

HIT Standards Committee Privacy and Security Workgroup

Final Recommendations for NwHIN Governance RFI Assigned Questions

**Dixie Baker, Chair
Walter Suarez, Co-Chair**

June 20, 2012

Privacy and Security Workgroup

- Dixie Baker, SAIC
- John Blair, Taconic IPA
- Anne Castro, BlueCross BlueShield of South Carolina
- Mike Davis, Veterans Health Administration
- Lisa Gallagher, HIMSS
- Chad Hirsch, Mayo
- Jeff Jonas, IBM
- Ed Larsen
- David McCallie, Cerner Corporation
- John Moehrke, General Electric
- Wes Rishel, Gartner
- Kevin Stine, NIST
- Walter Suarez, Kaiser Permanente
- Sharon Terry, Genetic Alliance

Governance RFI: Assignment of Priority Areas to P&S WG

- 66 Questions throughout RFI
- Privacy and Security WG reviewed the six (6) questions assigned to it, plus one additional question of high interest to WG members
 - Preliminary recommendations reported at May HITSC meeting
 - Changes and additions to those recommendations are shown in red type

Questions Reviewed by P&S Workgroup

Question 4: Would a voluntary validation approach as described above sufficiently achieve this goal? If not, why?

Context: ONC is considering a validation process where entities that facilitate electronic exchange would, voluntarily, become Network Validated Entities (NVEs) by demonstrating compliance with CTEs to Validation Bodies that have been accredited by an Accreditation Body named by ONC

P&S WG Comments:

The key factor is building a trust fabric to support health information exchange – NVE validation must clearly contribute to this goal.

People in the marketplace do not know about or understand yet what “NwHIN” or “NVE” mean. The recognition and perceived value of the NVE ‘brand’ will need to build over time.

Make clear what NVE validation enables exchanging parties to do that without validation they could not do. Federal partners can play a key role here; for example, a CMS requirement that health information be exchanged with them only through an NVE would clearly demonstrate value.

The integrity of the validation process, and ongoing oversight and policy enforcement, are critical to the success of the voluntary approach.

**NO CHANGE FROM
COMMENTS REPORTED
AT MAY HITSC MEETING**

Questions Reviewed by P&S Workgroup

Re Condition [S-1]: An NVE must comply with sections 164.308, 164.310, 164.312, and 164.316 of title 45 of the Code of Federal Regulations as if it were a covered entity, and must treat all implementation specifications included within sections 164.308, 164.310, and 164.312 as “required.”

Question 22: Are there HIPAA Security Rule implementation specifications that should not be required of entities that facilitate electronic exchange? If so, which ones and why?

P&S WG Comments:

Agree that making “addressable” implementation specifications (IS) “required” would build trust and reduce variability

Note that implementation specifications are very general and that to truly reduce variability, standards may be needed to constrain implementations for validation. Such “standards” may include both SDO standards (e.g., encryption) and specific processes and procedures.

After further review, the P&S WG concluded that none of the addressable implementation specifications are unreasonable to “require” of an NVE.

Questions/concerns about the voluntary nature of the validation process, and the potentially side-effects from making all of these addressable specifications required.

NOTE: A list of all Addressable Implementation Specifications from HIPAA Security is provided in Appendix for HIT Standards Committee reference only; not intended to be included in our RFI comments

Questions Reviewed by P&S Workgroup

Question 23: Are there other security frameworks or guidance that we should consider for this CTE? Should we look to leverage NISTIR 7497 Security Architecture Design Process for Health Information Exchanges? 32 If so, please also include information on how this framework would be validated.

P&S WG Comments:

NISTIR 7497 focuses on the Exchange architecture and specifications and was developed before the Direct protocol was developed, and would need to be refreshed.

Good guidance for organizations implementing the Exchange specifications. However, as guidance, it should not be mentioned or prescribed in the governance regulation.

As mentioned in our response to question 45, we do not believe the governance regulation should be transport-specific. However, we do think it would be appropriate for ONC to make transport-specific guidance, such as NISTIR 7497, known to NVEs implementing the such transports.

**NO CHANGE FROM
COMMENTS REPORTED
AT MAY HITSC MEETING**

Questions Reviewed by P&S Workgroup

Re Condition [I-1]: An NVE must be able to facilitate secure electronic health information exchange in two circumstances: (1) When the sender and receiver are known; and (2) when the exchange occurs at the patient's direction.

Question 45: What types of transport methods/standards should NVEs be able to support? Should they support both types of transport methods/standards (i.e., SMTP and SOAP), or should they only have to meet one of the two as well as have a way to translate (e.g., XDR/ XDM)?

P&S WG Comments:

We do not think it is appropriate for an NwHIN governance model to dictate the transport protocols NVEs should support. Rather, the model should be equally appropriate regardless of the transport mechanism(s) supported.

Most importantly, the NVEs should be required to publish the transport protocol(s) they support and the mechanisms they use to implement these protocols.

The governance model should specify a standard for publishing the protocol(s) supported and mechanisms used.

**NO CHANGE FROM
COMMENTS REPORTED
AT MAY HITSC MEETING**

Questions Reviewed by P&S Workgroup

Re Condition [I-2]: An NVE must follow required standards for establishing and discovering digital certificates.

Question 47: Are the technical specifications (i.e., Domain Name System (DNS) and the Lightweight Directory Access Protocol (LDAP)) appropriate and sufficient for enabling easy location of organizational certificates? Are there other specifications that we should also consider?

P&S WG Comments:

Governance regulation should not include this level of detail.

The definition and scope, and associated roles and responsibilities, of validation, accreditation, and certification are confusing and need to be clarified. For example, what role would existing bodies such as DirectTrust.org, NwHIN Oversight Committee, existing certificate authorities, and EHR technology certification play in these activities?

Governance process needs to capitalize on existing processes and services.

**NO CHANGE FROM
COMMENTS REPORTED
AT MAY HITSC MEETING**

Questions Reviewed by P&S Workgroup

Question 56: Which CTEs would you revise or delete and why? Are there other CTEs not listed here that we should also consider?

P&S WG Comments:

Detailed recommendations on next 2 slides

Some of the CTEs are duplicative with S-1 (which makes HIPAA Security Rule “addressable” implementation specifications “required”). Duplicate requirements will create revision problems downstream. We recommend eliminating all duplicative requirements in the final regulation.

Questions Being Reviewed by P&S Workgroup

Safeguards CTEs	P&S Workgroup Comment
[S-1]: An NVE must comply with sections 164.308, 164.310, 164.312, and 164.316 of title 45 of the Code of Federal Regulations as if it were a covered entity, and must treat all implementation specifications included within sections 164.308, 164.310, and 164.312 as “required.”	Comments provided earlier
[S-2]: An NVE must only facilitate electronic health information exchange for parties it has authenticated and authorized, either directly or indirectly to a trusted root/trust anchor consistent with the Federal Identity, Credential, and Access Management (FICAM) Trust Framework, at assurance level 2 or higher, and must implement an appropriate certificate policy (CP/CPS) that accounts for identity proofing and level of assurance.	Revise as shown. The HITSC Privacy and Security Workgroup reasserts our recommendation that all digital certificates used by organizations exchanging information within the NwHIN must be issued by certificate authorities that meet FICAM standards.
[S-3]: An NVE must ensure that individuals are provided with a meaningful choice regarding whether their IIHI may be exchanged by the NVE.	Would not apply to every NVE. Would apply if they have their own repository. HIE participants (e.g., providers) will also have a responsibility to offer meaningful choice

Questions Being Reviewed by P&S Workgroup

Safeguards CTEs	P&S Workgroup Comment
<p>[S-4]: An NVE must only ensure that IIHI is exchange encrypted III when being exchanged.</p>	<p>Revise as shown.</p>
<p>[S-5]: An NVE must make publicly available a notice of its data practices describing why IIHI is collected, how it is used, and to whom and for what reason it is disclosed.</p>	<p>This CTE does not capture the nuances explained in the RFI re how this notice differs from the HIPAA Notice of Privacy Practices (NPP). Also, need to clarify what information the notice needs to include when describing the actual instances when IIHI is collected, used, disclosed, including to whom and for what purpose, and when/how the notice would need to be updated.</p> <p>What if there is no consumer-facing presence? May not apply to every NVE.</p> <p>The overarching Governance Authority should make these Notices available for every validated NVE.</p>

Questions Being Reviewed by P&S Workgroup

Safeguards CTEs	P&S Workgroup Comment
<p>[S-6]: An NVE must not use or disclose de-identified health information to which it has access for any commercial purpose.</p>	<p>This requirements goes beyond current HIPAA and HITECH policy regarding de-identified information. Tiger Team and ONC should discuss. Having the statement focus only on de-identified information gives the impression that use/disclosure of <u>identified</u> information is OK</p>
<p>[S-7]: An NVE must publish its actual availability, and describe the method used to measure availability operate its services with high availability.</p>	<p>Revise as shown. Transparency of actual availability is essential.</p>

Questions Being Reviewed by P&S Workgroup

Safeguards CTEs	P&S Workgroup Comment
<p>GENERAL COMMENT RE S-8 and S-9. These CTEs provide a channel that undermines a clinician's professional responsibility to withhold information deemed potentially harmful to the patient.</p>	
<p>[S-8]: If an NVE assembles or aggregates health information that results in a unique set of IHH, then it must provide individuals with an electronic copy of access to their unique set of IHH.</p>	<p>Revise as shown. Recommendation to delete "that results in a unique set of IHH" reflects concerns about how to define what a "unique set" is. Recommendation regarding electronic access is necessary to clarify that the NVEs are not required to provide individuals direct access to the NVE's electronic repositories.</p>
<p>[S-9]: If an NVE assembles or aggregates health information which results in a unique set of IHH, then it must provide individuals with the right to request a correction and/or annotation to this unique set of IHH.</p>	<p>See above. An NVE should not be responsible for changing clinical data; rather the NVE should refer the patient to the organization that provided the data, should any corrections be warranted. Also, this CTE provides an opportunity for a malicious patient to wrongfully change data (e.g., a drug abuser).</p>

Questions Being Reviewed by P&S Workgroup

Safeguards CTEs	P&S Workgroup Comment
<p>[S-10]: An NVE must have the means to verify that a provider requesting an individual's health information through a query and response model has given as the purpose of use or is in the process of establishing a treatment of the patient whose information is being requested relationship with that individual.</p>	<p>Revise as shown.</p>

Questions Reviewed by P&S Workgroup

Question 57: Should one or more of the performance and service specifications implemented by the participants in the Exchange be included in our proposed set of CTEs? If so, please indicate which one(s) and provide your reasons for including them in one or more CTEs. If not, please indicate which one(s) and your reasons (including any technical or policy challenges you believe exist) for not including them in one or more CTEs.

P&S WG Comments:

Tight governance as described in the Data Use and Reciprocal Support Agreement (DURSA) is unlikely to work on a national scale that encompasses both public and private entities, ranging in size from small private practices to federal agencies.

While service level agreements (SLAs) like those contained in the DURSA may be appropriate and enforceable within a tightly controlled consortium like the Exchange, this level of specificity is inappropriate for a national governance model.

We recommend a governance model that requires NVEs to publish their SLAs and their performance against these SLAs.

**NO CHANGE FROM
COMMENTS REPORTED
AT MAY HITSC MEETING**

Looking Ahead

- HIT Policy Committee Privacy and Security Tiger Team has been given charge to consider identity management within the context of the National Strategy for Trusted Identities in Cyberspace (NSTIC)
 - Initial focus on physician authentication
 - Patient/consumer authentication to be considered later
- Planning joint, in-person, public hearing co-chaired by Chairs of HITPC P&S Tiger Team and HITSC P&S Workgroup – scheduled for July 11
 - Panels will address:
 - Current identity challenges in a clinical setting
 - Current status of NSTIC
 - Federal use cases and application of NSTIC
- P&S Tiger Team to present recommendations to HITPC on August 1; anticipate that we may be asked to provide standards recommendations to support policy direction

**Appendix A:
HIPAA Security Rule
“Addressable” Implementation
Specifications**

HIPAA Security Addressable Implementation Specifications

SECTION I - ADMINISTRATIVE SAFEGUARDS

Citation	Standard	ADDRESSABLE (A) Implementation Specifications		Description
164.308(a)(3)	Workforce security	Authorization and/or supervision	(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
		Workforce clearance procedure	(A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
		Termination procedure	(A)	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
164.308(a)(4)	Information access management	Access authorization	(A)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
		Access establishment and modification	(A)	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
164.308(a)(5)	Security awareness and training	Security reminders	(A)	Provide periodic security updates.
		Protection from malicious software	(A)	Procedures for guarding against, detecting, and reporting malicious software.
		Log-in monitoring	(A)	Procedures for monitoring log-in attempts and reporting discrepancies.
		Password management	(A)	Procedures for creating, changing, and safeguarding passwords.
164.308(a)(7)	Contingency plan	Testing and revision procedure	(A)	Implement procedures for periodic testing and revision of contingency plans.
		Applications and data criticality analysis	(A)	Assess the relative criticality of specific applications and data in support of other contingency plan components.

HIPAA Security Addressable Implementation Specifications

SECTION II - PHYSICAL SAFEGUARDS

Citation	Standard	ADDRESSABLE (A) Implementation Specifications		Description
164.310(a)(1)	Facility access controls	Contingency operations	(A)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		Facility security plan	(A)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		Access control and validation procedures	(A)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		Maintenance records	(A)	Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (e.g., hardware, walls, doors, locks).
164.310(d)(1)	Device and media controls	Accountability	(A)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
		Data back-up and storage	(A)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

SECTION III - TECHNICAL SAFEGUARDS

Citation	Standard	ADDRESSABLE (A) Implementation Specifications		Description
164.312(a)(1)	Access control	Automatic log-off	(A)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		Encryption and decryption	(A)	Implement a mechanism to encrypt and decrypt electronic protected health information.
164.312(c)	Integrity	Mechanism to authenticate electronic protected health information	(A)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
164.312(e)(1)	Transmission security	Integrity controls	(A)	An implement security measure to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
		Encryption	(A)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.