



**Certification Commission
for Healthcare
Information Technology**

233 N. Michigan Avenue, Suite 2150
Chicago, Illinois 60601-5800
Tel 312.233.1582 Fax 312.896.1466
www.cchit.org

**2008 Certification Criteria – Second Draft
Network Criteria
January 14, 2008**

Background

The 2nd draft of certification criteria is the cumulative work of ten different work groups and expert panels. This is the second draft of the 2008 criteria which will be finalized in May 2008. The criteria will be further refined and published as a proposed final draft prior to the final certification criteria for 2008 being released.

The focus of the 2nd draft has been:

- Further refining the wording and compliance dates for new criteria.
- Harmonizing criteria recommendations from all groups into certification tracks (Ambulatory, Cardiovascular, Child Health, Emergency Department, Inpatient and Network).
- Incorporating public comments from the 1st draft into criteria published for the 2nd draft.

Certification Tracks

CCHIT continues to expand the certification options available for Healthcare IT vendors. The 2008 criteria will include certification tracks for Ambulatory, Emergency Department, Inpatient and Network. Additional population care and specialty certifications, both Cardiovascular and Child Health, will be offered to vendors completing Ambulatory, Emergency Department or Inpatient Certification.

The chart below illustrates the criteria that are included in each certification track.

Certification Track	Work Group Criteria	Additional Expert Panel Recommendations	Documents to Review
Ambulatory	Ambulatory + Foundation	Interoperability, Privacy & Compliance, Security	Ambulatory Certification PDF
Emergency Department	Emergency Department	Child Health, Foundation, Privacy & Compliance, Security	Emergency Department Certification PDF
Inpatient	Inpatient + Foundation	Child Health, Interoperability, Privacy & Compliance, Security	Inpatient Certification PDF
Network	Network Core + Network Modular	Privacy & Compliance, Security	Network Certification PDF
Cardiovascular	(Primary Certification in Ambulatory) +		Cardiovascular and Ambulatory Certification PDFs

	Cardiovascular		
Child Health	(Primary Certification in Ambulatory or Emergency Department or Inpatient) + Child Health		Child Health and Primary Certification PDFs

Overview of the Published Documents

The second draft of the 2008 certification criteria has been published as six individual PDF documents (Ambulatory, Cardiovascular, Child Health, Emergency Department, Inpatient and Network). These documents represent the different individual certification tracks that will be offered for 2008 certification. The documents contain certification criteria from the core work group and may also contain Foundation, Interoperability, Privacy & Compliance, Security and general Child Health criteria. Each spreadsheet contains filters to view criteria from each work group or expert panel independent of the certification track.

Explanation of columns

The following columns are included in both the PDF files and the spreadsheet:

- Item #: Reference number used to submit public comments
- Internal WG #: Includes 2007 numbers for previously published criteria and temporary internal numbers used internally by the work groups. These numbers will be replaced by 2008 identification numbers prior to the final publication of the criteria.
- Source WG: The work group or expert panel that originally authored the criteria.
 - Ambulatory – AM, Cardiovascular – CV, Child Health – CH, Emergency Department – ED, Foundation – FN, Inpatient – IP, Interoperability – IO, Privacy & Compliance – PC and Security – SC
 - This column is also used to differentiate the Network core and modular criteria: Network Core – NC and Network Modular – NM
- Certification Track: Identifies the 2008 certification options.
 - Ambulatory – AM, Cardiovascular – CV, Child Health – CH, Emergency Department – ED, Inpatient – IP and Network – NT
- Compliance columns: Identifies the year that criteria will become required for certification.
 - 2008 Criteria – These are being proposed for inclusion in next year’s certification requirements.
 - Road map 2009 – These criteria are tentatively scheduled to become required in 2009 and may be modified prior to 2009.

- Road map 2010 and beyond – These criteria are being proposed for certification beyond 2009. They will be reviewed during the 2009 development cycle and will most likely change prior to being required for certification in 2010 or later.
- Each of the columns may contain the following abbreviations:
 - P = Previously published criteria.
 - M = Criteria that has been modified since being published last year.
 - N = New criteria not previously published.
- Source or Reference: Identifies published resources used to develop criterion.

Scope of 2008 Network Certification Criteria

The Network Certification Work Group has narrowed the scope of the certification criteria for 2008. The Work Group is recommending that 2008 certification focus on criteria in the areas of security and interoperability. Criteria in other areas that were previously proposed for 2008 certification are now proposed as 2009 certification criteria.

Network Certification Program Structure

HIEs seeking certification will be required to demonstrate compliance with all 2008 security criteria. Certification will also require the HIE to demonstrate compliance with at least one transaction set. In 2008 the transaction sets will be Laboratory and CCD.

Timeline for Initiation of Certification Program

The Network Certification Work Group and the CCHIT Commission have determined that Network Certification will begin in October 2008. This will allow additional time for development of test scripts, conduct of pilot testing, and provide additional opportunities to solicit public comment and respond to the valuable input we receive from the HIE community.

Approach to Testing

The Network Work Group has explored a number of approaches to testing for HIE certification. We are seeking to strike a balance between practicality and rigor.

For transactions we expect to follow the approach of other CCHIT certification programs – following a sample transaction from a simulated originator and to a simulated recipient. It is likely that HIE certification will incorporate the Laika testing tools currently under development.

Security criteria testing must be feasible and credible in an operational environment. The Network Work Group has begun to explore the trade offs between the use of documentation review for security criteria and the use of live security testing techniques, e.g., attempting to breach a firewall. The Work Group recognizes that the live techniques are likely to incur a higher cost. As we examine testing options we will be weighing the cost and complexity of

the security testing approaches against the value of any additional demonstration of security protections.

The Network Work Group will be developing a revised timeline for the publication of test scripts. These revisions will be consistent with the change in launch date for Network Certification to October 1, 2008. The revised timeline will be announced after review and approval by the CCHIT Commissioners.

Questions for Reviewers

The Network Work Group would benefit from reviewers comments on the following:

- Modifications to the 2008 criteria that would improve their applicability to HIEs
- Feedback on whether these criteria will represent a meaningful indication of an HIE's capabilities
- Additions or changes to the security criteria that would increase the assurances that certification would provide to patients and participants in HIEs
- Suggestions on approaches to HITSP interoperability requirements for XDS transactions that are HIE architecture neutral
- Suggestions on mandatory vs. optional transport standards
- Suggestions on approaches to interoperability testing
- Suggestions on approaches to security testing

Stakeholder Feedback

Stakeholders are encouraged to submit comments during the 30 day public comment period. We are hoping these comments will include reactions to the wording and proposed compliance dates for new criteria. We also encourage the submission of general comments regarding the development of certification criteria.

Comments may be submitted through the CCHIT web site, <http://www.cchit.org>. Stakeholder groups planning to submit large numbers of comments are encouraged to use the website, however requirements for submitting comments via electronic file can be obtained by emailing info@cchit.org.



2008 Network Certification
Second Draft Criteria
 January 14, 2008

© 2007 The Certification Commission for Healthcare Information Technology

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										<div style="border: 1px solid black; padding: 5px;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>	
8001	NT.1	NM	NT	Data Services	HIE must be able to demonstrate the capability to both push and pull data	The HIE shall receive queries	N			assumes compliance with security assumes electronic interchange	
8002	NT.2	NM	NT	Data Services	HIE must be able to demonstrate the capability to both push and pull data	The HIE determines which systems contain the queried-for information and the HIE forwards the queries to those data sources.	N			assumes compliance with security assumes electronic interchange	
8003	NT.3	NM	NT	Data Services	HIE must be able to demonstrate the capability to both push and pull data	The HIE shall receive responses to queries	N			assumes compliance with security assumes electronic interchange	
8004	NT.4	NM	NT	Data Services	HIE must be able to demonstrate the capability to both push and pull data	The HIE shall forward query responses to the data requestor	N			assumes compliance with security assumes electronic interchange	
8005	NT.5	NC	NT	Data Services	HIE must be able to demonstrate the capability to both push and pull data	The HIE shall receive messages		N		assumes compliance with security assumes electronic interchange	
8006	NT.6	NC	NT	Data Services	HIE must be able to demonstrate the capability to both push and pull data	The HIE shall identify intended recipients of the message		N		assumes compliance with security assumes electronic interchange	
8007	NT.7	NC	NT	Data Services	HIE must be able to demonstrate the capability to both push and pull data	The HIE shall forward the message to the intended recipients		N		assumes compliance with security assumes electronic interchange	
8008	NT.8	NC	NT	Patient data matching capabilities		The HIE shall publish information on: ---The minimum data set it uses for patient data matching ---The threshold it requires to assert a patient data match	N				
8009	NT.9	NC	NT	Patient data matching capabilities		The HIE shall respond to data matching queries with only records that unambiguously meet the published matching criteria. The response should indicate the source of the data. (source OID).		N			
8010	NT.10	NC	NT	Patient data matching capabilities		The HIE shall have a mechanism to notify the source of the query that no match was found.		N			
8011	NT.11	NM	NT	Summary patient record exchange		HIE shall receive summary patient record query			N		
8012	NT.12	NM	NT	Summary patient record exchange		HIE shall request summary patient record data			N		

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	
8013	NT.13	NM	NT	Summary patient record exchange		HIE shall send summary patient record data to requestor			N		
8014	NT.14	NC	NT	Data integrity and non-repudiation checking		S28: The HIE shall support protection of integrity of all Protected Health Information (PHI) delivered over the Internet or other known open networks via SHA1 hashing and an open protocol such as TLS, SSL, IPsec, XML digital signature, or S/MIME or their successors.			N	We expect that there will be a higher level of protection in the future	CC SFR: FPT_RCV
8015	NT.15	NC	NT	Data integrity and non-repudiation checking		S24: The HIE shall support protection of confidentiality of all Protected Health Information (PHI) delivered over the Internet or other known open networks via encryption using triple-DES (3DES) or the Advanced Encryption Standard (AES) and an open protocol such as TLS, SSL, IPsec, XML encryptions, or S/MIME or their successors.			N	We expect that there will be a higher level of protection in the future	Canadian: Alberta 7.4.6.2 & 8.4.6.2 (Technical); CC SFR: FCS_COP; SP800-53: SC-13 CRYPTOGRAPHIC OPERATIONS; HIPAA: 164.312(e)(1)
8016	NT.16	NC	NT	Data integrity and non-repudiation checking		The HIE shall require that sending systems provide evidence of the origin of the information. This evidence must be verifiable by the HIE.			N		ISO/IEC 15408-2 Information Technology Security Techniques – Evaluation criteria for IT security – Part 2: Security functional requirements
8017	NT.17	NC	NT	Data integrity and non-repudiation checking		The HIE shall provide to senders of data to the HIE evidence of a receipt of information			N		ISO/IEC 15408-2 Information Technology Security Techniques – Evaluation criteria for IT security – Part 2: Security functional requirements
8018	NT.18	NC	NT	Data integrity and non-repudiation checking		S 8.1 -- The HIE shall be able to support time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.			N		CC SFR: FPT_STM; SP800-53: AU-8 TIME STAMPS
8019	NT.19	NC	NT	Audit logging and error handling for data access and exchange		S37: The HIE shall support logging to a common audit engine using the schema and transports specified in the Audit Log specification of IHE Audit Trails and Node Authentication (ATNA) Profile			N		NIST 800-92/SP 800-92
8020	NT.20	NC	NT	Audit logging and error handling for data access and exchange		S6: The HIE shall record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the system (e.g. software component, hardware component) where the event occurred; (3) type of event (including: data description and patient identifier when relevant); (4) subject identity (e.g. user identity); and (5) the outcome (success or failure) of the event.			N		CC SFR: FAU_GEN; SP800-53: AU-3 CONTENT OF AUDIT RECORDS, AU-10 NON-REPUDIATION; HIPAA: 164.312(b)

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										<div style="border: 1px solid black; padding: 5px;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>	
8021	NT.21	NC	NT	Audit logging and error handling for data access and exchange		S5.2: The HIE shall be able to detect security-relevant events that it mediates and generate audit records for them. At a minimum the events shall include: relevant administrative security events, start/stop, user login/logout, session timeout, account lockout, patient record created/viewed/updated/deleted, scheduling, query, order, node authentication failure, signature created/validated, PHI export (e.g. print), PHI import, and security administration events. Note: The system is only responsible for auditing security events that it mediates. A mediated event is an event that the system has some active role in allowing or causing to happen or has opportunity to detect. The system is not expected to create audit logs entries for security events that it does not mediate.	N			Duplicate of NT 102	CC SFR: FAU_GEN; SP800-53: AU-2 AUDITABLE EVENTS; HIPAA: 164.312(b)
8022	NT.22	NG	NT	Audit logging and error handling for data access and exchange		The HIE shall have procedures and policies for review of audit logs and retention of audit log data. Be able to retrieve audit logs within ___ time.	N				
8023	NT.23	NM	NT	Support for secondary use of clinical data including data provisioning and distribution of data transmission parameters		The HIE shall be able to send queries with selection rules			N		
8024	NT.24	NM	NT	Support for secondary use of clinical data including data provisioning and distribution of data transmission parameters		The HIE shall be able to receive responses to queries for secondary use			N		
8025	NT.25	NM	NT	Support for secondary use of clinical data including data provisioning and distribution of data transmission parameters		The HIE shall be able to forward responses to legally authorized health agency or other authorized recipient.			N		

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
8026	NT.26	NM	NT	Support for secondary use of clinical data including data provisioning and distribution of data transmission parameters		HIEs shall have a mechanism to identify records for public health reporting			N		
8027	NT.27	NM	NT	Support for secondary use of clinical data including data provisioning and distribution of data transmission parameters		HIEs shall be able to forward data to appropriate public health authority			N		
8028	NT.28	NM	NT	Support for secondary use of clinical data including data provisioning and distribution of data transmission parameters		The HIE shall be able to pseudo-anonymize and re-identify records as defined in HITSP T24. The pseudo identifier will be unique to the patient and the data source, i.e., it will not be unique to the patient			N	This criteria is also addressed in the Network transaction criteria	HITSP Pseudonymize Transaction
8029	NT.29	NM	NT	Support for secondary use of clinical data including data provisioning and distribution of data transmission parameters		The HIE shall be able to re-identify a pseudo-anonymized record upon request from an authorized authority and with appropriate controls			N		
8030	NT.30	NM	NT	Support for secondary use of clinical data including data provisioning and distribution of data transmission parameters		The HIE shall be able to deidentify data for secondary use.			N		

Compliance Key:
P = Previous Criteria
M = Modified for Year
N = New for Year

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										<div style="border: 1px solid black; padding: 5px;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>	
8031	NT.31	NM	NT	Consumer Services	Management of consumer identified locations for the storage of their personal health records	The HIE shall have the capability to collect, store, and transmit information on patient designated locations/systems for their personal health information			N	The HIE registers the consumers preference and the network participants can act on the request. There will need to be a means to know where a patient wants their data forwarded and be able to forward data consistent with this registered preference	
8032	NT.32	NM	NT	Consumer Services	Management of consumer identified locations for the storage of their personal health records	The HIE shall have the capability to transmit clinical information in standard formats to consumer designated locations for their personal health information			N	Will be modular at this point. May become core based on future work group consideration	
8033	NT.34	NM	NT	Support of consumer information location requests and data routing to consumer identified personal health records		The HIE shall be able to identify the location of consumer clinical records			N	There may be policies or laws that limit the types of data that can be directly shared with a patient	
8034	NT.35	NM	NT	Support of consumer information location requests and data routing to consumer identified personal health records		The HIE shall be able to respond to consumer electronic queries to retrieve copies of their electronic clinical records consistent with local law and policy			N		
8035	NT.36	NM	NT	Management of consumer-controlled providers of care and access permission information		HIE shall route transactions consistent with the permissions designated in a PHR application			N		
8036	NT.37	NC	NT	Management of consumer choices for participation in network services		The HIE shall be able to register patient preferences to participate or not participate in the HIE for uses other than their direct care or for legally authorized public health reporting or otherwise authorized or permitted data sharing.			N	This is not intended to restrict the business arrangement between an ancillary service and a provider. This should not prevent the provision of data for the active care of an individual patient or for legally authorized public health reporting or otherwise authorized or permitted data sharing.	

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										<div style="border: 1px solid black; padding: 5px;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>	
8037	NT.38	NC	NT	Management of consumer choices for participation in network services		The HIE shall be able to apply the patient preference to participate or not participate in the HIE for uses other than their direct care or for legally authorized public health reporting or otherwise authorized or permitted data sharing.			N	This is not intended to restrict the business arrangement between an ancillary service and a provider. This should not prevent the provision of data for the active care of an individual patient or for legally authorized public health reporting or otherwise authorized or permitted data sharing.	
8038	NT.39	NC	NT	Consumer access to audit logging and disclosure information for PHR and HIE data		The HIE shall support the ability of consumers to request and receive access and disclosure reports which identify HIE users who have viewed or accessed their clinical data			N		
8039	NT.40	NC	NT	Routing of consumer requests for data corrections		HIE shall be able to receive requests for data correction and forward them to the data owner			N	There could be instances where the HIE may not know the source of the data. But where it does it should be able to route the request.	
8040	NT.41	NC	NT	User and Subject Identity Management	Support for the process of user identity proofing, and/or attestation of third party identity proofing for those connected through the HIE -- includes user authentication	1. For every participating organization (a business entity that participates in the HIE) that provides or obtains protected health information enabled by the HIE: a. The HIE shall ensure that there is a unique ID that identifies that organization.	N			Needs to be a better definition of Organization	
8041	NT.42	NC	NT	User and Subject Identity Management	Support for the process of user identity proofing, and/or attestation of third party identity proofing for those connected through the HIE -- includes user authentication	b. The HIE has a framework in which the participating organization assumes liability for failures to (a) protect personal health information, and (b) properly identify PHI that is transmitted through the HIE--	N				
8042	NT.43	NC	NT	User and Subject Identity Management	Support for the process of user identity proofing, and/or attestation of third party identity proofing for those connected through the HIE -- includes user authentication	S29 -- The HIE shall support ensuring the authenticity of remote nodes (mutual node authentication) when communicating Protected Health Information (PHI) over the Internet or other known open networks using an open protocol (e.g. TLS, SSL, IPsec, XML sig, S/MIME).	N				CC SFR: FPT_RCV; HITSP T17
8043	NT.44	NC	NT	User and Subject Identity Management	Support for the process of user identity proofing, and/or attestation of third party identity proofing for those connected through the HIE -- includes user authentication	The HIE shall provide a means to add a system and its associated certificate to the list of authorized systems that may access information through the HIE (consistent with HITSP TP17)	N				

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										<div style="border: 1px solid black; padding: 5px;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>	
8044	NT.45	NC	NT	User and Subject Identity Management	Support for the process of user identity proofing, and/or attestation of third party identity proofing for those connected through the HIE -- includes user authentication	The HIE shall provide a means to suspend a system's authorization to access information through the HIE		N			
8045	NT.46	NC	NT	User and Subject Identity Management	Support for the process of user identity proofing, and/or attestation of third party identity proofing for those connected through the HIE -- includes user authentication	The HIE shall provide a means to establish an effective date and an expiration date for a system's authorization to access information through the HIE.		N			
8046	NT.47	NC	NT	User and Subject Identity Management	Support for the process of user identity proofing, and/or attestation of third party identity proofing for those connected through the HIE -- includes user authentication	<p>For every person that obtains protected health information enabled by the HIE, the following criteria must be met:</p> <p>a. The identity of the person shall have been verified by a responsible organization. (The organization doing identity proofing may be a third party, e.g., the county medical society)</p> <p>b. Such verification shall include determining the specific professional (e.g., provider, clerical staff) or consumer role of the person. Have a tiered set of role definitions that are consistent within the HIE. (Future year criteria may specify standardized roles to be used by all HIEs)</p> <p>c. The HIE shall require that the organization that assigns user IDs assure that the IDs are unique within the organization and that the identity of the user be provided upon request.</p>		N	<p>Comment: The combination of a user ID and the ID of the organization that assigned the user ID shall be unique across the HIE.</p> <p>Comment: If an ID is reused the organization must be able to track the assignment of the ID by date and time.</p>		
8047	NT.48	NM	NT	User and Subject Identity Management	Support for the process of user identity proofing, and/or attestation of third party identity proofing for those connected through the HIE -- includes user authentication	Where the HIE provides functionality directly to end users, it shall meet the requirements describing organizations above.		N	<p>Comment : The user in this sense is not the same as the party who is responsible for the contents of some information. For example a clinical report may have been signed by a person that is not a user of any system. Furthermore, some information is sent automatically by batch processes where there is no specific person directly responsible for initiating each transaction.</p>		

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References	
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond			
8048	NT.49	NC	NT	User and Subject Identity Management	Support for the process of user identity proofing, and/or attestation of third party identity proofing for those connected through the HIE -- includes user authentication	Every transaction that requests or contains protected health information, and is imputed directly to a specific user shall contain an unambiguous ID of the user and any organization IDs that are necessary to ensure that the combination of the IDs identifies a unique user within an HIE		N		<div style="border: 1px solid black; padding: 5px; width: fit-content;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>		
8049	NT.50	NC	NT	User and Subject Identity Management	Support for the process of user identity proofing, and/or attestation of third party identity proofing for those connected through the HIE -- includes user authentication	Transactions imputable to a user will contain the role of the user in a standard representation			N		Pending the establishment of standards	
8050	NT.51	NC	NT	Support of HIE level, non-redundant methodology for managed identities		HIEs shall obtain a unique identifier for the HIE			N		Pending the availability of an enumerator	
8051	NT.52	NC	NT	Support of HIE level, non-redundant methodology for managed identities		When sending user identity information between HIEs, both the HIE identifier and the unique user identity within the sending HIE must be used to ensure uniqueness between HIEs.			N		Pending the availability of an enumerator	
8052	NT.53	NC	NT	Support of HIE level, non-redundant methodology for managed identities		Patient identities contained in transactions sent through the HIE must be defined in a way that will not be ambiguous within the scope of the transaction.			N		Comment: typically this would be accomplished by combining an organizational identifier with the patient's unique ID (e.g., MRN) as assigned by that organization for transactions within the HIE and by including a unique HIE identifier on inter-HIE transactions.. Alternate approaches such as a community-wide master patient identifying authority would also satisfy this requirement for transactions within the HIE	
8053	NT.54	NC	NT	Support of HIE level, non-redundant methodology for managed identities		When exchanging patient identity information between HIEs, both the HIE identifier and the unique patient identity within that HIE must be used to ensure uniqueness between HIEs.			N			

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
8054	NT.55	NC	NT	Support of HIE level, non-redundant methodology for managed identities		Security New -- When interconnecting with other systems, the HIE shall support auditing and logging of activities that occur between the interconnected systems.	N			Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	NIST 800-47
8055	NT.56	NM	NT	HIEs that provide Portal Access		S1 -- The HIE shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g. System Administration, Clerical, Nurse, Doctor, etc.), or processes acting on behalf of users, for the performance of specified tasks.		N			ISO 17799: 9.1.1.2.b; HIPAA: 164.312(a)(1)
8056	NT.57	NM	NT	HIEs that provide Portal Access		S2 -- The HIE shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups.		N			Canadian: Alberta 4.1.3 (EMR); CC SFR: FMT_MSA; SP800-53: AC-5 LEAST PRIVILEGE; HIPAA: 164.312(a)(1)
8057	NT.58	NM	NT	HIEs that provide Portal Access		S3 -- The HIE must be able to associate permissions with a user using one or more of the following access controls: 1) user-based (access rights assigned to each user); 2) role-based (users are grouped and access rights assigned to these groups); or 3) context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)		N			Canadian: Ontario 5.3.12.e (System Access Management); CC SFR: FDP_ACC, FMT_MSA; ASTM: E1985-98; SP800-53: AC-3 ACCESS AND INFORMATION FLOW CONTROL; HIPAA: 164.312(a)(1)
8058	NT.59	NM	NT	HIEs that provide Portal Access		S4 -- The HIE shall support removal of a user's privileges without deleting the user from the system. The purpose of the criteria is to provide the ability to remove a user's privileges, but maintain a history of the user in the system.		N			
8059	NT.60	NM	NT	HIEs that provide Portal Access		S12 -- The HIE shall authenticate the user before any access to Protected Resources (e.g. PHI) is allowed, including when not connected to a network e.g. mobile devices.		N			Canadian: Alberta 1.1; CC SFR: FIA_UAU, FIA_UID; SP800-53: IA-2 USER IDENTIFICATION AND AUTHENTICATION; HIPAA: 164.312(d)

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										<div style="border: 1px solid black; padding: 5px;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>	
8060	NT.61	NM	NT	HIEs that provide Portal Access		S13 -- When passwords are used, the HIE shall support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.		N		This is a duplicate of S20	Canadian: Alberta 7.3.12 (Security) Canadian Ontario 5.3.12.b (System Access Management); CC SFR: FIA_SOS, FIA_UAU, FIA_UID; ASTM: E1987-98; SP800-53: IA-2 USER IDENTIFICATION AND AUTHENTICATION (no strength of password); ISO 17799: 9.3.1.d; HIPAA: 164.
8061	NT.62	NM	NT	HIEs that provide Portal Access		S14 -- The HIE upon detection of inactivity of an interactive session shall prevent further viewing and access to the system by that session by terminating the session, or by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The inactivity timeout shall be configurable.		N			Canadian: Alberta 7.3.14 (Security) Canadian Ontario 5.6.12.a (Workstation Security); CC SFR: FTA_SSL, FMT_SAE; SP800-53: AC-11 SESSION LOCK; HIPAA: 164.312(a)(1)
8062	NT.63	NM	NT	HIEs that provide Portal Access		The HIE shall provide a means to establish an effective date and an expiration date for an end user's authorization to access information through the HIE.					
8063	NT.64	NM	NT	HIEs that provide Portal Access		S15 -- The HIE shall enforce a limit of (configurable) consecutive invalid access attempts by a user. The system shall protect against further, possibly malicious, user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm).		N			Canadian: Ontario 5.3.12.c (System Access Management); CC SFR: FIA_AFL, FMT_SAE; SP800-53: AC-6 UNSUCCESSFUL LOGIN ATTEMPTS, AC-11 SESSION LOCK ; ISO 17799: 9.3.1.e, 9.5.2.e; HIPAA: 164.312(a)(1)
8064	NT.65	NM	NT	HIEs that provide Portal Access		S 16.1 -- When passwords are used, the HIE shall provide an administrative function that resets passwords.		N			CC SFR: FMT_MTD; ISO 17799: 9.2.3.b, (9.3.1.f); HIPAA: 164.312(d)
8065	NT.66	NM	NT	HIEs that provide Portal Access		S 16.2 When passwords are used, user accounts that have been reset by an administrator shall require the user to change the password at next successful logon.		N			CC SFR: FMT_MTD; ISO 17799: 9.2.3.b, (9.3.1.f); HIPAA: 164.312(d)

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	
8066	NT.67	NM	NT	HIEs that provide Portal Access		S17 -- The HIE shall provide only limited feedback information to the user during the authentication.		N			CC SFR: FIA_UAU; SP800-53: IA-6 AUTHENTICATOR FEEDBACK; HIPAA: 164.312(d)
8067	NT.68	NM	NT	HIEs that provide Portal Access		S 18 -- The HIE shall support case-insensitive usernames that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).		N			CC SFR: FMT_MTD
8068	NT.69	NM	NT	HIEs that provide Portal Access		S19 -- When passwords are used, the system shall allow an authenticated user to change their password consistent with password strength rules (S13).		N			CC SFR: FMT_MTD
8069	NT.70	NM	NT	HIEs that provide Portal Access		S20 -- When passwords are used, the system shall support case-sensitive passwords that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).		N			Canadian: Ontario 5.3.12 (b); SP 800-63
8070	NT.71	NM	NT	HIEs that provide Portal Access		S21 -- When passwords are used, the HIE shall not store passwords in plain text.		N			
8071	NT.72	NM	NT	HIEs that provide Portal Access		S 22 -- When passwords are used, the HIE shall prevent the reuse of passwords previously used within a specific (configurable) timeframe (i.e., within the last X days, etc. - e.g. "last 180 days"), or shall prevent the reuse of a certain (configurable) number of the most recently used passwords (e.g. "last 5 passwords").		N		Should we add a restriction on using dictionary words.	CC SFR: FMT_MTD; ISO 17799 9.5.4.f; HIPAA 164.312(d)
8072	NT.73	NM	NT	HIEs that provide Portal Access		S25 -- When passwords are used, the HIE shall not transport passwords in plain text.		N			Canadian: Ontario 5.3.12.a (System Access Management); CC SFR: FCS_CKM; SP800-53: SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT; HIPAA: 164.312(e)(1)
8073	NT.74	NM	NT	HIEs that provide Portal Access		S 26 -- When passwords are used, the HIE shall not display passwords while being entered.		N			CC SFR: FPT_ITC; ISO 17799 9.2.3; HIPAA 164.312(a)(1)
8074	NT.75	NM	NT	HIEs that provide Portal Access		S 31 -- The HIE shall support two-factor authentication in alignment with NIST 800-63 Level 3 Authentication. Note: The standards in this area are still evolving.			N		CC SFR: FIA_UAU; SP800-53: IA-2/AC-19, OMB M-06-16
8075	NT.76	NM	NT	HIEs that provide Portal Access		The HIE shall create an audit record of any password changes		N			

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	
8076	NT.77	NM	NT	HIEs that provide Portal Access		S33 -- The HIE system, prior to a user login, shall display a (configurable) notice warning (e.g. "The system should only be accessed by authorized users").		N			CC 2.1 L.4 TOE access banners (FTA_TAB); CC 3.0 FIA_TIN.1 Advisory warning message
8077	NT.78	NC	NT	Subject and user identity arbitration with like identities from other HIEs		The HIE shall provide a standard means to match patients based on demographics on an inter-HIE basis.		N		Comment: This will require a HITSP standard	
8078	NT.79	NC	NT	Subject and user identity arbitration with like identities from other HIEs		The HIE shall provide a standard means to match providers based on demographics on an inter-HIE basis.			N	NPI, DEA number can be considered for matching	
8079	NT.80	NC	NT	Subject and user identity arbitration with like identities from other HIEs		The HIE shall publish information on: —The minimum data set it uses for subject matching —The threshold it requires to assert a subject match	N				
8080	NT.81	NC	NT	Management Services	Management of available capabilities and services information for connected user organizations and other HIEs -- Directory Services	The HIE shall maintain a directory of entities that participate in the HIE. The directory shall include: entity name, address, HL7 OID, principal contact name and phone number, modes of participation in the NHIN, message types supported			N	Assumes that appropriate standards are defined	
8081	NT.82	NC	NT	Management Services	Management of available capabilities and services information for connected user organizations and other HIEs -- Directory Services	The HIE shall be able to share its directory of entities with other HIEs			N	Assumes that appropriate standards are defined	
8082	NT.83	NC	NT	Management Services	Management of available capabilities and services information for connected user organizations and other HIEs -- Directory Services	An HIE shall be able to correctly identify an entity that it provides services to.			N	Assumes that appropriate standards are defined	
8083	NT.84	NC	NT	Management Services	Management of available capabilities and services information for connected user organizations and other HIEs -- Directory Services	An HIE shall be able to provide another HIE with information to correctly identify an entity that it provides services to.			N	Assumes that appropriate standards are defined	
8084	NT.85	NC	NT	Management Services	Management of available capabilities and services information for connected user organizations and other HIEs -- Directory Services	An HIE shall be able to correctly identify an entity that is served by another HIE			N	Assumes that appropriate standards are defined	
8085	NT.86	NC	NT	Intrusion Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall implement firewall protections to prevent unauthorized access		N			

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	
8086	NT.87	NC	NT	Intrusion Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall monitor network traffic to detect intrusions and block illegitimate activities.		N			
8087	NT.88	NC	NT	Intrusion Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall monitor computer and network activities to detect intrusions		N			
8088	NT.89	NC	NT	Intrusion Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall have protection against viruses, spyware, and other malicious intrusions that can originate with Web browsing			N		
8089	NT.90	NC	NT	Email Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall filter email for malicious content			N		
8090	NT.91	NM	NT	Email Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall be able to send and receive encrypted email		N			
8091	NT.92	NC	NT	Email Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall archive email		N			
8092	NT.93	NC	NT	Vulnerability Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall conduct internal and external scanning to identify system vulnerabilities to unauthorized access	N				
8093	NT.94	NC	NT	Vulnerability Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall have tools to enable remote assessment of system failures		N			
8094	NT.95	NC	NT	Vulnerability Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall implement tools to monitor its websites for failures or outages			N	Depends upon HIE model (ASP, VPN, etc)	
8095	NT.96	NC	NT	Vulnerability Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall implement measures to prevent phishing and pharming		N			
8096	NT.97	NC	NT	Vulnerability Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall implement measures to prevent rogue network access			N		
8097	NT.98	NC	NT	System Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall have in place anti virus protections	N				
8098	NT.99	NC	NT	System Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall have policies to ensure timely implementation of software patches	N				
8099	NT.100	NC	NT	System Defense	The HIE shall have mechanisms to detect and document perimeter violations	R10-- The HIE shall have documentation that describes the patch (hot fix) handling process the HIE will use for applications, operating system and underlying tools	N				CC SFR: AGD_ADM
8100	NT.101	NC	NT	System Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall conduct regular system audits	N				

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
8101	NT.102	NC	NT	System Defense	The HIE shall have mechanisms to detect and document perimeter violations	S 5.2 The HIE system shall be able to detect security-relevant events that it mediates and generate audit records for them. At a minimum the events shall include: start/stop, user login/logout, session timeout, account lockout, patient record created/viewed/updated/deleted, scheduling, query, order, node-authentication failure, signature created/validated, PHI export (e.g. print), PHI import, and security administration events. Note: The system is only responsible for auditing security events that it mediates. A mediated event is an event that the system has some active role in allowing or causing to happen or has opportunity to detect. The system is not expected to create audit logs entries for security events that it does not mediate. This criteria is intended to apply to system administrative functions performed by the HIE.	N			Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	CC SFR: FAU_GEN; SP800-53: AU-2 AUDITABLE EVENTS; HIPAA: 164.312(b)
8102	NT.103	NC	NT	System Defense	The HIE shall have mechanisms to detect and document perimeter violations	S6 – The HIE system shall record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the system (e.g. software component, hardware component) where the event occurred; (3) type of event (including data description and patient identifier when relevant); (4) subject identity (e.g. user identity); and (5) the outcome (success or failure) of the event.	N			Duplicate of NT20	CC SFR: FAU_GEN; SP800-53: AU-3 CONTENT OF AUDIT RECORDS, AU-10 NON-REPUDIATION; HIPAA: 164.312(b)
8103	NT.104	NC	NT	System Defense	The HIE shall have mechanisms to detect and document perimeter violations	S7 – The HIE system shall provide authorized administrators with the capability to read all audit information from the audit records in one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format in such a manner as to allow correlation based on time (e.g. UTC synchronization).	N				CC SFR: FAU_SAR; SP800-53: AU-7 AUDIT REDUCTION AND REPORT GENERATION; HIPAA: 164.312(b)
8104	NT.105	NC	NT	System Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall be able to carry out remote backups		N			

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	
8105	NT.106	NC	NT	System Defense	The HIE shall have mechanisms to detect and document perimeter violations	R1 – The HIE system shall be able to generate a backup copy of the application data, security credentials, and log/audit files.		N			Canadian: Alberta 7.3.16 (Security); CC SFR: FDP_ROL, FPT_RCV; HIPAA: 164.310(d)(1)
8106	NT.107	NC	NT	System Defense	The HIE shall have mechanisms to detect and document perimeter violations	R2 – The HIE system restore functionality shall result in a fully operational and secure state. This state shall include the restoration of the application data, security credentials, and log/audit files to their previous state.		N			Canadian: Alberta 7.3.18.9 (Security); CC SFR: FAU_GEN; SP800-53: AU-2 AUDITABLE EVENTS; HIPAA: 164.310(d)(1)
8107	NT.108	NC	NT	System Defense	The HIE shall have mechanisms to detect and document perimeter violations	R3 – If the HIE system claims to be available 24x7 then the system shall have ability to run a backup concurrently with the operation of the application.		N			Canadian: Alberta 7.4.2.5 (Technica+D11); CC SFR: FDP_ROL; HIPAA: 164.310(d)(1)
8108	NT.109	NC	NT	User Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall be able to filter Web content		N			
8109	NT.110	NC	NT	User Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall have remote access controls	N				
8110	NT.111	NC	NT	User Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall be able to utilize identity tokens		N			
8111	NT.112	NC	NT	User Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall provide security training to its employees	N				
8112	NT.113	NC	NT	User Defense	The HIE shall have mechanisms to detect and document perimeter violations	The HIE shall provide Help Desk services to participating organizations and users.			N		
8113	NT.114	NC	NT	Physical Environment	The HIE shall have mechanisms to detect and document perimeter violations	R5 –The HIE system shall have documentation that covers the physical environment necessary for proper secure and reliable operation of the system including: electrical, HVAC, sterilization, and work area.	N				CC SFR: AGD_ADM
8114	NT.115	NC	NT	Timely intra-HIE and cross-HIE issue resolution		The HIE shall have formal agreements that specify the methods, policies, procedures, and timeframes for communicating and resolving any security incident	N				
8115	NT.116	NC	NT	Temporary and permanent de-authorization of direct and third party users when necessary		S4: The HIE shall have the ability to remove a user's or entity privileges without deleting the user or entity from the system. The purpose of the criteria is to provide the ability to remove a user's or entity's privileges, but maintain a history of the user or entity in the system.		N			

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										<div style="border: 1px solid black; padding: 5px;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>	
8116	NT.117	NC	NT	Temporary and permanent de-authorization of direct and third party users when necessary		The HIE shall maintain records of de-activation and the basis for deactivation of a user or entity. The HIE should have a mechanism for sharing this information with other HIEs.		N		Should HIEs be required to share with other HIEs. Could this be accomplished through the directory?	
8447	NT.148	NC	NT	Temporary and permanent de-authorization of direct and third party users when necessary		The HIE shall have policies for de-authorization that include inactivity, security breach, lack of compliance with technical standards, e.g., insufficient authentication, failure comply with terms of participation.	N			For example, automatic log off for three-failed access attempts. Assuming policy is certified	
8118	NT.119	NC	NT	Emergency access capabilities to support appropriate individual and population emergency access needs		S36 -- The HIE "break the glass" function must be capable of requiring the clinician requesting access to information to document and record the reason(s) for requesting access.		N			§164.312(a)(2)(ii), hitsp
8119	NT.120	NC	NT	Emergency access capabilities to support appropriate individual and population emergency access needs		S35 -- The HIE shall support access to information to a treating clinician, when the information is necessary for managing an emergency condition. Note: This is commonly known as a "break the glass" function. This does not provide increased access rights for the user. The system shall implement controls to terminate emergency access after a specified time period has elapsed		N		This should be focused on "break the glass" for inter-HIE interactions	§164.312(a)(2)(ii), hitsp
8420	NT.124	NC	NT	Emergency access capabilities to support appropriate individual and population emergency access needs		S36: The HIE "break the glass" function must be capable of requiring the clinician requesting access to information to document and record the reason(s) for requesting access.	N			This should be focused on "break the glass" for inter-HIE interactions	§164.312(a)(2)(ii), hitsp

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										<div style="border: 1px solid black; padding: 5px;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>	
8121	NT.122	NC	NT	Emergency access capabilities to support appropriate individual and population emergency access needs		The HIE shall have policies to govern the granting of emergency access. The policies should specify the criteria for emergency access, controls on emergency access, monitoring of emergency access, and deactivation of emergency access.	N			Assumes that policy is certified	
8122	NT.123	NM	NT	Electronic Health Record-Laboratory Results Reporting (HITSP/IS-01)	Transactions	The HIE SHALL have the ability to perform the roles of Sender and Receiver of clinical laboratory results using HL7 v.2.5.1 as specified in the HITSP Component 36 Lab Message and Component 35 EHR Lab Terminology.	N				HITSP IS-01 Component 35 EHR Lab Terminology and Component 36 Lab Message
8123	NT.124	NM	NT	Electronic Health Record-Laboratory Results Reporting (HITSP/IS-01)	Transactions	The HIE SHALL have the ability to perform the roles of Sender and Receiver of clinical laboratory results using HL7 CDA r2 as specified in the HITSP Component 37 Lab Report Document Structure with the contents and terminology specified in HITSP Component 36 Lab Message and Component 35 EHR Lab Terminology.	N				HITSP IS-01 Component 35 EHR Lab Terminology and Component 36 Lab Message and Component 37 Lab Report Document Structure
8124	NT.125	NM	NT	Electronic Health Record-Laboratory Results Reporting (HITSP/IS-01)	Transactions	The HIE SHALL have the ability to perform the role of Patient Identifier Cross Reference Consumer and Patient Identifier Cross Reference Manager as documented in HITSP Transaction Package 22 Patient ID Cross Referencing.	N				HITSP IS-01 Transaction Package 14 Send Lab Result Message and Transaction Package 22 Patient ID Cross Referencing
8125	NT.126	NM	NT	Electronic Health Record-Laboratory Results Reporting (HITSP/IS-01)	Transactions	The HIE SHALL have the ability to perform the roles of Document Consumer, Document Source, Document Repository, Document Registry and Patient Identity Source as documented in HITSP Transaction Package 13 Manage Sharing of Documents, as updated in 2007 IHE XDS-b and IHE XCA. The document repository may be in the HIE itself, or in an edge system participant in the network.E27	N				HITSP IS-01 Transaction Package 13 Manage Sharing Of Documents
8126	NT.127	NM	NT	Electronic Health Record-Laboratory Results Reporting (HITSP/IS-01)	Transactions	The HIE SHALL have the ability to perform the roles of Patient Demographics Supplier and Patient Demographics Consumer as documented in HITSP Transaction 23 Patient Demographics Query.	N				HITSP IS-01 Transaction 23 Patient Demographics Query

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										<div style="border: 1px solid black; padding: 5px; width: fit-content;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>	
8127	NT.128	NM	NT	Electronic Health Record-Laboratory Results Reporting (HITSP/IS-01)	Transactions	IF transmitting, transporting, translating or mapping lab result terminology THEN the HIE SHALL have the ability to support SNOMED-CT VA Problem List Subset (FDA Structured Product Labeling Problem List Subset), SNOMED-CT Lab Test Findings Table, SNOMED-CT Organisms, Laboratory LOINC, and Universal Codes for Units of Measure (UCUM), as documented in HITSP C35 Lab Result Terminology.	N				HITSP IS-01 Transaction Package 13 Manage Sharing of Documents and Transaction 18 View Lab Result From Web Application and Component 36 Lab Result Message and Component 37 Lab Report Document Structure
8128	NT.129	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	The HIE SHALL have the ability to perform the role of Patient Identifier Cross Reference Consumer and Patient Identifier Cross Reference Manager as documented in HITSP Transaction Package 22 Patient ID Cross Referencing.		N			HITSP IS-02 Transaction Package 22 Patient ID Cross Referencing
8129	NT.130	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	The HIE SHALL have the ability to perform the roles of Document Consumer, Document Source, Document Repository, Document Registry and Patient Identity Source as documented in HITSP Transaction Package 13 Manage Sharing of Documents, and in HITSP Transaction Package 49 Sharing Radiology Results, as updated in 2007 IHE XDS-b and IHE XCA, and using IHE XDS-I for Radiology results. The document repository may be in the HIE entity itself, or in an edge system participant in the network.E13		N			HITSP IS-02 Transaction Package 13 Manage Sharing Of Documents and Transaction Package 49 Sharing Radiology Results
8130	NT.131	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	The HIE SHALL perform the roles of Patient Identity Cross-Reference Manager and Pseudonymization Service as documented in "HITSP_v2.0_2007_T24 - Notification of Document Availability." Patient Identifier Cross-Reference Manager invokes Pseudonymization Service via a remote procedure call (RPC) to which it passes patient demographic information that is mapped using a cryptographic algorithm by Pseudonymization Service to the pseudo-identifying information that is returned to the caller.		N			HITSP IS-02 Transaction 24 Pseudonymize Patient ID Cross-Reference Manager and Pseudonymization Service Technical Actor

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	
8131	NT.132	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	The HIE SHALL have the ability to perform the roles of Sender and Receiver of HL7 v2 resource utilization messages as documented in the HITSP Component 47 Resource Utilization Message.		N			HITSP IS-02 C47 Resource Utilization Message
8132	NT.133	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	The HIE SHALL have the ability to perform the roles of Sender and Receiver of HL7 v2 encounter messages as documented in the HITSP Component 39 Encounter Message.		N			HITSP IS-02 C39 Encounter Message
8133	NT.134	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	The HIE SHALL have the ability to perform the roles of Sender and Receiver of HL7 CDAR2 encounter documents as documented in the HITSP Component 48 Encounter Document.		N			HITSP IS-02 C48 Encounter Document
8134	NT.135	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	The HIE SHALL have the ability to perform the roles of Sender and Receiver of HL7 v2 radiology messages as documented in the HITSP Component 41 Radiology Message.		N			HITSP IS-02 C41 Radiology Message
8135	NT.136	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	The HIE SHALL have the ability to perform the roles of Sender and Receiver of clinical laboratory results using HL7 v.2.5.1 as specified in the HITSP Component 36 Lab Message and Component 35 EHR Lab Terminology.		N			HITSP IS-02 Component 35 EHR Lab Terminology and Component 36 Lab Message
8136	NT.137	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	The HIE SHALL have the ability to perform the roles of Sender and Receiver of clinical laboratory results using HL7 CDA r2 as specified in the HITSP Component 37 Lab Report Document Structure with the contents and terminology specified in HITSP Component 36 Lab Message and Component 35 EHR Lab Terminology.		N			HITSP IS-02 Component 35 EHR Lab Terminology and Component 36 Lab Message and Component 37 Lab Report Document Structure
8137	NT.138	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	IF transmitting, transporting, translating or mapping lab result terminology THEN the HIE SHALL have the ability to support SNOMED-CT VA Problem List Subset (FDA Structured Product Labeling Problem List Subset), SNOMED-CT Lab Test Findings Table, SNOMED-CT Organisms, Laboratory LOINC, and Universal Codes for Units of Measure (UCUM), as documented in HITSP C35 Lab Result Terminology.		N			HITSP IS-02 Transaction Package 13 Manage Sharing of Documents and Component 36 Lab Result Message and Component 37 Lab Report Document Structure

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	
8138	NT.139	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	The HIE SHALL have the ability to perform Acknowledgements as documented in HITSP Component 45 Acknowledgements.		N			HITSP IS-02 Component 45 Acknowledgements
8139	NT.140	NM	NT	Biosurveillance-Connecting to Clinical Care (HITSP/IS-02)	Transactions	The HIE SHALL have the ability to perform the roles of Form Manager, Form Receiver and Form Archiver as documented in HITSP Transaction Package 50 Retrieve Form For Data Capture.		N			HITSP IS-02 Transaction Package 50 Retrieve Form For Data Capture
8140	NT.141	NM	NT	Consumer Empowerment - Registration Summary and Medication History (HITSP/IS-03)	Transactions	The HIE SHALL have the ability to perform the roles of Document Consumer, Document Source, Document Repository, Document Registry and Patient Identity Source as documented in HITSP Transaction Package 13 Manage Sharing of Documents, as updated in 2007 IHE XDS-b and IHE XCA. The document repository may be in the HIE entity itself, or in an edge system participant in the HIE.		N			HITSP IS-013 Transaction Package 13 Manage Sharing Of Documents
8141	NT.142	NM	NT	Consumer Empowerment - Registration Summary and Medication History (HITSP/IS-03)	Transactions	The HIE SHALL have the ability to perform the role of Patient Identifier Cross Reference Consumer and Patient Identifier Cross Reference Manager as documented in HITSP Transaction Package 22 Patient ID Cross Referencing.		N			HITSP IS-013 Transaction Package 22 Patient ID Cross Referencing
8142	NT.143	NM	NT	Consumer Empowerment - Registration Summary and Medication History (HITSP/IS-03)	Transactions	The HIE SHALL have the ability to perform the roles of Patient Demographics Supplier and Patient Demographics Consumer as documented in HITSP Transaction 23 Patient Demographics Query.		N			HITSP IS-03 Transaction 23 Patient Demographics Query
8143	NT.144	NM	NT	Consumer Empowerment - Registration Summary and Medication History (HITSP/IS-03)	Transactions	The HIE SHALL have the ability to perform the roles of Document Consumer, Document Source, Document Repository, Document Registry and Patient Identity Source as documented in HITSP Transaction Package 13 Manage Sharing of Documents, as updated in 2007 IHE XDS-b and IHE XCA, and using HITSP Component 32 Registration Summary and Medication History for the specification of the HL7/ASTM Continuity of Care Document (CCD) healthcare summary document, as updated by HITSP in 2007.		N			HITSP IS-03 Transaction Package 13 Manage Sharing Of Documents Document Registry Technical Actor and Component 32 Registration Summary and Medication History

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										<div style="border: 1px solid black; padding: 5px;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>	
8144	NT.145	NM	NT	Consumer Empowerment - Registration Summary and Medication History (HITSP/IS-03)	Transactions	The HIE SHALL have the ability to send and receive the HL7/ASTM Continuity of Care Document (CCD) healthcare summary document, as updated by HITSP in 2007.		N			HITSP IS-03 Component 32 Registration Summary and Medication History
8145	NT.146	NM	NT	Emergency Responder		No criteria in this area until HITSP finalizes their standards			N		
8146	NT.147	NM	NT	Part D ePrescribing		The HIE shall perform bi-directional translation between NDPDP eprescribing messages and HL7 ePrescribing messages as allowed in Medicare Part D for delivery systems to communicate with retail pharmacies.		N			HL7v2, NCPDP Script 8.1
8147	NT.148	NM	NT	Part D ePrescribing		The HIE SHALL have the ability to Send an electronic prescription to pharmacy using NCPDP Script 8.1 (NEWRX)		N		Will be aligned with Medicare Part D final regulations	NCPDP Script 8.1 (NEWRX)
8148	NT.149	NM	NT	Part D ePrescribing		The HIE SHALL have the ability to Respond to a request for a refill sent from a pharmacy using NCPDP Script 8.1 (REFREQ, REFRES)		N		Transaction is now wide spread use so that systems that send new prescriptions need to be ready to respond to requests for refills.	NCPDP Script 8.1 (REFREQ, REFRES)
8149	NT.150	NM	NT	Part D ePrescribing		The HIE SHALL have the ability to Send a cancel prescription message to a pharmacy using NCPDP Script 8.1 (CANRX, CANRES)		N		Sent by the prescriber to cancel a prescription that was sent previously	NCPDP Script 8.1 (CANRX, CANRES)
8150	NT.151	NM	NT	Part D ePrescribing		The HIE SHALL have the ability to Respond to a request for a prescription change from a pharmacy using NCPDP Script 8.1 (RXCHG, CHGRES)		N		Sent by the pharmacy to request that the prescriber make changes to a prescription before it is filled.	NCPDP Script 8.1 (RXCHG, CHGRES)
8151	NT.152	NM	NT	Part D ePrescribing		The HIE SHALL have the ability to Send electronic prescription to pharmacy including structured and coded SIG instructions using NCPDP Script 11.1 not available yet		N		Standard has been written but has not been finalized, balloted, or implemented. Will work with Ambulatory Functionality WG to align functionality criteria and interoperability roadmap dates in preparation for next round of public comments.	NCPDP Script 11.1 not available yet
8152	NT.153	NM	NT	Part D ePrescribing		The HIE SHALL have the ability to Send a query to verify prescription drug insurance eligibility and coverage using X12 270/271/ CORE Phase I Rules		N		An essential first step prior to sending a query for medication history or formulary information directed at prescription drug coverage.	X12 270/271/ CORE Phase I Rules
8153	NT.154	NM	NT	Part D ePrescribing		The HIE SHALL have the ability to Access and view formulary information from pharmacy or PBM using NCPDP Formulary and Benefit Standard Implementation Guide v1.0		N		Usually preceded by a query for insurance eligibility to verify potential source of data.	NCPDP Formulary and Benefit Standard Implementation Guide v1.0

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										<div style="border: 1px solid black; padding: 5px; width: fit-content;"> Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year </div>	
8154	NT.155	NM	NT	Part D ePrescribing		The HIE SHALL have the ability to Send a query for medication history to PBM or pharmacy to access and view medication list from EHR using NCPDP Script 8.1 (RXHREQ, RXHRES), RxNorm, NDC codes		N		Part of ONC CE-PHR Use Case, used effectively during Medicare Part D pilots.	NCPDP Script 8.1 (RXHREQ, RXHRES), RxNorm, NDC codes
8155	NT.156	NM	NT	Part D ePrescribing		The HIE SHALL have the ability to Receive medication fulfillment history using NCPDP Script 8.12 (RXFILL)		N		Sent by pharmacy after medication has been dispensed to the patient, not currently in wide spread use but is a priority for providers	NCPDP Script 8.12 (RXFILL)
8156	NT.157	NM	NT	Part D ePrescribing		The HIE SHALL have the ability to Access and view a medication history from a PHR using HITSP IS-03 CE-PHR Interoperability Specification HL7-ASTM CCD, IHE XDS/XCA		N		Part of ONC CE-PHR Use Case, may use PHR standards such as HL7/CCD and ASTM CCR instead of NCPDP standards. Will probably use RxNORM medication codes that are more appropriate for consumers and providers than the NDC codes used by pharmacies.	HITSP IS-03 CE-PHR Interoperability Specification HL7-ASTM CCD, IHE XDS/XCA
8157	NT.158	NM	NT	Part D ePrescribing		The HIE SHALL have the ability to Respond to a query for medication history sent by a PHR using HITSP IS-03 CE-PHR Interoperability Specification		N		Part of ONC CE-PHR Use Case, may use PHR standards such as HL7/CCD and ASTM CCR instead of NCPDP standards, final standards to be specified by HITSP.	HITSP IS-03 CE-PHR Interoperability Specification
8158	NT.159	NM	NT	Inter-physician "clinical memos"		The HIE SHALL have the ability to perform the roles of Document Consumer, Document Source, Document Repository, Document Registry and Patient Identity Source as documented in HITSP Transaction Package 13 Manage Sharing of Documents, as updated in 2007 IHE XDS-b and IHE XCA.		N			HITSP IS-01, 02, 03 Transaction Package 22 Patient ID Cross Referencing
8159	NT.160	NM	NT	Managing the exchange of clinical documents		The HIE SHALL have the ability to perform the roles of Document Consumer, Document Source, Document Repository, Document Registry and Patient Identity Source as documented in HITSP Transaction Package 13 Manage Sharing of Documents, as updated in 2007 IHE XDS-b and IHE XCA.		N			HITSP IS-01, 02, 03 Transaction Package 22 Patient ID Cross Referencing
8160	NT.161	NM	NT	Manage the exchange of results other than labs		The HIE SHALL have the ability to perform the roles of Document Consumer, Document Source, Document Repository, Document Registry and Patient Identity Source as documented in HITSP Transaction Package 13 Manage Sharing of Documents, as updated in 2007 IHE XDS-b and IHE XCA.		N			HITSP IS-01, 02, 03 Transaction Package 22 Patient ID Cross Referencing

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance			Discussion / Comments	Source or References
							2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond		
										Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	
8161	NT.162	NM	NT	Update demographics and identification information -- users, patients, entities		The HIE SHALL have the ability to perform the role of Patient Identifier Cross Reference Consumer and Patient Identifier Cross Reference Manager as documented in HITSP Transaction Package 22 Patient ID Cross Referencing.		N			HITSP IS-01, 02, 03 Transaction Package 22 Patient ID Cross Referencing
8162	NT.163	NM	NT	Update or query consent		Criteria will be developed based on HITSP 3.0 deliverables in 2008			N		
8163	NT.164	NM	NT	Continuity of Care Document	Import Patient Summary information via HITSP C32 document	IF-11.03 The HIE shall perform the role of Document Consumer as specified in the HITSP C32 Document	N				HITSP IS-03 Consumer Empowerment HL7 CCD - Document Type HITSP C32 v2.0 - Registration and Medication History Document Content Component