Disgruntled or Dishonest Employees May Be the Source of a Security Breach

With all of the security breaches in the news recently, many medical practices have taken extra steps to keep their patient records safe. Employee training and awareness, installation of virus and malware protection, regular data back-up, purchase of a cybersecurity insurance policy, and hiring an IT person to help keep systems up to date are examples of ways to make a medical practice more secure. However, no matter what is done to protect sensitive data, sometimes the biggest threat to patient records is located right in your office.

Employees must have access to sensitive data, such as patients' protected health information (PHI) in order to perform their job duties. However, sometimes employees will access information that is outside the scope of their employment. Employee access of PHI without a job related reason could be considered a criminal violation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. In addition, this type of unauthorized access of PHI generally requires the practice to notifiy the patient, government and in some cases the local media under the Breach Notification Rule.

Many times, a breach of PHI is unintentional. A patient's PHI may be inadvertently mailed to the wrong patient, or a patient's lab results are accidentally handed to the wrong person. However, in some cases an employee may have less than honorable intentions when accessing sensitive data. In all cases, the SVMIC policyholder should report the incident as soon as it is discovered to the claims department.

The following are examples of actual claims that illustrate circumstances when an employee was the source of a breach. These claims are being responded to by NAS Insurance Services either through the coverage included in the SVMIC professional liability policy or in additional limits purchased through SVMIC's partnership with NAS:

- A practice received an anonymous call advising that a current employee was selling their patients' personal information. The caller proved this by giving the manager names, social security numbers and dates of birth of three patients.
- A long time billing employee was terminated. It was discovered that he had run several reports including patient data that were unrelated to his job duties. It is unknown for what purpose he gathered the information. In addition, he had previously admitted to another employee that he had taken credit card receipts with account information for many patients, and two receipts were found in his desk.

Fortunately, to date there have not been any complaints from patients regarding their credit card accounts.

Disgruntled or dishonest employees are often at the root of cybersecurity claims reported to NAS. In some circumstances, an unhappy employee may decide to take records with them when they leave, as in the following examples:

- Two employees left a policyholder's employment under unfavorable terms. The policyholder learned that these former employees downloaded patient information to a flash drive and took it with them when their employment ended. This claim is being covered under the cyber liability provision of the practice's SVMIC cyber coverage.
- An enterprising nurse left the employ of one plastic surgeon and went to work for a different plastic surgeon. The first practice was notified by several patients that they had received emails from the nurse advising them that she had left and inviting them to transfer their care to her new employer. This is unauthorized use of electronic data since she was no longer an employee. The practice's cyber liability policy will cover this situation.

As mentioned previously, to safeguard patient data, practices may rely on an IT expert. In order to do so, the IT expert is granted access to the entire system. However, if the relationship should ever become hostile and the trusted expert is no longer trustworthy, their access gives them the ability to destroy or otherwise keep data from being accessed by employees. For one medical practice, that is exactly what happened:

- The quality of work of the contract IT employee that the practice used for all of their computer work had deteriorated and it was time to end the employment agreement. There was a fee dispute, and in retaliation the IT employee remotely accessed the practice's computer systems and blocked the group's access to their billing and business records. The group's cyber liability coverage provided within their SVMIC policy is helping the practice recover any unavailable records.

Health and Human Services (HHS), the agency that enforces HIPAA rules, requires the practice to have protocols that outline the circumstances in which PHI can be accessed and what to do once unauthorized access is discovered. As a first step, a unique username and password for each employee who has access to sensitive data is one way to ensure that only those employees who are authorized to access patient records are able to do so. However, the responsibility of the practice does not end with a secure login. The HIPAA Security Rule requires certain administrative, physical and technical safeguards to be implemented to protect the confidentiality, integrity and availability of all electronic PHI that the practice creates, receives, transmits and stores. The following technical safeguards are outlined on the HHS website:

Technical Safeguards

- Access Control
- Audit Controls
- Integrity Controls
- Transmission Security

In addition to compliance with the HIPAA Security Rule, it is necessary that a practice have a plan in place for when a breach is discovered. For instance, there are steps to take to determine the extent of the breach. Once it is determined how many records are involved, there are rules regarding notification. These rules apply not only to a cyber-attack but also to the examples listed above. The following checklist can be found here:

In the event of a cyber-attack or similar emergency an entity:

- Must execute its response and mitigation procedures and contingency plans.
- Should report the crime to other law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation (FBI), and/or the Secret Service.
- Should report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs.
- Must report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting.

For more information regarding these security and response requirements, visit https://www.hhs.gov or https://www.healthit.gov. For additional information regarding the Breach Notification Rule and the steps that must be taken when a breach occurs, visit https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.
