136	394801008	Surgery-Trauma and orthopedics
	408463005	Surgery-Vascular
	419321007	Surgical oncology
	394576009	Surgical-Accident & emergency
	394590007	Thoracic medicine
	409967009	Toxicology
	408448007	Tropical medicine
62, 154	419043006	Urological oncology
61, 109, 148	394612005	Urology
33, 29, 30, 84, 122, 150, 34, 87, 122, 125, 149	394733009	Medical specialty--**OTHER--NOT LISTED**
	394732004	Surgical specialty--**OTHER-NOT LISTED**

9.3.1.5 classCode and classCodeDisplayName

The code specifying the particular kind of document (e.g. prescription, discharge summary, report). It is suggested that the XDS affinity domain draws these values from a coding scheme. These values SHALL be populated with the LOINC code set corresponding to the IHE content profile specification. Where not specified by IHE profile, the value SHALL be drawn from the list below. The classCode and classCodeDisplayName value set includes all LOINC values listed in the table 8.4.1.5-1 below, and all LOINC values whose SCALE is DOC in the LOINC database.

Table 8.4.1.5-1 classCode Value Set Definition

classCode (LOINC CODE)	classCodeDisplayName (LOINC Short Name)	Definition (LOINC Long Common Name)
11369-6	History of Immunization	History of Immunization

classCode (LOINC CODE)	classCodeDisplayName (LOINC Short Name)	Definition (LOINC Long Common Name)
11485-0	Anesthesia Records	Anesthesia records
11486-8	Chemotherapy Records	Chemotherapy records
11488-4	Consultation note	Consult Note
11506-3	Subsequent evaluation note	Provider-unspecified progress note
11543-6	Nursery Records	Nursery records
15508-5	Labor And Delivery Records	Labor and delivery records
18726-0	Radiology Studies	Radiology studies (set)
18761-7	Transfer summarization note	Provider-unspecified transfer summary
18842-5	Discharge summarization note	Discharge summary
26436-6	Laboratory Studies	Laboratory Studies (set)
26441-6	Cardiology Studies	Cardiology studies (set)
26442-4	Obstetrical Studies	Obstetrical studies (set)
27895-2	Gastroenterology Endoscopy Studies	Gastroenterology endoscopy studies (set)
27896-0	Pulmonary Studies	Pulmonary studies (set)
27897-8	Neuromuscular Electrophysiology Studies	Neuromuscular electrophysiology studies (set)
27898-6	Pathology Studies	Pathology studies (set)
28570-0	Procedure note	Provider-unspecified procedure note
28619-5	Ophthalmology Studies	Ophthalmology/optometry studies (set)
28634-4	Miscellaneous Studies	Miscellaneous studies (set)
29749-9	Dialysis Records	Dialysis records
29750-7	Neonatal Intensive Care Records	Neonatal intensive care records
29751-5	Critical Care Records	Critical care records
29752-3	Perioperative Records	Perioperative records
34109-9	Evaluation and management note	Evaluation and management note
34117-2	History and physical note	Provider-unspecified, History and physical note
34121-4	Interventional procedure note	Interventional procedure note
34122-2	Pathology procedure note	Pathology procedure note
34133-9	Summarization of episode note	Summarization of episode note
34140-4	Transfer of care referral note	Transfer of care referral note
34748-4	Telephone encounter note	Telephone encounter note
34775-7	Pre-operative evaluation and management note	General surgery Pre-operative evaluation and management note
47039-3	Admission history and physical note	Inpatient Admission history and physical note

classCode (LOINC CODE)	classCodeDisplayName (LOINC Short Name)	Definition (LOINC Long Common Name)
47042-7	Counseling note	Counseling note
47045-0	Study report	Study report Document
47046-8	Summary of death	Summary of death
47049-2	Communication	Non-patient Communication
57017-6	Privacy Policy	Privacy Policy Organization Document
57016-8	Privacy Policy Acknowledgment	Privacy Policy Acknowledgment Document
56445-0	Medication Summary	Medication Summary Document
53576-5	Personal health monitoring report	Personal health monitoring report Document

9.3.1.6 confidentialityCode

Multiple Security levels are supported by HITE-CT in alignment with ISO TS13606-4 Health informatics — Electronic health record communication — Part 4:Security.

All routine clinical documents SHALL be published with the HITE-CT policy OID: HITECTOID.1.3 Routine Clinical (PENDING) to identify the policy as listed in table 9.3.1.6-1 below.

The following OIDs SHALL be used to identify the sensitivity level in the confidentialityCode of the HITE-CT registered documents:

Table 9.3.1.6-1 confidentialityCode Value Set Definition

HITE-CT Sensitivity Classification OID	HITE-CT Sensitivity Classification Name	Use	ISO TS13606-4 Sensitivity value	ISO TS13606-4 Sensitivity level	Description of intended documents of this sens
1.3.6.1.4.1. 38571.1.1	Care management Administrative	Shall be used for administrative data	Care management	1	RECORD_COMPONENT need to be accessed by administrative staff to subject of care's acc services.
1.3.6.1.4.1. 38571.1.2	Clinical Administrative	Shall be used for clinical care management purposes SHALL be used for recording Patient Privacy Policy Acknowledgement Document where the content of the	Clinical management	2	Less RECORD_COMPONENT need to be accessed by a personnel not all of wh caring for the patient. staff)

		consent itself is not sensitive (opt-in) For consent to share legally protected data, or for Opt-Out documents, the sensitivity level SHALL be set to sensitive			
1.3.6.1.4.1. 38571.1.3	Routine Clinical (Normal)	Shall be used for routine clinical care data Default for normal clinical care access. (i.e. most clinical staff directly caring for the patient should be able to access nearly all of the EHR)	Clinical care	3	Default for normal clinic (i.e. most clinical staff di the patient should be nearly all of the EHR)
1.3.6.1.4.1. 38571.1.4	Legally Protected Sensitive (Restricted)	Shall be used for regulated data requiring specific authorizations. (e.g. mental health, substance abuse, AIDS, and genetics) SHALL be used for Patient Privacy Policy Acknowledgement Documents reflecting consent to share legally protected data, or for Opt-Out documents, the sensitivity level SHALL be set to sensitive	Privileged care	4	Access restricted to a people caring intimately perhaps an immediate senior clinical party. clinical setting needs to b mental health)
1.3.6.1.4.1. 38571.1.5	Patient-identified sensitive (Very Restricted)	Shall be used to indicate data restricted by the patient, but not of the protected class indicated by level 4. Until further notice, data of class 5 shall not be published to the HIE.	Personal care	5	To be shared by the s perhaps with only one people whom they trust accessible to the subject others by one-off authoris
1.3.6.1.4.1. 38571.1.1000	Unspecified	SHALL be used for indicating that the	NA	NA	NA

		document source does not support BPPC. The HIE SHALL transform documents with this confidentiality code according to the transformation rules below. Such transformation SHALL be negotiated on a case-by-case basis.			
1.3.6.1.4.1. 38571.1.1001	Emergency use only	SHALL be used to identify documents shared for emergency use only (e.g. Personal Health Record Summaries published by the consumer for use in an emergency)	NA	NA	NA

Personal care shall include documents that the patient has identified to be sensitive. Privileged health care documents shall be marked for all data subject to privacy protection requirements by regulation.

9.3.1.6.1 Derivation Rules for confidentialityCode

System-generated confidentialityCode MAY be applied by document source systems or by the HITE-CT Infrastructure Transformation Service in accordance with the following derivation rules:

Any documents generated with the following metadata indicating that the services were performed for mental health or substance abuse SHALL be assigned confidentialityCode for the HITE-CT Sensitivity Classification: Legally Protected Sensitive (Restricted):

Metadata Attribute	Value Set OID	Value Set Name	Derivation Rule
authorInstitution	NA		
authorPerson	NA		
authorRole	1.3.6.1.4.1. 38571.3.1	Mental Health Roles	IF authorRole CONTAINS Value Set ((Mental Health Roles) OR (Substance Abuse Roles)) THEN confidentialityCode := 1.3.6.1.4.1. 38571.1.4
	1.3.6.1.4.1. 38571.3.2	Substance Abuse Roles	
authorSpecialty	1.3.6.1.4.1. 38571.3.3	Mental Health Specialties	IF authorSpecialty CONTAINS Value Set ((Mental Health Roles) OR (Substance Abuse Roles)) THEN confidentialityCode := 1.3.6.1.4.1. 38571.1.4
	1.3.6.1.4.1. 38571.3.4	Substance Abuse Specialties	
classCode	NA		
classCode DisplayName	NA		
confidentialityCode	NA		
creationTime	NA		
healthcareFacility TypeCode	1.3.6.1.4.1. 38571.3.5	Mental Health Facility Types	IF healthcareFacilityTypeCode CONTAINS Value Set ((Mental Health Roles) OR (Substance Abuse Roles)) THEN confidentialityCode := 1.3.6.1.4.1. 38571.1.4
	1.3.6.1.4.1. 38571.3.6	Substance Abuse Facility Types	
health careFacility TypeCodeDisplay Name	NA		
legalAuthenticator	NA		
patientId	NA		
practiceSettingCode	1.3.6.1.4.1. 38571.3.7	Mental Health Practice Settings	IF practiceSettingCode CONTAINS Value Set ((Mental Health Roles) OR (Substance Abuse Roles)) THEN confidentialityCode := 1.3.6.1.4.1. 38571.1.4
	1.3.6.1.4.1. 38571.3.8	Substance Practice Settings	
practiceSettingCode DisplayName	NA		
sourcePatientId	NA		
sourcePatientInfo	NA		

9.3.1.7 healthcareFacilityTypeCode and healthcareFacilityTypeCodeDisplayName

This code represents the type of organizational setting of the clinical encounter during which the documented act occurred.

Health care organizations SHALL identify the setting for healthcareFacilityType using the HITSP-specified value set for facility type as indicated in table 9.3.1.7-1 where healthcareFacilityTypeCode is the standard type and healthcareFacilityTypeCodeDisplayName is the description. Setting SHALL be identified by document source as appropriate for the facility

Table 9.3.1.7-1 Healthcare Facility Type Value Set

healthcareFacilityTypeCode	healthcareFacilityTypeCodeDisplayName
	INPATIENT HEALTH FACILITY CARE
82242000	Hospital-children's
225732001	Hospital-community
79993009	Hospital-government
32074000	Hospital-long term care
4322002	Hospital-military field
224687002	Hospital-prison
62480006	Hospital-psychiatric
80522000	Hospital-rehabilitation
36125001	Hospital-trauma center
48311003	Hospital-Veterans' Administration
284546000	Hospice facility
42665001	Nursing home
45618002	Skilled nursing facility
	HOSPITAL OUTPATIENT CLINIC-AMBULATORY CARE
418518002	Dialysis unit--hospital
73770003	Emergency department--hospital
69362002	Hospital ambulatory surgery facility
52668009	Hospital birthing center
360957003	Hospital outpatient allergy clinic
10206005	Hospital outpatient dental clinic
37550003	Hospital outpatient dermatology clinic
73644007	Hospital outpatient endocrinology clinic
31628002	Hospital outpatient family medicine clinic
58482006	Hospital outpatient gastroenterology clinic
90484001	Hospital outpatient general surgery clinic
1814000	Hospital outpatient geriatric health center
22549003	Hospital outpatient gynecology clinic
56293002	Hospital outpatient hematology clinic
360966004	Hospital outpatient immunology clinic

healthcareFacilityTypeCode	healthcareFacilityTypeCodeDisplayName
2849009	Hospital outpatient infectious disease clinic
14866005	Hospital outpatient mental health center
38238005	Hospital outpatient neurology clinic
56189001	Hospital outpatient obstetrical clinic
89972002	Hospital outpatient oncology clinic
78088001	Hospital outpatient ophthalmology clinic
78001009	Hospital outpatient orthopedics clinic
23392004	Hospital outpatient otorhinolaryngology clinic
36293008	Hospital outpatient pain clinic
3729002	Hospital outpatient pediatric clinic
5584006	Hospital outpatient peripheral vascular clinic
37546005	Hospital outpatient rehabilitation clinic
57159002	Hospital outpatient respiratory disease clinic
331006	Hospital outpatient rheumatology clinic
50569004	Hospital outpatient urology clinic
79491001	Hospital radiology facility
33022008	Hospital-based outpatient clinic or department--OTHER-NOT LISTED
	INDEPENDENT PROVIDER OF OUTPATIENT AMBULATORY CARE
19602009	Fee-for-service private physicians' group office
39350007	Private physicians' group office
83891005	Solo practice private office
394759007	Independent ambulatory care provider site--OTHER--NOT LISTED
	CLINIC/CENTER AMBULATORY OUTPATIENT CARE
405607001	Ambulatory surgery center
309900005	Care of the elderly day hospital
275576008	Elderly assessment clinic
10531005	Free-standing ambulatory surgery facility
91154008	Free-standing birthing center
41844007	Free-standing geriatric health center
45899008	Free-standing laboratory facility
51563005	Free-standing mental health center
1773006	Free-standing radiology facility
72311000	Health maintenance organization
6827000	Local community health center
309898008	Psychogeriatric day hospital
39913001	Residential school infirmary
77931003	Rural health center
25681007	Sexually transmitted disease health center

healthcareFacilityTypeCode	healthcareFacilityTypeCodeDisplayName
20078004	Substance abuse treatment center
46224007	Vaccination clinic
81234003	Walk-in clinic
35971002	Ambulatory care site--OTHER--NOT LISTED
	OTHER OUTPATIENT CARE SITE
11424001	Ambulance-based care
409519008	Contained casualty setting
901005	Helicopter-based care
2081004	Hospital ship
59374000	Traveler's aid clinic
	OTHER CARE SITE
413456002	Adult day care center
413817003	Child day care center
310205006	Private residential home
419955002	Residential institution
272501009	Sports facility
394777002	Health encounter site--NOT LISTED

9.3.1.8 legalAuthenticator

Where the document is digitally signed, legalAuthenticator SHALL contain the identifier of the individual or organization that has signed the document using the identifier schemes listed in section 9.1.1 of this document.

practiceSettingCode and practiceSettingCodeDisplayName

The code specifying the clinical specialty where the act that resulted in the document was performed. This value SHALL draw from the HIPAA Provider Taxonomy Codes specialty codes listed in table 9.3.1.8-1 below that align with the practice specialty recognized by the state of Connecticut:

Table 9.3.1.8-1 Practice Setting Value Set

CT DPH Organization License Class Code (PENDING)	CT DPH Organization License Class Code	practiceSetting Code	practiceSetting DisplayName
0		NA	Unlicensed.
1	**CCNH**	**311ZA0620X**	Chronic and Convalescent Nursing Home
2	**RHNS**	**10400000X**	Rest Home with Nursing Supervision

CT DPH Organization License Class Code (PENDING)	CT DPH Organization License Class Code	practiceSetting Code	practiceSetting DisplayName
3	**CCRH**	**313M00000X**	Chronic and Convalescent Nursing Home and Rest Home with Nursing Supervision
4	**RCH**	**311Z00000X**	Residential Care Home
5	**GH**	**282N00000X**	General Hospital.
6	**CH**	**282NC2000X**	Children's Hospital
7	**CDH**	**281P00000X**	Chronic Disease Hospital
8	**PSY**	**283Q00000X**	Hospital for Mentally Ill Persons
9	**OPC**	**261Q00000X**	Outpatient Clinic
10	**ASC**	**261QA1903X**	Outpatient Surgical Facility
11	**----**	**302F00000X**	Outpatient HMO
12	**HEMO**	**261QE0700X**	Outpatient Dialysis Unit
13	**MATH**	**311Z00000X**	Maternity Home
14	**MHDT**	**261QM0801X**	Mental Health Day Treatment Facility
15	**MHIT**	**320800000X**	Mental Health Intermediate Treatment Facility
16	**POCA**	**261QM0801X**	Psychiatric Outpatient Clinic for Adults
17	**MHRL**	**3104A0625X**	Mental Health Residential Living Center
18	**ALSA**	**310400000X**	Assisted Living Services Agency
19	**MHCR**	**320800000X**	Mental Health Community Residence
20	**SA**	**324500000X**	Facility for the Care or Treatment of Substance Abusive or Dependent Persons
21	**HHC**	**251E00000X**	Home Health Care Agency
22	**HHHA**	**251E00000X**	Homemaker-Home Health Aide Agency
23	**RCC**	**261QR0800X**	Recovery Care Center
24	**FP**	**261QF0050X**	Family Planning Clinic
25	**INF**	**261QS1000X**	Infirmary Operated by an Educational Institution
26	**MAT**	**282NW0100X**	Maternity Hospital
27	**WCC**	**261QC1500X**	Well Child Clinic
28	**CLAB, RLAB**	**291U00000X**	Laboratory

CT DPH Organization License Class Code (PENDING)	CT DPH Organization License Class Code	practiceSetting Code	practiceSetting DisplayName
29	**NA**	**322D00000X**	Family Care Group Homes
30	**HSPC**	**315D00000X**	Inpatient Hospice
31	**NHMG**	**PENDING**	Nursing Home Management Company
32		**NA**	Funeral Home
33	C	**261QE0002X**	Certified EMS Organization
34	VEH	**3416L0300X**	Emergency Ambulance
35	VEH	**3416S0300X**	Emergency Boat
36	VEH	**3416A0800X**	Emergency Helicopters
37	VEH	**3416L0300X**	Emergency Coach
38	VEH	**261QE0002X**	Non-Transporting Emergency Medical Service
39	L	**261QE0002X**	Licensed EMS Organization
40	FR	**261QE0002X**	First Responder EMS Organization
41	SR	**261QE0002X**	Supplemental Responder EMS Organization
42	SH	**NA**	Sponsor Hospital

9.3.2 XDS Submission Set Metadata

The Submission Set Metadata SHALL be constrained in the same manner as the XDS Submission Set data.

9.3.3 Folder Metadata

The XDS Folder Metadata SHALL be constrained in the same manner as the XDS Submission Set data.

9.3.4 Supported Content

An authorized Document Source MAY publish those content profiles identified in Table 8.1.6-2. Provide and Register Document Set Content Options.

9.3.4.1 Document Content Specialization and Extensions

This section specifies any specialization of attributes and terminology to be used in the actual document content. All HITSP component specifications SHALL use the vocabulary constraints specified by the HITSP component. No additional constraints apply to the documents.

All IHE document content profiles not constrained by HITSP SHALL use the vocabulary constraints specified by IHE.

All documents containing Drug/Alcohol Treatment Program content SHALL document the treatment in the list of procedures listed by value set 1.3.6.1.4.1. 38571.3.9 HITE-CT Drug/Alcohol Treatment Program Value Set in the Procedures and Interventions section (OID 1.3.6.1.4.1.19376.1.5.3.1.1.13.2.11) Procedure ID entry of the CDA.

No additional constraints apply to the documents.

9.3.4.2 Connecticut Public Health Reporting

HITE-CT will offer services to facilitate reporting of laboratory results and immunizations to public health. Source systems relying upon this service MAY arrange with HITE-CT to send a Continuity of Care Document (CCD) containing immunizations or laboratory results, or other message as mutually negotiated that will be parsed for reporting rules. Public Health Immunizations and Laboratory reports will be forwarded as CDA documents to the State Department of Public Health interface engine using IHE XDR. Redaction services MAY be applied as necessary to support the transaction.

10 Patient Privacy and Consent

10.1 General Guidelines Regarding Document Access and Use

The following general guidelines SHALL be followed regarding the access and use of medical information in in HITE-CT managed systems.

Information access control SHALL be restricted to the document if specified by the patient through an opt-out BPPC document or other policies as defined in Table 10.2.3-1 Patient Privacy Policies. Further granularity in access disclosures SHALL be based upon provider local system configuration and is not specified by this policy agreement.

Those documents that are protected by law (e.g. HIV, Substance abuse) are subject to the Opt-in for Legally Protected Data (ALL) policy as defined in Table 10.2.3-1 Patient Privacy Policies.

A HITE-CT PHCS publishing patient information related to a Mental Health, HIV, Genetics, or Drug/Alcohol Treatment Program MUST submit a new consent form specifying expiration of access to all of that patient's documents after two years.

For any instance of a document published with HIV, Mental Health, genetics, or Drug/Alcohol Treatment Program content, a BPPC document SHALL be published that

updates the patient consent with a consent expiration date of two years from the ambulatory visit date or inpatient discharge date.

The trigger for the consent expiration update MAY be based upon human or machine input.

HIV content is defined by the following value sets (as represented by SNOMED-CT or by associated ICD9/ICD10 mapping) and CDA locations:

- Problem code in Active Problems (CDA Template ID: 1.3.6.1.4.1.19376.1.5.3.1.3.6):
- Containing value set 1.3.6.1.4.1. 38571.3.9 HIV Findings, enumerated in Appendix A of this Affinity Domain Policy

Genetic content is defined by the following value sets (as represented by LOINC and SNOMED-CT or by associated ICD9/ICD10 mapping) and CDA locations:

- Result Type code in Coded Results (CDA Template ID: 1.3.6.1.4.1.19376.1.5.3.1.3.28):
    - Containing value set 1.3.6.1.4.1. 38571.3.10 Genetic Results, enumerated in Appendix A of this Affinity Domain Policy
- Procedure code in Procedures (CDA Template ID: 1.3.6.1.4.1.19376.1.5.3.1.4.19):
    - Containing value set 1.3.6.1.4.1. 38571.3.11 Genetic Procedures, enumerated in Appendix A of this Affinity Domain Policy

NOTE: This policy is subject to review and updated upon extension of the HIE use to purposes other than patient care.

10.2 Patient consent

The rules for patient consent SHALL be harmonized or agreements SHALL be defined on how differences SHALL be bridged when harmonization is not possible. Both parties SHALL agree to this in the Policy Agreement.

Patient privacy is a key issue in trans-border information exchange.

10.2.1 In order to gain a patient's full confidence with the information transactions it is of utmost importance that the rules are clear and easily understood by the patients. BPPC

Patent Opt-out and other consent policies SHALL be instantiated using the IHE-BPPC profile. The OID's for this policy are as referenced in section 102.3, Table 10.2.3-1 Patient Privacy Policies.

10.2.2 Common Consent Agreements

The patient Opt-in authorization for use or disclosure of restricted health information

(HIV, Substance Abuse, and Mental Health) and other policies defined in Table 10.2.3-1 Patient Privacy Policies SHALL use the common authorization document published on http://www.hitect.org/agreements [PENDING] unless otherwise specified within this table.

10.2.3 Policy OIDs Supported for Patient Authorization

The following Policy OIDS are supported in conformance to BPPC as the Patient Privacy Policy Domain: Each Patient Privacy Policy will be given a unique identifier (OID) known as a Patient Privacy Policy Identifier. The overall policy identifier scheme as aligned with standard vocabularies for data sensitivity and purposes of use is as follows:

1.3.6.1.4.1. 38571 (x), HITECT Patient Privacy Policy Identifier (2) Opt-Out (1),

1.3.6.1.4.1. 38571 (x), HITECT Patient Privacy Policy Identifier (2) Opt-In (2),

Administrative purposes (1) NOT SUPPORTED AT THIS TIME

- Anonymized/Pseudonymized Research Purposes: (1)
- Financial/insurance support: Administration of care for an individual subject of care (2)
- Education (3)
- Market Studies (4)
- Legal investigation or inquiry (5)

Clinical Care Support Activities purposes: (2)

- Supporting Clinical Services: Support of care activities within the provider organization for an individual subject of care (1)
- Quality Services Management Health service management and quality assurance: (2)
- Population Health Management (3)
- Public Health Surveillance, Disease Control (4)
- Public safety emergency (5)

Clinical Care Treatment/Provision purposes: (3)

- Routine Care: Clinical care provision to an individual subject of care (1)
- Emergency Care: Emergency care provision to an individual subject of care (2)
- Patient Directed Care: Subject of Care Uses (3)

Privileged Care: (4)

- HIV: (1)
- Substance Abuse: (2)
- Mental Health: (3)
- Sexual Health: (4)
- Genetic Health: (5)

Personal Care: (5) (patient-directed not supported at this time)

Drawing from this identification scheme, the following list of Patient Privacy Policy Identifier OIDs SHALL be used by the HIE to reflect the HITE-CT authorizations supported at this time. Privacy Policy Acknowledgement Document are not required for the release of routine clinical care data for Clinical Care Treatment Provision, Payment, and Operations purposes (see HITE-CT Purpose of Use Policy http://www.hitect.org/policies). For release of Privileged Care information, a consent document SHALL be registered with HITE-CT in the form of a BPPC conformant document using the Opt-in for Legally Protected Data (ALL) policy. Where the consumer does not wish to have their health information available to HITE-CT PHCSs, a consent document SHALL be registered with HITE-CT in the form of a BPPC conformant document using the Opt-Out (Routine Care) and at the direction of the consumer, Opt-Out (Emergency Care). All Opt-in documents SHALL include an expiration date. This date SHOULD be recorded as two (2) years from the date the agreement is executed. All policies are global within the HIE such that an Opt-Out or Opt-In captured at one location covers all HIE member organizations. Common consent language shall be provided by HITE-CT.

Table 10.2.3-1 Patient Privacy Policies

Patient Privacy Policy Identifier OID	Use	Consent Document to be Filed
1.3.6.1.4.1. 38571.2.1.3.1	Opt-Out (Routine Care): Opt-out is specific to Restricted to viewing data registered in HITE-CT and SHALL NOT reflect restrictions pertaining to any exchanges not delivered through HITE-CT.	HITE-CT Opt-Out Routine Care
1.3.6.1.4.1. 38571.2.1.3.2	Opt-Out (Emergency Care):	HITE-CT Opt-Out Emergency Care
1.3.6.1.4.1. 38571.2.2.3.1	Opt-in for general use (OPTIONAL use where PHCS has captured or chooses to capture specific consent for HIE participation from consumer)	OPTIONAL: Provider Generated Document
1.3.6.1.4.1. 38571.2.2.4	Opt-in for Legally Protected Data (ALL)	HITE-CT Opt-In for Legally Protected Data
1.3.6.1.4.1. 38571.2.2.4	Reflect that acknowledgement of information exchange practices has been collected from the healthcare consumer or their authorized representative	HITE-CT Acknowledgement of Information Exchange Practices

Example: A consumer had elected to Opt-Out of sharing routine clinical health information through HITE-CT. A Privacy Policy Acknowledgement Document is submitted through the consumer's primary care provider recording the document as a scanned document under the Patient Privacy Policy Identifier OID 1.3.6.1.4.1.38571.2.1.3.2 in the XDSDocumentEntry.eventCodeList. The documentationOf/serviceEvent is populated with an effective time reflecting the current

date as the 'low value' and the current date +24 months as the effective data 'high value'.

10.3 Privacy Override Guidelines

The HITE-CT requires no authorization from the subject of care (health care consumer) to release information from the HITE-CT. The existance of registered documents:

- MAY be disclosed to the HITE-CT user with a break-glass emergency access privileges should the patient not be able to provide the opt-in to sensitive data at the time of treatment
- Opt-Out documents SHALL explicitly specify whether the Opt-Out applies to emergency care. Opt-Out of Emergency Care HITE-CT access SHALL require that the consumer explicitly acknowledge the risk of life-threatening consequences of withholding clinical information from the care team, and include a hold-harmless agreement for providers administering care in the absence of otherwise available clinical history.
- Audit logs in the case of a break-glass event shall include: BPPC OID, Reason for override, incident ID, indication of verbal consent where provided

#	Item	Description	HIE Response

11 Technical Security

11.1 Authorization

Authorization is managed by the document consumer entity (Provider EMR, Portal).

The authorization process SHALL be defined in the policy agreement both within the domain and externally in the other jurisdiction domains.

11.1.1 Role Management

Roles for the HIE are based upon National and International standards. This includes functional and structural roles. Roles are defined within each domain. Rights and responsibilities in specific contexts are defined in policies that are bound to one or more roles.

11.1.1.1 Functional and Structural Roles

The following tables list currently permitted standard Functional and Structural Roles for the Affinity Domain that MAY be used for access control policies with the affinity domain. There are no affinity-domain level policies at this time that require assertion of functional or structural roles. The HITE-CT member SHOULD record Functional Role in its system audit log. Structural Roles are defined within the mapping sections that

follow. The roles for health care professionals and employees using HITE-CT SHOULD be mapped from provider local roles to the standard ISO TS21298 role or to the standard ASTM E1986 as described in table 11.1.1.2.3-1:

Table 11.1.1.1-1 Functional Roles

Functional Role	Brief description	ISO OID
Subject of care	The principal data subject of the electronic health record	1.0.21298.4.01
Subject of care agent	E.g. parent, guardian, carer, or other legal representative	1.0.21298.4.02
Personal health care professional	The health care professional or professionals with the closest relationship to the patient, often the patient's GP	1.0.21298.4.03
Privileged health care professional	Nominated by the subject of care OR nominated by the health care facility of care (if there is a nomination by regulation, practice, etc. such as an emergency over-ride)	1.0.21298.4.04
Health care professional	Party involved in providing direct care to the patient	1.0.21298.4.05
Health-related professional	Party indirectly involved in patient care, teaching, research, etc.)	1.0.21298.4.06
Administrator	Any other parties supporting service provision to the patient	1.0.21298.4.07

11.1.1.2 Mapping of Structural Roles to Functional Roles

11.1.1.2.1 Subject of Care

No structural role mapping.

11.1.1.2.2 Subject of Care Agent

No structural role mapping

11.1.1.2.3 Privileged health care professional

No structural role mapping.

11.1.1.2.4 Healthcare Professional

Health care professionals SHALL reference the following regulated practitioner types corresponding to the CT State License Categories below:

Table 11.1.1.2.1-1 Mapping of CT Licensed Practitioners to Healthcare Professionals

CT State License Category	State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
43	Acupuncturist	171100000N	Traditional and complementary medicine practitioners	3238
17	Audiologist	231H00000X	Audiologists and speech therapists	2246
7	Chiropractic Physician	111N00000X	Health associate professionals not elsewhere classified	3239
58	Clinical Social Worker	1041C0700X	Social work and counseling professionals	2636
2	Dentist	122300000X	Dentists	2241
1	Medical Doctor	208D00000X	2211 Generalist medical practitioners, 2212 Specialist medical practitioners	2211, 2212
1 (with specialty of psychiatry)	Medical Doctor Psychiatry	2084P0800X	Specialist medical practitioners	2212
1 (with sub-specialty of public health)	Medical Doctor Public Health	2083P0901X	Specialist medical practitioners	2212
46	Mental Health Counselor	101YM0800N	Social work and counseling professionals	2636
16	Midwife	176B00000X	Midwifery professionals	2222
5	Naturopathic Physician	175F00000X	Traditional and complementary medicine practitioners	3238
12	Advanced Registered	363L00000X	Nursing professionals	2221

CT State License Category	State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
	Nurse Practitioner			
10	Registered Nurse	163W0000X	Nursing professionals	2221
11	Licensed Practical Nurse	164W00000X	Nursing associate professionals	3221
36	Nursing Home Administrator	376G00000X	General managers in personal care, cleaning and related services	1318
1	Osteopathic Physician	208D00000X	Specialist medical practitioners	2212
23	Physician Assistant	363A00000X	Doctor's assistants	3211
19	Podiatric Physician	213E00000X	Specialist medical practitioners	2212
8	Psychologist	103T00000X	Social work associate professionals	2635
8	School Psychologist	103TS0200X	Psychologists	2635
9	Homeopath	175L00000X	Traditional and complementary medicine practitioners	3238
1	Allopath	208D00000X	Traditional and complementary medicine practitioners	3238
12	Advanced Practice Registered Nurse (NP, NM, CAN, CNS)	363L00000X	Nursing professionals	2221
11	Licensed Vocational Nurse (Same as LPN)	164W00000X	Nursing associate professionals	3221

11.1.1.2.5 Health-Related Professionals

All regulated professions listed in Table 9.1.1.4-1 Connecticut CT DPH Regulated Professions not in the table above SHALL be classified as health-related professionals. Health care professionals SHALL reference the following regulated practitioner types corresponding to the CT State License Categories below:

Table 11.1.1.2.5-1

State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298

State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
Athletic Trainer	2255A2300X	Fitness and recreation instructors and program leaders	3433
Audiology Assistant	2355A2700X	Health care assistants	5133
Chiropractic Assistant	246QM0706X	Physiotherapy technicians and assistants	3235
Clinical Lab Director	246QL0901X	Managing directors and chief executives	1120
Clinical Lab Supervisor	246QL0900X	Health service managers	1342
Clinical Lab Technician	247200000X	Medical laboratory technicians	3142
Clinical Lab Technologist	246QM0706N	Medical laboratory technicians	3142
Dental Hygienist	124Q00000X	Dental assistants and therapists	3231
Dental Radiographer	2471R0002X	Medical equipment technicians	3236
Dietetics/Nutritionist	133V00000X	Dieticians and nutritionists	2245
Nutrition Counselors	133NN1002X	Dieticians and nutritionists	2245
Electrologist	246QM0706X	Health associate professionals not elsewhere classified	3239
Hearing Aid Specialists	237700000X	Medical and dental prosthetic and related technicians	7314
Massage Therapist	225700000X	Physiotherapy technicians and assistants	3235
Diagnostic Radiological Physicist	2085R0205X	Medical equipment technicians	3236
Therapeutic Radiological Physicist	2085R0203X	Medical equipment technicians	3236
Medical Nuclear Radio Physicist	2085N0904X	Medical equipment technicians	3236
Medical Health Physicist	246QM0706X	Physicists and astronomers	2111

State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
Mental Health Counselor	101YM0800N	Social work and counseling professionals	2636
Ancillary Service Providers - Occupational Therapy	225X00000X	Aged care service managers	1343
Occupational Therapy Assistant	224Z00000X	Health professionals not elsewhere classified	2249
Optician	156FX1800X	Optometrists and opticians	3234
Optometrist	152W00000X	Optometrists and opticians	3234
Orthotics	222Z00000X	Medical and dental prosthetic and related technicians	7314
Orthotic Fifter	225000000X	Medical and dental prosthetic and related technicians	7314
Orthotic Fifter Assistant	246QM0706X	Medical and dental prosthetic and related technicians	7314
Prosthetist-Orthotist	224P00000X	Medical and dental prosthetic and related technicians	7314
Pharmacist	183500000X	Pharmacists	2242
Nuclear Pharmacist	1835N0905X	Pharmacists	2242
Ancillary Service Providers - Physical Therapist	225100000X	Physiotherapists	2244
Physical Therapist Assistant	225200000X	Physiotherapy technicians and assistants	3235
Prosthetist-Orthotist	222Z00000X	Medical and dental prosthetic and related technicians	7314
Prosthetist	224P00000X	Medical and dental prosthetic and related technicians	7314
Pedorthist	246QM0706X	Medical and dental prosthetic and related technicians	7314
Respiratory Care	227900000X	Physiotherapists	2244
Respiratory Therapy Technician	227800000X	Physiotherapy technicians and assistants	3235

State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
Speech-Language Pathology	235Z00000X	Audiologists and speech therapists	2246
Speech-Language Pathology Assistant	2355S0801X	Physiotherapy technicians and assistants	3235
Audiology Assistant	2355A2700X	Physiotherapy technicians and assistants	3235

11.1.1.2.6 Administrators

All non-regulated health care employee structural roles SHALL be classified as Administrator.

The roles for health care employees using HITE-CT SHOULD be mapped from provider local roles to the standard ISO TS21298 role or to the standard ASTM E1986 as described in table 11.1.1.2.3-1:

Table 11.1.1.2.3-1

State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
Traditional Medicine Provider, Homeopath	175L00000X	Traditional and complementary medicine practitioners	3238
Traditional Medicine Provider, Naturopath	175F00000X	Traditional and complementary medicine practitioners	3238
Cast Technician	246ZS0400X	Life science technicians (except medical)	3141
Prosthetic Technician	225000000X	Medical and dental prosthetic and related technicians	7314
Technician, Procedure-based	247100000X	Life science technicians (except medical)	3141
Technician, Departmental	247100000X	Life science technicians (except medical)	3141
Technician, Specialty	247100000X	Life science technicians (except medical)	3141
Technician, General	247100000X	Life science technicians (except medical)	3141
Nurse's Aide	376K00000X	Health care assistants	5133
Orderly	376K00000X	Health care assistants	5133
Phlebotomist	246RP1900X	Life science technicians (except	3141

State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
		medical)	
Counsellor, Bereavement	1041C0700X	Social work associate professionals	3421
Volunteer	376K00000X	Community health workers	3233
Technician	374700000X	Life science technicians (except medical)	3141
Patient Transportation Personnel	347E00000X	Transport conductors	5112
Specimen Transportation Personnel	347C00000X	Transport conductors	5112
Health Record Transportation Personnel	2470A2800X	Mail carriers and sorting clerks	4142
Emergency Services	146N00000X	Paramedical practitioners	2231
Emergency Services, Paramedic	146L00000X	Emergency paramedics	2232
Emergency Services, EMT	146M00000X	Emergency paramedics	2232
Emergency Services, EMS	146D00000X	Ambulance officers	5135
Emergency Services, Ambulance Driver	314600000X	Ambulance officers	5135
Emergency Services, Air Transport Pilots	3416A0800X	Ambulance officers	5135
Secular Services	101YP1600X	Religious professionals	2637
Patient Advocate	209800000X	Legal professionals not elsewhere classified	2619
Interpreters	273091	Philologists, translators and interpreters	2634
Clerical and administrative Personnel	43471	Other client information workers	4229
Clerical and administrative Personnel, Encounter Registration Clerk	43471	Other client information workers	4229
Clerical and administrative Personnel, Admission Clerk	43471	Other client information workers	4229
Clerical and administrative Personnel, Ward/Unit/Clinic Clerk	43471	Other client information workers	4229
Clerical and administrative Personnel, Departmental Clerk, Clinical Services	43471	Other client information workers	4229
Clerical and administrative Personnel, Departmental Clerk, Laboratory Services	43471	Other client information workers	4229
Clerical and administrative Personnel, Departmental Clerk, Imaging Services	43471	Other client information workers	4229
Clerical and administrative	43471	Other client information workers	4229

State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
Personnel, Departmental Clerk, Pharmacy Services			
Clerical and administrative Personnel, Departmental Clerk, Social Services	43471	Other client information workers	4229
Clerical and administrative Personnel, Departmental Clerk, Ancillary Services	43471	Other client information workers	4229
Disposition/Discharge Clerks	43471	Other client information workers	4229
Administrative Support Staff and Services, Physician Office	436013	Medical records and health information technicians	3232
Administrative Support Staff and Services, Non-physician Provider Office	436013	Medical records and health information technicians	3232
Administrative Support Staff and Services, Clinical Department	436013	Medical records and health information technicians	3232
Administrative Support Staff and Services, Administrative Department	436013	Medical records and health information technicians	3232
Administrative Support Staff and Services, Health Records/Health Information Management	2470A2800X	Medical records and health information technicians	3232
Administrative Support Staff and Services, Department	436013	Medical records and health information technicians	3232
Administrative Support Staff and Services, Quality Assurance	436013	Medical records and health information technicians	3232
Transcription Personnel	2470A2800X	Scribes and related workers	4144
Transcription Personnel, Transcriptionist	2470A2800X	Scribes and related workers	4144
Transcription Personnel, Proofreader	2470A2800X	Coding, proof-reading and related clerks	4143
Transcription Personnel, QA Personnel	2470A2800X	Coding, proof-reading and related clerks	4143
Transcription Personnel, Clerks	43471	Coding, proof-reading and related clerks	4143
Transcription Personnel, Students	2470A2800X	Scribes and related workers	4144
Transcription Personnel, Supervisors/Managers	2470A2800X	Scribes and related workers	4144
Transcription Personnel, Vendors	2470A2800X	Scribes and related workers	4144
Transcription Personnel, Maintenance and System Support Personnel	2470A2800X	Scribes and related workers	4144
File Clerk	434071	Library and filing clerks	4141
File Clerk, Clinical Department	434071	Library and filing clerks	4141

State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
File Clerk, Administrative Department	434071	Library and filing clerks	4141
File Clerk, Health Records/Health Information Management	2470A2800X	Medical records and health information technicians	3232
File Clerk, Department	434071	Library and filing clerks	4141
File Clerk, Quality Assurance	434071	Library and filing clerks	4141
Supervisory Personnel	431011	Health service managers	1342
Supervisory Personnel, Administrative Department	113011	Health service managers	1342
Supervisory Personnel, Health Records/Health Information Management	119081	Medical records and health information technicians	3232
Supervisory Personnel, Quality Assurance	519061	Environmental and occupational health and hygiene professionals	3237
Health Records/Health Information Management	247000000X	Medical records and health information technicians	3232
Health Records/Health Information Management, Department	247000000X	Medical records and health information technicians	3232
Health Records/Health Information Management, Administration	247000000X	Medical records and health information technicians	3232
Health Records/Health Information Management, Administrative Support	2470A2800X	Medical records and health information technicians	3232
Health Records/Health Information Management, File Clerks	2470A2800X	Medical records and health information technicians	3232
Health Records/Health Information Management, Information Management Personnel	247000000X	Medical records and health information technicians	3232
Information Services, Database Administrator	151061	Database designers and administrators	2521
Information Services, Network Administrator	151071	Computer network professionals	2531
Information Services, Analyst, Network/Data Communications	151081	Computer network professionals	2531
Information Services, Electrical Engineer, Telecommunications	172071	Telecommunications engineering professionals	2532
Information Services, Systems Analyst, Operations	152031	Systems analysts	2511
Information Services, Security Administrator	173023	Policy administration professionals	2422
Information Services, Trainer, end user	151033	Information technology trainers	2355
Information Services, Help Desk	151033	ICT user support technicians	3512

State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
Information Services, Operations Support	152031	ICT operations technicians	3511
Information Services, System Administrator	151071	Systems administrators	2522
Information Services, Applications Support	151031	Software and multimedia developers and analysts not elsewhere classified	2519
Information Services, Business Analyst	151051	Systems analysts	2511
Information Services, Programmers	151021	Software developers	2512
Information Services, Engineer, Computer Applications	151031	Applications programmers	2514
Information Services, Engineer, Software-Operating Systems	151032	ICT network and hardware professionals not elsewhere classified	2539
Information Services, Specialist, Computer Support	151033	ICT network and hardware professionals not elsewhere classified	2539
Information Services, Specialist, Computer, NOS	151099	ICT network and hardware professionals not elsewhere classified	2539
Information Services, Statistician	152041	Mathematicians, actuaries and statisticians	2120
Information Services, Biostatistician	246ZB0600X	Mathematicians, actuaries and statisticians	2120
Information Services, Third Party Support (vendors/consultants)	151033	Software and multimedia developers and analysts not elsewhere classified	2519
Information Services, Biomedical Engineer	246ZB0301X	ICT network and hardware professionals not elsewhere classified	2539
Information Services, Security Officer	113021	Policy administration professionals	2422
Information Services, Information Officer	113021	Information and communications technology service managers	1330
Financial Services, Billing and Claims	13071	Insurance representatives	3321
Financial Services, Billing and Claims, Billing File Clerk	13071	Statistical, finance and insurance clerks	4122
Financial Services, Billing and Claims, Billing Personnel	13071	Statistical, finance and insurance clerks	4122
Financial Services, Billing and Claims, Claims Personnel	13071	Statistical, finance and insurance clerks	4122
Financial Services, Billing and Claims, Coders/Reimbursement Specialists	13071	Coding, proof-reading and related clerks	4143
Financial Services, Billing and Claims, Administrative Support	13071	Statistical, finance and insurance clerks	4122

State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
Personnel			
Financial Services, Billing and Claims, Collections Personnel	13071	Debt-collectors and related workers	4214
Financial Services, Billing and Claims, Cost and Quality Analysts	152011	Statistical, finance and insurance clerks	4122
Quality Assurance	519061	Environmental and occupational health and hygiene professionals	2243
Utilization Review	151011	Statistical, finance and insurance clerks	4122
Discharge Planning	225X00000X	Health professionals not elsewhere classified	2249
Infection Control	246ZB0500X	Environmental and occupational health and hygiene professionals	2243
Risk Management	152011	Statistical, finance and insurance clerks	4122
Health Plan/Insurer	13071	Insurance representatives	3321
Health Plan/Insurer, Claims File Clerk	13071	Statistical, finance and insurance clerks	4122
Health Plan/Insurer, Claims Review Personnel	13071	Statistical, finance and insurance clerks	4122
Health Plan/Insurer, Claims Adjudication Personnel	13071	Statistical, finance and insurance clerks	4122
Health Plan/Insurer, Internal Quality Assurance	519061	Statistical, finance and insurance clerks	4122
Health Plan/Insurer, Health Care Provision Quality Assurance	519061	Statistical, finance and insurance clerks	4122
Health Plan/Insurer, Internal Utilization Review Personnel	151011	Statistical, finance and insurance clerks	4122
Health Plan/Insurer, Health Care Provision Utilization Review Personnel	151011	Statistical, finance and insurance clerks	4122
Health Plan/Insurer, Administrative Support Personnel	13071	Statistical, finance and insurance clerks	4122
Medical Malpractice, Health Records File Clerk	2470A2800X	Medical records and health information technicians	3232
Medical Malpractice, Health Records Supervisor	247000000X	Medical records and health information technicians	3232
Medical Malpractice, Lawyer	231011	Lawyers	2611
Medical Malpractice, Judge	231011	Judges	2612
Medical Malpractice, Legal Aide	232011	Legal professionals not elsewhere classified	2619
Medical Malpractice, Legal Secretary	232011	Legal professionals not elsewhere classified	2619

State Role Description	ASTM Role (NUCC)	ISCO-08 Role Description	ISO TS21298
Medical Malpractice, Governmental File Clerk	232092	Customs, tax and related government associate professionals not elsewhere classified	3359
Accrediting and Regulatory Agencies	132011	Environmental and occupational health and hygiene professionals	2243
Accrediting and Regulatory Agencies, JCAHO Auditors	132011	Environmental and occupational health and hygiene professionals	2243
Accrediting and Regulatory Agencies, NCQA Auditors	132011	Environmental and occupational health and hygiene professionals	2243
Accrediting and Regulatory Agencies, Local/State/Federal Agencies	132011	Environmental and occupational health and hygiene professionals	2243
Accrediting and Regulatory Agencies, Local/State/Federal Surveyors	132011	Environmental and occupational health and hygiene professionals	2243
Administrative Management, Executive Officers	111021	Managing directors and chief executives	1120
Administrative Management, Board of Trustees	111021	Managing directors and chief executives	1120
Administrative Management, Medical Staff Administration	113049	Human resource managers	1213
Administrative Management, Administrative Support Staff	439199	Administrative and executive secretaries	3343
Librarian	254031	Librarians and similar information professionals	2622

11.1.2 Authentication of Users/Role

Portal access from locations outside of compliant locations or PHCS controlled networks SHALL require 2-factor authentication. This SHALL be done either through FIPS 140-2 protected digital identities using the identity management requirements of the HITE-CT Identity Management Policy (see http://www.hitect.org/policies), or through a portal utilizing secure tokens where the issuing authority is managed by the HITE-CT member.

The credential-issuing authority and any associated healthcare roles SHALL be passed in the ID Credentials in any identity assertion.

Digital identities where used SHOULD be issued by a Federal Bridge Cross-Certified Certification Authority. The HITE-CT Identity Management Policy indicates face-to-face attestation, demonstration of government issued photo-id, and attestation of practitioner or employee role (see http://www.hitect.org/policies)

Authorization to issue the HITE-CT TLS or VPN certificate requires:

- A site visit OR a digital identity issued by a Federal Bridge Cross-Certified Certification Authority or equivalent assurance
- A signed participation agreement
- All HITE-CT members are required to perform a risk assessment and submit to HITE-CT for review prior to authorization of the TLS certificate. HITE-CT reserves the right to negotiate the level of risk assessment with the member.

11.1.2.1 User/Role Certificates Management

There is no affinity-domain level certification authority for user/role certificates at this time. Digital identities where used SHOULD be issued by a Federal Bridge Cross-Certified Certification Authority. Issuance/revocation of User identities and role management is the responsibility of the HITE-CT member organization. This includes assuring that all users are valid and in good standing.

Authorized nodes shall be provided digital identities as specified for server/organization certificates in the HITE-CT Identity Management Policy (see http://www.hitect.org/policies).

11.1.3 Attestation rights

The policy agreement SHALL name the individuals in the organization who have the right to assign roles and attestation authority to employees. An employee or medical staff with attestation authority has the right to attest medical information.

Attestation via digital signature SHALL be allowed by organization – this is signature where the machine ID credential is under the responsibility of the source organization. Attestation via digital signature MAY be allowed by provider.

The assignment of these roles for an organization SHALL be determined by human resources, medical staff or information technology staff as determined by the participating organization. The organization SHALL identify the responsible department and persons eligible to assign these roles.

11.1.4 Delegation rights

Delegation is often necessary in daily operation. In order to be able to keep this under control delegation rights have to be specified in the agreement since it is particularly difficult to know who has which rights inside and between the domains. Delegation has to be well structured in order for it to be possible to follow up.

HIE-wide delegation is not currently supported. Delegation at the local level (HITE-CT member) is based upon system access credentials and associated locally defined rules.

Responsibility for such delegation resides with the participating organization. HITE-CT members MAY refer to sample procedures from HITE-CT.

11.1.5 Validity time

Authorization, roles, attestation rights, delegation rights SHALL have a well-defined and specified time period for the access rights to information both within the domain and across domain borders. The HITE-CT member SHALL validate its active identities and roles annually. The member SHALL also review its identity management process with HITE-CT as part of its risk assessment.

11.2 Node Authentication

ATNA Secure Node and Secure Application Profiles are supported for Node Authentication. VPN/firewall MAY be used for TCP/IP/MLLP transactions.

11.2.1 Node Certificates Management

Authorized nodes SHALL be provided digital identities by the HITE-CT Infrastructure. Application for node certificates MAY be submitted after all HITE-CT participation agreements and site verifications are completed. Certificate request MAY be submitted as a PKCS10 digital certificate request initiated by the HITE-CT member-authorized technical contact to the HITE-CT Infrastructure technical contact. Upon request, a PKCS12 identity MAY be provided via secure delivery methods.

Authorized nodes shall be provided digital identities as specified for server/organization certificates in the HITE-CT Identity Management Policy (see http://www.hitect.org/policies).

11.3 Information Access

This section describes how access to the information SHOULD be controlled in the XDS affinity domain, depending upon whether it is contained on a computer system, removable media, or being transferred over a network.

11.3.1 Security Audit Log Access

Security audit logs are maintained by the HITE-CT infrastructure. All document source and document consumers within the HITE-CT SHALL send auditable events to the HITE-CT Audit Record Repository. A local audit record repository MAY be utilized upon negotiation with HITE-CT such that HITE-CT may review audit logs in conformance with HITE-CT Audit policy (https://www.HITECT.org/policies). The connection details for the audit record repository are: _____PENDING VENDOR INPUT for ARR connection details__.

11.3.2 Network Communication Access Security Requirements

The network access security requirements for the affinity domain SHALL be TLS as specified by the IHE ATNA profile.

11.3.2.1 Node Access Security Requirements

The system node access security requires that all affinity domain nodes SHALL conform to the IHE ATNA secure node Actor/Profile.

11.3.2.2 Removable Media Access Security Requirements

Media transfer of XDS content is permitted as part of the affinity domain, only where the media itself or the individual files are encrypted to achieve minimum recommendations for health care or better.

11.4 Agreement validity period

This policy SHALL be valid for the period specified by the HITE-CT Participation and Services Agreement entered into by the member with HITE-CT.

11.5 Information Integrity

The integrity of the data SHALL be checked in order to detect corruption of data during transfer between the domains. This SHALL be accomplished using IHE DSG. Where not supported, upon negotiation, it MAY be omitted with a transition plan for addition of machine signatures.

11.5.1 Network Communication Integrity Requirements

Communication integrity SHALL be asserted using IHE audit trail and node authentication.

11.5.2 Document Digital Signature Requirements/Policy

It is necessary to digitally sign any of the content in order to ensure the lifetime integrity of the data, or to allow authentication of the identity entity that created, authorized, or modified the content.

All repository documents SHALL be protected from modification and SHALL carry source verification through the use of IHE document digital signature (IHE-DSG).

11.5.3 Document Update and Maintenance Policies

All document update and maintenance policies are managed by the HITE-CT member.

11.5.4 Folder Update and Maintenance Policies

All document update and maintenance policies are managed by the HITE-CT member.

11.6 Ethics

No stipulation.

11.7 Secure Audit Trail

All transactions SHALL be logged. This section SHALL define the use of the ATNA Audit Logging feature.

The Audit Log SHALL be able to:

- Provide an accounting of disclosures for a given patient
- Filter log information for a given patient(s)
- Send alerts to designated the HITE-CT Privacy Officer (privacy_officer@HITECT.org) in response to specified events
- Provide a list of access events for a given organization or user
- Provide a list of any “break-glass” actions (where a user has accessed patient information with good reason, despite lack of permission)
- Forward to other Audit Record Repositories

The ATNA Audit Record Repositories MAY be centralized, distributed or a combination.

Audit records are identified by a unique record key or number and include

a. The HITE-CT’s audit logs shall include:
    a. User ID,
    b. A date/time stamp,
    c. Identification of all data transmitted, and
    d. Any authorizations needed in order to disclose the data.

b. For purposes of information disclosure, audit SHALL include documentation of the following:
    a. The date and time of the request,
    b. The reason for the request,
    c. A description of the information requested, including the data accessed, the data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to another party,
    d. The ID of person/system requesting disclosure,

e. The ID/verification of the party receiving the information,
f. The ID of the party disclosing the information.
g. A consent ID SHALL be logged, if it exists, for transactions that require a consent or authorization to be tracked for audit purposes.

c. For purposes of information requests, a written policy is required that includes the following components :
   a. The date and time of the request,
   b. The reason for the request,
   c. A description of information requested, including the data accessed, data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to, or printed by another party,
   d. The ID of person/system requesting disclosure,
   e. The ID/verification of the party receiving the information,
   f. The ID of the party disclosing the information,
   g. The method used for verification of the requesting entity's identity.

11.8 Consistent Time

In order to be able to ensure high quality logging, time stamping is necessary. All information transactions SHALL have a time stamp. All systems SHALL use the NIST time server.

11.9 Audit Check

HITE-CT SHALL check audit logs quarterly and handle events as required in the HITE-CT Audit policy. HITE-CT members SHALL report breaches as required in the HITE-CT Breach Notification policy.

11.10 Risk Analysis

If risks are observed during a risk assessment, all parties have jointly to evaluate them and decide whether the risks can be accepted or not. The risks have to be documented in the project agreement. If the risks can be accepted all parties SHALL approve it. If the risks are not acceptable a plan detailing resource requirements for risk reduction SHALL be included in the project agreement.

HITE-CT members SHOULD conduct a risk analysis at least on an annual basis. HITE-CT MAY conduct risk analysis of members as well.

11.11 General Mitigations

HITE-CT SHALL adhere to its security policies and procedures. HITE-CT members SHOULD procedures recommended by HITE-CT or according to industry best practices.

11.11.1 Common Criteria (ISO/IEC 15408)

Policy makers are encouraged to make use of the security framework defined in the Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC). Common Criteria is an international standard (ISO/IEC 15408) for computer security.

Common Criteria is based upon a framework in which computer system users can specify their security requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.

The framework can thus be used to translate the security requirements for the XDS Affinity Domain into specific requirements that MUST be met in order for systems to connect to others within the Affinity Domain. Demonstrating that these requirements are met then allows some proof that organizations are maintaining technical security before a user in that organization connects to the XDS Affinity Domain. Risks for the HITE-CT are identified below.

11.11.2 Identified Risks

Table 10.10.2-1 provides a high level assessment of the threats to the confidentiality, integrity and availability of health information assets as identified by ISO IS27799.

Table 10.10.2-1 Identified Risks

Threat	Description	Risk	Mitigation
'Masquerade by insiders' (including masquerade by health professionals and support staff)	Masquerade by insiders consists of system use by those who make use of accounts that are not their own. As such, it constitutes a breakdown in secure user authentication. Many cases of masquerade by insiders are committed simply because it makes it easier for people to do their work. For example, when one health professional MAY replace another at a workstation and continues to work on an already active patient record, there is a strong temptation to skip the inconvenience of the first user logging out and the second user logging in. Nevertheless, masquerade by insiders is also the source of serious breaches in confidentiality. Indeed, the majority of breaches of confidentiality are committed by organizational insiders. Masquerade by insiders can also be carried out with the intention to cover up cases where harm has been caused.	High	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require personnel training including training on HIE practices and policies as part of current HIPAA training • Participation agreement signed by an officer of the corporation, including attestation that read the responsibilities • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Audit may be performed by HITE-CT periodically or upon request • Breech of the contract MAY result in removal of privileges for accessing the HIE • Subject to any and all requirements of the law (state, federal) and associated enforcements Information Security Policy:

Threat	Description	Risk	Mitigation
			• Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require personnel training • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Audit Policy: • Require Meaningful Use Audit Log Tested EHRs • Require Meaningful Use Accounting of disclosures Tested EHRs (NOTE: Optional MU test for EHRs) • Require routine audit review of all HIE participants and infrastructure • Audit review supporting inquiry by patient or provider required of all HIE participants and infrastructure • Audit repository reporting support for ‘ all HITE-CT users who have accessed or modified a given subject of care’s PHI in the HITE-CT over a given period of time’ • Audit repository reporting support for ‘the identification of all subjects of care whose PHI has been accessed or modified by

Threat	Description	Risk	Mitigation
			a given HITE-CT user over a given period of time' • Suspicious Activity Reporting • HIE participation agreement require sanction policies by HIE members • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes • Consistent Time (CT) required
Masquerade by service providers (including contracted maintenance personnel such as system software engineers, hardware repair personnel and others who MAY have a pro-forma legitimate reason to access systems and data)	Masquerade by service providers consists of contracted personnel using their privileged access to systems (such as during on-site testing and repair of malfunctioning equipment) to gain unauthorized access to data. As such, it is a breach of – or failure to properly provide for – secure outsourcing arrangements. Though rarer than masquerade by insiders, masquerade by service providers can also be the source of serious breaches in patient confidentiality.	Low	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs

Threat	Description	Risk	Mitigation
			• Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Audit Policy: • Require Meaningful Use Audit Log Tested EHRs • Audit sample to verify that sensitivity OIDs are appropriately applied • Require Meaningful Use Accounting of disclosures Tested EHRs (NOTE: Optional MU test for EHRs) • Require routine audit review of all HIE participants and infrastructure • Audit review supporting inquiry by patient or provider required of all HIE participants and infrastructure • Audit repository reporting support for ' all HITE-CT users who have accessed or modified a given subject of care's PHI in the HITE-CT over a given period of time' • Audit repository reporting support for 'the identification of all subjects of care whose PHI has been accessed or modified by a given HITE-CT user over a given period of time' • Suspicious Activity Reporting • HIE participation agreement require sanction policies by HIE members • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes • Consistent Time (CT) required Access Control Policy • Require Meaningful Use Access Control Tested EHRs • Verification of consents managed according to consent policy • Documents with sensitive, protected content (mental health, HIV, substance abuse, genetics) shall be marked with OID indicating restricted document • Document consumers shall enforce protections associated with content marked as sensitive Consent Policy • Basic Patient Privacy Consents (BPPC) to manage consents • Specify purpose of use
Masquerade by outsiders (including hackers).	Masquerade by outsiders occurs when unauthorized third parties gain access to system data or resources, either by impersonating an authorized user or by fraudulently becoming an authorized user (for example, through so-called "social engineering"). In addition to hackers, masquerade by outsiders is	High	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require personnel training Information Security Policy:

Threat	Description	Risk	Mitigation
	also committed by journalists, private investigators, and "hacktivists" (hackers who work on behalf of, or in sympathy with, political pressure groups). Masquerade by outsiders constitutes a failure of one or more of the following security controls: • User identification; • User authentication; • Origin authentication; or • Access control and privilege management.		• Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Audit Policy: • Require Meaningful Use Audit Log Tested EHRs • Require Meaningful Use Accounting of disclosures Tested EHRs (NOTE: Optional MU test for EHRs) • Require routine audit review of all HIE participants and infrastructure • Audit review supporting inquiry by patient or provider required of all HIE participants and infrastructure • Audit repository reporting support for ' all HITE-CT users who have accessed or modified a given subject of care's PHI in the HITE-CT over a given period of time' • Audit repository reporting support for 'the identification of all subjects of care whose PHI has been accessed or modified by

Threat	Description	Risk	Mitigation
			a given HITE-CT user over a given period of time' • Suspicious Activity Reporting • HIE participation agreement require sanction policies by HIE members • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes • Consistent Time (CT) required Access Control Policy • Require Meaningful Use Access Control Tested EHRs • Verification of consents managed according to consent policy • Documents with sensitive, protected content (mental health, HIV, substance abuse, genetics) shall be marked with OID indicating restricted document • Document consumers shall enforce protections associated with content marked as sensitive Consent Policy • Use Basic Patient Privacy Consents (BPPC) to manage consents • Specify purpose of use
Unauthorized use of a health information application	It can be surprisingly easy to obtain unauthorized access to a health information application (for example, by a patient walking up to an unattended workstation in a physician care office and browsing the screen). Authorized users can also perform *un*authorized actions; such as maliciously altering data. In the UK, Dr. Harold Shipman attempted to hide the notorious murder of scores of his patients by altering records on his computer system. The critical importance of correctly identifying patients and correctly matching them to their health records leads health organizations to collect detailed identifying information on patients treated. This identifying information is of great potential value to those who would use it to commit identity theft and so MUST be rigorously protected. In general, unauthorized use of health information applications constitutes a failure of one or more of the following: • Workgroup access control (e.g., by allowing a user to access the records of patients with whom the user has no legitimate	Med	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training • Require personnel Sanction Policy Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training • Require personnel Sanction Policy Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key

Threat	Description	Risk	Mitigation
	relationship); • Accountability and audit control (e.g., by allowing inappropriate user actions to go unnoticed); or • Personnel security (e.g., by providing inadequate training to users or making clear that their access to records is subject to audit and review).		Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Audit Policy: • Require Meaningful Use Audit Log Tested EHRs • Require Meaningful Use Accounting of disclosures Tested EHRs (NOTE: Optional MU test for EHRs) • Require routine audit review of all HIE participants and infrastructure • Audit review supporting inquiry by patient or provider required of all HIE participants and infrastructure • Audit repository reporting support for ' all HITE-CT users who have accessed or modified a given subject of care's PHI in the HITE-CT over a given period of time' • Audit repository reporting support for 'the identification of all subjects of care whose PHI has been accessed or modified by a given HITE-CT user over a given period of time' • Suspicious Activity Reporting • HIE participation agreement require sanction policies by HIE members • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes • Consistent Time (CT) required Access Control Policy • Require Meaningful Use Access Control Tested EHRs • Verification of consents managed according to consent policy • Documents with sensitive, protected content (mental health,

Threat	Description	Risk	Mitigation
			HIV, substance abuse genetics) shall be marked with OID indicating restricted document • Document consumers shall enforce protections associated with content marked as sensitive • Role Management Consent Policy • Use Basic Patient Privacy Consents (BPPC) to manage consents • Specify purpose of use
Introduction of damaging or disruptive software (including viruses, worms, and other "malware")	Most IT security incidents involve computer viruses. Introduction of damaging or disruptive software constitutes a failure in anti-virus protection or in software change control. While typically within the remit of network sysops, the proliferation of email worms and viruses as well as exploitation by hackers of weaknesses in server software have combined to greatly complicate measures taken to prevent the introduction of damaging or disruptive software.	Med	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training • Require antivirus/malware software installation and update management at least weekly or upon update of vendor definition files, files, and threat detection • Require personnel Sanction Policy Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training • Require antivirus/malware software installation and update management at least weekly or upon update of vendor definition files, files, and threat detection • Require personnel Sanction Policy Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID

Threat	Description	Risk	Mitigation
			• Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Access Control Policy • Require Meaningful Use Access Control Tested EHRs • Verification of consents managed according to consent policy • Documents with sensitive, protected content (mental health, HIV, substance abuse, genetics) shall be marked with OID indicating restricted document • Document consumers shall enforce protections associated with content marked as sensitive • Role Management
Misuse of system resources	This threat includes users using health information systems and services for personal work, users downloading non-work related information from the Internet onto computers intended solely to support health information systems, users setting up databases or other applications for non-work related matters, or users degrading the availability of health information system by, for example, using network bandwidth to download streaming video or audio for personal use. Such misuse constitutes a failure to enforce acceptable use agreements or to educate users about the importance of maintaining the integrity and availability of health information resources	High	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training • Require personnel Sanction Policy • Require antivirus/malware software installation and update management at least weekly or upon update of vendor definition files, files, and threat detection Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training

Threat	Description	Risk	Mitigation
			• Require personnel Sanction Policy • Require antivirus/malware software installation and update management at least weekly or upon update of vendor definition files, files, and threat detection
Communications infiltration	Communications infiltration of electronic communications occurs when an individual (a hacker, for example) tampers with the normal flow of data across a network. The most common result is a denial of service attack (in which servers or network resources are effectively taken off-line), but other forms of communication infiltration are possible (such as a replay attack, in which a valid but out-of-date message is retransmitted in a way that makes it appear current). Communications infiltration constitutes a failure of intrusion detection and/or network access controls and/or risk analysis (specifically vulnerability analysis) and/or system architecture (which needs to be designed with defense against denial-of-service attacks).	Med	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training • Require personnel Sanction Policy • Require Meaningful Use General Encryption Tested EHRs • Require Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require verification of audit review requests to mitigate denial of service attacks • Require Intrusion Detection measures Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require personnel training • Require equivalent capabilities as required for Meaningful Use General Encryption Tested EHRs • Require equivalent capabilities as required for Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require verification of audit review requests to mitigate denial of service attacks • Require Intrusion Detection measures • Require personnel Sanction Policy Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require personnel training • Require equivalent capabilities as required for Meaningful Use General Encryption testing • Require equivalent capabilities as required for Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require verification of audit review requests to mitigate denial of service attacks

Threat	Description	Risk	Mitigation
			• Require Intrusion Detection measures Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Audit Policy: • Require Meaningful Use Audit Log Tested EHRs • Require Meaningful Use Accounting of disclosures Tested EHRs (NOTE: Optional MU test for EHRs) • Require routine audit review of all HIE participants and infrastructure • Audit review supporting inquiry by patient or provider required of all HIE participants and infrastructure • Audit repository reporting support for ' all HITE-CT users who have accessed or modified a given subject of care's PHI in the HITE-CT over a given period of time' • Audit repository reporting support for 'the identification of all subjects of care whose PHI has been accessed or modified by a given HITE-CT user over a given period of time' • Suspicious Activity Reporting • HIE participation agreement require sanction policies by HIE members • Node Authentication and Audit Trails (ATNA) logging

Threat	Description	Risk	Mitigation
			requirements of all HIE nodes • Consistent Time (CT) required
Communications interception	If not encrypted during transmission, the confidentiality of information contained in a message can be abrogated by intercepting the communication. This is simpler than it sounds, as anyone on local area network can potentially install a so-called "packet sniffer" on their workstation and monitor much of the network traffic on their local area network, including reading emails during transmission. Hacker tools are readily available to automate and simplify much of this process. Communications interception constitutes a failure in secure communications.	Med	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require personnel training • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require Meaningful Use General Encryption Tested EHRs • Require Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require verification of audit review requests to mitigate denial of service attacks • Require Intrusion Detection measures Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training • Require equivalent capabilities as required for Meaningful Use General Encryption Tested EHRs • Require equivalent capabilities as required for Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require verification of audit review requests to mitigate denial of service attacks • Require Intrusion Detection measures Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified

Threat	Description	Risk	Mitigation
			relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes
Repudiation	This threat includes users denying that they sent a message (repudiation of origin) and users denying that they received a message (repudiation of receipt). Unambiguously establishing whether personal health information flowed from on health provider to another can be an essential feature of investigations into medical malpractice. Repudiation can constitute a failure to apply controls such as digital signatures on e-prescriptions (an example of repudiation of origin) or controls such as read receipts on email messages (an example of repudiation of receipt).	Med	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Encourage the use of Document Digital Signature Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Encourage the use of Document Digital Signature Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital

Threat	Description	Risk	Mitigation
			certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Audit Policy: • Require Meaningful Use Audit Log Tested EHRs • Require Meaningful Use Accounting of disclosures Tested EHRs (NOTE: Optional MU test for EHRs) • Require routine audit review of all HIE participants and infrastructure • Audit review supporting inquiry by patient or provider required of all HIE participants and infrastructure • Audit repository reporting support for ' all HITE-CT users who have accessed or modified a given subject of care's PHI in the HITE-CT over a given period of time' • Audit repository reporting support for 'the identification of all subjects of care whose PHI has been accessed or modified by a given HITE-CT user over a given period of time' • Suspicious Activity Reporting • HIE participation agreement require sanction policies by HIE members • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes • Consistent Time (CT) required
Connection failure (including failures of health information networks)	All networks are subject to periodic service outages. Quality of service is a major factor in the provisioning of network services in health care. Connection failure can also result from misdirection of network services (for example, malicious alteration of routing tables that cause network traffic to be diverted). Connection failures can facilitate the disclosure of confidential information by forcing users to send messages by a less secure mechanism, such as via fax or over the Internet.	High	Participation Agreement: • Require ISO 27799:2008, *Health informatics – Information security management in health using ISO/IEC 27002* • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 Information Security Policy: • Require ISO 27799:2008, *Health informatics – Information security management in health using ISO/IEC 27002* • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication,

Threat	Description	Risk	Mitigation
			General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16
Embedding of malicious code	This threat includes email viruses and hostile mobile code. While in no way unique to health information systems, the increasing use of wireless and mobile technologies by health care providers increases this threat's potential for damage. Embedding of malicious code constitutes a failure to effectively apply anti-virus software controls or intrusion prevention controls.	Med	Participation Agreement: • Require ISO 27799:2008, *Health informatics – Information security management in health using ISO/IEC 27002* • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training • Require antivirus/malware software installation and update management at least weekly or upon update of vendor definition files, files, and threat detection • Require Intrusion Detection measures Information Security Policy: • Require ISO 27799:2008, *Health informatics – Information security management in health using ISO/IEC 27002* • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training • Require antivirus/malware software installation and update management at least weekly or upon update of vendor definition files, files, and threat detection • Require Intrusion Detection measures Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates

Threat	Description	Risk	Mitigation
			Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Access Control Policy • Require Meaningful Use Access Control Tested EHRs • Verification of consents managed according to consent policy • Documents with sensitive, protected content (mental health, HIV, substance abuse, genetics) shall be marked with OID indicating restricted document • Document consumers shall enforce protections associated with content marked as sensitive Role Management
Accidental misrouting	This threat includes the possibility that information might be delivered to an incorrect address when it is being sent over a network. Accidental misrouting could constitute a failure in user education or a failure to maintain the integrity of directories of health providers (or both).	High	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training • Require processes for directory verification an review management by HIE participants Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require personnel training Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key

Threat	Description	Risk	Mitigation
			Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Access Control Policy • Require Meaningful Use Access Control Tested EHRs • Verification of consents managed according to consent policy • Documents with sensitive, protected content (mental health, HIV, substance abuse, genetics) shall be marked with OID indicating restricted document • Document consumers shall enforce protections associated with content marked as sensitive • Role Management
Technical failure of the host, storage facility, or network infrastructure	These threats include hardware failures, network failures, or failures in data storage facilities. Such failures typically constitute a failure of one or more of the operations management controls listed in section 10 of ISO/IEC 17799. While in no way unique to health information systems, the loss of availability of such systems can have life-threatening consequences for patients.	High	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic

Threat	Description	Risk	Mitigation
			health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16
Environmental support failure (including power failures and disruptions of service from natural or man-made disasters)	Health information systems can be critically needed during natural disasters and other events that can be life-threatening to large numbers of people. These same disasters can wreak havoc on the environmental support systems needed to maintain operations. A proper threat and risk assessment of health information will include an assessment of how critical such systems are in times of natural disaster and how robust their operations will be under such disaster scenarios.	Med	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require disaster recovery plans and controls Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require disaster recovery plans and controls
System or network software failure	Denial of service attacks are greatly facilitated by weaknesses in or miss configuration of operating system or network operating system software. System or network software failure constitutes a failure in software integrity checking, system testing, or software maintenance controls.	High	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require change management processes and controls • Require configuration management controls Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional)

Threat	Description	Risk	Mitigation
			• Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require parallel test environment for change management • Require change management processes and controls • Require configuration management controls
Application software failure (e.g., of a health information application)	Failures in application software can be exploited in a denial of service attack and can also be used to compromise the confidentiality of protected data. Application software failure constitutes a failure in software testing, software change controls, or software integrity checking.	Low	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require change management processes and controls • Require configuration management controls Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require parallel test environment for change management • Require change management processes and controls • Require configuration management controls
Operations error	Operator error accounts for a small but significant percentage of unintentional disclosures of confidential information and a large proportion of unintentional dispositions of data. Operator errors constitute a failure in one or more of the following: • Operations controls; • Personnel security (including effective training); or • Disaster recovery (including data backup and restoration).	Low	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require change management processes and controls • Require configuration management controls

Threat	Description	Risk	Mitigation
			• Require disaster recovery plans and controls • Require backup/restoration policy/procedures • Require personnel training Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require parallel test environment for change management • Require change management processes and controls • Require configuration management controls • Require disaster recovery plans and controls • Require backup/restoration policy/procedures • Require personnel training

Threat	Description	Risk	Mitigation
Maintenance error	Maintenance errors include mistakes by those responsible for maintaining systems hardware and software. Maintenance errors can be committed by staff members as well as third party employees contracted to perform maintenance duties. Such errors can, in turn, endanger the confidentiality of protected data. Misconfiguration of software during installation is a common cause of vulnerabilities later exploited by hackers. Maintenance errors constitute a failure in hardware maintenance controls, software maintenance controls, software change controls, or some combination of the above.		Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require change management processes and controls • Require configuration management controls • Require personnel training Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require parallel test environment for change management • Require change management processes and controls • Require configuration management controls • Require personnel training
User error	Error by users can, for example, result in confidential information being sent to the wrong recipient. User errors can sometimes constitute a failure in: • User controls (including user interfaces designed with security in mind); or • Personnel security (including training)		Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require personnel training Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require personnel training
Staff shortage	The threat of staff shortage includes the possibility of the absence of key personnel and the difficulty of replacing them; the vulnerability to this threat depends on the extent to which	Low	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic

Threat	Description	Risk	Mitigation
	shortage of staff would affect the business processes. In health care, an epidemic that greatly increases the demand for timely access to health information MAY also create a staff shortage that jeopardizes the availability of such systems. A failure of this kind constitutes a failure in business continuity management (see section 14 of ISO/IEC 17799).		Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require disaster recovery plans and controls Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require disaster recovery plans and controls
Theft by insiders (including theft of equipment or data)	Insiders typically have greater access to confidential information and are therefore in a favorable position to steal the information in order to sell it or to disclose it others. While comparatively rare, the threat of theft by insiders of personal health information increases with the fame or notoriety of the data subject (e.g., a celebrity or head of state) and decreases with the potential severity of punitive consequences (e.g., the loss by a physician of her license to practice). Theft by insiders constitutes a failure of one of many possible controls, including controls on hardcopy output, documents or media; physical security; or physical protection of equipment.	Low	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require Meaningful Use General Encryption Tested EHRs • Require Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require personnel training • Require personnel Sanction Policy Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require equivalent capabilities as required for Meaningful Use General Encryption Tested EHRs • Require equivalent capabilities as required for Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require Encryption of Data at Rest • Require conformance to security requirements of HITECH • Require personnel training

Threat	Description	Risk	Mitigation
			• Require personnel Sanction Policy Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Audit Policy: • Require Meaningful Use Audit Log Tested EHRs • Require Meaningful Use Accounting of disclosures Tested EHRs (NOTE: Optional MU test for EHRs) • Require routine audit review of all HIE participants and infrastructure • Audit review supporting inquiry by patient or provider required of all HIE participants and infrastructure • Audit repository reporting support for ' all HITE-CT users who have accessed or modified a given subject of care's PHI in the HITE-CT over a given period of time' • Audit repository reporting support for 'the identification of all subjects of care whose PHI has been accessed or modified by a given HITE-CT user over a given period of time' • Suspicious Activity Reporting • HIE participation agreement require sanction policies by HIE members • Node Authentication and Audit Trails (ATNA) logging

Threat	Description	Risk	Mitigation
			requirements of all HIE nodes • Consistent Time (CT) required Access Control Policy • Require Meaningful Use Access Control Tested EHRs • Verification of consents managed according to consent policy • Documents with sensitive, protected content (mental health, HIV, substance abuse, genetics) shall be marked with OID indicating restricted document • Document consumers shall enforce protections associated with content marked as sensitive Consent Policy • Use Basic Patient Privacy Consents (BPPC) to manage consents • Specify purpose of use
Theft by outsiders (including theft of equipment or data)	Theft by outsiders of data and equipment is a serious problem in some hospitals. Theft MAY result in breaches of confidentiality, either because confidential data resides on a server or laptop computer that is subsequently stolen or else because the data itself is the target of the theft. Theft by outsiders MAY constitute a failure in one of many controls; including mobile computing controls, secure media transport, incident handling, compliance checks, or physical theft protection.	Med	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require Meaningful Use General Encryption Tested EHRs • Require Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require conformance to security requirements of HITECH • Require personnel training • Require personnel Sanction Policy Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require equivalent capabilities as required for Meaningful Use General Encryption Tested EHRs • Require equivalent capabilities as required for Meaningful Use

Threat	Description	Risk	Mitigation
			Encryption When Exchanging Electronic Health Information Tested EHRs • Require Encryption of Data at Rest • Require conformance to security requirements of HITECH • Require personnel training • Require personnel Sanction Policy Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Audit Policy: • Require Meaningful Use Audit Log Tested EHRs • Require Meaningful Use Accounting of disclosures Tested EHRs (NOTE: Optional MU test for EHRs) • Require routine audit review of all HIE participants and infrastructure • Audit review supporting inquiry by patient or provider required of all HIE participants and infrastructure • Audit repository reporting support for ‘ all HITE-CT users who have accessed or modified a given subject of care’s PHI in the HITE-CT over a given period of time’ • Audit repository reporting support for ‘the identification of all subjects of care whose PHI has been accessed or modified by

Threat	Description	Risk	Mitigation
			a given HITE-CT user over a given period of time' • Suspicious Activity Reporting • HIE participation agreement require sanction policies by HIE members • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes • Consistent Time (CT) required Access Control Policy • Require Meaningful Use Access Control Tested EHRs • Verification of consents managed according to consent policy • Documents with sensitive, protected content (mental health, HIV, substance abuse, genetics) shall be marked with OID indicating restricted document • Document consumers shall enforce protections associated with content marked as sensitive Consent Policy • Use Basic Patient Privacy Consents (BPPC) to manage consents • Specify purpose of use
Willful damage by insiders	Willful damage by insiders includes acts of vandalism and other cases where physical damage is caused to IT systems or their supporting environment by people who have been granted access. The users of health information systems are typically dedicated health professionals and willful damage is rare. Willful damage by insiders constitutes a failure of human resources security (see section 8 of ISO/IEC 17799).		Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require Meaningful Use General Encryption Tested EHRs • Require Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require personnel training • Require personnel Sanction Policy Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC

Threat	Description	Risk	Mitigation
			(infrastructure), SAS70 (nodes), SSAE 16 • Require equivalent capabilities as required for Meaningful Use General Encryption Tested EHRs • Require equivalent capabilities as required for Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require Encryption of Data at Rest • Require conformance to security requirements of HITECH • Require personnel training • Require personnel Sanction Policy Audit Policy: • Require Meaningful Use Audit Log Tested EHRs • Require Meaningful Use Accounting of disclosures Tested EHRs (NOTE: Optional MU test for EHRs) • Require routine audit review of all HIE participants and infrastructure • Audit review supporting inquiry by patient or provider required of all HIE participants and infrastructure • Audit repository reporting support for ' all HITE-CT users who have accessed or modified a given subject of care's PHI in the HITE-CT over a given period of time' • Audit repository reporting support for 'the identification of all subjects of care whose PHI has been accessed or modified by a given HITE-CT user over a given period of time' • Suspicious Activity Reporting • HIE participation agreement require sanction policies by HIE members • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes • Consistent Time (CT) required
Willful damage by outsiders	The threat of willful damage by outsiders includes acts of vandalism and other cases where physical damage is caused to IT systems or their supporting environment by people who have not been granted access to such systems. While in most industrial sectors, failures of this kind constitute a failure to effective apply physical security controls, access by patients and their friends and relatives to operational areas of hospitals, clinics and other health organizations make such threats much more difficult to prevent than in most other operational environments. The security controls in section 9 of ISO/IEC 17799 need to be	Med	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require Meaningful Use General Encryption Tested EHRs • Require Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs

Threat	Description	Risk	Mitigation
	carefully selected and applied to minimize such threats.		• Require Intrusion Detection measures • Require personnel training • Require personnel Sanction Policy Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require equivalent capabilities as required for Meaningful Use General Encryption Tested EHRs • Require equivalent capabilities as required for Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require Encryption of Data at Rest • Require conformance to security requirements of HITECH • Require Intrusion Detection measures • Require personnel training • Require personnel Sanction Policy Identity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs

Threat	Description	Risk	Mitigation
			• Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Audit Policy: • Require Meaningful Use Audit Log Tested EHRs • Require Meaningful Use Accounting of disclosures Tested EHRs (NOTE: Optional MU test for EHRs) • Require routine audit review of all HIE participants and infrastructure • Audit review supporting inquiry by patient or provider required of all HIE participants and infrastructure • Audit repository reporting support for ' all HITE-CT users who have accessed or modified a given subject of care's PHI in the HITE-CT over a given period of time' • Audit repository reporting support for 'the identification of all subjects of care whose PHI has been accessed or modified by a given HITE-CT user over a given period of time' • Suspicious Activity Reporting • HIE participation agreement require sanction policies by HIE members • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes • Consistent Time (CT) required Access Control Policy • Require Meaningful Use Access Control Tested EHRs • Verification of consents managed according to consent policy • Documents with sensitive, protected content (mental health, HIV, substance abuse, genetics) shall be marked with OID indicating restricted document • Document consumers shall enforce protections associated with content marked as sensitive Consent Policy • Use Basic Patient Privacy Consents (BPPC) to manage consents • Specify purpose of use
Business Threats	This includes failure of business continuity. The requirements for data retention, destruction, or hand-off to other resources		
Data/Information integrity	Failure of MPI matching Document Replacement: every encounter; previous record:		Participation Agreement: • Best practices: update the information as close to the patient visit as possible

Threat	Description	Risk	Mitigation
	Non-repudiation – retention of documents that have been used for decisions		• All nodes shall support the update notification option •
Records sent in advance of a relationship with a patient			Audit Policy: If requested information, but didn't provide a summary – may need to be refined; limit to primary care (consult is less likely) Participation Agreement
Integrity of data segregation	Marking of sensitive information		
Terrorism	The threat of terrorism includes acts by extremist groups wishing to cause damage or disruption to the work of health organizations, to harm health care providers, or to disrupt the operations of health information systems. While no such large-scale attacks have occurred yet, planners need to consider the threat of terrorism, especially when large-scale health information systems are designed, as an attack on such systems could increase the effectiveness of bioterrorist and other attacks that cause a health-related crisis.	Low	Participation Agreement: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require Meaningful Use General Encryption Tested EHRs • Require Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require Intrusion Detection measures • Require personnel training • Require personnel Sanction Policy Information Security Policy: • Require ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002 • Require policies and protections for Access control, Automatic Logoff, Audit log, Emergency Access, Integrity, Authentication, General encryption, Encryption when exchanging electronic health information, Accounting of disclosures (optional) • Require HIE Infrastructure Service components to be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 (nodes), SSAE 16 • Require equivalent capabilities as required for Meaningful Use General Encryption Tested EHRs • Require equivalent capabilities as required for Meaningful Use Encryption When Exchanging Electronic Health Information Tested EHRs • Require Encryption of Data at Rest • Require conformance to security requirements of HITECH • Require Intrusion Detection measures

Threat	Description	Risk	Mitigation
			• Require personnel training • Require personnel Sanction PolicIdentity Management Policy • Entity Identity Assertion (XUA) Requirements • Certification Authority requirements for conformance to ISO IS17090 Health Informatics – Public Key Infrastructure • Certification Authority requirements for Federal Public Key Infrastructure (PKI) Bridge Certified CA • Require procedures for account revocation upon employee severance and notifications for HIE account revocations • Identity proofing requiring A government issued photographic identification or ID • Affiliation proofing with healthcare licensure or identified relationship with healthcare organization • Account subscriber agreements requiring protection of identity credential • Trusted Third Party Attestation of organization system digital certificates Authentication Policy: • Require Meaningful Use Authentication Tested EHRs • Require Meaningful Use Emergency Access Tested EHRs • Require Meaningful Use Automatic Loggoff Tested EHRs • Strong authentication required for remote access • Node Authentication and Audit Trails (ATNA) logging requirements of all HIE nodes Audit Policy: • Require Meaningful Use Audit Log Tested EHRs • Require Meaningful Use Accounting of disclosures Tested EHRs (NOTE: Optional MU test for EHRs) • Require routine audit review of all HIE participants and infrastructure • Audit review supporting inquiry by patient or provider required of all HIE participants and infrastructure • Audit repository reporting support for ' all HITE-CT users who have accessed or modified a given subject of care's PHI in the HITE-CT over a given period of time' • Audit repository reporting support for 'the identification of all subjects of care whose PHI has been accessed or modified by a given HITE-CT user over a given period of time' • Suspicious Activity Reporting • HIE participation agreement require sanction policies by HIE members • Node Authentication and Audit Trails (ATNA) logging

Threat	Description	Risk	Mitigation
			requirements of all HIE nodes • Consistent Time (CT) required Access Control Policy • Require Meaningful Use Access Control Tested EHRs • Verification of consents managed according to consent policy • Documents with sensitive, protected content (mental health, HIV, substance abuse, genetics) shall be marked with OID indicating restricted document • Document consumers shall enforce protections associated with content marked as sensitive Consent Policy • Use Basic Patient Privacy Consents (BPPC) to manage consents • Specify purpose of use
Lack of Consumer Trust and Participation Barriers	Lack of trust of the part of consumers that their health information will be managed securely and appropriate information use can limit participation in the HIE, the associated HIE benefits and other business-level concerns.	High	Consumer Policy • Consumer policy rights to request record • Consumer remedies • Describe rights and Process for complaints if there is a breech • Request accounting of disclosures • Personal Health Record Interoperability Policies and Procedures o Disclosure has to come through a covered entity • Format of record o One summary record o List of all documents o Limited to the type of documents collected by the HIE • Proved procedures and instructions for how to Opt-Out of the Health Information Exchange • Disclosures of purposes of use of the HIE managed information • Patient education regarding risk mitigation • Participation agreements • If sending patient data to their selected PHR, assure that encryption is applied to the information

The reader is referred to the ISO 27799:2008, *Health informatics – Information security management in health using ISO/IEC 27002* for details regarding security management in health care.

The threats listed above are of particular concern in the context of:

- Identity theft
- Masquerade
- Data Modification
- Data availability
- Patient Safety

11.12 Future system developments

The policy agreement SHALL commit all parties to implement their systems according to this and other accepted standards in order to facilitate future co-operation for information transfer between their systems. All information exchange functions are specified in the policy agreement.

Appendix X: HITE-CT Specification of Value Sets used to support the HITE-CT Affinity Domain Policy

A.1 HITE-CT Mental Health Role codes

A.1.1 Metadata

Metadata Element	Description	Mandatory
Identifier	This is the unique identifier of the value set	1.3.6.1.4.1. 38571.3.1
Name	This is the name of the value set	HITE-CT Mental Health Role
Source	This is the source of the value set, identifying the originator or publisher of the information	HITE-CT
Purpose	Brief description about the general purpose of the value set	To Reflect those roles dedicated to mental health care provision
Definition	A text definition describing how concepts in the value set were selected	Extensional definition: The value set was constructed by enumerating the codes from the list of values supporting the HITE-CT metadata authorRole
Source URI	Most sources also have a URL or document URI that provides further details regarding the value set.	http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html
Version	A string identifying the specific version of the value set.	Version 1.0
Status	Active (Current) or Inactive	Active
Effective Date	The date when the value set is expected to be effective	10/20/2011
Expiration Date	The date when the value set is no longer expected to be used	N/A

Metadata Element	Description	Mandatory
Creation Date	The date of creation of the value set	9/7/2011
Revision Date	The date of revision of the value set	N/A
Groups	The identifiers of the groups that include this value set. A group may also have an OID assigned.	HITE-CT Metadata

A.1.2 HITE-CT Mental Health Role Value Set Table

The HITE-CT Mental Health Role Value Set uses the values from the subset of SNOMED-CT code system to identify its contents define in Table 9.1.1.4-1 Connecticut CT DPH Regulated
1835 Professions. Codes that are used within the scope of this Affinity Domain Policy are listed below:

Value Set:		1.3.6.1.4.1. 38571.3.1	
Vocabulary:			*2.16.840.1.113883.6.96*
CT License Code	**SNOMED-CT Code**	**CT License Description**	**SNOMED-CT Code description**
1 WHERE SPECIALTY = Psychiatry	80584001	Physician/Surgeon	Psychiatrist (occupation)
8	59944000	Psychologist	Psychologist (occupation)
27	224596008	Marital and Family Therapist	Marriage guidance counselor (occupation)
46	310190000	Mental Health Counselor	Mental health counselor (occupation)
58	106328005	Clinical Social Worker	Social worker (occupation)

A.2 HITE-CT Substance Abuse Role codes

A.2.1 Metadata

Metadata Element	Description	Mandatory
Identifier	This is the unique identifier of the value set	1.3.6.1.4.1. 38571.3.2
Name	This is the name of the value set	HITE-CT Substance Abuse Role
Source	This is the source of the value set, identifying the originator or publisher of the information	HITE-CT
Purpose	Brief description about the general purpose of the value set	To Reflect those roles dedicated to substance abuse care provision

Metadata Element	Description	Mandatory
Definition	A text definition describing how concepts in the value set were selected	Extensional definition: The value set was constructed by enumerating the codes from the list of values supporting the HITE-CT metadata authorRole
Source URI	Most sources also have a URL or document URI that provides further details regarding the value set.	http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html
Version	A string identifying the specific version of the value set.	Version 1.0
Status	Active (Current) or Inactive	Active
Effective Date	The date when the value set is expected to be effective	10/20/2011
Expiration Date	The date when the value set is no longer expected to be used	N/A
Creation Date	The date of creation of the value set	9/7/2011
Revision Date	The date of revision of the value set	N/A
Groups	The identifiers of the groups that include this value set. A group may also have an OID assigned.	HITE-CT Metadata

A.2.2 HITE-CT Substance Abuse Role Value Set Table

The HITE-CT Substance Abuse Role Value Set uses the values from the subset of SNOMED-CT code system to identify its contents define in Table 9.1.1.4-1 Connecticut CT DPH Regulated Professions. Codes that are used within the scope of this Affinity Domain Policy are listed below:

Value Set:		1.3.6.1.4.1. 38571.3.2	
Vocabulary:			*2.16.840.1.113883.6.96*
CT License Code	**SNOMED-CT Code**	**CT License Description**	**SNOMED-CT Code description**
44	446701002	Licensed Alcohol and Drug Counselor	Addiction medicine specialist (occupation)
45	446701002	Certified Alcohol and Drug Counselor	Addiction medicine specialist (occupation)

A.3 HITE-CT Mental Health Role codes

A.3.1 Metadata

Metadata Element	Description	Mandatory

Metadata Element	Description	Mandatory
Identifier	This is the unique identifier of the value set	1.3.6.1.4.1. 38571.3.3
Name	This is the name of the value set	HITE-CT Mental Health Specialty
Source	This is the source of the value set, identifying the originator or publisher of the information	HITE-CT
Purpose	Brief description about the general purpose of the value set	To Reflect those specialties dedicated to mental health care provision
Definition	A text definition describing how concepts in the value set were selected	Extensional definition: The value set was constructed by enumerating the codes from the list of values supporting the HITE-CT metadata authorRole
Source URI	Most sources also have a URL or document URI that provides further details regarding the value set.	http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html
Version	A string identifying the specific version of the value set.	Version 1.0
Status	Active (Current) or Inactive	Active
Effective Date	The date when the value set is expected to be effective	10/20/2011
Expiration Date	The date when the value set is no longer expected to be used	N/A
Creation Date	The date of creation of the value set	9/7/2011
Revision Date	The date of revision of the value set	N/A
Groups	The identifiers of the groups that include this value set. A group may also have an OID assigned.	HITE-CT Metadata

A.3.2 HITE-CT Mental Health Specialty Value Set Table

1850 The HITE-CT Mental Health Specialty Value Set uses the values from the subset of SNOMED-CT code system to identify its contents define in Table 9.3.1.4-1 authorSpecialty Value Set Definition. Codes that are used within the scope of this Affinity Domain Policy are listed below:

Value Set:		1.3.6.1.4.1. 38571.3.3	
Vocabulary:			*2.16.840.1.113883.6.96*
CT Specialty Code	**SNOMED-CT Code**	**CT Specialty Description**	**SNOMED-CT Code description**
NA	408467006	NA	Adult mental illness
141	394588006	Adolescent Medicine	Pediatric (Child and adolescent) psychiatry
56	394587001	Psychiatry	Psychiatry
106		Psychiatry	
145		Psychiatry	

NA	394913002	NA	Psychotherapy

A.4 HITE-CT Substance Abuse Specialty codes

A.4.1 Metadata

Metadata Element	Description	Mandatory
Identifier	This is the unique identifier of the value set	1.3.6.1.4.1. 38571.3.4
Name	This is the name of the value set	HITE-CT Substance Abuse Specialty
Source	This is the source of the value set, identifying the originator or publisher of the information	HITE-CT
Purpose	Brief description about the general purpose of the value set	To Reflect those specialties dedicated to substance abuse care provision
Definition	A text definition describing how concepts in the value set were selected	Extensional definition: The value set was constructed by enumerating the codes from the list of values supporting the HITE-CT metadata authorRole
Source URI	Most sources also have a URL or document URI that provides further details regarding the value set.	http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html
Version	A string identifying the specific version of the value set.	Version 1.0
Status	Active (Current) or Inactive	Active
Effective Date	The date when the value set is expected to be effective	10/20/2011
Expiration Date	The date when the value set is no longer expected to be used	N/A
Creation Date	The date of creation of the value set	9/7/2011
Revision Date	The date of revision of the value set	N/A
Groups	The identifiers of the groups that include this value set. A group may also have an OID assigned.	HITE-CT Metadata

A.4.2 HITE-CT Substance Abuse Specialty Value Set Table

The HITE-CT Substance Abuse Specialty Value Set uses the values from the subset of SNOMED-CT code system to identify its contents define in Table 9.3.1.4-1 authorSpecialty Value Set Definition. Codes that are used within the scope of this Affinity Domain Policy are listed below:

		Value Set:	1.3.6.1.4.1. 38571.3.4
		Vocabulary:	*2.16.840.1.113883.6.96*
CT Specialty Code	**SNOMED-CT Code**	**CT Specialty Description**	**SNOMED-CT Description**

None			

A.5 HITE-CT Mental Health Facility Type codes

A.5.1 Metadata

Metadata Element	Description	Mandatory
Identifier	This is the unique identifier of the value set	1.3.6.1.4.1. 38571.3.5
Name	This is the name of the value set	HITE-CT Mental Health Facility Type
Source	This is the source of the value set, identifying the originator or publisher of the information	HITE-CT
Purpose	Brief description about the general purpose of the value set	To Reflect those Facility Types dedicated to mental health care provision
Definition	A text definition describing how concepts in the value set were selected	Extensional definition: The value set was constructed by enumerating the codes from the list of values supporting the HITE-CT metadata facilityType
Source URI	Most sources also have a URL or document URI that provides further details regarding the value set.	http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html
Version	A string identifying the specific version of the value set.	Version 1.0
Status	Active (Current) or Inactive	Active
Effective Date	The date when the value set is expected to be effective	10/20/2011
Expiration Date	The date when the value set is no longer expected to be used	N/A
Creation Date	The date of creation of the value set	9/7/2011
Revision Date	The date of revision of the value set	N/A
Groups	The identifiers of the groups that include this value set. A group may also have an OID assigned.	HITE-CT Metadata

A.5.2 HITE-CT Mental Health Facility Type Value Set Table

The HITE-CT Mental Health Facility Type Value Set uses the values from the subset of SNOMED-CT code system to identify its contents define in Table 9.3.1.7-1 Healthcare Facility Type Value Set. Codes that are used within the scope of this Affinity Domain Policy are listed below:

Value Set:	**1.3.6.1.4.1. 38571.3.5**
Vocabulary:	***2.16.840.1.113883.6.96***

SNOMED-CT Code	SNOMED-CT Description
62480006	Hospital-psychiatric
14866005	Hospital outpatient mental health center
51563005	Free-standing mental health center
309898008	Psychogeriatric day hospital

A.6 HITE-CT Substance Abuse Facility Type codes

A.6.1 Metadata

Metadata Element	Description	Mandatory
Identifier	This is the unique identifier of the value set	1.3.6.1.4.1. 38571.3.6
Name	This is the name of the value set	HITE-CT Substance Abuse Facility Type
Source	This is the source of the value set, identifying the originator or publisher of the information	HITE-CT
Purpose	Brief description about the general purpose of the value set	To Reflect those Facility Types dedicated to substance abuse care provision
Definition	A text definition describing how concepts in the value set were selected	Extensional definition: The value set was constructed by enumerating the codes from the list of values supporting the HITE-CT metadata facilityType
Source URI	Most sources also have a URL or document URI that provides further details regarding the value set.	http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html
Version	A string identifying the specific version of the value set.	Version 1.0
Status	Active (Current) or Inactive	Active
Effective Date	The date when the value set is expected to be effective	10/20/2011
Expiration Date	The date when the value set is no longer expected to be used	N/A
Creation Date	The date of creation of the value set	9/7/2011
Revision Date	The date of revision of the value set	N/A
Groups	The identifiers of the groups that include this value set. A group may also have an OID assigned.	HITE-CT Metadata

A.6.2 HITE-CT Substance Abuse Facility Type Value Set Table

The HITE-CT Substance Abuse Facility Type Value Set uses the values from the subset of SNOMED-CT code system to identify its contents define in Table 9.3.1.7-1 Healthcare Facility Type Value Set. Codes that are used within the scope of this Affinity Domain Policy are listed below:

B

Value Set:	1.3.6.1.4.1. 38571.3.6
Vocabulary:	*2.16.840.1.113883.6.96*
SNOMED-CT Code	**SNOMED-CT Description**
20078004	Substance abuse treatment center

B.1 HITE-CT Mental Health Practice Setting codes

B.1.1 Metadata

Metadata Element	Description	Mandatory
Identifier	This is the unique identifier of the value set	1.3.6.1.4.1. 38571.3.7
Name	This is the name of the value set	HITE-CT Mental Health Practice Setting
Source	This is the source of the value set, identifying the originator or publisher of the information	HITE-CT
Purpose	Brief description about the general purpose of the value set	To Reflect those Facility Types dedicated to mental health care provision
Definition	A text definition describing how concepts in the value set were selected	Extensional definition: The value set was constructed by enumerating the codes from the list of values supporting the HITE-CT metadata practiceSetting
Source URI	Most sources also have a URL or document URI that provides further details regarding the value set.	http://www.adldata.com/Downloads/Provider-Taxonomy.html
Version	A string identifying the specific version of the value set.	Version 1.0
Status	Active (Current) or Inactive	Active
Effective Date	The date when the value set is expected to be effective	10/20/2011
Expiration Date	The date when the value set is no longer expected to be used	N/A
Creation Date	The date of creation of the value set	9/7/2011
Revision Date	The date of revision of the value set	N/A
Groups	The identifiers of the groups that include this value set. A group may also have an OID assigned.	HITE-CT Metadata

B.1.2 HITE-CT Mental Health Practice Setting Value Set Table

The HITE-CT Mental Health Practice setting Value Set uses the values from the subset of SNOMED-CT code system to identify its contents define in Table 9.3.1.8-1 Practice Setting Value Set. Codes that are used within the scope of this Affinity Domain Policy are listed below:

Value Set:	1.3.6.1.4.1. 38571.3.7

Vocabulary:			2.16.840.1.114222.4.11.1066
CT Practice Setting Code	**Healthcare Provider Taxonomy (HIPAA) Code**	**CT Practice Setting Description**	**Healthcare Provider Taxonomy (HIPAA) Description**
RCH	**311Z00000X**	Residential Care Facility	Residential Care Home
PSY	**283Q00000X**	Hospitals for Mentally Ill Persons	Hospital for Mentally Ill Persons
MHDT	**261QM0801X**	Mental Health Day Treatment	Mental Health Day Treatment Facility
MHIT	**320800000X**	Mental Health Intermediate Treatment	Mental Health Intermediate Treatment Facility
POCA	**261QM0801X**	Psychiatric Outpatient Clinic	Psychiatric Outpatient Clinic for Adults
MHRL	**3104A0625X**	Mental Health Residential Living	Mental Health Residential Living Center
MHCR	**320800000X**	Mental Health Community Residence	Mental Health Community Residence

B.2 HITE-CT Substance Abuse Practice Setting codes

B.2.1 Metadata

Metadata Element	Description	Mandatory
Identifier	This is the unique identifier of the value set	1.3.6.1.4.1. 38571.3.8
Name	This is the name of the value set	HITE-CT Substance Abuse Practice Setting
Source	This is the source of the value set, identifying the originator or publisher of the information	HITE-CT
Purpose	Brief description about the general purpose of the value set	To Reflect those Practice Settings dedicated to substance abuse care provision
Definition	A text definition describing how concepts in the value set were selected	Extensional definition: The value set was constructed by enumerating the codes from the list of values supporting the HITE-CT metadata practiceSetting
Source URI	Most sources also have a URL or document URI that provides further details regarding the value set.	http://www.adldata.com/Downloads/Provider-Taxonomy.html

Metadata Element	Description	Mandatory
Version	A string identifying the specific version of the value set.	Version 1.0
Status	Active (Current) or Inactive	Active
Effective Date	The date when the value set is expected to be effective	10/20/2011
Expiration Date	The date when the value set is no longer expected to be used	N/A
Creation Date	The date of creation of the value set	9/7/2011
Revision Date	The date of revision of the value set	N/A
Groups	The identifiers of the groups that include this value set. A group may also have an OID assigned.	HITE-CT Metadata

B.2.2 HITE-CT Substance Abuse Practice Setting Value Set Table

The HITE-CT Substance Abuse Practice Setting Value Set uses the values from the subset of SNOMED-CT code system to identify its contents define in Table 9.3.1.8-1 Practice Setting Value Set. Codes that are used within the scope of this Affinity Domain Policy are listed below:

Value Set:		**1.3.6.1.4.1. 38571.3.8**	
Vocabulary:			**2.16.840.1.114222.4.11.1066**
CT Practice Setting Code	**Healthcare Provider Taxonomy (HIPAA) Code**	**CT Practice Setting Description**	**Healthcare Provider Taxonomy (HIPAA) Description**
SA	**324500000X**	Substance Abuse	Facility for the Care or Treatment of Substance Abusive or Dependent Persons

1.1 HIV Findings (SNOMED-CT)

1.1.1 Metadata

Metadata Element	Descritption	Mandatory
Identifier	This is the unique identifier of the value set	1.3.6.1.4.1. 38571.3.9
Name	This is the name of the value set	HIV Finding Value Set
Source	This is the source of the value set, identifying the originator or publisher of the information	HITE-CT
Purpose	Brief description about the general purpose of the value set	To Reflect HIV Findings using SNOMED-CT concepts

Metadata Element	Descritption	Mandatory
Definition	A text definition describing how concepts in the value set were selected	Extensional definition: The value set was constructed by enumerating the codes from SNOMED-CT
Source URI	Most sources also have a URL or document URI that provides further details regarding the value set.	http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html
Version	A string identifying the specific version of the value set.	Version 1.0
Status	Active (Current) or Inactive	Active
Effective Date	The date when the value set is expected to be effective	10/20/2011
Expiration Date	The date when the value set is no longer expected to be used	N/A
Creation Date	The date of creation of the value set	10/20/2011
Revision Date	The date of revision of the value set	N/A
Groups	The identifiers of the groups that include this value set. A group may also have an OID assigned.	HITE-CT Sensitive Data

1.1.2 HIV Findings Value Set

	Value Set:	1.3.6.1.4.1. 38571.3.9
	Vocabulary:	*2.16.840.1.113883.6.96*
Sequence	SNOMED-CT Code	Description
1	165816005	Human immunodeficiency virus (HIV) positive (finding)
2	111880001	Acute HIV infection (disorder)
3	86406008	Human immunodeficiency virus infection (disorder)
4	62479008	Acquired immune deficiency syndrome (AIDS) (disorder)
5	359791000	Acquired immunodeficiency syndrome (AIDS) with dermatomycosis (disorder)
6	77070006	Acquired immunodeficiency syndrome (AIDS) with Salmonella infection (disorder)
7	240611008	Acquired immune deficiency syndrome-related complex (disorder)
8	236406007	Acquired immune deficiency syndrome-related nephropathy (disorder)
9	91923005	Acquired immunodeficiency syndrome (AIDS) virus infection associated with pregnancy (disorder)
10	91948008	Asymptomatic human immunodeficiency virus infection in pregnancy (disorder)
11	62246005	Acquired immunodeficiency syndrome (AIDS)-like syndrome (disorder)
12	111880001	Acute HIV infection (disorder)
13	91947003	Asymptomatic human immunodeficiency virus infection (disorder)
14	52079000	Congenital human immunodeficiency virus infection (disorder)

15	276665006	Congenital acquired immune deficiency syndrome (disorder)
16	276666007	Congenital human immunodeficiency virus positive status syndrome (disorder)
17	186723002	Human immunodeficiency virus (HIV) disease resulting in Burkitt's lymphoma (disorder)
18	186719005	Human immunodeficiency virus (HIV) disease resulting in candidiasis (disorder)
19	186718002	Human immunodeficiency virus (HIV) disease resulting in cytomegaloviral disease (disorder)
20	186726005	Human immunodeficiency virus (HIV) disease resulting in lymphoid interstitial pneumonitis (disorder)
21	186721000	Human immunodeficiency virus (HIV) disease resulting in multiple infections (disorder)
22	186725009	Human immunodeficiency virus (HIV) disease resulting in multiple malignant neoplasms (disorder)
23	186717007	Human immunodeficiency virus (HIV) disease resulting in mycobacterial infection (disorder)
24	87117006	Human immunodeficiency virus (HIV) infection with acute lymphadenitis (disorder)
25	315019000	Human immunodeficiency virus (HIV) infection with aseptic meningitis (disorder)
26	5810003	Human immunodeficiency virus (HIV) infection with infection by another virus (disorder)
27	48794007	Human immunodeficiency virus (HIV) infection with infectious mononucleosis-like syndrome (disorder)
28	402915006	Human immunodeficiency virus (HIV) seroconversion exanthem (disorder)
29	402916007	Human immunodeficiency virus (HIV) seropositivity (disorder)
30	235726002	Human immunodeficiency virus enteropathy (disorder)
31	281390005	Human immunodeficiency virus HIV-related gut disease - cause unknown (disorder)
32	40780007	Human immunodeficiency virus I infection (disorder)
33	79019005	Human immunodeficiency virus II infection (disorder)
34	186706006	Human immunodeficiency virus infection constitutional disease (disorder)
35	186707002	Human immunodeficiency virus infection with neurological disease (disorder)
36	186708007	Human immunodeficiency virus infection with secondary clinical infectious disease (disorder)
37	230201009	Human immunodeficiency virus myelitis (disorder)
38	240103002	Human immunodeficiency virus myopathy (disorder)
39	186709004	Human immunodeficiency virus with secondary cancers (disorder)
40	235009000	Human immunodeficiency virus-associated periodontitis (disorder)
41	397763006	Human immunodefiency virus encephalopathy (disorder)
42	398329009	Human immunodefiency virus encephalitis (disorder)
43	230180003	Human immunodefiency virus leukoencephalopathy (disorder)
44	416491000	Immune recovery uveitis (disorder)
45	230598008	Neuropathy due to human immunodeficiency virus (disorder)
46	405631006	Pediatric human immunodeficiency virus infection (disorder)
47	95892003	Persistent generalized lymphadenopathy (disorder)
48	78466009	Positive serological AND/OR viral culture findings for human immunodeficiency

		virus (disorder)
49	365866002	Finding of HIV status (finding)
50	365587003	Finding of human immunodeficiency virus antibody titer (finding)
51	165816005	Human immunodeficiency virus (HIV) positive (finding)
52	402901009	Oral hairy leukoplakia associated with HIV disease (disorder)
53	414376003	Hairy leukoplakia of tongue associated with HIV disease (disorder)
54	414604009	Leukoplakia of tongue associated with HIV disease (disorder)
55	402916007	Human immunodeficiency virus (HIV) seropositivity (disorder)
56	281388009	Human immunodeficiency virus HIV-related sclerosing cholangitis (disorder)
57	103415007	Human immunodeficiency virus (HIV) World Health Organization (WHO) class I (finding)
58	103416008	Human immunodeficiency virus (HIV) World Health Organization (WHO) class II (finding)
59	103417004	Human immunodeficiency virus (HIV) World Health Organization (WHO) class III (finding)
60	103418009	Human immunodeficiency virus (HIV) World Health Organization (WHO) class IV (acquired immunodeficiency syndrome) (AIDS) (finding)
61	385354005	Human immunodeficiency virus (HIV) World Health Organization (WHO) class finding (finding)
62	103406000	Human immunodeficiency virus (HIV) Centers for Disease Control and Prevention (CDC) category A1 (finding)
63	385353004	Human immunodeficiency virus (HIV) Centers for Disease Control and Prevention (CDC) category finding (finding)
64	103407009	Human immunodeficiency virus (HIV) Centers for Disease Control and Prevention (CDC) category A2 (finding)
65	103408004	Human immunodeficiency virus (HIV) Centers for Disease Control and Prevention (CDC) category A3 (AIDS) (finding)
66	103409007	Human immunodeficiency virus (HIV) Centers for Disease Control and Prevention (CDC) category B1 (finding)
67	103410002	Human immunodeficiency virus (HIV) Centers for Disease Control and Prevention (CDC) category B2 (finding)
68	103411003	Human immunodeficiency virus (HIV) Centers for Disease Control and Prevention (CDC) category B3 (AIDS) (finding)
69	103412005	Human immunodeficiency virus (HIV) Centers for Disease Control and Prevention (CDC) category C1 (AIDS) (finding)
70	103413000	Human immunodeficiency virus (HIV) Centers for Disease Control and Prevention (CDC) category C2 (AIDS) (finding)
71	103414006	Human immunodeficiency virus (HIV) Centers for Disease Control and Prevention (CDC) category C3 (AIDS) (finding)

B.3 Genetic Results (LOINC)

B.3.1 Metadata

1900 Genetic Results Value Set Metadata Shall contain the following content:

Metadata Element	Description	Mandatory
Identifier	This is the unique identifier of the value set	1.3.6.1.4.1. 38571.3.10

Metadata Element	Description	Mandatory
Name	This is the name of the value set	Genetic Results Value Set
Source	This is the source of the value set, identifying the originator or publisher of the information	HITE-CT
Purpose	Brief description about the general purpose of the value set	To Reflect those results related to genetics
Definition	A text definition describing how concepts in the value set were selected	Extensional definition: The value set was constructed by enumerating the codes from LOINC
Source URI	Most sources also have a URL or document URI that provides further details regarding the value set.	http://loinc.org
Version	A string identifying the specific version of the value set.	Version 1.0
Status	Active (Current) or Inactive	Active
Effective Date	The date when the value set is expected to be effective	10/20/2011
Expiration Date	The date when the value set is no longer expected to be used	N/A
Creation Date	The date of creation of the value set	10/20/2011
Revision Date	The date of revision of the value set	N/A
Groups	The identifiers of the groups that include this value set. A group may also have an OID assigned.	HITE-CT Sensitive Data

B.3.2 Genetic Results Value Set

Genetic Results Value Set will use the LOINC code system to identify its contents. Codes that are used within the scope of this profile are listed below:

Value Set :	1.3.6.1.4.1. 38571.3.10
Vocabulary	2.16.840.1.113883.6.1
LOINC Code	LOINC Description
47998-0	DNA sequence variation display name
48003-8	DNA sequence variation identifier
55207-5	Genetic analysis discrete result panel
55233-1	Genetic analysis master panel
55232-3	Genetic analysis summary panel
51969-4	Genetic analysis summary report
51966-0	Genetic disease DNA analysis panel
53039-4	Genetic disease analysis overall carrier interpretation

Value Set :	1.3.6.1.4.1. 38571.3.10
Vocabulary	2.16.840.1.113883.6.1
LOINC Code	LOINC Description
51968-6	Genetic disease analysis overall interpretation
51967-8	Genetic disease assessed
53037-8	Genetic disease sequence variation interpretation
48674-6	Genetic diseases
46738-1	Genetic disorders
19102-3	Genetic screen
48007-9	Genetic variant allelic state
47997-2	Genetic variant clinical significance
48013-7	Genomic reference sequence identifier
48002-0	Genomic source class

1.1 Genetic Procedures (SNOMED-CT)

1.1.1 Metadata

Metadata Element	Descritption	Mandatory
Identifier	This is the unique identifier of the value set	1.3.6.1.4.1. 38571.3.11
Name	This is the name of the value set	Genetic Procedures Value Set
Source	This is the source of the value set, identifying the originator or publisher of the information	HITE-CT
Purpose	Brief description about the general purpose of the value set	To Reflect Genetic Procedures using SNOMED-CT concepts
Definition	A text definition describing how concepts in the value set were selected	Extensional definition: The value set was constructed by enumerating the codes from SNOMED-CT
Source URI	Most sources also have a URL or document URI that provides further details regarding the value set.	http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html
Version	A string identifying the specific version of the value set.	Version 1.0
Status	Active (Current) or Inactive	Active
Effective Date	The date when the value set is expected to be effective	10/20/2011

Metadata Element	Descritption	Mandatory
Expiration Date	The date when the value set is no longer expected to be used	N/A
Creation Date	The date of creation of the value set	10/20/2011
Revision Date	The date of revision of the value set	N/A
Groups	The identifiers of the groups that include this value set. A group may also have an OID assigned.	HITE-CT Sensitive Data

1.1.2 Genetic Procedures Value Set

	Value Set:	1.3.6.1.4.1. 38571.3.11
	Vocabulary:	*2.16.840.1.113883.6.96*
Sequence	SNOMED-CT Code	Description
1	405824009	Genetic test (procedure)
2	405825005	Molecular genetic test (procedure)
3	405823003	BRCA1 mutation carrier detection test (procedure)
4	405826006	BRCA2 mutation carrier detection test (procedure)
5	444078002	Detection of Arg3500Gln mutation in apolipoprotein B-100 gene (procedure)
6	444149000	Detection of Arg506Gln mutation in gene of coagulation factor V gene and detection of G20210A mutation in gene of coagulation factor II (procedure)
7	444157002	Detection of BCR-ABL t(9;22) translocation (procedure)
8	444225007	Detection of G20210A mutation in gene of coagulation factor II (procedure)
9	444032005	Detection of mutation in apolipoprotein B-100 gene (procedure)
10	444226008	Detection of mutation in low density lipoprotein receptor gene (procedure)
11	443889002	Factor VIII mutation carrier detection test (procedure)
12	405839005	Familial medullary thyroid carcinoma mutation carrier detection test (procedure)
13	437742006	Huntington disease gene mutation carrier detection test (procedure)
14	405837007	Multiple endocrine neoplasia type 2A mutation carrier detection test (procedure)
15	405838002	Multiple endocrine neoplasia type 2B mutation carrier detection test (procedure)
16	405832001	Neurofibromatosis type 1 mutation carrier detection test (procedure)
17	405836003	Neurofibromatosis type 2 mutation carrier detection test (procedure)
18	443528002	Quantitation of BCR-ABL t(9;22) translocation (procedure)
19	421617007	RET proto-oncogene mutation analysis (procedure)

20	444260001	Screen for 20 common genetic mutations of cystic fibrosis using amplification refractory mutation system polymerase chain reaction assay technique (procedure)
21	443530000	Screen for 29 common genetic mutations of cystic fibrosis using amplification refractory mutation system polymerase chain reaction assay technique (procedure)
22	443982007	Targeted analysis for gene mutation (procedure)
23	443981000	Testing for known gene mutation in family member (procedure)
24	405835004	Von Hippel-Lindau disease mutation carrier detection test (procedure)
25	79841006	Genetic counseling (procedure)
26	386415003	Genetic risk identification (procedure)
27	305920002	Referral by genetic counselor (procedure)
28	306250006	Referral to genetic counselor (procedure)
29	306386005	Discharge by genetic counselor (procedure)
30	423641003	Genetic evaluation case management (procedure)
31	118124000	Genetic screening, molecular method (procedure)
32	28680007	Cryopreservation for genetic studies (procedure)
33	53973008	Genetic investigation procedure (procedure)
34	426417003	In vitro fertilization with preimplantation genetic diagnosis (procedure)
35	443212006	Screening test for genetic marker for thrombophilia using deoxyribonucleic acid analysis (procedure)
36	443530000	Screen for 29 common genetic mutations of cystic fibrosis using amplification refractory mutation system polymerase chain reaction assay technique (procedure)
37	444260001	Screen for 20 common genetic mutations of cystic fibrosis using amplification refractory mutation system polymerase chain reaction assay technique (procedure)

1910