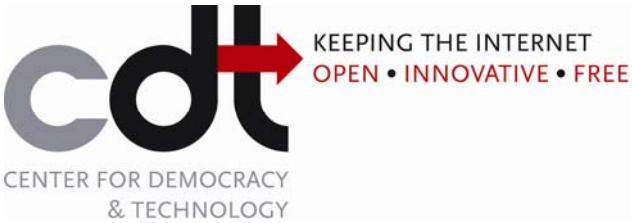

HEALTH PRIVACY & SECURITY

Report from the Tiger Team/Health IT Policy Committee

Deven McGraw
Director, Health Privacy Project
March 27, 2012

ONC Programs

- Stage 1 Meaningful Use Privacy and Security: Perform a security risk assessment and address deficiencies
  - Certification criteria includes a number of security functionalities
  - Measured through provider attestation
- May be more stringent criteria for Stage 2 (begins 2014)
  - Policy Committee recommended that security risk assessment require focus on encryption of data at rest
  - 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.
  - Proposed Rule adopts this approach; also certification proposed rule requires EHRs to have default capability of encrypting data on "managed" devices

ONC Programs (cont.)

- ONC to propose rule on governance of "Nationwide Health Information Network (NwHIN)" (early 2012)
- Expected that at least some recommendations of Health IT Policy Committee (including Tiger Team) will become "conditions" required to use NwHIN brand to exchange health information
- Who will be "required" to comply

What is the "Tiger Team"?

- First assembled in June 2010 to address some specific questions from ONC
- 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 (@ 2x/month)
- Recommendations go to Health IT Policy Committee, then ONC (or ONC and CMS in the case of meaningful use)

Health IT Policy Committee Privacy Recommendations

- Focus has largely been on policies to govern exchange among providers for Stages 1 and 2 of Meaningful Use (treatment & care coordination, quality reporting, public health); mostly focused on "push" transactions
- More recent recommendations have looked at some secondary uses
- Recommendations to ONC – what policy levers to enforce?
  - Meaningful use & certification (thus possibly some Medicaid)
  - Grant conditions
  - Nationwide Health Information Network (NwHIN) governance requirements

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Fair Information Practices

- Overarching recommendation – all entities involved in health information exchange need to implement rigorous fair information practices
  - Includes "intermediaries" or HIEs, third party service organizations
  - Limits on collection, use, disclosure, reuse and retention of identifiable health information – only what is needed to perform contracted functions
  - Transparency re: uses and disclosures of de-identified data
  - Business associate agreements provide one tool for accountability – but probably not sufficient (NwHIN governance)

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

General Consent (yes/no)

- Recommendations flow from core value that the physician-patient relationship is the foundation for trust in health information exchange
- Providers are responsible for maintaining the privacy and security of information they share. Delegation of functions to other parties (like business associates and HIEs) must be done in a way that maintains this trust.
- Assumes current law applies – consent recommendations are above and beyond

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

General Consent (cont.)

- No additional consent required for directed exchange where one provider exchanges with another known provider & *provider is in control of decision to disclose* (how much, to whom)
  - Consistent with what patients expect
- "Meaningful Consent" should be required for exchange arrangements where provider is no longer in control of disclosures from his/her records
  - For example, centralized HIE models and some federated models
- Meaningful consent – must have opportunity to make in advance, with full transparency, no discrimination

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Granular consent

- Technology hearing on June 29, 2010
- Addressed question of whether EHR technology has the capability to manage more granular consent (for example, consent by data type)
- Technology is promising in this area – but availability and use are not widespread
- ONC should spur further development and innovation in this space, such as through pilots
  - ONC is currently pursuing further through Data Segmentation Initiative

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

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.

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

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.

Exchange Requirements for Entities

- All entities involved in electronic health information exchange should be required to have digital 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
- Want high degree of assurance re: legitimate entity, and ideally ability to exchange with federal gov't (e.g., Fed'l Bridge cross-certification)
- Multiple credentialing organizations will need to be recognized to meet need

Identification and authentication – Provider EHR Users

- Provider entities are responsible for identity proofing individual users
- More than single factor authentication should be required as a baseline for remote access (not addressed in proposed Stage 2 EHR certification rule)
  - 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 (not in Stage 2 rule)
- ONC should develop and disseminate evidence about best practices; policies should keep up with innovation within the healthcare industry & other sectors

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Requirements for Stage 2 patient "view and download" capability

- 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 (not in Stage 2 rule)

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Additional Recommendations – View and download capability

- Patients should be provided with simple, layered notice on risks of view and download
- Entities should deploy audit trails for portals and make them available to patients upon request (in proposed Stage 2 rule)
- Portals should include provisions for data provenance, which is accessible to the user, both respect to access and upon download (data provenance included in Stage 2 rule)
- Portals should include mechanisms to ensure information in the portal can be securely downloaded to a third party authorized by the patient (included in Stage 2 rule)

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Secondary Uses

- Response to Common Rule Advance Notice of Proposed Rulemaking – focus on secondary uses of EHR data
  - Allow more quality assurance activities to be considered "operations," even if the results are publicly shared (contribute to "generalizable knowledge").
  - Rely more on institutions to be reliable data stewards, comply with fair information practices (vs. overreliance on consent).
- Initial policies for ONC's QueryHealth initiative (distributed population health network)

cdt KEEPING THE INTERNET OPEN • INNOVATIVE • FREE

Questions?

Deven McGraw

202-637-9800 x115

deven@cdt.org

www.cdt.org/healthprivacy

KEEPING THE INTERNET OPEN • INNOVATIVE • FREE