10 Myths about HIPAA's Required Security Risk Analysis

Dept. of Health and Human Services
OCT 21, 2013 3:40pm ET

With revamped HIPAA privacy and security rules now in effect that include higher emphasis on conducting a security risk analysis, the federal *HealthIT.gov* Web site dispels 10 pieces of misinformation about what the rules really require:

1. The security risk analysis is optional for small providers. False. All providers who are "covered entities" under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.

2. Simply installing a certified EHR fulfills the security risk analysis MU requirement. False. Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR.

3. My EHR vendor took care of everything I need to do about privacy and security. False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.

4. I have to outsource the security risk analysis. False. It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.

5. A checklist will suffice for the risk analysis requirement. False. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.

6. There is a specific risk analysis method that I must follow. False. A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule. This guidance assists

organizations in identifying and implementing the most effective and appropriate safeguards to secure e-PHI.

7. My security risk analysis only needs to look at my EHR. False. Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone). Remember that copiers also store data. Please see U.S. Department of Health and Human Services (HHS) guidance on remote use.

8. I only need to do a risk analysis once. False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections. For more on reassessing your security practices, please see the Reassessing Your Security Practice in a Health IT Environment.

9. Before I attest for an EHR incentive program, I must fully mitigate all risks. False. The EHR incentive program requires correcting any deficiencies (identified during the risk analysis) during the reporting period, as part of its risk management process.

10. Each year, I'll have to completely redo my security risk analysis. False. Perform the full security risk analysis as you adopt an EHR. Each year or when changes to your practice or electronic systems occur, review and update the prior analysis for changes in risks. Under the Meaningful Use Programs, reviews are required for each EHR reporting period. For EPs, the EHR reporting period will be 90 days or a full calendar year, depending on the EP's year of participation in the program.