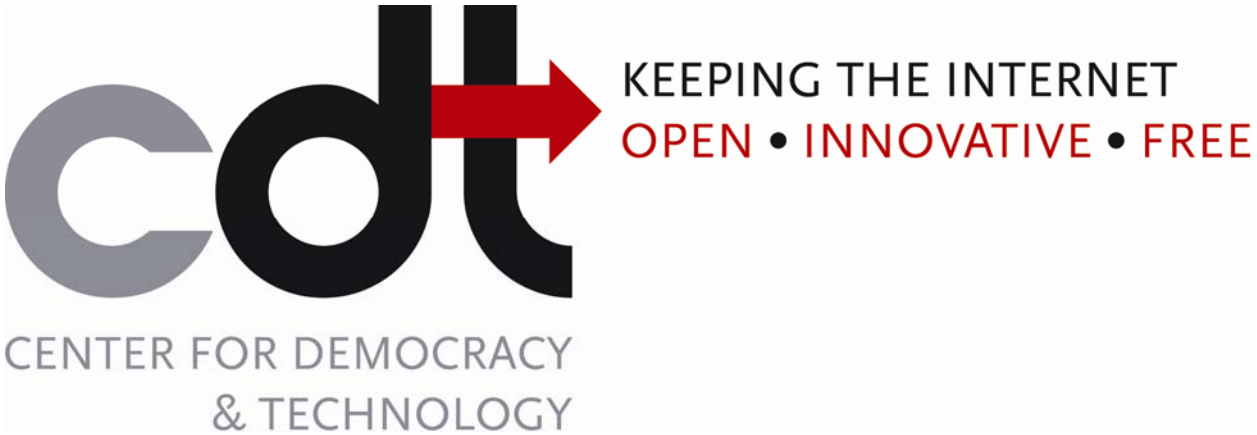

HEALTH IT Policy Committee

Tiger Team Recommendations on Security and Integrity of ePHI

Deven McGraw
Director, Health Privacy Project

July 15, 2011

What is the “Tiger Team”?

- First assembled in June 2010 to address some specific questions from ONC that needed to be addressed by the end of the summer.
- Comprised of members of the Health IT Policy and Standards Committees, and NCVHS.
- Initial aggressive summer 2010 schedule – average of 3 phone meetings every 2 weeks, at 3-4 hours per meeting
- Still meeting on privacy and security issues but on a more “reasonable” schedule (@ 2-3/month)
- Recommendations go to Health IT Policy Committee, then ONC (or ONC and CMS in the case of meaningful use)

HealthIT Policy Committee Tiger Team Recommendations

- Focus has been on policies to govern exchange among providers for Stage 1 of Meaningful Use (treatment & care coordination, quality reporting, public health); mostly focused on “push” transactions
  - Limited set of health care activities/transactions
- Recommendations to ONC – what policy levers to enforce?
  - Meaningful use & certification
  - Grant conditions
  - Nationwide Health Information Network (NwHIN) governance requirements (governance rule expected “fall” 2011)

Health IT Standards Committee

- Establishes standards and technical requirements for certified EHRs
- First out of the gate with security functionalities required for certified EHRs for Stage 1.
  - Encryption of data at rest and in motion
  - Access Control
  - Emergency access
  - Auto log-off after inactivity
  - Audit log
  - Integrity (use of hashing algorithm ≥ SHA-1
  - Authentication

Policy Committee Recommendations - Matching Patients with their Information

- Use of any particular data field should not be required for matching. However, when a data field is used to match, standardized formats help increase accuracy.
  - Standards committee should recognize standard formats for commonly used data fields
  - Standards committee should develop standard for representing missing data
- Health care entities should evaluate the efficacy of their matching strategies and use such evaluations to internally improve accuracy.

Matching Patients to their Information (cont.)

- Matching accuracy should be enforced through HIE/NwHIN governance
  - HIEs should implement matching accuracy programs that are appropriate for the populations served and purposes for which data is exchanged
- ONC should establish a program or programs to develop and disseminate best practices in improving data capture and matching accuracy.
- Tiger Team supports meaningful use efforts to provide patients with greater access to their data to flag potential errors.

Exchange Requirements for Entities

- All entities involved in electronic health information exchange should be required to have digital certificates (entity level – not individual user – certificates)
- Entities must demonstrate they are a legitimate business and engaged in health care transactions; credentialing organizations should rely on existing criteria/processes (like the NPI) when appropriate
- Multiple credentialing organizations will need to be recognized to meet need
  - Initially recommended ONC establish accreditation program for credentialers – latest recommendation is for Federal Bridge cross-certification

Identification and authentication – Provider EHR Users (workforce)

- Provider entities are responsible for identity proofing individual users
- More than single factor authentication should be required as a baseline for remote access
  - But need not be as stringent as NIST or DEA criteria
  - Certified EHRs must be tested for ability to meet DEA standard for e-prescribing controlled substances
- ONC should develop and disseminate evidence about best practices; policies should keep up with innovation within the healthcare industry & other sectors

Identification and authentication – patient users of "portals" to EHRs

- Entities should set their own identification requirements; Tiger Team recommended principles that include knowing your population and not setting bar so high that you discourage participation
- Single factor authentication is sufficient as baseline policy – but entities can offer greater protections (as long as bar not set so high participation is discouraged)
- Certified EHRs should include capability for auto-lockout of programmatic and unauthorized user attacks

Additional Recommendations – Patient Portals

- Entities should deploy audit trails for portals and make them available to patients upon request
- Portals should include provisions for data provenance, which is accessible to the user, both respect to access and upon download
- Portals should include mechanisms to ensure information in the portal can be securely downloaded to a third party authorized by the patient

Security Risk Assessment for Meaningful Use Stage 2

- For Stage 2 of meaningful use, providers and entities should have to do a security risk assessment (just as in Stage 1)
- For Stage 2, providers and entities must address encryption/security functionalities for data at rest. Must attest that they have done this as part of their required security risk assessment.
  - Using meaningful use to shine a spotlight on this particular provision of the HIPAA Security Rule – breaches of >500 records reported to HHS indicate this provision of the Security Rule is not being well addressed. Cumulative reports of breach imperil public trust of health IT initiatives.

Amendments/Corrections to Health Data

1. Certified EHR Technology should have the capability in Stage 2 (meaningful use) to support amendments to health information. Specifically, the systems should make it technically possible for providers to:

   a. Make amendments to a patient's health information in a way that is consistent with the entity's obligations with respect to the legal medical record (i.e., there should be the ability to access/view the original data and to identify any changes to it).

   b. Append information from the patient and any rebuttal from the entity regarding disputed data.

2. Certified EHR Technology should have the ability by Stage 3 to transmit amendments, updates or appended information to other providers to whom the data in question has been previously transmitted.

Questions?

Deven McGraw

202-637-9800 x115

deven@cdt.org

www.cdt.org/healthprivacy

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE