FALL 2011 • VOLUME 25 / NUMBER 4 • www.himss.org

Gerry Blass and Susan A. Miller, JD

Meaningful Use: Stage 1

Information Security Risk Analysis Scope

A question that we have been asked by a number of our clients over the past six months is: "What do we really need to do for meaningful use Stage 1 in regards to information security risk analysis?" Just to clarify, for hospitals and critical access hospitals (CAH), the meaningful use requirement for information security risk analysis is in §495.6(f)(14)(i); for eligible professionals (EPs), it is in §495.6(d)(15)(i).

RULE REQUIREMENTS

Meaningful Use Core Objective: Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.

Meaningful Use Core Measure: Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

The meaningful use measure references§164.308(a)(1) Security Management—Implement policies and procedures to prevent, detect, contain, and correct security violations; specifically §164.308(a)(1)(ii)(A) Risk Analysis - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity; and §164.308(a)(1)(ii)(B) - Risk Management - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).

RECOMMENDATION

Our response is a conservative one. We recommend that HIPAA covered entities conduct a comprehensive assessment of all HIPAA Security standards and implementation specifications along and the HITECH Act of 2009.

Why? Because the requirements of §164.308(a)(1) Risk Analysis are to assess what can threaten confidentiality, integrity and availability of ePHI...." While Risk Analysis is only one implementation specification in the HIPAA Security rule, when you read the rest of the rule, you realize that all of the other HIPAA Security standards and implementation specifications are inter- related. You should therefore assess all of the administrative, physical and technical safeguards included in the HIPAA Security Rule along with the requirements of the HITECH Act.

The second half of the meaningful use requirement is to "correct identified security deficiencies as part of its risk management process." Your mitigation plan should be prioritized based on the level of risk, and you need to take action to implement your plan and lower risk. Examine system and network controls, conduct intrusion vulnerability risk assessments and an intrusion penetration tests, and fix identified deficiencies. Implement a risk management process for ongoing risk reduction that includes an executive mandate and organizational multi-disciplinary governance. Keep in mind that your risk assessment and management program is an ongoing process that never ends.

STARTING POINT

So what is your starting point? If you have never conducted an assessment, the time to do so is now. In doing so, you should record your current security controls and processes, your gaps and the risk for each gap , and your mitigation plan to fix gaps and to lower your overall risk.

If you have already conducted HIPAA and HITECH assessments, you should update them on a reasonable frequency for change management.

If you have recently conducted an assessment, your focus should now be ongoing risk management.

WE RECOMMEND THAT HIPAA covered entities conduct a comprehensive assessment of all HIPAA Security standards and implementation specifications along and the HITECH Act of 2009.

DOCUMENTATION, DOCUMENTATION, DOCUMENTATION

How ready are you for an Office of Civil Rights (OCR) audit? The answer to that question is not only based on what you have done so far, but what you have documented so far. Since many HIPAA covered entities have limited resources, the biggest challenge has been to document an audit trail of due diligence compliance activities.

You can start by making a list of documentation that you should have ready to show the OCR in an audit such as policies and supporting procedures, proof of training your workforce, plans and processes such as a contingency plan, facility security plans and audits, network and system audits and monitoring, and more. Your documentation should include technical security assessment results and mitigation, such as intrusion vulnerability and penetration testing. The bottom line is that you need to include all documentation related to your administrative, physical and technical safeguards that represents your audit trail of evidence for due diligence. As you develop your inventory of documentation think about how each document and related assessment activity are associated with what can threaten confidentiality, integrity and availability of ePHI held by your organization.

CONCLUSION

Both the HITECH Act of 2009 and the requirements of MU Stage 1 re-enforce the fact that the need to protect your organization's ePHI is growing in scope, and will continue to do so. The complexities continue to increase with HIEs (health information exchange, ACOs (accountable care organizations), and new technologies. HIPAA-covered entities and Business Associates should take this opportunity to implement an enterprise information risk assessment and management program that is operationally functional and well documented.

Finally, we recommend that you read some of our past *JHIM* columns for related content if you have not done so already. The columns are available online and via our HIPAA 411 linked-in group via discussions started by Gerry Blass. **JHIM**

Gerry Blass has over 35 years of experience in healthcare IT and compliance. Gerry provides IT and compliance consulting services and software that automates the management and documentation of healthcare compliance activities. Gerry is the President & CEO of Blass Consulting and Compliance LLC.

Susan A Miller, JD, has 35 years of professional leadership experience spanning teaching, biochemistry research and law. Since 2002, Susan has provided independent consultation and legal services to numerous healthcare entities including DHHS/CMS. Blass and Miller are co-founders of HIPAA 411, a linked-in group.