Health IT Policy Committee

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

August 16, 2011

Farzad Mostashari, MD, ScM
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. Mostashari:

The HIT Policy Committee (Committee) gave the following broad charge to the Privacy & Security Tiger Team (Tiger Team):

> **Broad Charge for the Privacy & Security Tiger Team**:
> The Tiger Team is charged with making short-term and long-term recommendations to the Health Information Technology Policy Committee (HITPC) on privacy and security policies and practices that will help build public trust in health information technology and electronic HIE, and enable their appropriate use to improve healthcare quality and efficiency, particularly as related to ARRA and the Affordable Care Act (ACA) which mandates a number of duties to the ONC relative to privacy and security.

This letter provides recommendations to the Department of Health and Human Services (HHS) on the capability for patients to view and download information about their health care. On August 3, 2011, the Tiger Team reported on and discussed its findings with the Committee, which subsequently approved the recommendations as outlined below.

Introduction

On June 8, 2011, the Meaningful Use Workgroup presented their proposed measures for Stage 2 of Meaningful Use to the Health IT Policy Committee. Included in the proposed measures approved by the Policy Committee was the capability for patients to view and download information about their health care:

- **Eligible Hospitals**: 10% of patients/families view and have the ability to download information about a hospital admission; information available for all patients within 36 hours of the encounter.
- **Eligible Physicians:** 10% of patients/families view and have the ability to download their longitudinal health information; information available to all patients within 24 hours of an encounter (or 4 days after information available to EPs).

With incentives coming from Meaningful Use as well as interest from patients themselves, the opportunities to access and retrieve personal health information will inevitably increase. However, along with this new functionality comes an increased risk to patients regarding the safeguarding of this personal health information. The Privacy & Security Tiger Team was requested by the Meaningful Use Workgroup to consider whether there should be guidance about these risks to patients exercising this function. This request was formally endorsed by the Health IT Policy Committee.

Background and Discussion

In 2008, ONC developed the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*.[1] The principles in the Nationwide Framework have roots in the Fair Information Practices, or FIPs. Two of these principles are particularly relevant to this discussion about patients' ability to view and download:

1. **Individual Access:** Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.
2. **Openness and Transparency:** There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.

The Tiger Team made previous recommendations on openness and transparency that are useful to these discussions:

- Relevant core values:
  - Patients should not be surprised to learn what happens to their health information.
  - The provider-patient relationship is the foundation for trust in health information exchange
  - Transparency about information exchange practices is a necessary component of establishing credibility with patients.

- Relevant recommendations:
  - Providers are responsible for being open and transparent with their patients about how their data is exchanged
  - Providers should provide a layered notice

The Tiger Team reviewed a policy brief prepared by the Markle Foundation on issues associated with the download capability in EHRs. That policy brief recommended that guidance be provided to help individuals make informed choices, including:

- Provide a clear, concise explanation of the download function and its most fundamental implications for the individual.

[1] "The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information". Office of the National Coordinator, December 15, 2008. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173

- Provide prominent links that enable individuals to view more details about the download process, including what basic security precautions to take on their own, how the service answers questions, and who to contact if they believe some of the downloaded information is in error.
- Obtain independent confirmation that the individual wants to download a copy of personal health information after presenting, at minimum, the following information:
    - *Health records can contain sensitive information.*
    - *If you download sensitive information to a shared or unsecured computer or device, others might see it.*
    - *You are responsible for protecting the information that you download, and for deciding with whom to share it.*
    - *Are you sure you want to download a copy of your personal health information to the computer or device you are using?*
- Present the individual with a conspicuous means to cancel the download at every step up to the final confirmation step. It is good practice to include not only a "yes" and a "no" option, but also a "tell me more" option, which enables the individual to get a more detailed explanation.[2]

In addition, the Tiger Team explored examples where patients are provided capabilities to download their information, including My HealtheVet Blue Button and Medicare Blue Button. In both of these examples notice was provided to the patient regarding the safeguarding of personal health information similar to the principles outlined in the Markle Foundation policy brief.

Tiger Team Recommendation on View and Download

The Tiger Team considered whether to recommend that EHR certification requirements in Stage 2 specifically address guidance to patients using the view and download functionality. Although the Tiger Team understood the appeal of requiring EHR vendors to address this issue, the Tiger Team felt that providers would want flexibility with respect to the type of guidance provided to patients. Requiring a certification "standard" could result in over-specification or create inflexibility. Instead, the Tiger Team opted to offer best practice guidance for providers (as well as vendors and software developers) participating in the Meaningful Use program as stated below. Such best practice guidance could be communicated by ONC through the Regional Extension Centers (RECs) as well as through the entities certifying EHR Technology.

Best Practices:

- **Providers participating in the Meaningful Use program should offer patients clear and simple guidance regarding use of the view and download**

[2] The Markle Foundation, (2010). Policies in Practice 1: The Download Capability. Accessed on June 23, 2011, http://www.markle.org/sites/default/files/20100831_dlcapability.pdf

functionality in Stage 2.

- **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.**

  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.

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

- **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.**

We appreciate the opportunity to provide these recommendations on view and download capability, and look forward to discussing next steps.

Sincerely yours,

/s/

Paul Tang
Vice Chair, HIT Policy Committee