Remaining HIPAA compliant: How to protect patient records

Mark Norris
Publish Date: FEB 10, 2014

Probably the least understood and greatest exposure and risk for practices attesting to Meaningful Use (MU) is the need to complete a security risk analysis. When it comes to the technical concepts like firewalls, routers, and security protocols, most offices just do not know where to begin. You trust your vendors and business associates to keep you compliant, but what if they do not?

The use of health information technology continues to expand in healthcare. Although these new technologies provide many opportunities and benefits for consumers, they also pose new risks to consumer privacy.

Because of these increased risks, the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) include national standards for the privacy of protected health information, the security of electronic protected health information, and for breach notification to consumers. HITECH also requires Health and Human Services (HHS) to perform periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

What is a security risk analysis?

A security risk analysis involves analyzing vulnerabilities and threats to your system to safeguard electronic protected health information (E PHI). It means reviewing your policies, practices, and systems and correct any issues that may make EPHI vulnerable.

- Review Existing Security Of Protected Health Information
- Identify Threats And Vulnerabilities
- Assess Risks For Likelihood And Impact
- Mitigate Security Risks
- Monitor Results

Source: The Office of the National Coordinator for Health Information Technology
Many of the MU measures are already familiar to practices. Actions such as gathering vitals, demographic documentation, and medication histories physicians can perform in their sleep. While learning the interface of their new Electronic Health Record (EHR) system is a very real obstacle, in time, staff learn what button to push and box to click to be compliant.

But the technical issues can be much trickier for physicians, who aren't necessarily IT experts.

An example: In a recent visit at a rural practice, a national telecommunications provider had been onsite to upgrade the practice’s broadband connection. In the process, they disconnected the firewall because they could not configure it correctly, and left it unplugged. They did not notify the practice of their actions and left after assuming completion of the job.
It was not until a week later, when the practice network went down and they called in their local hardware vendor, that they discovered the potential breach situation. The practice, through no fault of its own, was completely exposed. In a follow-up call to the vendor, they responded, “We don’t know what you are talking about.” Really? This time everyone got lucky.

Here is what medical practices attesting to meaningful use stage 1 need to know about completing a security risk analysis.

Risk analysis explained

The Centers for Medicare and Medicaid Services (CMS) defines the requirement this way: The practice must “Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities and conduct or review a security risk analysis per 45 CFR 164.308(a)(1), implement updates as necessary and correct identified security deficiencies as part of the eligible providers risk management process…”

Do you really understand what that means? If not, you are not alone. A lack of technology expertise is the problem. You are not an IT guru and must depend on others, who may not be protecting your best interests.

To make a simplistic medical analogy, a security risk analysis is the examination and testing you do to assess clinical risk and diagnose a clinical condition applied to your practice’s information technology infrastructure and operations. Just as you use a diagnosis and other clinical data to plan treatment, you will use the risk analysis to create an action plan to make your practice better at protecting patient information. Further, privacy and security are like chronic diseases that require treatment, ongoing monitoring and evaluation, and periodic adjustment. A security risk analysis is a systematic and ongoing process of both:

- Identifying and examining potential threats and vulnerabilities to protected health information in your medical practice.
- Implementing changes to make patient health information more secure than at present, then monitoring results (i.e., risk management).

The HIPAA Security Rule requires covered entities to conduct a risk analysis to identify risks and vulnerabilities to electronic protected health information (EPHI). Risk analysis is the first step in an organization’s Security Rule compliance efforts. Following HIPAA risk analysis guidelines will help you establish the safeguards you need to implement based on the unique circumstances of your healthcare practice.

After completing a risk analysis, which will identify your areas of risk, policies and procedures

<table>
<thead>
<tr>
<th>Security Components</th>
<th>Examples</th>
<th>Examples of Security Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>• Your facility and other places</td>
<td>• Building alarm systems</td>
</tr>
</tbody>
</table>
must be put in place to document and mitigate these risks. Risk analysis is an ongoing process that should provide your medical practice with a detailed understanding of the risks to the confidentiality, integrity, and availability of EPHI.

HIPAA requires that covered entities “implement policies and procedures to prevent, detect, contain, and correct security violations” by conducting “an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the [organization].”

Providers should develop a risk analysis that addresses these criteria by evaluating the impact and likelihood of potential breaches, implementing security features, cataloguing security features, and maintaining security protections.

**HIPAA Omnibus final rule summary**

There are three areas that physicians will need to focus on to comply with the new HIPAA rules:

- **Privacy, security, and breach notification policies and procedures (and in some cases, new workflows and forms),**
- **notice of privacy practices,** and
- **business associate agreements.**

All of these forms must be updated. This updated documentation to identify your risks and how you will address them must be dated during the attestation period, not after.

The bottom line is this: If you do not document it, you did not do it.

*Mark Norris is chief executive officer of Medical Record Services, Inc., which works with practices on meaningful use compliance, privacy and security, and attestation. He is former executive director of NEO HealthConnect, one of The Ohio Health Information Partnership’s (OHIP) seven Regional Extension Centers (REC). He oversaw 350 primary care physicians on issues of meaningful use compliance and attestation.*