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 (NPRM) Comments

Deven McGraw, Chair
Stanley Crosley, Co-chair

May 22, 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
   - Privacy and Security Issues Related to Increasing Patient Access to Data through either View, Download, and Transmit (VDT) Technologies or Application Programming interfaces (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.
- The Workgroup recommends a **mixture of timely, meaningful guidance for consumers, health care providers, and vendors, as well as further exploration of an evaluation effort** that facilitates differentiation of mobile tools and meets a wide range of stakeholder needs, including privacy, security, usability, and clinical validity.

Recommendations

1. ONC is already working with FTC and OCR to develop mobile health best practice guidance for developers which will eventually promote protection of user data. We urge the agencies to work quickly to widely disseminate this guidance so it can be useful for Stages 2 and 3 of MU. Such guidance should include:
   - Guidance for app developers on best practices for protecting privacy and security of information collected by the app and connecting with EHRs covered by HIPAA.
2. Additionally, we recommend development of guidance for patients/consumers and providers. Guidance should include:
   - Checklists for consumers on what to look for in a privacy/data use policy;
   - Mechanisms for consumers to compare privacy policies across apps (similar to ONC's model PHR notice)*

* Personal Health Record (PHR) Model Privacy Notice. http://www.healthit.gov/policy-researchers-implementers/personal-health-record-phr-model-privacy-notice

Recommendations (cont.)

3. ONC and OCR should **issue guidance addressing the intersection between the MU patient engagement objectives, the certification requirements, and HIPAA's patient access rights. Such guidance also is needed to help providers in Stages 2 and 3 of MU**. Issues include:
   - How to do a security risk assessment on patient app/device connections (such as through the API) and 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 providers to charge fees for meaningful use access.

Recommendations (cont.)

3. The Health IT Policy Committee previously issued recommendations urging ONC and CMS to provide specific guidance to health care providers participating in MU and vendors of CEHRT to help them manage the risks of "view and download.''* *(see back-up slides)* **This guidance should be updated to also address transmit-related risks and issued in a timely fashion to assist providers (and CEHRT vendors) in making VDT and APIs available to patients as part of MU.** Such guidance should address;
   - When liability for data shifts from providers to patients, and the extent to which providers must make patients aware when patients take responsibility for protecting data.
   - Best practices for counseling patients on assessing and managing privacy and security risks.
   - Responsibilities of vendors to include the CEHRT security safeguards in VDT and API modules.
   - Technical approaches vendors may take to further protect data (for example, "just in time" notices before download and transmit that should be able to be turned off by the patient after the first notice, and non-caching of data).
   - ONC also should act on prior recommendations on for guidance on **identity proofing and authentication of patients, family members, friends and personal representatives**.

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

Recommendations (cont.)

4. **Timely guidance is needed – but is not enough. We call for <u>further exploration</u> of a multi-stakeholder (including industry and patients) developed program for evaluating patient-facing health apps.**

- The Workgroup sees value in a program to evaluate such apps – but believes they should be evaluated on a range of aspects, including privacy and security, usability for consumers/patients, and clinical validity.
- The effort should leverage the guidance developed by federal government entities (see above).
- **Even a voluntarily adopted guidelines could have some teeth: The FTC under – its existing FTCA authority - can enforce voluntary best practices for those who adopt.**
- The evaluation effort also could enhance transparency about privacy and security practices**.**

Recommendations (cont.)

- **The Consumer Workgroup (with assistance from the P&S Workgroup) should continue work to flesh out the details of a program to evaluate patient-facing health apps, considering such issues as:**
  - Whether it should be a certification program, which includes testing (similar to the CEHRT program), or some other evaluation vehicle (accreditation, registry, etc.).
  - Whether it should be voluntary or connected to the CEHRT and/or MU program.
  - Potential incentives/disincentives for vendors to participate.
  - What should be the focus of the program.
  - What should be the role of ONC and other federal entities.
  - Costs and potential impact on innovation.

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.