Privacy and Security Tiger Team

Report to the Health IT Policy Committee Meeting

June 5, 2013

Tiger Team Members

- **Deven McGraw, Chair**, Center for Democracy & Technology
- **Paul Egerman, Co-Chair**
- **Dixie Baker**, Martin, Blanck, and Associates
- **Judy Faulkner**, Epic
- **Leslie Francis**, University of Utah College of Law
- **Gayle Harrell**, Consumer Representative/Florida
- **John Houston**, University of Pittsburgh Medical Center
- **David McCallie**, Cerner Corporation
- **Wes Rishel**, Gartner
- **Micky Tripathi**, Massachusetts eHealth Collaborative
- **Kitt Winter,** Social Security Administration

MU3 RFC Comments

- The Tiger Team's goal was to determine if there were relevant policy considerations to discuss, based on the feedback received from the MU3 Request for Comments period, and whether previous Tiger Team recommendations address the questions.
- In addition, it determined whether particular questions assigned to the Tiger Team would be better served by a discussion and response by the HIT Standards Committee and its Privacy and Security Workgroup.

PSTT01 Summary: 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?**

  Response: **The Tiger Team's September 2012 recommendations on provider user identity management, adopted by the Policy Committee, already address this issue.** 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.**

**Source: Sept 2012 HITPC Recommendations to ONC
http://www.healthit.gov/sites/default/files/transmittal_092512_pstt_recommendations_provider_authentication.pdf

PSTT02 Summary: Certification Criteria for Testing Authentication

- **How would ONC test the HITPC's recommendation (for two-factor authentication) in certification criteria?**
- Response: As the question does not request a policy-based response, the Tiger Team believes this question would be best answered by the HITSC Privacy and Security Workgroup.

PSTT03 Summary: 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?**
- Response: Yes. ONC should permit certification of both a stand-alone EHR and an EHR along with a third-party authentication service provider.

PSTT04 Summary: MU Attestation for Security

- **What, if any, security risk issues (or Health Insurance Portability and Accountability Act (HIPAA) Security Rule provisions) should be subject to Meaningful Use attestation in Stage 3?**
- Question: Should this be in lieu of, or added to, the existing attestation requirements (completion of security risk assessment and addressing encryption of data at rest)?

PSTT04 Summary: MU Attestation for Security

- The Tiger Team concluded that it would like to further investigate methods beyond attestation to call greater attention to existing HIPAA requirements, such as risk assessments, through the Meaningful Use Program.
- It has convened a subgroup of its members for this purpose. It will also examine the effectiveness of the attestation process.
- The HITPC will receive an update on PSTT04 at a future meeting.

PSTT05 Summary: Certification Standard for Audit Logs

- **Is it feasible to certify the compliance of EHRs based on the prescribed [ASTM] standard for [audit logs]?**
- Response: The Tiger Team suggests that the HITSC Privacy and Security Workgroup 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.

PSTT06 Summary: 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?**
- Response: The HIPAA Security Rule does not require that audit logs are 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.

PSTT07 Summary: 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?**
- Response: 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.

PSTT08 Summary: Audit Log File Specifications

- **Are there any specifications for audit log file formats that are currently in widespread use to support such applications?**
- Response: The Tiger Team recommends following the guidance of the HIPAA Security Rule, which does not require any particular format. The HITSC Privacy and Security Workgroup can determine whether particular specifications should be required for EHR certification.

MU4 Summary: 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.** ***Three questions were put forth.***

MU4 Summary: Patient Consent

1) ***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?***

2) ***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?***

3) ***Are there existing standards, such as those identified by the Data Segmentation for Privacy Initiative Implementation Guide, that are mature enough to facilitate the exchange of this type of consent information in today's EHRs and HIEs?***

MU4 Summary: Patient Consent

- Response: 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.
  - Data holders and requesters should comply with applicable law and 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.
- The Tiger Team has deferred further discussion on data segmentation** until it has received an update on the DS4P Initiative pilot projects.

**Source: Sept 2010 HITPC Recommendations to ONC
http://www.healthit.gov/sites/default/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf

Virtual Hearing on Non-Targeted Query

- An effort to uncover what sort of policies are deployed to ensure that a “non-targeted query” for a patient record is appropriate, legal, and authorized.
  - Such policies may include limitations on who can conduct the query, the purposes for which a query can be conducted, geographic or other limits intended to help assure proper access to a patient’s records.
  - The Tiger Team also wants to learn about the thought processes behind the development of any such policies.
- Focus of the hearing is on policy and not security methodology.
- Invitation to a small group of HIEs and HIE/Infrastructure Marketplace Vendors.