Connecticut Law Tribune
May 12, 2014 ctlawtribune.com An ALM Publication

HEALTH LAW

HIPAA Breaches: Getting It Right

Steps providers should consider when faced with a breach

By JOAN W. FELDMAN and WILLIAM J. ROBERTS

Anyone who has been to a doctor's office in the last 12 years, by now, knows that the federal government enacted a privacy and security law known as the Health Insurance Portability and Accountability Act. If you have actually taken the time to read the notice of privacy practices presented to you by your doctor, you would know that HIPAA offers patients certain protections with respect to their health information, including notifying them of a "breach" of their health information.

Joan W. Feldman

William J. Roberts

Health-care providers have an enormous amount of information about their patients that is essential for them to provide treatment, operate their facilities and receive payment for their services. Unfortunately, and most often unintentionally or inadvertently, this health information may be accessed or disclosed by or to an unauthorized third party. When this happens, providers must respond swiftly and precisely to mitigate any harm to the subject patients. The following sets forth an overview of the steps providers should consider when confronted with such a breach.

- **Be prepared.** If you have not already organized a breach response team, identify the individuals who will be determining: (1) whether an actual breach occurred; (2) the extent of the breach; and (3) the response. Typically, this would include the privacy officer, the security officer, a representative from human resources, in-house counsel and, if appropriate, your communications or public relations staff.
- **Investigate the breach.** Before beginning the investigation, determine whether it will be conducted at the direction of legal counsel and, thus, protected by the attorney-client privilege. If the breach occurred as a result of a crime, a police report to the local police department may be indicated. Given that the breach is most likely the result of conduct involving the provider's employees or agents, the provider must conduct interviews of the individuals involved in the breach to determine how the unauthorized access or disclosure occurred. These interviews should be conducted with more than one person present and if the provider's employees are protected by a collective-bargaining agreement, a union representative may also attend the interview. If the breach

Joan W. Feldman is chairwoman of Shipman & Goodwin's health law practice group and represents health-care providers in health-care, business, regulatory and administrative law matters, including corporate governance, privacy and HIPAA issues, government audits and investigations, mergers, acquisitions and Medicare and Medicaid fraud and abuse. She can be reached at jfeldman@goodwin.com. William J. Roberts is a member of the firm's health law practice group and life sciences and medical products client team. He advises clients on corporate and regulatory compliance, privacy breaches, fraud and abuse, contracting, licensure, government investigations, and risk management issues. He can be reached at wroberts@goodwin.com.

involved unauthorized access to an electronic network, or a lost or stolen mobile device, laptop computer or other electronic storage medium, you may want to engage a forensic information security expert to determine the scope and nature of the possible access by unauthorized third parties.

- **Risk assessment.** Once you have conducted your investigation, a determination must be made with respect to whether the unauthorized access or disclosure constitutes a breach under HIPAA. It defines a breach as any use or disclosure of unsecured health information in violation of HIPAA, unless there is a low probability that the health information has been compromised, or an exception under HIPAA applies.

At least the following four factors should be considered in determining whether there is a low probability that the health information has been compromised: (1) the type and amount of information involved in the incident (e.g., the health information involves sensitive information such as behavioral health or financial information); (2) the identity of the recipient of the unauthorized disclosure (e.g., the patient's rheumatologist versus the patient's oncologist); (3) whether the information was actually accessed by the third-party recipient; and (4) the extent to which the provider mitigated the potential for access (e.g., prompt remote wiping of the electronic device).

With respect to whether a HIPAA exception applies, determine whether: (1) the access was unintentional and in good faith by a workforce member acting within the scope of their authority; (2) one workforce member authorized to access the health information disclosed it to an unauthorized workforce member (and is not further used or disclosed in violation of HIPAA); or (3) the provider has a good-faith belief that the recipient of the health information would not reasonably have been able to access such information (e.g., a medical record was provided to the wrong patient but the wrong patient never had the opportunity to review the record, or an email was sent to the wrong recipient but forensic analysis determined that the attachment containing the health information was never opened).

If a breach involves more than 500 individuals in one state or jurisdiction, the provider must notify the local media of the breach.

- **Responding to the breach.** Once you determine that a breach occurred under HIPAA, reporting obligations must be identified. All HIPAA breaches must be reported to the Office for Civil Rights of the U.S. Department of Health and Human Services. On receipt of notice, the OCR may request specific information regarding the breach. Please note that HIPAA breaches may also trigger reporting obligations under various state personal information privacy laws. For example, in Connecticut, if the information was in electronic format and contained a combination of the patient's last and first name or initial and Social Security number, driver's license, state identification number or certain financial account information, the provider must notify the Connecticut Office of Attorney General of the breach. There may be additional regulatory reporting obligations depending on the nature of the provider's operations, such as to the U.S. Department of Education or the Federal Trade Commission.
- **Mitigating harm to the patient.** Patients must be timely notified of the breach. The sooner the patient is made aware of the breach, the sooner the patient can be put on alert for any possible identity theft or other harm. Depending on the nature of the breach, the provider may offer the patient credit-monitoring services for a specific duration of at least one year along with identity-theft insurance. Typically, patients are informed of the breach by letter and told of the various services being offered by the provider to mitigate any harm to the patient. Many providers choose to establish a toll-free telephone service for patients to call and have their concerns and questions regarding the breach addressed. If a breach involves more than 500 individuals in one state or jurisdiction, the provider must notify the local media of the breach. Most providers choose press releases and provide information for the subject patients on their websites.
- **Plan of correction.** Concurrently, the provider must conduct a root-cause analysis to determine how and why the breach occurred. Review of current policies, employee training, and existing privacy and security practices must be conducted promptly to address any deficiencies or areas for improvement. If the breach was caused by an employee or contractor misconduct, disciplinary action may be appropriate, including termination of the employee or contractor. Typically, the individuals involved in the breach will need to undergo additional remedial training.

Preparation Is Key

Despite formidable privacy and security practices, most providers will undoubtedly experience breaches given the large amount of individuals involved in the delivery of health care and the opportunities for inadvertent disclosures. It is important to be prepared and to respond in a timely and comprehensive manner in order to mitigate any potential harm to the subject patients and the provider alike. Providers who are lax in responding and mitigating potential harm may face significant penalties and regulatory enforcement. ■