

DRAFT

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.

Introduction

As part of our ongoing deliberations, we compared previous recommendations on privacy and security made by the Health IT Policy Committee (HITPC) for inclusion in Stage 2 of the meaningful use (MU) incentive program to what was included in two Notices of Proposed Rule Making (NPRM) – one on the Stage 2 meaningful use criteria proposed by the Centers for Medicare and Medicaid Services (CMS) and one on the new EHR technology certification requirements proposed by the Office of the National Coordinator for Health Information Technology (ONC). In its NPRM, CMS proposed specific criteria which Eligible Professionals (EPs), eligible hospitals (EHs), and Critical Access Hospital (CAHs) (collectively, “providers”) must meet in order to qualify for a meaningful use (MU) incentive payment.¹ In its NPRM, ONC proposed certification criteria, which would establish the technical capabilities and specify the related standards and implementation specifications that Certified Electronic Health Record (EHR) Technology would need to include to, at a minimum, support the achievement of MU by providers under the Medicare and Medicaid EHR Incentive Programs.²

Based on our discussion of these two NPRMs, we are providing the following comments for consideration by the HITPC.

¹ The Department of Health and Human Services notices of proposed rulemaking (NPRMs) related to Stage 2 Meaningful Use: Medicare and Medicaid Programs; Electronic Health Record Incentive Program available at 77 FR 13698: <https://www.federalregister.gov/articles/2012/03/07/2012-04443/electronic-health-record-incentive-program--stage-2-medicare-and-medicaid-programs>.

² The Department of Health and Human Services notices of proposed rulemaking (NPRMs) related to Stage 2 Meaningful Use: Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology available at 77 FR 13832: <https://www.federalregister.gov/articles/2012/03/07/2012-04430/electronic-health-record-technology-2014-edition-health-information-technology-implementation>.

DRAFT

Comments

We are pleased that the NPRMs address many of the Committee's previous privacy and security recommendations. Specifically:

1. **With respect to the proposed Stage 2 meaningful use objectives, CMS proposes to require providers to perform a security risk assessment (the same criterion currently included for Stage 1). CMS also proposes to require providers to specifically attest to addressing encryption of data at rest in Stage 2.** Both of these criteria are the two objectives required for privacy and security as part of meaningful use criteria. These criteria were both recommended by the Health IT Policy Committee. Addressing security of data at rest requires assessments of at least three situations: (a) data on portable devices or media; (b) data on devices in public areas or locales with poor physical security and data on servers in locales that are physically and electronically protected well. Addressing encryption of data at rest may result in different solutions in these locales. In particular, the requirement to attest to addressing the issue of encryption of data at rest is critical in protecting against data breaches involving portable media.
2. With respect to new proposed certification criteria, **ONC proposes that Certified EHR Technology have the capability to make amendments to a patient's health data and be able to append information from the patient and any rebuttal from the entity regarding the data.** These criteria will help support providers' compliance with the HIPAA Privacy Rule.
3. **ONC also proposes that Certified EHR Technology include a patient accessible log to track the use of the view, download, and transmit capabilities for Stage 2 MU Certified EHR Technology certification.**

The adoption of these Policy Committee recommendations provides some of the policies, technical capabilities and controls necessary for ensuring the privacy and security of patient health information, and **we urge both CMS and ONC to retain them in the final rule.**

The following comments address previous Policy Committee recommendations that were not adopted in the NPRMs.

EHR Modules

Providers need to have sufficient technical capabilities to protect patient data. In Stage 1, ONC requires Certified EHR Technology to include basic security functionalities. Such certification is required of Complete EHRs and EHR modules, although modules may be exempted from the criteria if (1) they are testified for certification with other modules (as a bundle) and one of the other modules provides the required security capabilities or (2) the module can demonstrate that a security criterion is inapplicable or would be technically infeasible to meet.

DRAFT

In the proposed Stage 2 rule, ONC proposes to exempt EHR modules from being required to meet the security criteria. However, in the proposed rule ONC also introduces a new concept of a Base EHR, which provides core functionalities needed to meet meaningful use. Providers seeking meaningful use incentives must have a Base EHR that meets all of the security criteria. According to ONC's proposed rule, "a Base EHR can be satisfied through a Complete EHR, through a single EHR module, or a combination of modules." **The Tiger Team agrees that a Base EHR should demonstrate the required security functionalities.**

The Tiger Team wants vendors of EHR modules to be able to succeed in the marketplace. However, a number of Tiger Team members are concerned that exempting all EHR modules from the requirement to be certified to all of the basic security criteria will potentially leave providers without basic technical capabilities to deploy security safeguards for protected health information (PHI) in a module. In addition, because the concept of the Base EHR is new, it is unclear whether requiring certification of security capabilities for Base EHRs will provide sufficient security capabilities for PHI in Certified EHR Technology.

A number of members of the Tiger Team sought to endorse the recommendation put forth by the Health IT Standards Privacy and Security Workgroup, which would require EHR modules to either implement the required security functionality within the Complete EHR or EHR Module(s) submitted for certification; or assign the function to a third-party component or service, and demonstrate how the certified EHR product, integrated with its third-party components and services, meets the criterion. However, others expressed concern that such an approach would result in the certification program becoming a test for implementation or overall EHR architecture, which it was not intended to be. **The Tiger Team did not have sufficient time to reach consensus on this issue.**

Patient Portals (View, Download, Transmit)

The HITPC previously recommended that providers should require at least single factor authentication for patients using view, download, and transmit functionalities. We recognize that the HIPAA Security Rule already addresses technical safeguards requiring person or entity authentication, and requires covered entities to verify that a person or organizations seeking access to PHI is the one claimed. However, we noted that there is some inconsistency in how authentication is described in ONC's NPRM, which may be misleading to providers. For example, the proposed rule states that Certified EHR Technology must authenticate users for secure messaging; however, there is no comparable authentication requirement for patient access to view, download, and transmit. **To ensure that providers understand the need to authenticate patients, we recommend that ONC clarify in the NPRM preamble that the term "user" includes patients using the view, download, and transmit capabilities.**

The HITPC also recommended that EHRs be certified to ensure information can be securely downloaded from patient portals, either to the patient or to a third party at the patient's request. This recommendation was not adopted in ONC's NPRM.

DRAFT

Because the HIPAA Security Rule does require physical, technical and administrative safeguards for portals, it is important for providers to understand how these providers can meet these legal obligations with respect to the portals. **We recommend that the HHS Office for Civil Rights, which oversees and enforces the HIPAA Security Rule, provide guidance to providers on application of the Security Rule to the portal. We also recommend that ONC provide technical guidance to providers who will be purchasing Certified EHR Technology that will include this functionality.**

The HITPC also recommended that certification of portal functionalities include requirements for data provenance. **We note that the NPRM states that the adoption of the Consolidated CDA addresses the need for data provenance, which is accessible to the user, as recommended by the Committee. However, we are concerned that the rule might not be sufficiently clear that data provenance information is to be visible to the patient. Thus, we agree with this approach, provided that ONC include in the final rule clarification that the data provenance information must be visible to the patient in human-readable form.**

While briefly mentioned in CMS's NPRM for Stage 2 MU, we also want to underscore the Committee's previous recommendations with respect to providing guidance (as opposed to certification criterion) for providers, vendors, and software developments on being transparent with patients about the potential risks associated with patient portals when using the view, download and transmit capabilities. **We encourage ONC to more formally endorse these best practices and to provide clear guidance to providers.** As patient portals are expected to be in more robust use by 2014, **we strongly encourage ONC to develop and implement a dissemination strategy for this guidance**, such as through the Regional Extension Centers.

Amendments

ONC also specifically requested comment on whether Certified EHR Technology should be required to be capable of appending patient supplied information in both free text and scanned format or only one or these methods to be certified to this proposed certification criteria. **We agree that both formats should be required. We note that public comments provided for the April 9th Tiger Team meeting suggested that these requirements be broadened to include patient-supplied images.**

We also recommend that ONC signal to vendors that by Stage 3 MU, Certified EHR Technology demonstrate capability to transmit amendments and appended information to other providers. This capability is important to providers when they determine that another provider should receive the amended and appended information, or when the provider has a legal obligation to transmit such information.

Digital Certificates

The Tiger Team assumes that the transport standards proposed in ONC's NPRM address the validation aspects of the entity-level authentication recommendations previously

DRAFT

issued by the HITPC.³ **With respect to the HITPC’s previous recommendation that entity-level authentication credentials be issued with a high degree of assurance, the Tiger Team urges ONC to address level of assurance in the governance rule for the Nationwide Health Information Network (NwHIN).**

Patient Matching

In response to specific questions posed by ONC in its NPRM, the Tiger Team concludes that EHR technology is not sufficiently mature to do “automatic” matching of patient data. **However, the Tiger Team continues to recommend that EHRs be tested and certified for (1) the capability to correctly populate standardized demographic data fields for outgoing patient data and (2) the capability to make incoming patient demographic data readable and available to assist recipients in matching this data to the correct patient record.** As a best practice, entities participating in the meaningful use program should be encouraged to use U.S.P.S. normalization as a mechanism for validating addresses. **ONC should include this best practice in the preamble to the final rule.**

As a final note, although automated patient matching capability is largely not present in EHR technology today, some software vendors have developed (or are developing) the technical capability. ONC should monitor technology developments in this area and consider potentially requiring such capability by the last stage of the HITECH incentive program.

³ The Department of Health and Human Services notices of proposed rulemaking (NPRMs) related to Stage 2 Meaningful Use: Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology available at 77 FR 13832: <https://www.federalregister.gov/articles/2012/03/07/2012-04430/electronic-health-record-technology-2014-edition-health-information-technology-implementation>.

Transport Standards. a) Directed exchange.

- (1) Standard. Applicability Statement for Secure Health Transport (incorporated by reference in § 170.299).
- (2) Standard. External Data Representation and Cross-Enterprise Document Media Interchange for Direct Messaging (incorporated by reference in § 170.299).
- (3) Standard. Simple Object Access Protocol (SOAP)-Based Secure Transport Requirements Traceability Matrix (RTM) version 1.0 (incorporated by reference in § 170.299).

These transport standards include the two transport specifications developed under the Direct Project: (1) Applicability Statement for Secure Health Transport and (2) External Data Representation (XDR) and Cross-Enterprise Document Media Interchange (XDM) for Direct Messaging. The Applicability Statement for Secure Health Transport specification describes how electronic health information can be securely transported using simple mail transport protocol (SMTP), Secure/ Multipurpose Internet Mail Extensions (S/MIME), and X.509 certificates. The XDR and XDM for Direct Messaging specification describes the use of XDR and XDM as a means to transport electronic health information and serve as a bridge between entities using/ following Web services and SMTP transport methods.