Health IT Policy Committee

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

Privacy and Security Workgroup

Notice of Proposed Rulemaking (NRPM) Comments

Deven McGraw, Chair
Stanley Crosley, Co-chair

May 12, 2015

PSWG Members

- **Deven McGraw**, Chair, Manatt, Phelps & Phillips, LLP
- **Stanley Crosley,** Co-Chair, Drinker Biddle & Reath LLP
- **Donna Cryer,** Member, CryerHealth
- **Gayle B. Harrell**, Member, Florida State House of Representatives
- **Linda Kloss,** Member, Kloss Strategic Advisors, Ltd.
- **David Kotz,** Member, Dartmouth College
- **Gilad Kuperman,** Member, NewYork-Presbyterian Hospital
- **Manuj Lal,** Member, PatientPoint Enterprise
- **David McCallie, Jr.,** Member, Cerner Corporation
- **Micky Tripathi,** Member, Massachusetts eHealth Collaborative
- **John Wilbanks,** Member, Sage Bionetworks
- **Kristen Anderson,** Ex Officio, Federal Trade Commission
- **Sarah Carr,** Ex Officio, NIH Office of Science Policy
- **Adrienne Ficchi,** Ex Officio, Veterans Health Administration
- **Stephania Griffin,** Ex Officio, Veterans Health Administration
- **Cora Tung Han,** Ex Officio, Federal Trade Commission
- **Taha Kass-Hout,** Ex Officio, Food and Drug Administration
- **Bakul Patel,** Ex Officio, Food and Drug Administration
- **Linda Sanches,** Ex Officio, Office for Civil Rights-Health and Human Services
- **Kitt Winter,** Ex Officio, Social Security Administration

Agenda

1. Meaningful Use Stage 3 NPRM
   - Objective 1 (Protect Patient Health Information)
   - Privacy and Security Issues Related to Increasing Patient Access to Data through either VDT or APIs
2. Health IT Certification NPRM
   - Data Segmentation for Privacy (DS4P)
   - Pharmacogenomics Data

Meaningful Use Stage 3 NPRM

Privacy and Security Issues Related to Increasing Patient Access to Data through either VDT or APIs

Privacy and security issues related to increasing patient access to data

- Risks/Provider Responsibility:
  - Heightened security risks from increasing numbers of APIs connecting to EHRs.
  - Vendors' unclear or incorrect understanding and implementation of privacy and security legal requirements.
  - Vendors' inadequate or incorrect implementation of entity's privacy and security policies.
- Risks/Patient Responsibility:
  - Use of app/device with weak security controls.
  - Use of app/device without privacy policy, or with unclear policy, or with policy that shares data liberally with third parties or allows broad uses.

Summary of Discussion

- The Workgroup **supports the proposal to increase the opportunities for patient access to information** through the use of VDT technologies as well as open APIs.

- However, the Workgroup has **concerns about potential privacy and security risks** associated with increasing patient access to health information electronically.

Recommendations

The Workgroup recommends that:

1. ONC and CMS **reference and leverage previous recommendations on best practices for view and download.*** *(see back-up slides)*
2. ONC continue to work with FTC and OCR to **develop guidance for key stakeholders** to adopt the use of mobile IT, apps, and APIs.
   - Guidance for vendors should privacy and security best practices for collection, storage, access, use, transmission, and destruction of health information.
   - Guidance for application developers not covered by HIPAA, but their products capture data from entities covered by HIPAA.
   - Guidance for patients and providers on the safe use of apps and APIs. (e.g., a checklist for patients to consider when choosing apps)
   - Such guidance should be actively and widely disseminated

* 8/16/2011 HITPC Transmittal Letter. http://www.healthit.gov/sites/faca/files/HITPC_PSTT_Transmit_8162011.pdf

Recommendations (cont.)

3. ONC and OCR produce **educational materials for both patients and providers on the safe use of apps and APIs.**
   - Providers can play a key role in counseling patients, so some guidance should be aimed at helping providers fill this role.

4. ONC and OCR produce **educational materials for private industry application developers** about methods for clearly communicating their privacy policy and security practices to patients and providers.

5. Reference prior recommendations on **identity proofing and authentication of patients, family members, friends and personal representatives**.

Recommendations (cont.)

6. ONC and OCR should **issue guidance addressing the intersection between the MU patient engagement objectives, the certification requirements, and HIPAA's patient access rights.** Issues include:
   - the extent to which a provider may reject a patient's request for electronic access due to a perceived security risk for the provider;
   - the extent to which a provider may reject a patient's request for electronic access in the absence of a security risk;
   - the ability of provider's to charge fees for meaningful use access.
7. **Voluntary, yet meaningful and robust, effort by the industry to "certify" patient-facing health apps** to help patients choose apps. ONC and other federal agencies could advise such an initiative, particularly on privacy and security policies, which could help facilitate greater standardization.
   - FTC already has authority to enforce voluntary best practices for those who adopt.

Health IT Certification NPRM

Data Segmentation for Privacy (DS4P)

Data Segmentation for Privacy (DS4P)

- ONC proposes to adopt two new certification criteria that would focus on the capability to separately track ("segment") documents that contain sensitive health information
  - Data Segmentation for Privacy: Send
  - Data Segmentation for Privacy: Receive
- Use of HL7 standard
- Not part of Base EHR (providers not required to purchase it)

DS4P Send and Receive

- Proposal for Send: Technology must enable a user to create a summary record formatted in accordance with each of the standards adopted in § 170.205(a)(3) and (4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1).

- Proposal for Receive: Technology must enable a user to:
  (i) Receive a summary record that is tagged as restricted and subject to restrictions on re- disclosure according to the standard adopted in § 170.205(o)(1).
  (ii) Apply document-level tagging and sequester the document from other documents received.
  (iii) View the restricted document (or data), without incorporating the document (or data).

Summary of Discussion

- Proposed criteria are an **initial step toward the ability of an interoperable health care system** to compute and persist the applicable permitted access, use, or disclosure.
- Workgroup believes that **the DS4P technology should be available** for those who seek to implement it.
- However, the Workgroup has **significant concerns** with the proposed criteria.

Areas of Concern

Concerns previously expressed by the Tiger Team:

- **Obligations for DS4P-receive providers** who do not want to receive the information digitally.
- **Limitations of document level sequestration**, with a read-only capability.
- Uncertainties about extent to which the technology would enable **compliance with Part 2** after receipt of data.
- Uncertainties about **manual entry of similar data** received directly from a patient.
- Uncertainties about whether **DS4P Receive could facilitate compliance with other sensitive data**.
- **Incomplete electronic medical records** due to patients withholding data.

Additional Areas of Concern

- Offering DS4P for **voluntary certification** may create confusion among providers.
  - Sending provider may need to verify off-line (out of band communication) that the receiving provider possesses the technology.
  - Inability of receiving provider without the technology to view document-level security tags.
  - Receiving provider without the technology may not be aware of the re-disclosure restrictions; additional communications methods may be necessary to ensure compliance with law.
  - Lack of harmonization of state and federal laws regarding sensitive information compounds these challenges.

Recommendations

The Workgroup recommends that:

1. **The HIT Standards Committee assess the maturity of the DS4P standard** for inclusion in the 2015 Edition.
   - Reference previous Tiger Team recommendations*
2. **ONC educate providers and patients** about the features and limits of DS4P technology.
3. **ONC continue to pilot and test in order to refine technologies** that enable the sharing of sensitive data in compliance with law.

* http://www.healthit.gov/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf

Health IT Certification NPRM

Pharmacogenomics Data

Pharmacogenomics Data

- PSWG tasked to provide input on:
  - Factors to consider for health IT to allow use or disclosure of genetic information that complies with federal and state privacy laws
  - Leverage the proposed Data Segmentation for Privacy (DS4P) certification criteria for segmenting genetic information?
  - Balance patient benefit with avoiding discrimination
- 5 specific questions deal with privacy and security (10 questions overall)

Recommendations

- Introducing **certification for this functionality in the 2015 Edition is premature**.
  - We recommend ONC continue to review issues around accessing, sharing, and using pharmacogenomics data as the science evolves.
- Responses to specific questions:
  - *Apply different rules for the use and exchange of pharmacogenomics data (e.g., behavioral health)*?
    - **Strongly caution ONC against promoting policies that require higher or more complex protection than what is provided for in current law.**
  - *Does DS4P provide needed health IT functions on the storage, use, transmission, and disclosure of pharmacogenomics information?*
    - No. **DS4P is not currently useful for providers** to comply with more sensitive laws governing pharmacogenomics data;
    - E.g., currently, DS4P **does not enable the use of decision-support software** (key use case for safe prescribing).

Meaningful Use Stage 3 NPRM

Objective 1 (Protect Patient Health Information)

Objective 1: Protect Patient Health Information

Proposed objective: Protect ePHI created or maintained by the CEHRT through the implementation of appropriate technical, administrative, and physical safeguards.

New: adding **Administrative safeguards** (e.g., risk analysis, risk management, training, etc.) and **Physical safeguards** (e.g., facility access controls, workstation security).

Consistent with previous Tiger Team recommendations*

* 10/29/2013 HITPC Transmittal Letter: http://www.healthit.gov/facas/health-it-policy-committee/health-it-policy-committee-recommendations-national-coordinator-health-it

Recommendation

The Workgroup **supports the proposed MU Stage 3 security requirements.** Adding administrative and physical safeguards to the current requirements more closely aligns the CEHRT risk assessments and attestations with the compliance requirements of the HIPAA Security Rule.

Backup Slides

Previous Recommendations on View and Download
(Source: 8/16/2011 HITPC Transmittal Letter)

- Offered flexibility of "best practices" for providers instead of a certification requirement or a "standard"
- Recommended that ONC share the guidance through REC and the entities certifying EHR technology

Best Practices for Providers:

- Providers participating in the MU program should offer patients clear and simple guidance regarding use of the view and download in functionality in Stage 2.
- With respect to the "**view**" functionality, such guidance should address the potential risks of viewing information on a public computer, or viewing sensitive information on a screen that may be visible to others, or failing to properly log out after viewing.

8/16/2011 HITPC Transmittal Letter. http://www.healthit.gov/sites/faca/files/HITPC_PSTT_Transmit_8162011.pdf

Previous Recommendations on View and Download
(Source: 8/16/2011 HITPC Transmittal Letter)

- With respect to the "**download**" functionality, such guidance should be offered at the time the patient indicates a desire to download electronic health information and, at a minimum, address the following three items:
  1. Remind patients that they will be in control of the copy of their medical information that they have downloaded and should take steps to protect this information in the same way that they protect other types of sensitive information.
  2. Include a link or links to resources with more information on such topics as the download process and how the patient can best protect information after download.
  3. Obtain independent confirmation that the patient wants to complete the download transaction or transactions.

Previous Recommendations on View and Download
(Source: 8/16/2011 HITPC Transmittal Letter)

- Providers should utilize techniques, if appropriate, that avoid or minimize the need for patients to receive repeat notices of the guidance on view and/or download risks.

- Providers should request vendors and software developers to configure the view and download functionality in a way that no cache copies are retained after the view session is terminated.

- Providers should request that their view and download functionality include the capability to automatically terminate the session after a period of inactivity.

Previous Recommendations on View and Download
(Source: 8/16/2011 HITPC Transmittal Letter)

- ONC should also provide the above guidance to vendors and software developers, such as through entities conducting EHR certification.

- Providers can review the Markle Foundation policy brief, and the guidance provided to patients as part of the MyHealtheVet Blue Button and Medicare Blue Button, for examples of guidance provided to patients using view and download capabilities.