

MetaStar Security Risk Assessments: HIPAA and Meaningful Use

Jay A. Gold, MD, JD, MPH; Brad Trudell, JD

Under both HIPAA and the meaningful use criteria of the Electronic Health Record (EHR) Incentive Program, providers are required to conduct a security risk assessment (SRA), which is an analysis of the provider's compliance with the 2005 HIPAA Security Rule. Hospitals and providers participating in the EHR Incentive Program must attest that they have conducted an SRA, which is a core measure of the program. The Centers for Medicare & Medicaid Services (CMS) oversees audits to ensure that those receiving incentive payments are complying with the program's core measures. The failure rate of attesting providers who have been audited is almost 25%, and one of the most commonly cited problems has been noncompliance with the requirement to conduct an SRA. Providers who fail an audit must repay funds received under the incentive program.

The Security Rule contains administrative, physical, and technical requirements that must be met in order to safeguard electronic protected health information (ePHI).

- Administrative safeguards include conducting risk assessments, naming a security official, providing security training, granting/terminating access to ePHI, managing passwords, responding to security

incidents, and planning for emergencies that may impact ePHI.

- Physical safeguards include limiting access to facilities, preventing theft of equipment, restricting access to workstations, and properly disposing of equipment that may contain ePHI.
- Technical safeguards include assigning unique usernames/passwords, automatic logoffs after inactivity, auditing activity in systems containing ePHI, and encrypting data at rest and in transit.

These safeguards are required so that providers protect the confidentiality, integrity, and availability of ePHI that they store and transmit.

Methodology for Conducting an SRA

While the Security Rule requires practices to conduct an SRA, it is silent as to what methodology must be used for the assessment. Several such methodologies exist but the NIST SP 800-30, which was released by the National Institute of Standards and Technology (NIST) in 2002, is considered by industry experts to be the gold standard. It is a relatively straightforward 9-step process that can be used by providers to develop a prioritized listing of their security risks, which represent gaps in compliance with the Security Rule's requirements.

Here is a high level summary of the 9 steps involved in the NIST SP 800-30 SRA methodology:

- System characterization—Define parameters of system to be assessed.
- Threat identification—Identify potential threats to system.

- Vulnerability identification—Identify system's weaknesses.
- Control analysis—Analyze controls in place to prevent vulnerabilities from being exploited.
- Likelihood determination—Determine probability of a vulnerability being exploited.
- Impact analysis—Analyze impact on organization should a vulnerability be exploited.
- Risk determination—Develop prioritized listing of risks (ie, gaps in compliance), achieved by multiplying likelihood determination by impact analysis.
- Control recommendations—Suggest controls for addressing identified risks.
- Results documentation—Develop SRA report showing prioritized risks and recommended controls.

Any robust assessment of a practice's compliance with the requirements of the Security Rule should follow this process or something similar.

HIPAA Audits

In addition to the ongoing meaningful use audits, the Department of Health and Human Services' Office of Civil Rights (OCR) has announced that in early 2016 it will launch Phase 2 of its audit program aimed at measuring compliance with HIPAA's privacy, security, and breach notification requirements. The HIPAA audits will include covered entities such as hospitals and providers as well as business associates. OCR plans to refine the audit protocol originally posted on its website

• • •

Jay A. Gold, MD, JD, MPH, is MetaStar's senior vice president and chief medical officer; Brad Trudell, JD, is MetaStar's HIPAA privacy and security lead.

in 2012, and over the next few months will identify and assess information about a pool of potential audit subjects. Ensuring that a thorough SRA has been completed recently will be very important for practices selected to take part in OCR's upcoming HIPAA audits.

MetaStar Services

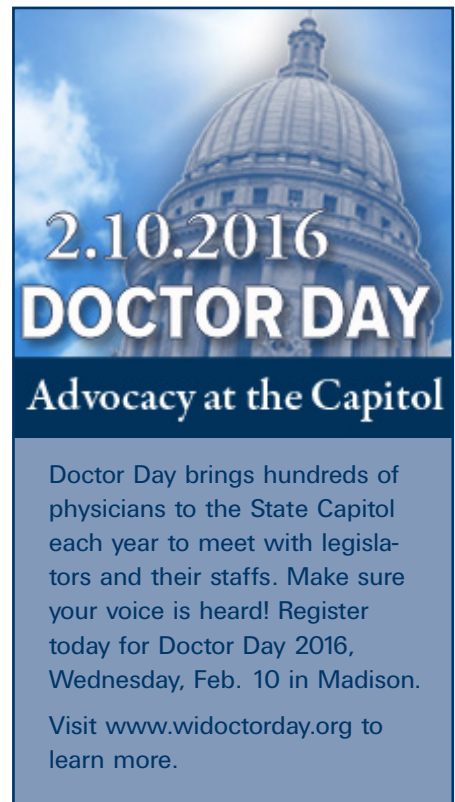
MetaStar offers both virtual and onsite SRAs. In a virtual SRA, MetaStar provides the client with access to and instruction on our robust web-based SRA tool, which incorporates the 9-step NIST SP 800-30 methodology. The client answers the SRA interview questions in the tool, with MetaStar providing assistance as needed. When the client has finished answering the interview questions, MetaStar then produces the client's final SRA report. MetaStar conducts virtual SRAs for clients located all over the United States.

For onsite SRAs, MetaStar staff travel to

the client's facility and work directly with the client's staff to answer all of the SRA interview questions, again using our robust web-based tool. While onsite, a physical walk-through of the client's facility is conducted with MetaStar's assistance to identify areas of potential concern. After the onsite visit is completed, MetaStar compiles the final SRA report for the client.

Much of the Security Rule is to ensure that certain policies, procedures, and other types of documentation are in place. Lack of adequate security policies and procedures is the most common cause of noncompliance with the Security Rule's requirements. To assist practices that may need help in this area, MetaStar also offers a policies and procedures service to help provide the documentation required to comply with HIPAA.

If your practice is interested in learning more about any of these services, e-mail info@metastar.com.

A graphic for Doctor Day 2016. The top half features a blue sky with a white dome of a state capitol building. Overlaid on the dome is the date "2.10.2016" in a large, white, serif font, and below it, the words "DOCTOR DAY" in a bold, white, sans-serif font. Below the dome image is a dark blue horizontal bar with the text "Advocacy at the Capitol" in a white, serif font. The bottom half of the graphic is a light blue rectangular area containing text in a dark blue, sans-serif font.

2.10.2016
DOCTOR DAY
Advocacy at the Capitol

Doctor Day brings hundreds of physicians to the State Capitol each year to meet with legislators and their staffs. Make sure your voice is heard! Register today for Doctor Day 2016, Wednesday, Feb. 10 in Madison.

Visit www.widoctorday.org to learn more.

advancing the art & science of medicine in the midwest

WMJ

WMJ (ISSN 1098-1861) is published through a collaboration between The Medical College of Wisconsin and The University of Wisconsin School of Medicine and Public Health. The mission of *WMJ* is to provide an opportunity to publish original research, case reports, review articles, and essays about current medical and public health issues.

© 2015 Board of Regents of the University of Wisconsin System and The Medical College of Wisconsin, Inc.

Visit www.wmjonline.org to learn more.