March 5, 2010

David Blumenthal, MD, MPP
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Dr. Blumenthal:

The HIT Policy Committee (HITPC) members identified and developed several recommendations on privacy and security issues. Specifically, the HITPC's Privacy & Security Workgroup (Workgroup) developed a number of recommendations for the Centers for Medicare & Medicaid (CMS) related to the privacy and security sections of the Notice of Proposed Rule Making (NPRM) on meaningful use (MU). The HITPC's Privacy & Security Workgroup also made recommendations to the Office of the National Coordinator for Health IT (ONC) that will enhance the ability of eligible professionals (EPs) and hospitals to meet the privacy and security MU criteria. The Workgroup also makes additional comments that are not specific to the NPRM, but instead signal the Workgroup's intent to focus on candidates for priorities for further standards development and Stage 2 MU and certification criteria.

We believe these recommendations, set forth below, will improve the public trust in Health Information Technology (HIT) and strengthen the goals of the CMS incentive program to increase the adoption and use of HIT and widespread health information exchange (HIE).

The Workgroup's recommendations were presented to the HIT Policy Committee at its meeting on February 17, 2010, and were approved. Two questions that were raised during the meeting were subsequently resolved by the Workgroup and are included in the recommendations below.

BROAD CHARGE FOR THE WORKGROUP

It is the charge of the Privacy & Security Workgroup to make 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. 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.

BACKGROUND AND DISCUSSION

Privacy and security are foundational to securing and maintaining trust in HIT and electronic information exchange. The MU criteria and certification standards are tools that can be leveraged to build this trust. Consequently, privacy and security provisions must be incorporated into each stage of HIT implementation to address risks associated with advancing levels of information sharing, access and use. Although this set of Workgroup recommendations focuses on the MU and certification criteria, the Workgroup also intends in the future to consider any necessary changes or "upgrades" to existing federal privacy and security rules.

HIT POLICY COMMITTEE RECOMMENDATIONS

I. Recommendations on the privacy and security sections of meaningful use (MU) Notice of Proposed Rule Making (NPRM)

A. Recommendations to Strengthen Existing MU Privacy and Security Criteria

The recommendations reference:

- **Stage 1 Objective**: Protect electronic health information created or maintained by the certified HER technology through the implementation of appropriate technical capabilities

- **Stage 1 Measure**: Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement security updates as necessary.

RECOMMENDATION 1: Make clear that for eligible professionals (EPs) and Hospitals who have never conducted a security assessment, the requirement is to conduct such an assessment (not review). The option to review risk analyses should only be for those entities that have recently conducted a security risk analysis and have not added new HIT capabilities.

RECOMMENDATION 2: Make clear in the final rule that MU criteria regarding uses of health information do not override existing state or federal law setting parameters around access, use and disclosure of health information.

RECOMMENDATION 3: Clarify what is meant by "implement security updates as necessary."

a. With respect to software updates, EPs and Hospitals should be required to have a written policy regarding how they will handle security updates from the vendor.

b. However, responding to these updates should not be enough – EPs and Hospitals should also address any deficiencies identified in the security risk assessment.

c. Response to security risk analysis should be required to include addressing how security capabilities in Certified EHR Technology will be utilized. This is consistent with current HIPAA security rule, which deems a number of implementation specifications to be "addressable."

RECOMMENDATION 4: Attestation for the privacy and security section of Stage 1 of MU should be two-fold: (1) the risk analysis was conducted or reviewed; and (2) the entity has mitigated risks identified (has a written policy regarding software updates and implemented updates per the policy; responded to deficiencies identified in the assessment; and, addressed how security capabilities in the Certified EHR Technology will be utilized).

RECOMMENDATION 5: Attestation should be reinforced through audit.

<u>B. Recommendations Related to MU Privacy and Security Criteria Originally Approved by the Policy Committee but not included in the NPRM</u>
<u>B. Recommendations Related to MU Privacy and Security Criteria Originally Approved by the HIT Policy Committee but not included in the NPRM</u>

RECOMMENDATION 6: Restore MU requirement to comply with HIPAA Privacy and Security Rules and set standards to establish when criteria have not been met.

6A. Restore MU requirement to comply with the HIPAA Privacy and Security Rules as a Stage 1 Objective.
To establish privacy and security as foundational to HIT and MU, the Workgroup believes compliance with the HIPAA Privacy and Security Rules should be the baseline standard for Stage 1 MU. Compliance with state privacy laws is also critical. However, states are in the best position to ensure compliance with state laws (and states have the option of asking CMS to allow them to add state law compliance as an additional Medicaid MU requirement).

6B. Establish that EPs and Hospitals have not met MU privacy and security objectives if they have been found liable (or guilty) and fined for a significant civil or criminal HIPAA violation.

1. This should apply only if a fine is levied or imposed – not at the complaint or investigation stage, or when an appeal is pending.
2. With respect to civil penalties, this should apply only in instances of willful neglect (top two penalty tiers) – not in cases of lack of knowledge or reasonable cause. Willful neglect means "conscious, intentional failure or reckless indifference to the obligation to comply with the …provision violated."
3. With respect to a criminal HIPAA investigation, applies only in the event of a criminal fine imposed against the entity in the case of a Hospital or other eligible entity (not one individual working in an enterprise).

4. Should apply in the year in which the violation occurred. If appeals process is not resolved until years later, and payment has already been made, should be subject to overpayment recoupment if fine is upheld.

In summary, the Workgroup believes that EPs and Hospitals fined for significant HIPAA violations should not be eligible for meaningful use payments.

An HIT Policy Committee member raised the issue of how violations spanning multiple years should be resolved; in subsequent deliberations, the Workgroup recommends that EPs and Hospitals be ineligible for MU in any year in which a willful neglect or criminal violation occurred and the EP or Hospital was required to pay a fine. Consequently, violations that took place over multiple years could render an EP or Hospital ineligible for MU payments in more than one payment year.

A question was also raised regarding whether the disqualification for MU payments would provide an additional incentive for EPs and Hospitals to pay a monetary settlement to avoid being found in significant violation of HIPAA and fined (and thus disqualified for a MU payment). The Workgroup feels that the mere fact of being fined for willfully neglecting HIPAA is likely sufficient motivation on its own for entities to settle these violations, and the addition of MU disqualification just adds one more factor.

II. Recommendations to ONC to Enhance Ability of EPs and Hospitals to Meet MU Privacy and Security Criteria

RECOMMENDATION 7: Guidance should be provided to EPs and hospitals on how to conduct an appropriate security assessment.

a. Guidance on HIPAA security audits issued by the HHS Office of Civil Rights (OCR) would be of most help in focusing entities on critical issues.
b. Materials from CMS, ONC, OCR, NIST should be made available through multiple channels, including state HIEs, Medicaid offices, CMS regional offices, regional extension centers, and others.
c. Such guidance should address environmental factors as well as risks inherent in technology.
d. Risk assessment guidance/materials should also include criteria that should trigger a security risk review.
e. Guidance should address risk-mitigation strategies tied to the security features required for Certified EHR Technology.

The Workgroup notes that per current HIPAA rules, EPs and Hospitals can – but are not required to-- use outside entities to conduct security risk assessments.

As Certified EHR Technology becomes more widely deployed, OCR should consider upgrading HIPAA security rule implementation specifications that today are "addressable" using certification standards to be "required" for EPs and Hospitals using Certified EHR Technology.

III. Additional Concerns re: IFR & Future Policy & Standards Priorities

COMMENT 1: Security standards and certification criteria are a good starter set – but Privacy & Security Workgroup members expressed some concern about standards/capabilities not included for 2011.

a. For example, a standard or functionality to verify that a person or entity seeking access to data has the patient's consent/authorization where it is required by current law or policy.

b. How will entities comply with different consent requirements or new ARRA requirements not to disclose protected health information (PHI) to health plans in certain circumstances (data segmentation is often mentioned as one potential tool for EHRs to implement this).

COMMENT 2: The Privacy & Security Workgroup will be doing further work on identifying privacy and security policy priorities for which standards or technical capabilities are needed. The hope is that these priorities can be addressed by the Standards Privacy & Security Workgroup – and the Standards Committee – in 2010, so that new certification criteria and standards can be incorporated into the EHR Technology certification program as soon as possible.

COMMENT 3: We also note that the NHIN Workgroup will be drilling down in more detail on privacy and security policy issues such as authentication and identity across a network, and a trust framework. We look forward to working closely with the NHIN Workgroup to come up with recommendations that establish a strong and accountable trust framework for the secure exchange of data across networks. Similarly ONC, through its state HIE grant program, should advance consistent interpretation and implementation of additional privacy and security requirements.

Sincerely yours,

Deven McGraw,
/Deven McGraw/
Co-Chair, HITPC Privacy and Security Workgroup

Sincerely yours,

Rachel Block,
/Rachel Block/
Co-Chair, HITPC Privacy and Security Workgroup