Health IT Policy Committee

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

December 14, 2011

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

Dear Dr. Mostashari:

The HIT Policy Committee (Committee), established by Congress in the Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of the American Recovery and Reinvestment Act of 2009 (ARRA), gave the following broad charge to its privacy and security policy working group (known as the Privacy & Security Tiger Team or "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 regarding a security policy framework for electronic health records (EHR). These recommendations were reported by the Tiger Team and approved by the Policy Committee on December 7, 2011.

Introduction

ONC, with the assistance of NIST, performed an analysis comparing the HIPAA Security Rule to other commonly used security frameworks. Security frameworks, which may be open standards or proprietary, are organized taxonomies of security controls, grouped into logically related families. Today's common frameworks rapidly evolved in the 1990s, based on earlier efforts. These frameworks include ISO 27001, the Federal Information Security Management Act (FISMA), COBIT (Control Objectives for Information and Related Technology), and others.

The ONC/NIST analysis involved mapping the requirements and addressable specifications in the HIPAA Security Rule to the security controls in the ISO 27001 and FISMA frameworks.

Recommendations

In the view of the ONC and NIST staff performing this analysis, there is some consistency in many of the controls specified in the HIPAA Security Rule and other commonly used security frameworks. However, significant gaps exist, and the Security Rule has not evolved in step with these other frameworks.

A detailed analysis of the specific gaps—and the development of recommendations to address specific security areas—is beyond the expertise of the Tiger Team and the Policy Committee. However, the Tiger Team believed the following high-level recommendations on security policy that were worth presenting to the Policy Committee.

1. Security policy for entities collecting, storing and sharing electronic health information (both HIPAA covered entities and business associates) needs to be responsive to innovation and changes in the marketplace.

2. Security policy needs to be flexible and scalable, given the difference in size and resources of entities covered by HHS rules and programs; at the same time, a solid baseline of security policies needs to be established and consistently implemented (e.g., there must be a floor of policies that apply to all). (The Tiger Team noted that this is currently the general approach of the HIPAA Security Rule.)

3. Providers need education and guidance on how to comply with security policy requirements.

    a. The Office for Civil Rights is required by HITECH to issue annual guidance on compliance with the HIPAA Security Rule, and since enactment of HITECH in 2009 they have issued guidance on how to complete a security risk analysis. This guidance is helpful for all entities covered by HIPAA (in particular those needing to do a risk assessment to qualify for Stage 1 of meaningful use). It can also serve as a good foundation for the development of more guidance on policy and countermeasures (business practices) for effectively managing identified risks.

    b. Guidance should provide specific examples of policies and measures providers can implement to counter identified risk.

    c. It is not clear how many providers know of the existence of this guidance. HHS needs to better educate providers about these resources (for example, through the RECs, professional societies and direct mail).

4. HHS also should have a consistent and dynamic process for updating security policies and the rapid dissemination of new rules and guidance to all affected. HHS should begin by evaluating the gap analysis performed by ONC and NIST in more detail. As part of

this process, HHS should continue to look to other frameworks in ensuring that the Security Rule keeps up with innovations in security protections.

The Policy Committee adopted these recommendations by consensus.

We appreciate the opportunity to provide these security recommendations and look forward to discussing next steps.

Sincerely yours,

/s/

Paul Tang

Vice Chair, HIT Policy Committee