SECURITY ARCHITECTURE

Privacy and Security Considerations for EHR Incentives and "Meaningful Use"

by Stephen Gantz, CISSP-ISSAP, CEH, CGEIT, CIPP/G

{An edited version of this article appeared in *ISACA Journal Online*, Volume 5, 2010}

One of the areas of emphasis in the American Recovery and Reinvestment Act of 2009[1] (ARRA) is expanding the use of health information technology, both in terms of storing and managing medical records in electronic form, and facilitating the exchange of information contained in such records. ARRA included significant funding that will provide incentive payments to healthcare providers to adopt Electronic Health Record (EHR) technology; these incentives require eligible providers not just to acquire and install systems, but to demonstrate "meaningful use" of electronic health records.[2] The criteria needed to show meaningful use were defined in a Notice of Proposed Rulemaking[3] published in the Federal Register on January 13, 2010, along with an Interim Final Rule detailing standards, specifications, and certification criteria for EHR systems used by providers.[4] A 60-day comment period on the proposed rules ended on March 15, 2010, and the meaningful use criteria are likely to be finalized in June 2010 as the mechanisms to implement the incentive payment provisions in the Health Information Technology for Economic and Clinical Health (HITECH) Act portion of the Recovery Act.[5] (Comment period notwithstanding, the Interim Final Rule became effective on February 12, 2010.) The rules are organized according to a set of five policy priorities specified by the Health IT Policy Committee, one of two advisory bodies (the other is the Health IT Standards Committee) created through provisions in the Recovery Act.[6] These priorities are: [7]

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

Once finalized, the Office of the National Coordinator for Health Information Technology (ONC) will implement the meaningful use measures and EHR certification criteria in a three-stage process, with certain measures and criteria taking effect in 2011, 2013, and 2015. The financial incentives associated with meaningful use will be administered by the Center for Medicare and Medicaid Services (CMS). For the certification criteria, each stage has a set of meaningful use objectives associated with the policy priorities, with one or more criteria in the draft rules corresponding to each objective. After initial review of the proposed meaningful use measures, the Health IT Policy

[1] American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009)
[2] American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 §4101 (Feb. 17, 2009)
[3] Electronic Health Record Incentive Program Proposed Rule, 75 Fed. Reg. 1858 (Jan. 13, 2010)
[4] Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology Interim Final Rule, 75 Fed. Reg. 2028 (Jan. 13, 2010)
[5] Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009)
[6] American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 §3002 (Feb. 17, 2009)
[7] Electronic Health Record Incentive Program Proposed Rule, 75 Fed. Reg. 1854-1858 (Jan. 13, 2010)

Committee recommended that the total number of measures be reduced for 2011 and that eligible hospitals and professionals should be given the flexibility to defer some of the criteria, rather than following the "all or nothing" approach in the proposed rule,[8] so the final set of measures is still subject to revision. This article focuses on the criteria associated with the fifth policy priority that addresses security and privacy protections for personal health information. For 2011, there is a single meaningful use measure for privacy and security, ten EHR certification criteria, and six technical standards recommended for adoption.

Privacy and Security Expectations

The objectives associated with the privacy and security priority identified in the Notice of Proposed Rulemaking[9] are:

- Ensuring privacy and security protections for confidential information through operating policies, procedures, and technologies and compliance with applicable law.
- Providing transparency of data sharing to patients.
- Protecting electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities. These capabilities correspond to certification criteria for EHR technology[10] and are summarized in Table 2.

The Health IT Policy Committee recommended additional objectives that specified the need for healthcare 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 ONC in December 2008. There are no specific meaningful use measures associated with this compliance, in part because covered entities are already obligated to comply whether or not they seek EHR incentives, and also because the assessment of meaningful use or use of certified EHR technology is not by itself indicative of compliance with HIPAA privacy or security requirements.

There is only one proposed privacy and security measure for meaningful use: "Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement security updates as necessary." The clause of the federal code cited is part of the statutory requirements associated with the Health Insurance Portability and Accountability Act of 1996 (HIPAA); more familiarly 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 requirements is intentional – by aligning certification criteria to existing HIPAA requirements, the intent is to try to help eligible professionals and hospitals that are the focus of the meaningful use rules to 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. The approach to EHR certification in the Interim Final Rule is also consistent with HIPAA safeguards and security control frameworks promulgated under other federal regulations in that it stops short of adopting specific standards or technologies where no clear federal guidance exists, or where such a declaration might favor a given vendor or otherwise preclude innovation. The security and privacy standards in the Interim Final Rule are summarized in Table 1.

[8] NPRM Recommendations, presented at the February 17, 2010 meeting of the Health IT Policy Committee
[9] Electronic Health Record Incentive Program Proposed Rule, 75 Fed. Reg. 1858 (Jan. 13, 2010)
[10] Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology Interim Final Rule, 75 Fed. Reg. 2028 (Jan. 13, 2010)
[11] Office of the National Coordinator for Health Information Technology, "Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information" (December 15, 2008)
[12] 45 CFR §164.308(a)(1)(ii)(A)

Table 1: EHR Certification Criteria Adopted Security and Privacy Standards

Purpose	Adopted Standard
General Encryption and Decryption of Electronic Health Information	A symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key must be used (*e.g.*, FIPS 197 Advanced Encryption Standard, (AES), Nov 2001).
Encryption and Decryption of Electronic Health Information for Exchange	An encrypted and integrity protected link must be implemented (*e.g.*, TLS, IPv6, IPv4 with IPsec).
Record Actions Related to Electronic Health Information (*i.e.*, audit log)	The date, time, patient identification (name or number), and user identification (name or number) must be recorded when electronic health information is created, modified, deleted, or printed. An indication of which action(s) occurred must also be recorded (*e.g.*, modification).
Verification that Electronic Health Information has not been Altered in Transit	A secure hashing algorithm must be used to verify that electronic health information has not been altered in transit. The secure hash algorithm used must be SHA-1 or higher (*e.g.*, Federal Information Processing Standards (FIPS) Publication (PUB) Secure Hash Standard (SHS) FIPS PUB 180–3).
Cross-Enterprise Authentication	Use of a cross-enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails (*e.g.*, IHE Cross Enterprise User Assertion (XUA) with SAML identity assertions).
Record Treatment, Payment, and Health Care Operations Disclosures	The date, time, patient identification (name or number), user identification (name or number), and a description of the disclosure must be recorded.

Source: ONC Interim Final Rule, Table 2B, 75 Fed. Reg. 2035 (January 13, 2010)

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; the HIPAA Security Rule has been in force since April 2003, and the deadline for entities to fully comply with the rule lapsed in April 2006. Despite this requirement, not all healthcare organizations comply. The results of a 2009 security survey[13] of 196 senior-level healthcare 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 healthcare organizations do not conduct risk analyses on a regular basis (and perhaps a quarter do not conduct them at all), and also that similar proportions of healthcare 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, and 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

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

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. Where product testing for conformance is concerned, NIST may choose to have the certification performed by one or more approved third parties, potentially including the Certification Commission for Health IT (CCHIT) or other independent testing organizations. Of the 22 general certification criteria enumerated, eight correspond to security requirements, and most of them reference one or more of the adopted standards shown in Table 1. What becomes apparent is that any entity tasked with assessing conformance to these criteria will need to make a highly subjective determination, as some of the "standards" listed are nothing more than functional characteristics. Potential issues and considerations related to the security-related certification criteria are summarized in Table 2.

Table 2: EHR Certification Criteria related to security

Function	Criterion	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 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.	The standard in question specifies the minimum information that must be logged, rather than any technical, format, or process requirement.
Integrity: In transit	Verify that electronic health information has not been altered in transit in accordance with the standard specified.	The referenced standard specifies the use of the SHA-1 or higher hash algorithm, corresponding to the five SHA hash variants specified in federal Secure Hash Standard (FIPS 180-3)
Detection	Detect the alteration and deletion of electronic health information and audit logs, in accordance with the standard specified.	
Authentication: Local	Verify that a 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.
Cross-network	Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified.	

Function	Criterion	Comments
Encryption: General	Encrypt and decrypt electronic health information according to user-defined preferences in accordance with the standard specified.	Requires symmetric 128 bit fixed-block cipher algorithm with 128 bit or greater encryption key.
Exchange	Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified.	Requires an encrypted link; usually interpreted to mean Transport Layer Security consistent with NIST Special Publication 800-52, although a specific technology is not specified.
Accounting of disclosures	Record disclosures made for treatment, payment, and healthcare 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 for first two columns: 45 CFR §170.302(o) through (v), 75 Fed. Reg. 2046 (January 13, 2010)

Privacy and Meaningful Use

Despite the inclusion of the word *privacy* in the fifth health outcomes policy priority listed in the meaningful use NPRM – "to ensure adequate privacy and security protections for personal health information" – as the meaningful use measures and certification criteria currently stand, there are no specific privacy requirements in order to demonstrate meaningful use. The healthcare providers, professionals, and organizations eligible to seek incentive funding to which the meaningful use determination applies are, without exception, HIPAA-covered entities, so there is an assumption that these entities' obligations under the HIPAA privacy rule serve to make a separate meaningful use privacy requirement redundant.

The Privacy and Security Policy workgroup of the Health IT Policy Committee proposed in its comments and recommendations on meaningful use rules that an explicit requirement should be added obligating eligible entities to demonstrate compliance with HIPAA Security and Privacy Rules as a stage 1 objective.[14] 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 they have been found liable or fined for a HIPAA violation. A somewhat broader recommendation is noted in the Notice of Proposed Rulemaking[15] 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. 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, 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 who are not currently 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.

[14] Comments and Recommendations presented at the February 19, 2010 meeting of the Privacy & Security Policy Workgroup

[15] Electronic Health Record Incentive Program Proposed Rule, 75 Fed. Reg. 1858 (Jan. 13, 2010)

Notably absent from meaningful use rules – as stressed by privacy advocates such as the Coalition for Patient Privacy[16] – are criteria that would 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[17] specifying practices for health record information disclosure with consent, as well as prohibiting re-disclosure absent such consent, but these rules only apply to records concerning alcohol and drug abuse, not healthcare in general. ONC has been working on consumer preferences since at least 2008, when they were identified as a gap in use cases prioritized for development by the American Health Information Community (AHIC), and has produced a Consumer Preferences Draft Requirements Document[18] 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 either of preparing to validate and demonstrate that their products already have the capabilities in question or prioritizing the addition of these capabilities into their product development roadmaps. 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 produce once 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 a Notice of Proposed Rulemaking published in March 2010,[19] 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 a sufficient number of third-party certification bodies are 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 proposed permanent program would 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 healthcare providers or organizations interested in qualifying for EHR incentives in order 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 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 healthcare providers to ensure that their information security and privacy practices include regular risk analyses. It is understandable that many organizations

[16] Coalition for Patient Privacy, Comments on meaningful use submitted to the Health IT Policy Committee (June 26, 2009) http://patientprivacyrights.org/media/L-Coalition_to_HIT_PC_Meaningful_Use.pdf
[17] 42 CFR Part 2, Subpart C
[18] Office of the National Coordinator for Health Information Technology, "Consumer Preferences Draft Requirements Document" (Oct. 5, 2009)
[19] Proposed Establishment of Certification Programs for Health Information Technology Proposed Rule, 75 Fed. Reg. 11328 (Mar. 10, 2010)

may place an emphasis on conducting and documenting a risk analysis in order to satisfy the meaningful use measure, but this type of activity should not be considered a one-time 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, healthcare 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 be able to demonstrate compliance with meaningful use requirements.

1. **Financial incentives** tied to meaningful use with require more and stronger qualifications 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.
2. **The HITECH Act strengthened many HIPAA requirements** and obligations in the HIPAA Privacy and Security Rules, and those provisions generally now 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 the requirements will not yet be enforced[20] – 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. This gives organizations a temporary opportunity to close any gaps in their conformance before they will be formally held accountable. OCR personnel have stated publicly[21] that health care organizations should be prepared for stronger enforcement measures, including proactive security and privacy audits, and hopes to begin conducting those audits by the end of 2010.
3. **New state-level data protection laws**, such as those in Massachusetts' new Standards for the Protection of Personal Information[22] that went into effect on March 1, 2010, require many of the same privacy and security practices to comply with non-health-specific legal requirements that healthcare organizations should be following under HIPAA and HITECH and to demonstrate meaningful use of EHR technology. Even for organizations without any Massachusetts residents among their patients or customers, the requirements in the Massachusetts law are likely to be replicated in other state laws, raising the probability that an organization will find itself subject to one or more of these state laws, even if no federal-level legislation is enacted.

Guidance on Risk Analysis

For organizations that do not already routinely conduct risk analyses, or who do so but are concerned that their processes may not be sufficiently robust to pass muster under meaningful use, the Health IT Policy Committee is considering recommendations from its own Privacy and Security Policy Workgroup and multiple outside reviewers that healthcare professionals and hospitals be given explicit guidance on performing risk analyses. The HHS Office of Civil Rights, which has responsibility for enforcing the provisions of both the HIPAA Security Rule and Privacy Rule, published draft guidance on risk analysis[23] that generally directs covered entities to follow relevant NIST documentation related to complying with the HIPAA Security Rule where the required risk analysis is codified. Both

[20] Comments of Office of Civil Rights attorney Adam Greene at the American Bar Association's 11th Annual Conference on Emerging Issues in Healthcare Law (Feb. 18, 2010)

[21] Transcript of Healthcare Info Security Interview, "HIPAA Audit Update" with Office of Civil Rights Deputy Director for Privacy Susan McAndrew (May 12, 2010)

[22] Standard for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17 (2009)

[23] Department of Health and Human Services (HHS) Office of Civil Rights, "HIPAA Security Standards: Guidance on Risk Analysis" (May 7, 2010)

NIST Special Publication 800-66[24] and CMS' Security Rule Education Paper Series[25] direct organizations to a standard security risk assessment process, documented in detail in NIST Special Publication 800-30.[26] For those preferring to seek guidance outside the U.S. federal standards, the ISO/IEC 27000 series of international standards covers risk assessment and risk management for information systems, particularly in ISO/IEC 27005,[27] and the risk assessment section of ISO/IEC 27002.[28] Those seeking to follow any of this guidance on risk management or 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 the organization has, not just the data associated with an EHR system. Organizations looking for more enterprise-level perspectives on assessing and managing risk can find relevant guidance in ISO 31000,[29] within major IT governance frameworks such as ISACA's Risk IT Framework[30] based on COBIT® or the Risk Management section of the Information Technology Infrastructure Library (ITIL®).[31]

Looking at risk analysis from a privacy perspective, organizations have few options in terms of official guidance for privacy risk assessments or even auditing compliance with the HIPAA Privacy Rule. While not health-specific, the American Institute of Certified Public Accountants (AICPA) developed and maintains a set of "generally accepted privacy principles," most recently updated in April 2009, which addresses risk assessment among many other criteria.[32] AICPA also produced a spreadsheet-based Privacy Risk Assessment Tool that addresses 66 criteria across the 10 principles in the GAPP.

While some healthcare 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 them.

Recommendations

Compared to the large volume of comments submitted that focus on reducing or making optional many of the 25 proposed meaningful use measures, relatively little attention has been paid to the sole security-related measure, which requires that health care providers perform security risk analyses. One explanation is that the potential recipients of EHR incentive funding made available through provisions in the HITECH Act are already required to

[24] NIST Special Publication 800-66, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule" (October 2008)

[25] CMS, HIPAA Security Series No. 6, "Basics of Risk Analysis and Risk Management" (March 2007)

[26] NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems" (July 2002)

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

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

[29] International Organization for Standardization, ISO 31000:2009 Risk Management—Principles and Guidelines

[30] ISACA, "Risk IT Framework" (2009), http://www.isaca.org/riskit

[31] Office of Government Commerce (U.K.), Information Technology Infrastructure Library V3 (2007)

[32] AICPA Generally Accepted Privacy Principles, http://infotech.aicpa.org/Resources/Privacy/

conduct risk analyses under the HIPAA Security Rule. In theory, this should make compliance with the security requirement a simple matter, but in practice it seems a large proportion of health care organizations have not adopted risk analysis as a regular part of their information security practices. While there may be little real downside to ignoring this requirement under HIPAA due to the lack of proactive enforcement of the Security Rule, under meaningful use the failure to comply could have a tangible financial impact if it prevents otherwise eligible providers from receiving funding from the EHR incentive program. With meaningful use coming into effect in 2011, now is the time for health care organizations to take a look at their internal security practices and make sure they are prepared to comply. The flow diagram in Figure 1 shows a representative process by which health care providers can evaluate their current status in terms of conducting risk analyses as required to demonstrate meaningful use. By asking and candidly answering a series of questions about internal risk analysis practices, providers can better understand what effort (if any) is likely to be needed to achieve compliance. These questions include:

- Has a risk analysis already been completed?
- If so, was the risk analysis completed within the past year (that is, is it current)?
- For an existing and up-to-date risk analysis, does its scope and level of detail appropriately address the EHR system and associated health information technology?

If the answer to all of these questions is "yes," then the current risk analysis may provide sufficient evidence to satisfy the meaningful use measure. If, however, the answer to any of these questions is "no," then a plan should be put in place to conduct a new risk analysis.

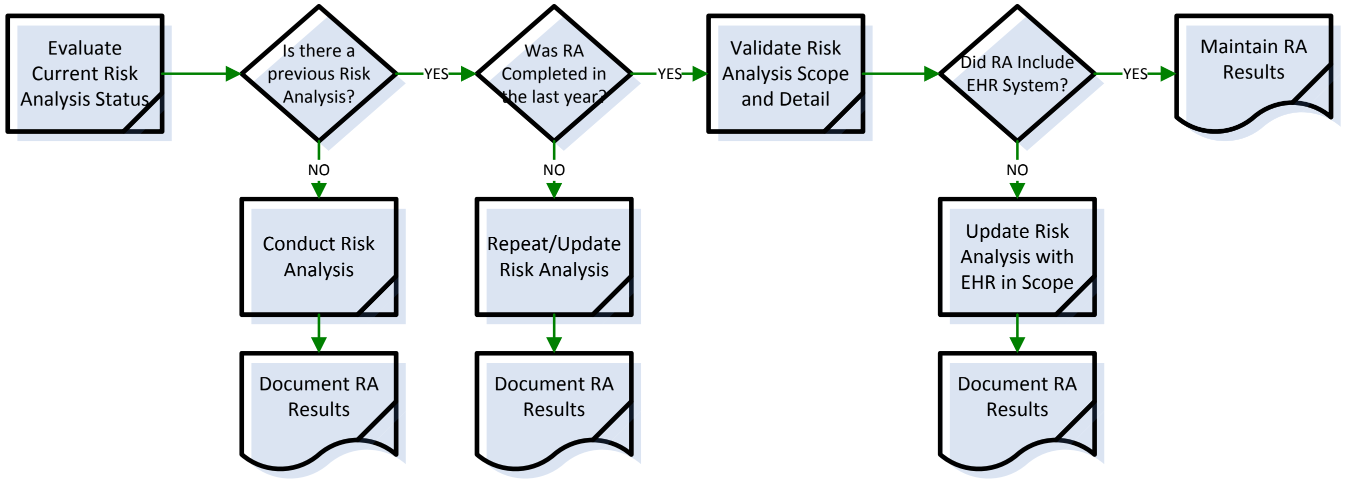

Evaluate Current Risk Analysis Status
Is there a previous Risk Analysis?
YES
Was RA Completed in the last year?
YES
Validate Risk Analysis Scope and Detail
Did RA Include EHR System?
YES
Maintain RA Results
NO
Conduct Risk Analysis
Document RA Results
NO
Repeat/Update Risk Analysis
Document RA Results
NO
Update Risk Analysis with EHR in Scope
Document RA Results

Figure 1: Internal risk analysis evaluation. Using a straightforward assessment of the existence and completeness of current risk analysis information, eligible providers can determine what additional effort, if any, is needed to satisfy the risk analysis requirement under meaningful use.

A separate sort of analysis is needed regarding privacy of electronic health records, especially the extent to which health care organizations will allow individual patients to control the use and disclosure of their personal health data. ONC commissioned a report[33] detailing different approaches and alternatives for providing consent to individual consumers such as patients, which organizations considering consent management may find helpful. The meaningful

[33] George Washington University School of Public Health and Health Services on behalf of the Office of the National Coordinator for Health IT, "Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis" (March 23, 2010)

use framework has no measures related to privacy (although it implies that health care organizations should be in full compliance with the HIPAA Privacy Rule), so providers should look beyond statutory requirements on privacy. One relevant consideration is the way that soliciting consent and otherwise affording patients the ability to control use and disclosure of their electronic health records can encourage patient participation and support for the use of electronic health records. Survey data suggests[34] that absent such individual controls, some patients are likely to withhold information from their doctors to keep it from being shared, a situation which could reduce the reliability and value of EHR systems for clinical support. Health care organizations may find that adding additional patient privacy and consent practices can increase the effectiveness and meaningful use of their EHR systems, even if privacy is not specifically measured as an eligibility qualification. As shown in Figure 2, there are several factors and influences that should be taken into account when deciding whether to actively solicit and manage consent and related consumer preferences, and what form and level of detail of any such consent management will have.

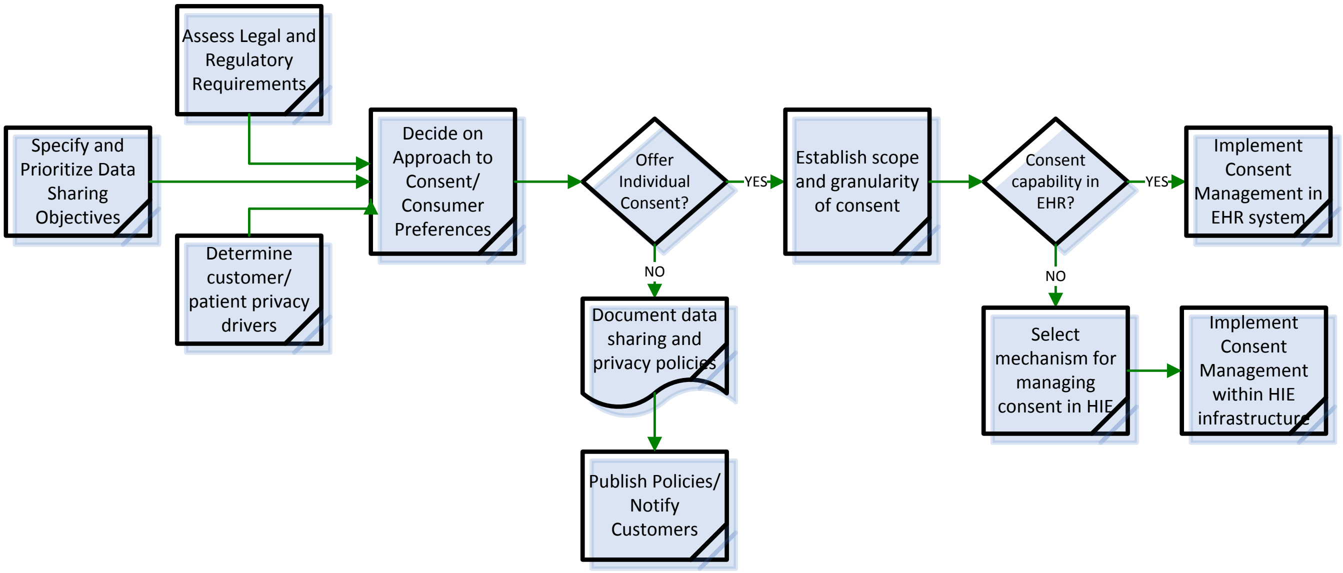
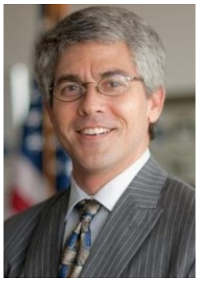

Assess Legal and Regulatory Requirements
Specify and Prioritize Data Sharing Objectives
Determine customer/ patient privacy drivers
Decide on Approach to Consent/ Consumer Preferences
Offer Individual Consent?
YES
NO
Establish scope and granularity of consent
Consent capability in EHR?
YES
NO
Implement Consent Management in EHR system
Document data sharing and privacy policies
Publish Policies/ Notify Customers
Select mechanism for managing consent in HIE
Implement Consent Management within HIE infrastructure

Figure 2: Decision process for patient consent. The choice to collect and honor consumer privacy preferences and manage consent for personal data disclosure is a business decision that should reflect health data sharing priorities, legal obligations, and patient desires.

Stephen Gantz, CISSP-ISSAP, CEH, CGEIT, CIPP/G, is founder and Principal Architect of SecurityArchitecture.com. 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. He is also an associate professor in information assurance at University of Maryland University College. His academic research focuses on trust frameworks, privacy and security models and control frameworks, and related technologies. He can be reached through the "Contact Us" link on the SecurityArchitecture.com website or by email at sgantz@securityarchitecture.com.



[34] California HealthCare Foundation, "Consumers and Health Information Technology: A National Survey," results released April 2010, http://www.chcf.org/topics/view.cfm?itemid=134205