Learning Forum Friday

Last Chance to Review Your Security Risk Analysis

Questions and Answers

Moderator

Denise Hudson
Health Informatics Specialist
Health Services Advisory Group (HSAG)

Speaker(s)

Emilie Sundie, MSCIS, PMP, CPHIMS
Director, Health IT Services
HSAG

Kari Vanderslice, MBA
Health Informatics Specialist
HSAG

November 17, 2017

DISCLAIMER: This presentation question-and-answer transcript was current at the time of publication and/or upload onto the *Learning Forum Friday* website. Medicare policy changes frequently. Any links to Medicare online source documents are for reference use only. In the case that Medicare policy, requirements, or guidance related to these questions and answers change following the date of posting, these questions and answers will not necessarily reflect those changes; given that they will remain as an archived copy, they will not be updated.

The written responses to the questions asked during the presentation were prepared as a service to the public and are not intended to grant rights or impose obligations. Any references or links to statutes, regulations, and/or other policy materials included are provided as summary information. No material contained therein is intended to take the place of either written laws or regulations. In the event of any conflict between the information provided by the question-and-answer session and any information included in any Medicare rules and/or regulations, the rules and regulations shall govern. The specific statutes, regulations, and other interpretive materials should be reviewed independently for a full and accurate statement of their contents.

Learning Forum Friday

Question 1:	**Are there sample SRAs available for solo providers to review?** Yes, there are. Two of those sample tools are available through the Office of the National Coordinator for Health Information Technology (ONC), the Security risk Assessment (SRA) Tool User Guide located at (https://www.healthit.gov/sites/default/files/attachmenta-security_risk_assessment_tool_user_guide_v6.pdf) and the National Institute of Standards and Technology (NIST) Toolkit available at NIST HIPAA Security Toolkit Application. There are also other resources available through professional societies and/or ACOs that may have tools that could be appropriate for your practice.
Question 2:	**Is there a small four- to five-page questionnaire for a solo practitioner, an SRA for our small practice and that we are supposed to answer?** The security rule specifies the standards, and they are not dependent on the size of the practice. If you are a small practice and the question is not applicable to your environment, a minimal answer is fine. Use a commonsense approach. There are no strict guidelines about what is enough for a small practice vs. a large practice. The standard is the standard and you need to go through and answer as appropriate for your environment. The auditors want to see a complete tool.
Question 3:	**If a person working in an outpatient center will not release the security risk analysis, how is a physician able to meet the requirements?** MIPS ACI attestations occur at either an individual or group level. If the clinician is attesting as an individual, he has no way of knowing whether he can attest "Yes" to the SRA measure unless he is at least permitted to review the assessment/review and documentation of the remediation work and system updates; he will not be able to demonstrate that he has met the measure if audited. Group ACI attestations occur at the Tax ID level. If the organization is attesting as a group, then the individual provider would have no control over the response to the SRA measure. The audit would occur at the organizational level, and all providers in the organization would be affected by its outcome. It seems the organization would have an interest in supporting any attestation, individual or group, that would affect payments made for the services they provide.
Question 4:	**How often should the information system be reviewed?** HIPAA doesn't specify any interval. If the environment is stable, reviews could be adequate for one or more years after an assessment. Given the rate of change in Certified Electronic Health Technology (CEHRT), however, it's hard to imagine a major upgrade or other significant change to the system would not occur every few years. Looking at the constraints imposed by the SRA measure,

	you do have an obligation to at least review, if not assess, a minimum of once yearly.
Question 5:	**Do we just ask the vendor to provide the information, system activity, for the review?** A vendor may be able to provide some of that information, but you are responsible for the review. You need to go in there and look at the information. How often you do it, what kind of records you keep, that is up to you. If you've only got four people in your office, looking at user activity is going to be a very short exercise. This is about due diligence. Some large organizations do outsource management of this review process. However, even though a vendor provides the service, the organization still retains responsibility for having the reviews occur. At a minimum, organizations need to be aware of the system activity information they have, along with documentation showing they actually took a look at it and reacted appropriately to any security issues discovered.
Question 6:	**We have a current security risk analysis document for our practice. Must we also have written policy and procedure documents, as well?** There are many policies that are required for HIPAA. As part of your overall privacy and security program, you should have a manual With respect to the SRA requirement, you certainly must have a sanction policy. HIPAA requirements will specify that you have other policies as well, such as those related to data breaches. Refer to sample policies if you need to. If you are a small practice, it's easy for you to download and modify those policies that are appropriate to your environment.
Question 7:	**I am being told by CMS and an HSAG Representative that you can only submit improvement activities through the QPP website, not quality.** Please contact our toll-free assistance line at 844.472.4227 and we will be able to assist with that question.

This material was prepared by Health Services Advisory Group, the Medicare Quality Improvement Organization for Arizona, California, Florida, Ohio, and the U.S. Virgin Islands, under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. The contents presented do not necessarily reflect CMS policy. Publication No. QN-11SOW-D.1-11222017-01