Health IT Policy Committee

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

May 7, 2010

David Blumenthal, MD, MPP
Chair, HIT Policy Committee
U.S. Department of Health and Human Services
200 Independence Avenue, S.W., Room 746
Washington, D.C. 20201

Dear Dr. Blumenthal:

The HIT Policy Committee (Committee) has endorsed the following broad charge for the Privacy and Security Workgroup:

> **Broad Charge to the Workgroup**: To make short-term and long-term recommendations to the Committee 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. Specifically, the Workgroup will seek to address the complex privacy and security requirements through the development of proposed policies, governance models, solutions, and approaches that enhance privacy and security while also facilitating the appropriate collection, access, use, disclosure and exchange of health information to improve health outcomes.

This letter provides recommendations on the Department of Health and Human Services' (HHS) proposed rulemaking regarding the establishment of a permanent certification program for purposes of testing and certifying health information technology.

BACKGROUND AND DISCUSSION

The American Recovery and Reinvestment Act of 2009 (ARRA) established the HIT Policy Committee as a Federal Advisory Committee. The Committee is charged with recommending to the National Coordinator a policy framework for the development and adoption of a nationwide health information technology infrastructure that permits the electronic exchange and use of health information, consistent with the Federal Health IT Strategic Plan and that includes recommendations on other issues, including areas in which standards, implementation specifications, and certification criteria are needed.

On March 10, 2010, HHS proposed a rule regarding the establishment of two certification programs for purposes of testing and certifying health information technology. The recommendations below are directed to the permanent certification program, and

specifically the certification of EHR Modules for meeting the privacy and security certification criteria adopted by the Secretary.

RECOMMENDATIONS

Proposed 45 CFR 170.450 provides that with respect to EHR module testing and certification, EHR modules are required to be tested and certified to all privacy and security certification criteria adopted by the Secretary unless one of three exceptions applies. The Workgroup endorses a default rule that each EHR module must meet all privacy and security certification criteria *when the module is being used as intended.* However, the Workgroup does not believe the NPRM appropriately recognizes that the security functionality that any specific EHR module needs to provide will vary depending upon the environment in which it is intended to be used.

For all EHR modules potential purchasers will need clear information about their features and limitations. We recommend that each EHR module submitted for certification provide the following as part of certification:

1) A complete description of the environment within which the module is intended to operate (in other words, the assumptions about how the module will be used, what other interfaces are necessary, whether features are not functional under certain conditions, etc.);
2) Which of the privacy and security certification criteria are accomplished by the EHR module and which are not (again, when used as intended); and
3) If the product is designed to perform a specific privacy and security capability, a specification of the interface through which the security and/or privacy services will be provided to other EHR modules.

In addition, consistent with the recommendations of the Certification-Adoption Workgroup, we recommend that such products have a label containing this information. Such information will provide eligible providers and hospitals with information that will enable them to integrate the module with other EHR modules such that all privacy and security certification criteria can be met by the integrated set of modules, and the information needed to complete the annual risk assessment required by the HIPAA Security Rule.

With respect to the exceptions set forth in Section 170.450(c), the Workgroup agrees that two of the three exceptions –

> -Exception 2 (170.450(c)(2)), where the presenter for an EHR module can demonstrate that it would be technically infeasible for the module to be tested and certified to meet some or all of the criteria, and
>
> -Exception 3 (170.450(c)(3)), where the EHR module is designed to perform a specific privacy and security capability –

are circumstances where the certifying body could reasonably exempt an EHR module from having to meet one or more of the privacy and security certification criteria. With respect to exception 2, the Workgroup recommends that HHS provide specific examples of instances of technical infeasibility in order to be more clear to the public about the circumstances that would justify granting an exemption from the requirement to meet all privacy and security requirements.

However, the Workgroup recommends that HHS provide further clarification on the circumstances under which Exception 1 (170.450(c)(1)) would apply.[1] Exception 1 deals with EHR modules are presented as an "integrated" bundle, which would allow them to be certified similar to a Complete EHR. If a group of modules are tested for privacy and security as a bundle as if the bundle were a Complete EHR, we recommend that certification should only apply to the entire bundle and not to any of the individual module components. A label should be required which indicates that certification only applies to the bundle, and the label should list the component parts.

However, the proposed rule states that this exception does not apply to those EHR modules that are "integrated" but yet out of the end user's direct control. It's not clear to the Workgroup what HHS intends with this "exception to the exception" as currently worded. The Workgroup urges HHS to proceed with a more clear rule: If modules are not being presented for certification as an integrated "bundle," they should be required to be separately certified as EHR modules, addressing all privacy and security certification criteria unless exception (2) or (3) applies. If they are presented for certification as an integrated bundle similar to a Complete EHR, the certification should apply to the bundle per the above discussion. Labels indicating the form and scope of certification can help clarify this to prospective purchasers.

We thank you for the opportunity to submit these comments.

Sincerely yours,
/s/

Deven McGraw
Co-Chair
Privacy and Security Workgroup

Sincerely yours,
/s/

Rachel Block
Co-Chair
Privacy and Security Workgroup

[1] This recommendation regarding exception 1 (170.450(c)(1)) was previously submitted by the Policy Committee to ONC in response to the temporary certification program rule.