Codify
BY AAPC

Health Information Compliance Alert

Get Started Today: Sample Risk Analysis Plan

Learn the basics of a complete risk analysis process.

Your risk analysis process may look entirely different from another provider's approach, but most processes are similar in certain ways. After all, electronic health records (EHRs) pose the same basic risks for one entity as another. And if you want to stay in the good graces of HIPAA compliance auditors, you need to nip those risks in the bud right away.

"It's very difficult to have a standardized, one-size-fits-all kind of approach," says **Jim Sheldon-Dean**, Director of Compliance Services for **Lewis Creek Systems, LLC** based in Charlotte, VT. "Every organization is different and has a different way of approaching [its] risk analysis."

Follow 8 Risk Analysis Steps

Although neither the HIPAA Security Rule nor the EHR Incentive Program mandate how you must perform the risk analysis, the **Centers for Medicare & Medicaid Services** (CMS) **Office of Civil Rights** (OCR) offers the following eight steps as a template to develop your own process.

1. Identify the scope: Your risk analysis should encompass all the potential risks and vulnerabilities to all the electronic protected health information (ePHI) that your practice creates, receives, maintains or transmits. This includes all ePHI in all forms of electronic media, which can include CDs, hard drives, mobile devices, transmission media, electronic storage media and much more.

2. Gather data: Gather data on where you store, receive, maintain or transmit ePHI. You may need to look at more than a single department check out any data exchanges between vendors and business associates, as well as any ePHI in different physical locations or electronic media. Also, you must document how, when and what data-gathering activities you performed.

3. Identify and document potential threats and vulnerabilities: You're not looking for any and all conceivable threats, but instead you should identify and document all "reasonably anticipated" threats. Examine threats based on these categories:

Natural -- floods, earthquakes, tornadoes, landslides.

Human -- intentional or unintentional actions (e.g., unauthorized access to e-PHI, network and computer based attacks, malicious software upload, inadvertent data entry or detection, inaccurate data entry).

Environmental -- power failures, pollution, chemicals, liquid leakage.

4. Assess current security measures: Compare your existing security measures with the potential threats and vulnerabilities you've identified. Evaluate all your security measures (technical and non-technical), such as your access controls, authentication, encryption methods, automatic logoff and audit controls, as well as your policies, procedures, guidelines, accountability and responsibility, and physical and environmental security measures.

5. Determine the likelihood of threat occurrence: Weigh the probability that a threat will trigger or exploit a particular vulnerability, and then estimate the potential impact on your organization. Categorize each specific threat as "high likelihood," "medium likelihood" or "low likelihood." Use your determinations to create a list prioritizing your risk mitigation efforts.

6. Determine the potential impact of threat occurrence: Estimate the possible threat's potential outcome or

impact. This may include: unauthorized access to or disclosure of ePHI; permanent loss or corruption of ePHI; temporary loss or unavailability of ePHI; loss of physical assets; or loss of cash flow. Similar to ranking likelihood, organize the potential impacts as "low," "medium," and "high."

7. Determine the level of risk: Cross-reference the likelihood rankings with the potential impacts to determine your risk level for each identified threat. Risk ranking helps you to prioritize mitigation activities -- meaning, what you should fix first. Look at any potential threats that rank "high" on both the likelihood and impact scales.

8. Identify security measures and finalize documentation: Beginning with the highest-risk items, identify the security measures necessary to manage the risk. When evaluating appropriate security measures, consider their:

Effectiveness;

Related legislative or regulatory requirements for implementation; and

Relation to your own organization's policies and procedures.

Although the HIPAA Security Rule requires that you document the risk analysis, it doesn't provide or require a specific format. Try this: You can create a risk analysis report to document your process, the output of each step and your initial identification of security measures, CMS suggests.

Resource: To view the complete risk analysis guide, go to http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf