Privacy and Security Considerations for EHR Incentives and Meaningful Use

Stephen Gantz, CGEIT, CEH, CIPP/G, CISSP-ISSAP, is a health IT strategist and security and privacy analyst for the Health Solutions division of Vangent, a leading global provider of information management and business process outsourcing services. He has 20 years' experience in technology-related professional services and software development, specializing in enterprise and security architecture, information privacy, strategic planning, IT governance, and risk management. Gantz is also an associate professor in information assurance at the University of Maryland University College (USA).

To encourage adoption of electronic health record (EHR) technology, the Health Information Technology for Economic and Clinical Health (HITECH) Act portion of the US American Recovery and Reinvestment Act (ARRA) of 2009 includes financial incentives for health care providers and professionals who can demonstrate "meaningful use" of electronic health records. While meaningful use measures cover a wide range of functional and technical capabilities, there is only one measure related to security and privacy: Organizations implementing EHR technology must "conduct or review a security risk analysis…and implement security updates as necessary," something they are already required to do under the US Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The fact that this measure is already an obligation under HIPAA should make it easy to satisfy, but many health care organizations are not prepared to comply.

There are no specific privacy measures in the proposed rules on meaningful use, nor are there privacy certification criteria or standards required for EHR technology. The health care providers and professionals eligible for the incentive funding are typically HIPAA-covered entities, so there is an assumption that obligations of these entities under the HIPAA Privacy Rule serve to make a separate meaningful use privacy requirement redundant. Privacy advocates, however, find the absence of explicit privacy requirements problematic, particularly the lack of criteria to ensure that individual patients can control the use or disclosure of information in their EHRs.

This article focuses on the privacy and security aspects of the measures, EHR certification criteria, and standards included in meaningful use, and it addresses expectations and compliance drivers that face health care providers and professionals who seek government funding through the EHR incentive program.

MEANINGFUL USE INCENTIVES

ARRA[1] emphasizes expanding the use of health information technology, particularly in terms of storing and managing medical records in electronic form. The Act includes significant funding to provide incentive payments to health care providers to adopt EHR technology; these incentives require eligible providers not just to acquire and install systems, but also to demonstrate "meaningful use" of electronic health records.[2] The criteria needed to show meaningful use were defined in a notice of proposed rulemaking (NPRM)[3] published in the *Federal Register* in January 2010, along with an interim final rule detailing standards, specifications and certification criteria for EHR systems.[4] A 60-day comment period on the proposed rules ended 15 March 2010. The meaningful use criteria were finalized in July 2010 as the mechanism to implement the incentive payment provisions in the HITECH Act portion of ARRA.[5] (Comment period notwithstanding, the interim final rule became effective on 12 February 2010, although the standards and certification criteria were updated in the final version of the rule published on 28 July 2010.) The rules are organized according to five policy priorities specified by the Health IT Policy Committee, an advisory body created by a provision in ARRA.[6] These priorities are:[7]

1. Improving quality, safety, efficiency and reducing health disparities
2. Engaging patients and families in their health care
3. Improving care coordination
4. Improving population and public health
5. Ensuring adequate privacy and security protections for personal health information

Meaningful use measures and EHR certification criteria will be implemented in a three-stage process, with certain measures and criteria taking effect in 2011, 2013 and 2015. Each stage has a set of meaningful use objectives associated with the policy priorities, with one or more certification criteria corresponding to each objective. After initial review of the proposed meaningful use measures, the Health IT Policy Committee recommended that the total number of measures for 2011 be reduced and that eligible hospitals and professionals be allowed to defer some of the criteria, rather than follow the "all or nothing" approach in the proposed rule.[8]

PRIVACY AND SECURITY EXPECTATIONS

The objectives associated with the privacy and security priority identified in the NPRM[9] are:

- Ensure privacy and security protections for confidential information through operating policies, procedures and technologies, and compliance with applicable law
- Provide transparency of data sharing to patient
- Protect electronic health information created or maintained by the certified EHR technology through the

Figure 1—EHR Certification Criteria Related to Security

Function	Criteria	Comments
Access control	Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.	No specific requirements for identification and authentication are associated with meaningful use, but many dependencies exist for requirements within these rules and are incorporated by reference from HIPAA or other legislation.
Emergency access	Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.	This "break glass" provision is intended to give an exception to consent requirements, although support for consumer preferences tracking and adherence is not explicitly required for meaningful use.
Automatic log off	Terminate an electronic session after a predetermined time of inactivity.	Automatic log off is a HIPAA Security Rule technical safeguard specified as part of the access control standard.
Audit log	Record actions related to electronic health information in accordance with the standard specified, and enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard.	The standard in question specifies the minimum information that must be logged, rather than any technical, format or process requirement.
Integrity	Create a message digest, in accordance with the standard specified. Verify, in accordance with the standard specified, that upon receipt of electronically exchanged health information, such information has not been altered. Detect the alteration of audit logs.	The referenced standard specifies the use of the SHA-1 or higher hash algorithm, corresponding to the five Secure Hash Algorithm (SHA) hash variants specified in the federal Secure Hash Standard (FIPS 180-3).
Authentication	Verify that the person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.	No specific requirements for identification and authentication are associated with meaningful use, and the referenced standard addresses the sufficiency of identity information in an electronic transmission subject to authentication and authorization, rather than any specific practice or protocol.
Encryption: General	Encrypt and decrypt electronic health information, in accordance with the standard specified, unless the secretary determines that the use of such algorithm would pose a significant security risk to certified EHR technology.	It requires a symmetric 128-bit fixed-block cipher algorithm with a 128-bit or greater encryption key.
When Exchanging Electronic Health Information	Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified.	It requires an encrypted link; usually interpreted to mean TLS consistent with NIST Special Publication 800-52, although a specific technology is not specified.
Accounting of disclosures (optional criterion)	Record disclosures made for treatment, payment and health care operations in accordance with the standard specified.	Similar to the audit log function, the standard specifies the minimum information to be recorded about any health record information disclosure.

Source: 45 CFR §170.302(o)-(v)

Figure 2—EHR Certification Criteria Adopted Security and Privacy Standards

Purpose	Adopted Standard
General encryption and decryption of electronic health information	Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2
Encryption and decryption of electronic health information for exchange	Any encrypted and integrity-protected link
Recording of actions related to electronic health information (i.e., audit log)	The date, time, patient identification and user identification must be recorded when electronic health information is created, modified, accessed or deleted, and an indication of which action(s) occurred and by whom must also be recorded.
Verification that electronic health information has not been altered in transit	A hashing algorithm with a security strength equal to or greater than SHA-1 (as specified by NIST in FIPS Publication [October 2008]) must be used to verify that electronic health information has not been altered.
Recording of treatment, payment and health care operations disclosures	The date, time, patient identification, user identification and a description of the disclosure must be recorded for disclosures of treatment, payment and health care operations, as these terms are defined in 45 CFR §164.501.
Source: 45 CFR §170.210(a)-(d)	

implementation of appropriate technical capabilities. These capabilities correspond to certification criteria for EHR technology[10] and are summarized in **figure 1**.

The Health IT Policy Committee recommended additional objectives that specified the need for health care providers to comply with the HIPAA Privacy and Security Rules, and with the data-sharing practices contained in the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*,[11] released by the Office of the National Coordinator (ONC) in December 2008. No specific meaningful use measures are associated with this compliance, in part because covered entities are already obligated to comply whether or not they seek EHR incentives. There is just one proposed privacy and security measure for meaningful use: "Conduct or review a security risk analysis per 45 CFR §164.308(a)(1) of the certified ERH technology, and implement security updates and correct identified security deficiencies as part of its risk management process." The federal code cited is part of the statutory requirements in HIPAA (1996); the requirement for HIPAA-covered entities to conduct regular risk analyses is one of the administrative safeguards addressed in the HIPAA Security Rule.[12] The reference to HIPAA is intentional—by aligning certification criteria to existing HIPAA requirements, the intent is to try to help the eligible professionals and hospitals that are the focus of the meaningful use rules improve their privacy and security practices in general. The certification criteria extend HIPAA requirements with the declaration of specific technical standards and, in some cases, explicit capabilities corresponding to the more general security controls articulated in the law.

For HIPAA-covered entities seeking to qualify for health IT incentives, the fact that the privacy and security measure is already an obligation under HIPAA should, in theory, make this particular measure easy to satisfy—even more so because the requirement under meaningful use applies only to certified EHR technology used by the entities. The HIPAA Security Rule has been in force since April 2003, and the deadline for entities to comply fully with the rule elapsed in April 2006. Despite this requirement, however, not all health care organizations comply; the results of a 2009 security survey[13] of 196 senior-level health care professionals conducted by the Healthcare Information Management and Systems Society (HIMSS) found that only 74 percent of these organizations actually perform risk analyses and, of those, just over half (55 percent) do so with at least annual frequency. This suggests that as many as 40 percent of health care organizations do not conduct risk analyses on a regular basis (and perhaps a quarter do not conduct them at all), and further suggests that similar proportions of health care organizations do not appear prepared to satisfy the single privacy and security measure for meaningful use.

In addition to the security standards adopted in the interim final rule, some of the detailed certification criteria for electronic health record systems are security requirements. These criteria will be codified at 45 CFR §170.32 and will become the basis for conformance testing and an input to determinations to certify EHR modules and systems. The idea with the certification criteria is that an approved testing provider would evaluate the EHR systems and report the results of those tests to one or more approved certifying bodies. HITECH delegates the responsibility for certifying health information technology, including EHR systems, to the National Institute for Standards and Technology (NIST), which is also responsible for testing standards and implementation specifications adopted by ONC.[14] Of the 22 general certification criteria enumerated, eight correspond to security requirements and most reference one or more of the adopted standards shown in **figure 2**. What becomes apparent is that any entity tasked with assessing conformance to these criteria will need to make a subjective determination, as some of the "standards" listed are nothing more than functional characteristics. Considerations related to the security-related certification criteria are summarized in **figure 1**.

PRIVACY AND MEANINGFUL USE

Despite the inclusion of the word "privacy" in the fifth health outcomes policy priority listed in the meaningful use NPRM, as the measures and certification criteria currently stand, there are no specific privacy requirements that demonstrate meaningful use. However, the health care providers, professionals and organizations that are eligible to seek incentive funding and to which the meaningful use determination applies are, without exception, HIPAA-covered entities; therefore, there is an assumption that the obligations of these entities under the HIPAA Privacy Rule make a separate meaningful use privacy requirement redundant.

The Privacy and Security Policy Workgroup of the Health IT Policy Committee has proposed that an explicit requirement should be added obligating eligible entities to demonstrate compliance with HIPAA Security and Privacy Rules as a stage 1 objective for 2011.[15] The rationale behind this recommendation is less about strengthening privacy provisions in the rules and more about making sure an entity cannot be considered to have met meaningful use requirements if it has been found liable or fined for a HIPAA violation. A somewhat broader recommendation is noted in the NPRM[16] to include language requiring compliance with both the HIPAA Privacy and Security Rules and the fair data-sharing practices in the Nationwide Privacy and Security Framework. However, the US Department of Health and Human Services (HHS) determined that meaningful use is not the appropriate regulatory tool to ensure such compliance, choosing to omit compliance as a formal requirement as requested by the Health IT Policy Committee, while acknowledging that the use of certified EHR technology should support compliance.

At the end of the day, at least for 2011, this means the meaningful use rules will not impose any additional privacy requirements on HIPAA-covered entities or business associates, beyond what is already required under HIPAA as strengthened by the HITECH Act. However, organizations that are not fully compliant with those requirements may put themselves at risk of being found ineligible for EHR incentives, particularly if they have been the subject of any complaints or claims of violations.

Notably absent from meaningful use rules—as stressed by privacy advocates such as the Coalition for Patient Privacy[17]—are criteria to ensure that individuals (patients) can control the use or disclosure of the information in their electronic health records. Closely related to this is the ability for EHR systems and the providers that use them to capture, manage and respect consumer preferences about information disclosure, but this functionality is also not among the criteria published in the interim final rule. Statutory language already exists[18] that specifies practices for health record information disclosure with consent and prohibits redisclosure absent of such consent, but these rules apply only to records that concern alcohol and drug abuse, not health care in general. ONC has been working on consumer preferences since at least 2008, when they were identified as gap-in-use cases prioritized for development by the American Health Information Community (AHIC), and it has produced a *Consumer Preferences Draft Requirements Document*[19] that is likely to serve as a key input should ONC move to add consumer preferences criteria to any of the meaningful use stages.

IMPACTS AND IMPLICATIONS

For EHR technology vendors, the implication of the certification criteria contained in the interim final rule is quite clear. Their products will need to include the functional and technical capabilities associated with meaningful use if they hope to leverage the EHR incentive program as a selling point. These vendors should already be in the process of either preparing to validate and demonstrate that their products already have the capabilities in question or of prioritizing the addition of these capabilities into their product development road maps. This is true irrespective of the specific organization or authorities given the task of certifying products. The responsibility for testing products for certification and for officially approving those products once they are certified will be divided, with NIST overseeing the testing and certification process (including determining testing standards) and ONC delegating product approval to organizations such as the Certification Commission for Health Information Technology (CCHIT) or other third parties. In an NPRM published in March 2010,[20] ONC indicated its intention to roll out the certification program in two phases, beginning with a temporary program during which ONC would both approve third parties to perform testing and certification of EHR systems and modules, and perform some of the responsibilities associated with testing and certification until such time that a sufficient number of third-party certification bodies have been authorized. Under the permanent certification program as envisioned by ONC, qualified certification bodies would be authorized by ONC, while the accreditation of EHR testing labs would be handled by NIST through its National Voluntary Laboratory Accreditation Program. The permanent program, as proposed, would therefore separate the functions of testing EHR systems and modules from the process of certifying those products, with the idea that authorized certification bodies would rely on results from accredited testing labs in making certification decisions.

For health care providers or organizations interested in qualifying for EHR incentives to acquire, implement and adopt EHR systems and related health information technologies, the meaningful use criteria will likely have both external and internal impacts. The externally facing implications are the constraints that the EHR certification criteria and technical standards will put on health IT solutions, particularly including technology acquisition steps such as vendor evaluation and product selection, but also in terms of environment configuration, technical architecture and systems integration. From an internal organizational perspective, it is imperative for health care providers to ensure that their information security and privacy practices include regular risk analyses. It is understandable that many organizations may place an emphasis on conducting and documenting a risk analysis to satisfy the meaningful use measure, but this type of activity should not be considered a onetime event, especially in light of the fact that there will be stronger and additional criteria applied in future years.

Although the meaningful use standards do not come into effect until late 2011, health care providers and other HIPAA-covered entities and business associates who expect to participate in the movement toward electronic health records have several incentives to act now to take appropriate steps to demonstrate compliance with meaningful use requirements. First among these are the financial incentives tied to meaningful use—qualification factors that will be added and strengthened in two additional phases in 2013 and 2015. The subsequent eligibility criteria are intended to be additive, so organizations that fall behind or are unable to demonstrate meaningful use against the first phase criteria for 2011 may find themselves in an ongoing struggle to catch up as new and more robust requirements come into effect. Second, many of the requirements and obligations in the HIPAA privacy and security rules were made tougher under the provisions of the HITECH Act, and those provisions generally apply directly to business associates just as they do to covered entities. These stricter rules are already in effect, but the HHS Office of Civil Rights (OCR) has suggested that the requirements will not yet be enforced[21]—as much or more due to OCR's lack of readiness to begin enforcement and still-pending audit standards to be applied, than to covered entities' or business associates' lack of readiness to comply. OCR personnel have stated publicly[22] that health care organizations should be prepared for stronger enforcement measures, including proactive security and privacy audits, and the OCR hopes to begin conducting those audits by the end of 2010. This gives organizations a temporary opportunity to close any gaps in their conformance before they will be formally held accountable. Third, many of the privacy and security practices that health care organizations should be following under HIPAA and HITECH to demonstrate meaningful use of EHR technology are the same as those needed to comply with nonhealth-specific legal requirements, such as those in the new Standards for the Protection of Personal Information,[23] which went into effect on 1 March 2010 in Massachusetts, USA. Even for organizations without Massachusetts residents among their patients or customers, the requirements in the law are likely to be replicated in other state-level laws, raising the probability that an organization will find itself subject to such a law, even if no federal legislation is enacted.

For organizations that do not already routinely conduct risk analyses, or that do so but are concerned that their processes may not be sufficiently robust to be satisfactory under meaningful use, the Health IT Policy Committee is considering recommendations from its own Privacy and Security Policy Workgroup and multiple outside reviewers that health care professionals and hospitals be given explicit guidance on performing risk analyses. The HHS OCR, which has responsibility for enforcing the provisions of both the HIPAA Security Rule and Privacy Rule, published draft guidance on risk analysis[24] that generally directs covered entities to follow relevant NIST documentation related to complying with the HIPAA Security Rule in which the required risk analysis is codified. Both the NIST Special Publication 800-66[25] and CMS' Security Rule Education Paper Series[26] direct organizations to a standard security risk assessment process, documented in detail in NIST Special Publication 800-30.[27] For those preferring to seek guidance outside US federal standards, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)'s ISO/IEC 27000 series of international standards covers risk assessment and risk management for information systems, particularly in ISO/IEC 27005[28] and the risk assessment section of ISO/IEC 27002.[29] Those seeking to follow any of this guidance on risk management or on performing risk analysis should be aware that substantially all of the guidance is written in a way that focuses on risk assessments of individual information systems, not on organizations overall. This limitation is important because the risk analysis requirement under the HIPAA Security Rule is not limited to systems used by covered entities, so it is reasonable to assume that despite the emphasis of the meaningful use rules on EHR systems, the scope for a risk analysis conducted to satisfy the meaningful use measure should address all potential risks to health information. Organizations looking for more enterprise-level perspectives on assessing and managing risk can find relevant guidance in ISO 31000,[30] within major IT governance frameworks such as ISACA's Risk IT: Based on COBIT®[31] or the risk management section of the Information Technology Infrastructure Library (ITIL®).[32]

Looking at risk analysis from a privacy perspective, organizations have few options in terms of official guidance for privacy risk assessments or even for auditing compliance with the HIPAA Privacy Rule. While not health-specific, the American Institute of Certified Public Accountants (AICPA) developed and maintains the Generally Accepted Privacy Principles (GAPP), most recently updated in April 2009, which addresses risk assessment among many other criteria.[33] AICPA also produced a spreadsheet-based Privacy Risk Assessment Tool that addresses 66 criteria across the 10 principles in the GAPP.

CONCLUSION

While some health care organizations may respond with a sense of relief that the meaningful use rules do not contain more specific requirements about security and, especially, privacy, it seems highly unlikely that this will remain the case for future stages in 2013 and 2015. These organizations should instead look to the absence of new requirements as an opportunity to either validate existing security and privacy protections and practices, or to establish or augment appropriate security controls and privacy practices before organizations become subject to audit or are otherwise held accountable for privacy practices.

ENDNOTES

[1] US Congress, American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, USA, 17 February 2009

[2] *Ibid*. Pub. L. No. 111-5 §4101

[3] Department of Health and Human Services (HHS), Electronic Health Record Incentive Program Proposed Rule, 75 Fed. Reg. 1858, USA, 13 January 2010

[4] Department of Health and Human Services, Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology Interim Final Rule, 75 Fed. Reg. 2028, USA, 13 January 2010

[5] US Congress, Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the ARRA, Pub. L. No. 111-5, USA, 17 February 2009

[6] *Op cit*, ARRA, Pub. L. No. 111-5 §3002

[7] *Op cit*, HHS, 75 Fed. Reg. 1854-1858

[8] NPRM Recommendations, presented at the 17 February 2010 meeting of the Health IT Policy Committee

[9] *Op cit*, HHS, 75 Fed. Reg. 1858

[10] *Op cit*, HHS, 75 Fed. Reg. 2028

[11] Office of the National Coordinator (ONC) for Health IT, *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*" 15 December 2008

[12] 45 CFR §164.308(a)(1)(ii)(A)

[13] 2009 HIMSS Security Survey Final Report, 3 November 2009

[14] *Op cit*, ARRA, Pub. L. No. 111-5 §13201

[15] Comments and recommendations presented at the 19 February 2010 meeting of the Privacy and Security Policy Workgroup

[16] Electronic Health Record Incentive Program Proposed Rule, 75 Fed. Reg. 1858, 13 January 2010

[17] Coalition for Patient Privacy, Comments on meaningful use submitted to the Health IT Policy Committee, 26 June 2009, *http://patientprivacyrights.org/media/L-Coalition_to_HIT_PC_Meaningful_Use.pdf*

[18] 42 CFR Part 2, Subpart C

[19] ONC for Health IT, *Consumer Preferences Draft Requirements Document*, 5 October 2009

[20] Department of Health and Human Services (HHS), Proposed Establishment of Certification Programs for Health Information Technology Proposed Rule, 75 Fed. Reg. 11328, USA, 10 March 2010

[21] Greene, Adam; Comments of Office of Civil Rights attorney Adam Greene, American Bar Association's 11th Annual Conference on Emerging Issues in Healthcare Law, 18 February 2010

[22] McAndrew, Susan; Transcript of Healthcare Info Security Interview, HIPAA Audit Update: OCR's Susan McAndrew, USA, 12 May 2010

[23] Commonwealth of Massachusetts, Standard for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17, USA, 2009

[24] Department of Health and Human Services (HHS) Office of Civil Rights, "HIPAA Security Standards: Guidance on Risk Analysis," USA, May 2010, *www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf*

[25] National Institute of Standards and Technology (NIST), Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, USA, October 2008

[26] Centers for Medicare & Medicaid Services (CMS), HIPAA Security Series No. 6, "Basics of Risk Analysis and Risk Management," USA, March 2007

[27] National Institute of Standards and Technology (NIST), Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, USA, July 2002

[28] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27005:2008, *Information technology—Security techniques—Information security risk management*, 2008

[29] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27002:2005, *Information technology—Security techniques— Code of practice for information security management*, 2005

[30] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO 31000:2009, *Risk Management—Principles and Guidelines*, 2009

[31] ISACA, *The Risk IT Framework*, 2009, USA, *www.isaca.org/riskit*

[32] Office of Government Commerce (UK), Information Technology Infrastructure Library V3, 2007

[33] American Institute of Certified Public Accountants (AICPA), Generally Accepted Privacy Principles (GAPP), *http://infotech.aicpa.org/Resources/Privacy*

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.

www.isaca.org