ACHIEVING COMPREHENSIVE HEALTH IT PRIVACY AND SECURITY

What's New in HIPAA Compliance and Key Steps to Completing the Meaningful Use Risk Assessment

Author: Jared Rhoads

Privacy and security have become mission-critical issues for hospitals. Achieving full HIPAA compliance and satisfying the meaningful use risk assessment requirement may sound daunting, but it is very much a goal within reach.

Privacy and security have become mission-critical issues for hospital executives now that the proposed changes to the HIPAA regulations are about to be finalized and the risk assessment requirement for the electronic health record (EHR) incentive program is in full force. Organizations can no longer think of privacy and security as a set of disjointed or poorly-enforced HIPAA requirements. The new requirements extend to the activities of covered entities, as well as those of their business associates, and the rules are being strongly enforced. The Office for Civil Rights (OCR) has already assumed a more active role in investigating entities that have experienced breaches and privacy incidents, in some cases issuing million-dollar plus fines.[1]

The Centers for Medicare & Medicaid Services (CMS) sent a signal on the importance of privacy and security in July 2010 when it made the protection of electronic PHI created or maintained by EHRs a core requirement for hospitals and eligible professionals to receive payments under the EHR incentive program. Under the rules for both Stage 1 and Stage 2, meaningful users must conduct a security risk analysis in accordance with Rule 45 CFR 164.308(a)(1) and correct any identified deficiencies by implementing the appropriate policies and technical capabilities.

As a result, in order to be HIPAA-compliant and to achieve meaningful use, privacy and security need to become an integral part of an organization's comprehensive IT strategy.

Achieving full HIPAA compliance and satisfying the meaningful use requirements may sound daunting, but it is very much a goal within reach. The proposed rule changes are still not finalized, and many experts believe that some of the more burdensome requirements could be relaxed. It is also helpful to realize that the security-related measure in the meaningful use criteria is not substantially new: it essentially reiterates the existing HIPAA rule that requires covered entities to conduct a risk analysis, which includes taking action to mitigate risks.[2] The main difference with regard to meaningful use is that organizations now have to attest to having completed the risk assessment.

In our previous paper on privacy and security ("Update on Patient Health Information: Privacy, Security, and Enforcement"), we described the proposed changes to the HIPAA regulations, including the new requirements for breach notification, the extension of HIPAA responsibilities to business associates, and the restrictions on the sale and marketing use of PHI. Those proposed changes are expected to be finalized as an omnibus rule sometime before the end of 2011.[3] In this paper, we examine new changes regarding the accounting of disclosures, and we address for the first time the topics of encryption and two-factor authentication as they relate to HIPAA and meaningful use. We conclude the paper by offering specific guidance on how to approach the meaningful use risk assessment.

What's New in Privacy and Security Compliance

Although some rules, such as the rule requiring covered entities to notify affected individuals of breaches, went into effect following the release of the 2009 interim final rule, regulators continue to respond to public comments and hone the new privacy and security requirements.

Table 1 shows the ten major privacy and security topics that are currently under agency or committee review, what their development has been and where they stand today. All of the final rules implementing changes to privacy and security are expected to be issued together by the end of 2011, with the exception of the final rule on accounting of disclosures, which is undergoing a separate rulemaking process.[4] That final rule may be published at the same time as the others, but officially it will be issued as a separate rule.

Table 1. Ten key privacy and security topics awaiting final decisions

Issue/Topic	Last Ruling	Final Rule Expected	Comments/Outlook
Accounting of Disclosures	July 2010	End of 2011 (not part of omnibus)	Very controversial; many stakeholders believe the requirements are too burdensome
Encryption	July 2010	Fall or end of 2011	Not required, but covered entities must justify their policy if they choose not to encrypt
Two-Factor Authentication	Not addressed	Fall or end of 2011	Has not been proposed as a requirement yet, but is being discussed for data exchange
Breach Notification	August 2009	Fall or end of 2011	Previous rule was pulled by OCR, but there is no indication of what might change, if anything
Breach Penalties	October 2009	Fall or end of 2011	These provisions are not expected to change in the final rule
Extension of Rules to Business Associates (BAs)	July 2010	Fall or end of 2011	Discussion continues as to whether subcontractors of BAs should be included
Marketing Restrictions	July 2010	Fall or end of 2011	More exceptions could be added, relaxing proposed requirements in this area
Sale of PHI	July 2010	Fall or end of 2011	More exceptions could be added, relaxing proposed requirements in this area
Research Activities	July 2010	Fall or end of 2011	No indication of any significant changes has been given
Notices of Privacy Practices	July 2010	Fall or end of 2011	May be expanded to include notification of patient's rights to an access report

Most of the issues in Table 1 have not undergone substantial discussion or review in the past year. However, three areas that *have* received considerable new attention from the Department of Health and Human Services (HHS), the HIT Policy Committee, and stakeholders are: accounting of disclosures, encryption and two-factor authentication.

Update on Accounting of Disclosures

On May 31, 2011, HHS issued a notice of proposed rulemaking modifying the HIPAA Privacy Rule and aligning it with the goals for patient rights to health information that were enacted by the HITECH Act. Under the HITECH Act, an individual has a right to receive a report showing all of the disclosures of his or her information made to carry out treatment, payment and healthcare operations.[5] The new notice conveys details on how covered entities and business associates must account for disclosures of PHI.[6]

Under the new proposed rule, the entire topic of accounting of disclosures would be split into two separate but complementary rights for the patient. Instead of a right to just an accounting of disclosures, patients would have the right to: a) *an*

accounting of disclosures, and b) an *access report*. The former would be defined as a detailed accounting of each disclosure of protected electronic health information, including information about the date, time, user and a description of the disclosure. The latter would be defined as a report that merely provides information on *who* has accessed an individual's electronic PHI, not including details about the discrete instances and purposes for which the information was accessed.

The intent of this new two-rights model is to create an alternative that is less burdensome to providers but that may still satisfy a patient's desire to know who has accessed his or her information.

The intent of this new two-rights model is to create an alternative that is less burdensome to providers but that may still satisfy a patient's desire to know who has accessed his or her information. During the public comment period, many organizations stated that their current EHR systems are decentralized and that they cannot generate a full accounting of disclosures automatically. The new access report option is easier to implement technologically — indeed, most commenters indicated that their current access logging systems already capture the relevant user information needed for such a report. By allowing the access report option, HHS believes it can reduce the number of accounting of disclosures requests that providers will be asked to compile manually.

Like other proposed HIPAA requirements, the new accounting of disclosures requirements will extend to business associates. Business associates include, for example, businesses hired by hospitals to provide coding and transcription services, and independent contractors that assist with billing, data backup and hardware disposal. The new disclosures rule requires the covered entity to provide either an accounting of the business associates' disclosures, or a list and contact information of all business associates.[7] The new guiding principle expressed by HHS is that if the main report received from a hospital or eligible professional does not contain all disclosures made by all business associates, then an individual at least ought to be able to contact each "downstream" business associate and request an accounting of the disclosures that were made by that particular associate.

As for the other details about the disclosure process laid out in the previous notice for proposed rulemaking (NPRM) in July 2010, those remain essentially the same in the new notice of proposed rulemaking. For instance, the accounting of disclosures and access reports still pertain only to information and disclosures made through an electronic health record, and the applicable reporting period remains the three years prior to the request.

The new notice of proposed rulemaking was open to public comment from its date of issuance (May 31) through August 1, 2011. HHS has not yet summarized the comments it received during this period, but several prominent organizations and associations have expressed in their own public statements that the new requirements are too burdensome and go beyond the intent of the HITECH Act. According to these groups, the requirements will be difficult and costly for providers to meet (especially small entities), and such a requirement could be a setback for the industry at a time when organizations are working hard to reduce their administrative costs. According to some concerned groups, the rules assume the existence of technical capabilities that are not widely available.[8]

Patient privacy advocates have also criticized the proposed rule, albeit from a different angle. They argue that requiring providers to produce an accounting of disclosures upon request is an "after-the-fact" approach that does little to prevent inappropriate access of PHI.[9] These stakeholders would prefer that a system be promulgated that enables patients to give consent *before* their doctor shares their health information electronically.

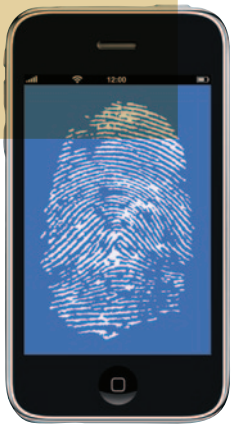
HHS is currently reviewing the latest round of public comments and will decide in the coming months whether to make any additional modifications. If not, then the new accounting of disclosures requirements as described above will go into effect 180 days after the effective date of the final regulation. As currently proposed, covered entities and their business associates who implemented EHRs after January 1, 2009, will be required to comply starting January 1, 2013. Covered entities and their business associates who implemented EHRs before January 1, 2009, will be given an extra year to comply. Their deadline is January 1, 2014.

Update on Encryption

Encryption is the process of converting data and information into a form that is unreadable by unauthorized parties. There are a variety of algorithms and methods available for encrypting data, and it is widely regarded as an effective way of protecting sensitive data.

Mobile device encryption, e-mail encryption, and single sign-on were most frequently identified by respondents as technologies not currently installed at their organizations, but planned for the future.

Source: HIMSS security Survey, November 2010



Neither HIPAA nor the HITECH Act specifically requires the use of encryption, but the HITECH Act, for example, requires entities to make PHI "unreadable, unusable, or indecipherable" to any unauthorized party that may gain access during a breach. When the HITECH Act first appeared in 2009, HHS offered guidance on this requirement and indicated that the two main methods it regards as sufficient to meet this standard are encryption and destruction.[10] HHS so strongly recommends and approves of the use of encryption that it exempted encrypted data from the breach notification rule: if the compromised data are encrypted, then covered entities and business associates are not required to provide the notification that would otherwise be required. In short, encrypting data provides a safe harbor.

In the past, CMS has stopped short of mandating encryption because the agency felt that setting a single encryption standard could place an unfair financial and technical burden on some covered entities.[11] As it stands today, encryption is an "addressable" item.[12] Addressable does not mean optional. Rather, it means that encryption must be implemented if, after an assessment, the entity has determined that it would be a reasonable and appropriate safeguard in its information system environment.[13] An entity *may* determine that encryption is not reasonable and appropriate in addressing a particular risk, but if it does, then it must document that determination and implement equivalent alternative safeguards. For Stage 1 meaningful use, encryption is addressable for data in motion (i.e., data being transmitted); for Stage 2, encryption is addressable for data in motion and data at rest (i.e., data on the hard drives of servers, laptops and mobile devices).

Despite extensive discussion on the topic, HHS is not expected to introduce an encryption requirement in the final rule due at the end of the year. However, the pressure to do so is increasing. Major breaches of unsecured, unencrypted PHI are increasingly common in news stories over past year. In May 2011, the Office of the Inspector General (OIG) sharply criticized the Office of the National Coordinator (ONC) for not making encryption a required security measure on portable media, such as CDs, DVDs and flash drives.[14] In the same report, OIG also indicated that it would like to see an encryption requirement for mobile media, such as smartphones and electronic tablets.

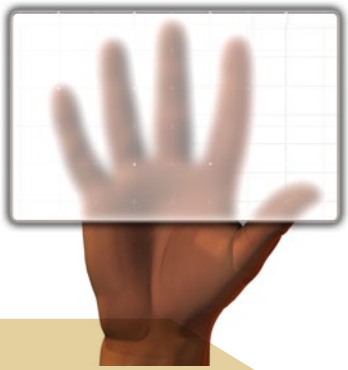
The best practices for security currently promoted by the National Institutes of Standards and Technology (NIST) include encryption.[15] The HIT Policy Committee's Privacy and Security Tiger Team cited the work of NIST when recommending that encryption be addressable for Stage 2. The reason the Tiger Team did not make it strictly *required* is because they felt that organizations may still have valid legacy-related reasons for using alternative methods to secure data depending on the location, portability and immediate use of the data.

Although encryption is not mandatory, the sanctions for failing to protect PHI are severe and the bar is high for proving that alternatives to encryption are satisfactory. As evidenced by recent discussions in key agencies and committees, the disposition of policymakers is increasingly towards encryption, not away

from it. In the immediate term, it is advisable that covered entities and business associates strongly consider incorporating encryption on systems that create, receive, maintain or transform PHI. Practically speaking, it is the best way to meet the standard of "addressability." Alternative methods for securing PHI exist, such as using transport layer security when the data are in motion, but they should be used only if there are compelling reasons not to encrypt. Best practices dictate that data at rest should be encrypted — particularly data on desktops, laptops and storage devices.

Update on Two-Factor Authentication

Two-factor authentication is an approach to authenticating users that requires the user to present two different kinds of evidence to prove their identity. Acceptable forms of evidence may include something the user knows (e.g., a password), something the user has (e.g., a physical token or digital key fob), or something the user is (e.g., retinal scan or fingerprint). Recently, it has also become possible to authenticate based on a fourth criterion: something that the user does (e.g., a particular keystroke pattern or hand gesture).[16]



Two-factor authentication is not expressly required by HIPAA or the HITECH Act, but it is a good practice to consider. Static passwords are no longer considered adequate security practice.

Two-factor authentication is a relatively new topic of discussion for the agencies and committees that set privacy and security policy. It was not mentioned at all in the July 2010 NPRM, *Modifications to the HIPAA Privacy, Security and Enforcement Rules*. Although two-factor authentication is not expressly required by HIPAA or the HITECH Act for meaningful use, it is offered by HHS and CMS as guidance for covered entities that allow users to access electronic PHI remotely.[17] This requirement will become increasingly relevant as participation in health information exchanges increases. New authentication techniques are already relevant given the prevalence of wireless networks in today's facilities, since best practices dictate that wireless access should be considered remote access — even if users are physically located in-house.

Although two-factor authentication has been discussed in the regulatory committees, new specifications requiring this technology are not expected to appear in the final omnibus rule. In March 2011, the Health IT Policy Committee's Tiger Team drafted recommendations that require the use of at least NIST Level-3 assurance (e.g., two-factor authentication) for entities that exchange PHI using the Nationwide Health Information Network.[18] However, they have not yet reached consensus on how the specific baseline requirement would be defined.

Similarly, in a May 2011 review of privacy and security requirements by the OIG, the agency stated that two-factor authentication is one of the security safeguards that should be added to future ONC meaningful use criteria.[19] Certain vendor groups concur and are actively communicating with policymakers. For instance, in April 2011, the Smart Card Alliance Healthcare Council submitted comments to the ONC arguing for the use of strong, multi-factor authentication to be incorporated into Stage 2 meaningful use in order to protect identities, networks and systems.[20]

As with encryption, the latest indications are that two-factor authentication will eventually be proposed as a requirement, once it can be defined and incorporated into the rules in an acceptable way. It is no longer considered adequate security practice to use only a static password to prevent unauthorized access to sensitive information.[21] Although some modes of two-factor authentication are not without their own vulnerabilities — witness the March 2011 incident in which the system of one of the leading secure token providers was compromised — the multi-factor approach does provide a much higher level of security and assurance than traditional passwords, and generally at a reasonable cost to the organization. Implementing two-factor authentication today is an opportunity for organizations to stay ahead of the regulatory curve.

Key Steps To Completing Your Meaningful Use Risk Assessment

According to a recent industry survey of large healthcare organizations, fewer than half of respondents (47 percent) reported that they conduct annual risk assessments, which are required under the HIPAA Security Rule. Nearly six in ten organizations said they have no security personnel or resources dedicated to the task.[22] This will have to change if organizations wish to protect their patients' PHI and participate in the EHR incentive program.

Figure 1. Text of the meaningful use risk assessment requirement

Core Measure Objective: Protect electronic health information (ePHI) created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.

Associated Measure: Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) of the certified EHR technology, and implement security updates and correct identified security deficiencies as part of its risk management process.

Method of Measure Calculation: Measure requires only a Yes/No attestation.

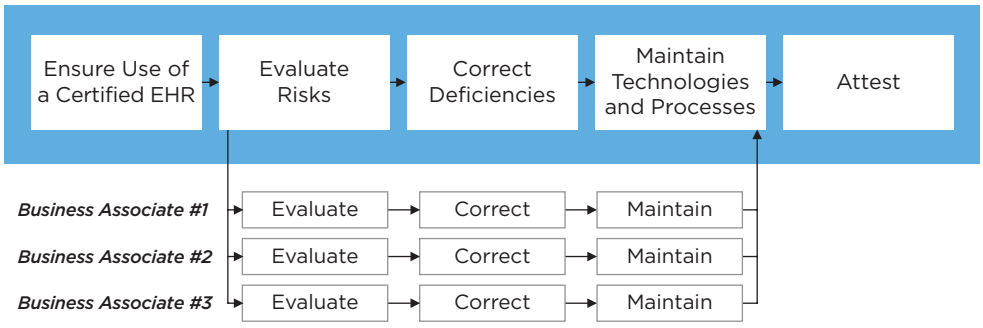
Threshold: Conduct one security risk assessment.

Exclusions: None.

In the meaningful use criteria, privacy and security are dealt with in one critical measure. That measure requires meaningful users of certified EHRs to conduct a security risk assessment (or thoroughly review the last risk assessment that they performed). As part of the assessment, organizations must correct deficiencies and update their management practices. Organizations indicate that they have completed this by a Yes/No attestation. The risk assessment requirement applies to eligible hospitals and eligible professionals.

The meaningful use risk assessment needs to be thorough, but it can be addressed by a relatively simple process of evaluation and correction (see Figure 2). Remember that business associates need to be included in the evaluation, even if they are physically separate from the covered entity. The additional work effort here is potentially very large. A typical hospital might have dozens or hundreds of business associates that it works with for services ranging from consulting and outsourcing to data backup and data disposal. The process for assessing BAs parallels the normal risk assessment procedure.

Figure 2. Key steps to completing the meaningful use risk assessment



1) Ensure That You Are Using a Certified EHR Technology

Use of a certified EHR system is a basic requirement for participating in the incentive program. Some current security-related certification standards include: support for data integrity controls, audits, emergency access, automatic log-off, event recording (e.g., for deletion of records) and accounting of disclosures. Note that certified EHR technologies include some capabilities, such as the ability to support encryption, that are not necessarily required to be used.[23] The purpose of this is to support future expansions to the definition of what constitutes meaningful use of an EHR. Generally it is a good idea to implement such capabilities sooner rather than later.

No EHR can guarantee security in and of itself. The EHR needs to be implemented properly in a secure environment. Despite the certification standards, vendors and system implementers still have substantial leeway in how they install and configure the systems, and which security features they make functional.[24] HHS has not set standards for many related components of the health IT ecosystem, such as hard drives, domain name systems and backup systems.[25] Care must be given to digitally and physically securing the whole environment, not just the EHR system. Remember that using a certified EHR does not guarantee or equate to HIPAA compliance — or vice versa — and nor does it absolve individual users from their HIPAA responsibilities.[26]

2) Evaluate the Risks

The meaningful use risk assessment requires a comprehensive evaluation of an organization's risks and vulnerabilities. This includes internal systems, internal users and third parties. For each of the broad categories below, organizations should determine the likelihood and potential impact of security threats.

Internal Systems

Health IT complexity has increased dramatically over the past decade. The assessment team needs to evaluate vulnerabilities associated with the hardware, software, system interfaces, networks and devices that are in use. Infrastructure that supports data transmission represents an especially high risk unless monitored closely to prevent unauthorized use or compromised data integrity. Unencrypted stores of data represent a high level of risk that is limited only by the systems and policies controlling user access.

The assessment team needs to consider all electronic PHI that the covered entity creates, maintains, receives or transmits. The scope of the analysis should include electronic PHI on all media, including hard drives, CDs, floppy disks, tape drives, DVDs, smart cards, thumb drives and mobile devices including laptops and tablets.

Automated tools exist that can assist in evaluating technical vulnerabilities. Network Access Control (NAC) technologies can scan the hospital's network and identify specific devices that present risks.[27] Networks can also be scanned to identify unprotected wireless networks, unidentified users and unencrypted portable media.[28] Security utilities can be used to identify out-of-date antivirus and anti-spyware software, and to patch systems that have not been properly updated or maintained.

As part of an evaluation of security risks, the U.S. Department of Homeland Security randomly dropped USB and optical drives on the ground outside of buildings at government and private contractor sites. Despite the risks of using a storage drive of unknown origin, nearly 60 percent of those who picked up one of the drives plugged it into their work computer.

Source: "Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy" Bloomberg, June 27, 2011

Clinicians and Management

End users are still unfortunately the greatest source of security breakdowns. Analysis of user accounts and role-based access rules may reveal excessive or out-of-date user access rights, and analysis of logs can be performed to reveal instances of unauthorized data access by users. It is important to investigate these instances and understand why they happened. The reason could be, for example, that employees were sharing accounts because they feel that signing off and signing in again is too slow. If so, that would be a tip to review the workstation timeout settings or to conduct a performance test of the single-sign-on module.

Training can mitigate most employee-based risks. As part of the risk evaluation, review training records to ensure that all employees have received the proper training. Building job-specific scenarios into the training will improve comprehension and retention. Also, verify that employees understand the proper escalation procedures for breaches and unauthorized disclosures. Organizations should always document all training and retain these records for compliance.

Third Parties (i.e., Business Associates)

One of the areas that organizations are most likely to be out of compliance is with regard to their business associates. Third parties represent a particularly challenging risk because their policies and practices are by definition outside of the covered entities' own control. To assess the risk posed by business associates, covered entities should request a detailed review of the contract terms and perform

an audit of current practices. Business associates should be willing to make assurances — in writing — about their HIPAA compliance. If resources allow, the risk evaluation should also extend to the business associate's sub-contractors.

3) Correct Deficiencies

Organizations are required to correct identified security deficiencies as part of the risk management process. CMS has not offered clarification on what qualifies as a deficiency or what type of corrective action is considered adequate.[29] Under the HIPAA law — which was influential in designing the meaningful use measures — covered entities are held to the standard of doing what is "reasonable and appropriate."

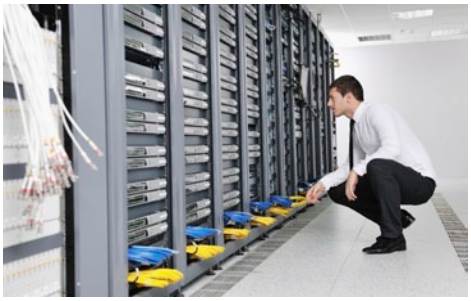
When deciding how to address a risk, organizations should take into consideration the potential impact of a risk, the cost of mitigating that risk and the extent of in-house technical capabilities. Each organization needs to weigh the costs and benefits of addressing each of its risks, and act accordingly. IT resources are always limited, so give priority to the risks that pose the largest (and most likely) potential impact to the most valuable enterprise assets.

A key part of addressing risk is knowing what risks are being accepted. Organizations should always document the decisions and rationale for addressing a potential risk (especially if one addresses a risk using an alternative method). For instance, if you decide not to closely monitor a particular server because it is relatively isolated, sees low usage and is physically well-protected in a locked closet, then document those reasons. Likewise, while encryption is best, if you decide not to encrypt a particular data store because it resides on a secure network with state-of-the-art intrusion detection, then document those reasons as well. Documentation of these activities and decisions must be retained for six years, according to the meaningful use risk assessment measure.[30] Demonstrating due diligence with regard to identifying risks and correcting deficiencies is key to surviving a potential audit. [31]

Although an organization's size and budget are part of the context in determining what corrective action is appropriate, outside expertise is always available and organizations will be expected to use it if the necessary skills and capabilities are not present internally. One growing trend is toward solutions that deliver security-as-a-service.[32] Through this approach it is possible to contract for constant virus definition updates, security administration services and monitoring of network endpoints from offsite.

With regard to business associates, writing detailed contract terms is a necessary but insufficient approach to ensuring security.[33] Work with them to ensure that they have appropriate security measures and training in place, and that they are properly logging activity. Access logs are indispensible in the event of a suspected breach and for complying with the proposed rule change pertaining to accounting of disclosures. If resources permit, create a formal vendor management program that clearly establishes the policies and procedures for engaging with vendors. [34]

Finally, it is important to recognize that not all risks can or should be mitigated using technology.[35] Some risks can be addressed more effectively by offering new or follow-up training, by increasing managerial oversight, or by redesigning processes. These are valid strategies for addressing risk and should be documented as part of the risk assessment, too.



4) Maintain Your Technologies and Processes

Security cannot be achieved in a single exercise or by buying a product; it is an ongoing part of IT management. At an enterprise level, privacy and security should be included as part of the strategic plan.[36] On a day-to-day level, organizations should follow a schedule for reassessing vulnerabilities and implementing security updates as needed.

The meaningful use rule requires organizations to "implement security updates as necessary." This applies equally to processes, not just hardware and software.

If processes are not already in place for updating management policies, user access policies and training materials, then they should be developed. Privacy- and security-related responsibilities should be assigned to everyone in a way that is appropriate for their role. If possible, entrust the communication and enforcement of new policies to a specially-designated privacy or security official. As with other actions, remember to document evidence of security awareness enforcement.

A comprehensive privacy and security plan also includes policies on what to do in the event of adverse incidents, such as a breach of the network. A breach management policy should describe response steps for all key roles, including IT personnel, senior management and clinicians. It should explain how the organization intends to respond from the point of discovery of the breach to the point at which management decides whether the breach must be reported.[37] In preparation for potential breaches and unauthorized disclosures, develop procedures and tools for compliant investigation, analysis and review.

5) Attest That the Risk Assessment Has Been Completed

Eligible professionals and hospitals attest to completing the risk assessment using CMS's online Registration and Attestation System. The attestation for this measure is a simple Yes/No. Note that attestation is legally binding and that any provider who attests may potentially be subject to an audit. We highly recommend retaining supporting documentation about the risk assessment, including documentation about the risk analysis and findings, and the corrections that were instituted.

Keeping Up With New Requirements (And HIPAA Audits)

Privacy and security experts are familiar with the need to stay abreast of the latest hacking methods and how to use new technologies to combat threats. The need to keep up with changing HIPAA rules and meaningful use requirements is much the same. We outlined the key topics to watch in Table 1 at the beginning of this paper. As discussed, the final rulings on those will be published later this year. Remember that it is also recommended that organizations keep up with relevant state regulations, especially in states like California and Massachusetts that have active health IT contingencies.[38]

Around the same time that the final rules are expected, the Office for Civil Rights will also begin a much-anticipated HIPAA compliance audit program.[39] Up to twenty test audits will soon be conducted, with a final audit program to be launched either late this year or in early 2012. The OCR has not yet decided whether the audit program will include business associates, but it will provide advance notice to entities and advance requests for documentation.

Audits and regulations may offer some motivation and guidance on how to secure PHI, but the deeper reason why organizations should address privacy and security comprehensively is because it is the right thing to do for patients. There are many new and changing rules to comply with, but fortunately what is contained in the rules should already be part of an organization's privacy and security strategy. By focusing on ensuring privacy and security through reasonable and appropriate means, full HIPAA compliance and satisfaction of the meaningful use criteria will follow naturally.

About the Author

Jared Rhoads is a senior research specialist with CSC's Global Institute for Emerging Healthcare Practices, the research arm of CSC's Healthcare Group.

Acknowledgements

The author would like to thank the following CSC experts for their input: Owen Pate, Healthcare Vertical Lead Information Risk Manager; Michele Mann, Principal IT Strategy; Linda Ricca, Principal IT Strategy; John Kahanek, Global Compliance Assurance Manager; Richard Staynings, Security Consulting; and Fran Turisco, Research Principal.

References

1. "How to survive a privacy breach audit" *Government Health IT*, June 7, 2011.
2. Anderson, H. "Spotlight on Protecting Stored Data" HealthcareInforSecurity.com, April 7, 2011.
3. "HHS To Release Final Rule on HIPAA Privacy, Security by End of Year" *iHealthBeat*, May 11, 2011.
4. McMahon, E.B. "Coming Soon: Final HITECH Regulations Will Amend HIPAA Privacy, Security, and Breach Notification Requirements" Valeo Online, March 22, 2011.
5. "HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act" Federal Register, 76:104, May 31, 2011.
6. Ibid.
7. Ibid.
8. Guerra, A. "CHIME Wants Reduced Reporting Burden In Proposed HIPAA Changes" HealthSystemCIO.com, July 21, 2011.
9. McCaughey, B. "How ObamaCare destroys your privacy" *New York Post*, June 16, 2011.
10. "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals..." Federal Register, 74:79, April 27, 2009.
11. "HIPAA Security FAQ" Centers for Medcare and Medicaid Services, 2005.
12. Anderson, H. "Spotlight on Protecting Stored Data" HealthcareInforSecurity.com, April 7, 2011.
13. "HIPAA Security FAQ" Centers for Medcare and Medicaid Services, 2005.
14. Keen, C. "OIG slams ONC for security omissions in 'meaningful use' rules" AuntMinnie Healthcare IT Digital Community (sponsored by Siemens), May 20, 2011.
15. Ting, D. "User Access Relevance in a HITECH Age" Imprivata, Inc., June 2, 2010.
16. Seng, et al. "Robust Watermarking Using Hand Gesture for Enhanced Autentication" *Malaysian Journal of Computer Science*, 24:2, 2011.
17. Braithwaite, W.R. "Why Two-Factor Authentication in Healthcare?" Anakam, Inc., 2009.
18. Anderson, H. "Spotlight on Protecting Stored Data" HealthcareInforSecurity.com, April 7, 2011.
19. Keen, C. "OIG slams ONC for security omissions in 'meaningful use' rules" AuntMinnie Healthcare IT Digital Community (sponsored by Siemens), May 20, 2011.
20. "Promoting Two-Factor Authentication for Provider and Patient Access to EHRs and PHRs along with Strong Patient Identity Management Are Priorities for 2011, Says Smart Card Alliance Healthcare Council" Smart Card Alliance, April 25, 2011.
21. Braithwaite, W.R. "Why Two-Factor Authentication in Healthcare?" Anakam, Inc., 2009.
22. McGraw, D. "Standards for Health IT: Meaningful Use and Beyond" September 30, 2010.
23. Gantz, S. "Changes in meaningful use rules on security should simplify compliance" *TechTarget*, July 13, 2010.
24. Ibid.
25. Zaltsman, A. "Privacy and Security in Meaningful Use Rule" HITECH Answers, January 4, 2010.
26. Ibid.
27. Merrill, M. "Top 5 security threats in healthcare" *Healthcare IT News*, June 28, 2011.
28. Keen, C. "OIG slams ONC for security omissions in 'meaningful use' rules" AuntMinnie Healthcare IT Digital Community (sponsored by Siemens), May 20, 2011.
29. Spearman, S. "Security Risk Analysis and the "Gray Areas" of HIPAA Compliance" HealthSecuritySolutions.com, August 2, 2011.
30. "Meaningful Use ePHI Privacy and Security compliance criteria" The HHS Regional Extension Center, June 4, 2011.
31. "HITRUST CSF Assurance Program: Simplifying the Meaningful Use Privacy and Security Risk Assessment" HITRUST, September 2010.
32. Penn, M. and H. Shey, "Services-Led Solutions Reshape The Security Market" Forrester Research, April 28, 2011.
33. Anderson, H. "Key Steps Can Help Prevent Breaches" HealthcareInfoSecurity.com, June 16, 2011.
34. Ibid.
35. Niner, P. "Meaningful Use and Security Risk Assessments" HITECH Answers, February 4, 2011.
36. Martin, W. "Privacy and Security Implications of Meaningful Use for Health Care Providers" North Carolina HIMSS Chapter.
37. Bilancieri, M. "Checklist for Healthcare IT Security Compliance: Q&A" Imprivata, Inc., February 7, 2011.
38. Ibid.
39. Anderson, H. "McAndrew Explains HIPAA Audits" HealthcareInfoSecurity.com, July 15, 2011.

BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING

Healthcare Group
3170 Fairview Park Drive
Falls Church, Virginia 22042
+1.800.345.7672
healthcaresector@csc.com

Worldwide CSC Headquarters

The Americas
3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+1.703.876.1000

Europe, Middle East, Africa
Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

Australia
26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(0)29034.3000

Asia
20 Anson Road #11-01
Twenty Anson
Singapore 079912
Republic of Singapore
+65.6221.9095

About CSC

The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.

For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."

www.csc.com

WA11_0233 HCG
August 2011