PHYSICIANS PRACTICE
YOUR PRACTICE YOUR WAY

Published on *Physicians Practice* (http://www.physicianspractice.com)

Navigating a HIPAA Breach at Your Medical Practice

Blog | February 24, 2015 | HIPAA, Healthcare Reform, Law & Malpractice, Patients, Risk Management
By Douglas M. Nadjari

A HIPAA data breach can bring a healthcare provider to its knees, as demonstrated by a large New York hospital system which entered into a $4.8 million settlement with the government, stemming from a personal information breach of more than 6,800 patients. Breaches in the healthcare industry can result in costly investigations and compliance efforts, litigation, catastrophic fines, and the dismissal of the officers and employees on whose watch the breach occurred. While the fallout can be catastrophic, an understanding of the rules, an awareness of a system's vulnerabilities, and some simple precautions can minimize the risks to the entity and its patients.

UNDERSTANDING A HIPAA 'BREACH'
A HIPAA "breach" is the unauthorized acquisition, access, use, or disclosure of unsecured personal health information (PHI) that compromises the security or privacy of the information. Since HIPAA Breach notification rules were enacted in 2009, over 1,000 reported breaches have compromised the personal data of more than 22.5 million Americans. The Office of Civil Rights (OCR) for HHS is charged with conducting proactive HIPAA audits, investigating complaints, and enforcing the nation's HIPAA security rules. When a misuse of PHI is suspected, a thorough analysis must be conducted and a determination made as to whether the breach must be reported.

In 2013, the regulation defining the parameters of a reportable breach changed dramatically, via the release of the HIPAA final omnibus rule. Previously, a reportable breach existed only if there was a significant risk of financial, reputational, or other harm. The new definition dispenses with the harm standard. Now, the entity must presume that the acquisition, access, use, or disclosure of PHI is a reportable breach unless it can demonstrate a "low probability" that PHI has been compromised.

Douglas M. Nadjari

REPORTING HIPAA BREACHES

If the risk is high or affects 500 or more people, a report to OCR from the medical practice is required. Furthermore, the Federal Trade Commission has issued its own Health Breach Notification Rule, requiring certain businesses not covered by HIPAA, such as vendors of healthcare records, to notify customers and others of the breach. State law may impose additional requirements. For example, New York may require reports to the state attorney general, the state department, the New York State Police, the state's office of professional medical conduct, the three major credit reporting agencies, and notification to the news media.

As soon as the breach is discovered, it is critical to retain a public relations firm with strong experience in crisis communications and reputation management capable of providing a strategic approach and assistance in the creation and implementation of a formal response plan for media and patient inquiries. The long-term health of the practice depends upon maintaining its reputation and the trust of its patients.

The costs of cooperating with OCR investigations and its potential fines are not the only source of exposure. Other costs include locating and notifying patients, extensive internal investigations, counsel to assist in risk assessment and breach reporting, credit monitoring, and incalculable reputational loss. The failure of executives to be proactive or ahead of the "hacking curve" can lead to the resignation of CEO and chief information officer positions. While HIPAA does not create a private right of action, it nonetheless "sets the bar." At least 10 states recognize it as the minimal standard for the protection of personal data, and the failure to meet that standard may form the basis for negligence cases. While shareholder derivative actions have traditionally been brought against officers and directors for failure to exercise due diligence in performance of their duties, legal experts see no reason why such rationale will not be applied to publicly held covered entities or their business associates.

12 HIPAA TIPS FOR YOUR PRACTICE

Minimize the risk of a breach with multi-layered and updated security protocols:

1. If a breach is suspected, act swiftly and decisively. Work with counsel to coordinate the investigation; engage your IT and PR departments (internal or external). Outside counsel will help determine whether a report is required, respond to OCR demands for further disclosure, and deal with the related fallout.

2. Keep HIPAA compliance plans current and implemented.

3. Update hardware and software consistently and ensure IT systems can accept downloads or patches designed to address current threats.

4. Conduct ongoing risk assessments that identify, address, and track system vulnerabilities.

5. Implement a formal response plan that includes a "response team" of appropriate inside personnel, outside counsel, and, if mass notification is required, an experienced PR firm to handle media and patient inquiries.

6. Change passwords regularly. Use automatic log-offs, screen savers, etc to protect on-screen information and access to practice computers.

7. Limit IT administrator controls to a few identified personnel.

8. Make sure vendors pay more than "lip service" to your latest HIPAA Business Associate agreements. Ensure they use "two-factor" identification and encryption software.

9. Train all new employees on HIPAA and conduct periodic HIPAA training for all personnel.

10. Be aware of unauthorized electronic equipment usage and unsecured paper containing PHI. Implement a "see something, say something" policy at your practice.

11. Limit the use of personal devices, flash drives, laptops, smart phones. PHI must be encrypted and these devices aren't often secure.

12. Explore data security breach insurance options, with awareness of the modest limitations of some policies.

Douglas M. Nadjari *is a partner in the law firm of New York-based Ruskin Moscou Faltischek, PC, where he is a senior member of the firm's healthcare, cyber-security, and white-collar crime departments. E-mail him here.*