# How Small Organizations Handle HIPAA Compliance



By Debi Primeau, MA, RHIA, FAHIMA

Smaller healthcare facilities typically lack the resources and expertise to address the constant flow of competing priorities, forcing leadership to wear many hats in a fragmented environment. Few have a designated privacy, security, or compliance officer, let alone the corporate support staff afforded by larger organizations. While HIPAA compliance may be recognized as a top priority, proper preparation often gets pushed to the bottom of the list.

When it comes to privacy and security, small, freestanding, individual providers are at the greatest risk of a breach. New external threats arise every day, along with inadvertent internal staff errors. Smaller, rural practice settings are especially high-risk target areas for a breach, as are:

- Behavior analysis providers
- Small ambulatory and specialty centers
- Practices acquired by a larger medical group

This article examines how smaller organizations are dealing with HIPAA compliance and suggests strategies to reduce audit risk and the threat of a breach.

**Take These Steps Now to Prevent Risk**

- Identify someone internally or externally to conduct a privacy and security risk analysis. If you've already identified a privacy/security officer, that person would be the logical choice.
- Be aware that a security analysis does not cover privacy areas. Although there is crossover, a privacy breach can occur despite a thorough security analysis.
- Begin with a security risk analysis to meet HIPAA compliance.
- Consider contracting with an outside vendor to conduct a privacy and security analysis if internal resources are not available.
- Assign a level of risk for all findings: high, medium, low. Tackle high-priority findings first—where your organization is most at risk—then progress to medium and low findings.
- Create a project plan to proactively remediate findings from the privacy and security risk analysis.

## Begin with a Risk Analysis

Protection against a security breach begins with establishing the correct identity of the patient during the initial check-in and registration process. That breach prevention must continue throughout the visit, at discharge, and during follow-up care—and then extends to the short- and long-term storage of any information/data created during that care encounter for as long as the information is retained. That is a big job that covers a lot of potential breach scenarios—which makes conducting a risk analysis a practical first step to see just what coverage gaps exist, and where holes appear in the defense of patient information.

Strategy presented in the "Leading the HIPAA Privacy Risk Assessment" article, posted in AHIMA's HIM Body of Knowledge, suggests three key reasons for performing a risk assessment:[1]

- System weaknesses can subject the organization to liability for breach of confidentiality and invasions of privacy.
- Inappropriate uses or disclosures of information can result in negative publicity, driving patients to choose other healthcare providers.

- System flaws and loopholes can result in corruption or loss of vital data, or inappropriate alteration or manipulation of data.

With these issues in mind, smaller organizations can develop practical strategies for HIPAA compliance—even with limited resources.

At one California-based specialty surgical hospital, a breach event occurred during the spring of 2015 despite confidence in the organization's privacy/security compliance. Immediately after the breach, the compliance team participated in a complete privacy and security risk analysis. The review provided compelling information on the most likely targets of another breach.

Responding to the analysis and overcoming deficiencies quickly was difficult and often overwhelming. Though the project required significant manpower and funding, the analysis established a critical baseline for compliance along with goals going forward.

The hospital continues dedicated efforts to address deficiencies and expand staff education. To that end, staff must participate in regular training sessions to keep abreast of privacy and security concerns. Ongoing education reduces the risk of unintentional disclosures in discussing privacy issues or leaving documents in common areas, while emphasizing the importance of observing and reporting suspicious events.

Of utmost importance, education and training should incorporate the development, implementation, periodic review, and revision of related policies and procedures. Employee orientation and annual reorientation in these areas are among the best strategies for proactively addressing problem areas.

# Develop Policies and Procedures

Developing meaningful, effective policies and procedures that meet an organization's specific needs is crucial. Resorting to a "boilerplate" template to save time and resources is not a wise choice. Organizations must be able to show an auditor exactly how certain practices follow established policies and procedures. In the risk analysis work done with the surgical hospital, and other small organizations, risk analysis findings revealed five areas to address in developing policies and procedures:

- High-profile patients
- "Bring Your Own Device (BYOD)" and remote wipe
- Confidentiality, storage, destruction, and disposal of personal health information (PHI)
- Encryption
- Physical security—alarms, storage, and limiting access to PHI

## High-profile Patients

Large health systems typically take measures to protect the privacy of high-profile patients such as political figures or celebrities. Likewise, smaller facilities must make sure records of high-profile patients, such as the mayor, chamber of commerce members, and others well known in the community are kept private and confidential. One option is to assign assumed names for these individuals and restrict access to the "need to know" list. This authorization can be handled within the electronic health record (EHR). However, a "break the glass" policy should be in place to allow internal access for treatment, administrative, or other specific purposes. Frequent audits are necessary to determine who is accessing information and whether they have a legitimate need to know.

## BYOD and Remote Wipe

Many small organizations do not have a BYOD policy. With the proliferation of personal laptops, tablets, and smartphones, BYOD policies and procedures are needed to define whether physicians, nurses, and administrative staff are allowed to access PHI on personal devices. And if so, what are the parameters? Are the devices encrypted? Are employees required to sign a "remote wipe" policy in case a phone is lost or stolen? (Remote wipe is a security feature that allows a device owner to remotely delete data from a lost mobile device.) To avoid such complexities, many large providers internally issue staff members phones, which can then be more easily secured and controlled. This can be cost prohibitive for small providers, but may be worth the investment to protect PHI.

### Confidentiality, Storage, Destruction, and Disposal of PHI

Ensuring proper retention and destruction of PHI in any format—paper or electronic—is critical. Policies and procedures should address the following: How and where will you securely store paper records? How will you dispose of those no longer needed? Is there a business associate (BA) agreement to destroy paper documents so they are not discoverable? For electronic PHI, what are the guidelines for keeping or archiving information?

Every healthcare organization, regardless of size, must have a retention and disposal program in place—a core principle of information governance. And with hacking, phishing, and ransomware attacks on the rise, data backup is more important than ever.

### Encryption

While most providers know they should have an encryption policy, many fail to create one. However, the industry is seeing a shift as more small practices realize the need to make encryption a requirement to protect PHI. Lack of awareness is no excuse. Encryption is a must.

### Physical Security

Physical security includes the use of alarm systems along with proper storage and access to PHI. A prime example is a breach that occurred as a result of access to a laptop located in an unlocked office. In another case, paper files were stored in the employee break area, allowing easy access to the documents. Small providers with limited space often face storage issues that must be resolved to protect PHI.

## Common Issues and Practical Strategies

The following are some common privacy and security issues smaller organizations face and some practical strategies for solving the issues.

### Update Job Descriptions

Job descriptions for privacy and security must be fully documented. Who will assume privacy and security roles? What are their specific responsibilities? For example, in one case seen by the author of this article an employee was designated as a security officer but it was not documented in the job description. This could cause problems during an audit. Dual roles are not uncommon. Sometimes an IT director serves as a security officer. An HIM or compliance director may serve as a privacy officer. In such cases, be sure job descriptions specify roles and responsibilities.

### Auditing and Monitoring

Managing competing priorities can result in a reactive approach to important processes, especially routine auditing and monitoring. Many say they'll audit if a potential problem arises—a strategy that could lead to a breach. Routine monitoring and reporting can indicate in advance who might be accessing information. A proactive approach is best practice.

### Notice of Privacy Practices

A Notice of Privacy Practices must be posted on all covered entities' websites and must contain all elements required under the HITECH-HIPAA Omnibus Rule. Review and make sure this notice is properly posted and that documentation demonstrates compliance with security, breach, and other provisions as required with BAs.

### Legal Health Record

The designated record set must be clearly defined and documented. Does it include records from other facilities? Does it include internal and external communication? Many providers struggle with the meaning of the legal health record and the definition of the designated record set. Educational efforts can alleviate confusion and avoid issues during an audit.

### Risk Assessment Resources

Does your organization have the internal resources and expertise to conduct the required risk assessment? Like many small facilities, the California surgical hospital mentioned above discovered it lacked the internal resources to meet this requirement. Partnering for outside support and access to assessment tools may be a viable option. Also, the Office of the National Coordinator for Health IT in collaboration with the Office for Civil Rights offers a security risk assessment tool to help guide the process, available at www.healthit.gov/providers-professionals/security-risk-assessment-tool.

## Risk Analysis is Not Optional

While cost and complexity are realistic concerns, private practices and small provider organizations should engage in risk analysis as a proactive means of breach prevention. This requires regular review of administrative processes, physical safeguards, and technical capabilities. Routine risk analysis is a requirement, not an option.

## Note

[1] Callahan Dennis, Jill. "Leading the HIPAA Privacy Risk Assessment." AHIMA Convention and Exhibit presentation, October 2001.

*Debi Primeau (dprimeau@primeauconsultinggroup.com) is president, Primeau Consulting Group.*

**Article citation**:
Primeau, Debra. "How Small Organizations Handle HIPAA Compliance" *Journal of AHIMA* 88, no.4 (April 2017): 18-21.