Health IT Policy Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

October 29, 2013
Jacob Reider, MD
Acting National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. Reider:

The HIT Policy Committee (Committee) gave the following broad charge to the Privacy & Security Tiger Team (Tiger Team):

Broad Charge for the Privacy & Security Tiger Team:
The Tiger Team is charged with making short-term and long-term recommendations to the Health Information Technology Policy Committee (HITPC) on privacy and security policies and practices that will help build public trust in health information technology and electronic HIE, and enable their appropriate use to improve healthcare quality and efficiency, particularly as related to ARRA and the Affordable Care Act (ACA) which mandates a number of duties to the Office of the National Coordinator (ONC) relative to privacy and security.

This letter provides recommendations to the National Coordinator, Department of Health and Human Services (HHS) based on the feedback received from the Meaningful Use Stage 3 Request for Comments. The Tiger Team also considered whether any of its previous recommendations addressed the questions or whether particular questions assigned to the Tiger Team would be better served by a discussion and response by the HIT Standards Committee.

Background
The HITPC held a series of public hearings with various stakeholders, gathering information on their current experience with MU, what lessons have been learned and what their future vision of MU is. In addition, the HITPC invited the public to provide feedback on Meaningful Use Stage 3.

ONC summarized these comments and presented those related to privacy and security to the Tiger Team for their consideration. The Tiger Team and the HITPC is providing recommendations after reviewing the responses to the RFC on Stage 3 of the MU program.

Recommendations
At the June 5, 2013, HIT Policy Committee meeting, the Tiger Team presented its initial recommendations for Stage 3 of Meaningful Use after reviewing public comments. The Policy Committee approved the recommendations except on the issue of Security Risk Assessment Attestation for Meaningful Use. The Tiger Team continued to discuss the Security Risk Assessment Attestation issue and presented its recommendations on that issue at the August 7, 2013 HITPC meeting, at which they were approved

This letter presents the Tiger Team's final recommendations, as approved by the HITPC, on all of the issues raised from comments received from the RFC for Stage 3 of the Meaningful Use program.

Re-Use of 3rd Party Credentials
How can the HITPC's recommendation be reconciled with the National Strategy for Trusted Identities in Cyberspace (NSTIC) approach to identification which strongly encourages the re-use of third party credentials?

1) The Tiger Team's September 2012 recommendations on provider user identity management, adopted by the Policy Committee, already address this issue[1]. The recommendations urged multi-factor authentication at NIST Level of Assurance (LoA) 3 for remote access to PHI; entities covered by HIPAA should also, as part of their security risk assessment, identify other access environments that may require multiple factors to authenticate an asserted identity. Provider users should continue to be identity proofed in compliance with HIPAA. Work being done as part of NSTIC to establish trusted, third-party credentials is ongoing but such solutions are not yet widely available, and may not be by Stage 3. Consequently, as recommended by the Policy Committee, ONC's efforts on this issue should continue to be informed by NSTIC developments, including (but not limited to) the work being done in the NSTIC pilots.

Certification Criteria for Testing Authentication
How would ONC test the HITPC's recommendation (for two-factor authentication) in certification criteria?

2) As the question does not request a policy-based response, the Tiger Team believes this question would be best answered by the HITSC.

EHR Certification – Standalone
Should ONC permit certification of an EHR as stand-alone and/or an EHR along with a third-party authentication service provider?

3) ONC should permit certification of both a stand-alone EHR and an EHR along with a third-party authentication service provider.

MU Attestation for Security
What, if any, security risk issues (or HIPAA Security Rule provisions) should be subject to Meaningful Use attestation in Stage 3?

4) The Tiger Team would like to improve accountability for complying with the existing meaningful use security measures – in particular, the requirement to perform a security risk analysis and correct identified deficiencies. For MU Stage 3, CMS should emphasize that when an entity attests to having conducted or reviewed a security risk analysis with respect to its certified EHR technology, the entity is attesting to compliance with the HIPAA Security Rule with respect to

[1] http://www.healthit.gov/FACAS/sites/faca/files/transmittal_092512_pstt_recommendations_provider_authentication.pdf

such analysis. To achieve compliance with this objective, entities must conduct a security risk analysis or review an existing risk analysis and document the results of the risk analysis or review, including the actions taken (or the schedule for actions planned to be taken) to correct any deficiencies identified during the analysis or review.

In addition, CMS should add an accountability measure, requiring entities to identify the individual(s) who is/are responsible for conducting and documenting the risk assessment. The objective here is not to single out an individual or individuals but to prompt professionals and hospitals to take seriously the obligation to conduct and document the risk assessment. The Tiger Team also recommends that CMS link attestation to specific MU objectives, rather than present it as a single, stand-alone measure. Specifically, CMS should require attestation that a risk assessment has been performed on any new functionality provided as a result of deploying the 2014 or subsequent MU criteria (those for 2014 focus on exchange and interoperability between organizations, and consumer engagement). The Tiger Team is concerned that the current approach may result in covered entities viewing the risk assessment as a separate requirement to be addressed solely by its security organization, rather than as an ongoing process that must be considered with respect to all aspects of the EHR system. In making this recommendation, the Tiger Team is seeking to re-emphasize the relationship between the risk assessment requirement and other MU measures, and the importance of involving security professionals fully in decisions about how EHR systems' functionality is deployed. Finally, such an attestation would indicate that the entity had complied with the HIPAA Security Rule by performing the required analysis and documenting the results, including correction of identified deficiencies.

CMS should provide additional education, such as FAQs, to the meaningful user community on the expectations and importance of conducting and documenting security risk analyses, and correcting deficiencies. For example, CMS can expand FAQs to discuss the availability/use/benefits of third-party assessment tools and services, and of risk analysis checklists, particularly those developed by the regulators. In addition, CMS can expand FAQs to clarify that a component of the risk analysis process includes the requirement to correct any deficiencies that impact compliance with the HIPAA Security Rule. CMS can also highlight (for larger entities with the requisite resources) the option/value of having internal auditors leverage OCR's audit program protocol to conduct substantive pre-audits.

Certification Standard for Audit Logs
Is it feasible to certify the compliance of EHRs based on the prescribed ASTM standard for audit logs?

5) The Tiger Team suggests that the HITSC address whether it is feasible to certify compliance of EHRs with the prescribed ASTM audit log standard. Some Tiger Team members also questioned the adequacy of the standard.

Attestation for Length of Time Logs
Is it appropriate to require attestation by meaningful users that such logs are created and maintained for a specific period of time?

6) The HIPAA Security Rule does not require that audit logs be maintained for a specific period of time. Consequently, the Tiger Team does not see a reason to require additional policy specifying a timeframe. Covered entities will make their own decisions on audit trail maintenance periods based on their internal policies.

Standard Format for Log Files
Is there a requirement for a standard format for the log files of EHRs to support analysis of access to health information access multiple EHRs or other clinical systems in a healthcare enterprise?

7) Although there are arguments in favor of standardizing formats for log files, this is a lower priority discussion in the context of Meaningful Use. The Tiger Team recommends following the guidance of the HIPAA Security Rule, which does not require any particular audit trail format.

Audit Log File Specifications
Are there any specifications for audit log file formats that are currently in widespread use to support such applications?

8) The Tiger Team recommends following the guidance of the HIPAA Security Rule, which does not require any particular format. The HITSC can determine whether particular specifications should be required for EHR certification.

Patient Consent
Some federal and state health information privacy and confidentiality laws, including but not limited to 42 CFR Part 2 (for substance abuse), establish detailed requirements for obtaining patient consent for sharing certain sensitive health information, including restricting the recipient's further disclosure of such information.

A. How can EHRs and HIEs manage information that requires patient consent to disclose so that populations receiving care covered by these laws are not excluded from health information exchange?
B. How can MU help improve the capacity of EHR infrastructure to record consent, limit the disclosure of this information to those providers and organizations specified on a consent form, manage consent expiration and consent revocation, and communicate the limitations on use and restrictions on re-disclosure to receiving providers?
C. Are there existing standards, such as those identified by the Data Segmentation for Privacy (DS4P) Initiative Implementation Guide, that are mature enough to facilitate the exchange of this type of consent information in today's EHRs and HIEs?

9) The Tiger Team refers to its recent recommendations (adopted by the Policy Committee) on Query/Response re: technical mechanisms to support communication of patient consent requirements[2]. In particular, data holders and requesters should comply with applicable law and

[2] http://www.healthit.gov/FACAS/sites/faca/files/HITPC_Transmittal_08212013.pdf

policy and should have a technical way to communicate applicable consent or authorization needs and requirements. They should also have a means to maintain a record of such transactions. The HITSC should further consider technical methods for giving providers the capacity to comply with applicable patient authorization requirements or policies. On the question related to data segmentation, the Tiger Team has deferred further discussion on the topic until it has received an update on the DS4P Initiative pilot projects[3].

We appreciate the opportunity to provide these recommendations on Stage 3 of the Meaningful Use Program and look forward to discussing next steps.

Sincerely yours,

/s/

Paul Tang
Vice Chair, HIT Policy Committee

[3] http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage