CCHIT
Certification Commission for Healthcare Information Technology
233 N. Michigan Avenue, Suite 2150
Chicago, Illinois 60601-5800

Network C

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

    - 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.

The Network Certification Work Gro

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

s The Network Work Group will be developing a revised timeli

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond	Discussion / Comments	Source or References
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**			ass361: compliance with security ass361: electronic interchange	
8002	**NT.2**										

							Compliance				
Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond	Discussion / Comments	Source or References
										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.				We expect that there will be a higher level of protection in the future	CC SFR: FNErn networks via

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

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	
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**		

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	2008 Certification	Roadmap 2009	Roadmap 2010 and BeyB

P = Previous 744 Tm (97 Tm

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	2008 Certification	Roa

							Compliance				
Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	2008 Certification	Roadmap 2009	Roadmap 2010 and Beyond	Discussion / Comments Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	Source or References
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**			
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**										

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	
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**				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 0 pESS AND

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance: 2008 Certification	Compliance: Roadmap 2009	Compliance: Roadmap 2010 and Beyond	Discussion / Comments	Source or References
8060	**NT.61**	NM	NT	HIEs that provide Portal Access		~~!"#$%%$&'()$*+,,-./0,$+/($1,(02$3'(456,'+77$,1**./3$*+,,-./0$,3/()83'$ /17(,$3'+3$+77.-$9./$::);:1:$)1:<(/$.9$='+/+=3(/,2$+)0$;)=71,;.)$.9$+7*'+%)1:(/;=$=.:*7(>;3?@$~~		**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)

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: 2008 Certification	Compliance: Roadmap 2009	Compliance: Roadmap 2010 and Beyond	Discussion / Comments	Source or References
										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: 2008 Certification	Compliance: Roadmap 2009	Compliance: Roadmap 2010 and Beyond	Discussion / Comments	Source or References
										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	Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	
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**				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					

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance: 2008 Certification	Compliance: Roadmap 2009	Compliance: Roadmap 2010 and Beyond	Discussion / Comments	Source or References
										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+D1l); CC SFR: FDP_ROL; HIPAA: 164.310(d)(1)
8108	**NT.109**	NC	NT	User Defense							

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	
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?	
~~**8117**~~	~~**NT.118**~~	~~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							

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance: 2008 Certification	Compliance: Roadmap 2009	Compliance: Roadmap 2010 and Beyond	Discussion / Comments	Source or References
										Compliance Key: P = Previous Criteria M = Modified for Year N = New for Year	
~~**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 Tj ET BT1 BT 0 6.6 -6..6 0 251.2798 489.7202 Tm /F6.0 1 Tf (N) Tj ET BT	**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 ry results using							

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	
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											

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 Resuorce 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 2 1177.2 317.87urveillan 0 1 62.51606 Tm (NT.135) 2 s					

Item #	Internal WG #	Source WG	Certification Track	Category	Category Description	Criteria	Compliance: 2008 Certification	Compliance: Roadmap 2009	Compliance: Roadmap 2010 and Beyond	Discussion / Comments	Source or References
										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 Democraphics 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

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