When PHI Walks Out the Door with a Departing Employee

By Justin Joy, JD, CIPP

Several recent closed cyber claims involve a similar scenario: An employee[1] leaves the employment of a clinic, often on a voluntary basis. Several days or weeks later, the clinic receives reports from existing patients that the former employee is contacting the clinic's patients and encouraging them to seek care at the former employee's new or prospective location. After an investigation, it is discovered that the former employee continues to have access to some information about the clinic's patients. Given the sustained high rate of turnover in the healthcare industry, these scenarios are likely to continue.

While not all these scenarios result in a reportable breach, most involve the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the HIPAA Privacy Rule. As a result, an investigation and assessment must be conducted to determine whether notification to patients, HHS, and perhaps the media is required under the HIPAA Breach Notification Rule.[2] There are several steps that medical groups can take before, during, and following an employment relationship to

reduce the privacy and data security risks associated with a staff member's departure.

At the time a new employment relationship begins, the prospective or new hire should be presented with a confidentiality statement to sign that includes an agreement to return any devices, data, or other information the employee has access to during the term of employment. While the specific terms of such an agreement should be drafted in consultation with the group's legal counsel, generally, the individual should agree to perpetually maintain the confidentiality of any PHI that the individual encounters or has access to during or after the term of employment. Additionally, a prospective or new hire should agree not to use or attempt to access any PHI maintained by the group at any time following separation from employment.

Some privacy and data security practices that medical groups should be routinely performing may help discourage employees from intentionally taking PHI with them following the term of employment and may also reduce the risk of individuals doing so inadvertently. A fundamental component of a comprehensive security risk analysis includes performing a complete inventory of all devices and media where PHI is stored. Relatedly, an updated list of all accounts assigned to current employees who have access to PHI should also be maintained. The inventory and account list should be regularly reviewed to confirm that a device or account assigned to an individual who is no longer employed has been promptly addressed. Groups that allow employees to utilize their personally owned devices ("BYOD") to create, store, and transmit PHI should have a clear BYOD policy in place stating, among other things, how the devices will be controlled by the group and an understanding from the employee that any PHI on the device will be remotely wiped at the time of employment separation.[3] Of course, in order to remotely erase a mobile device, the group must have some control over the device through a mobile device management service. In some contexts, groups may consider deploying a data loss prevention (DLP) solution to help enforce administrative policies addressing improper retention or transfer of sensitive data. As required by the HIPAA Security Rule, covered entities should also regularly review their procedure for information system activity review (e.g., an audit log review) and confirm that the procedure is properly in place. As part of initial and recurring training, as well as in periodic security reminders, a group should be clear about its system activity review efforts. Among other benefits in such transparency, an enterprising, perhaps soon-to-be-former-employee may think twice about accessing and copying patient information if he or she knows that such activity is subject to being monitored.

Medical groups should have comprehensive policies in place about the various steps, including those related to information security, to be taken at the time of employment separation, regardless of the reason for the end of the employment. When an employee has given notice of their intention to resign or if an employee has been terminated, a spot check of their activity over the preceding days or weeks in the electronic medical record may reveal an anomalous pattern of use which may give rise to further investigation. Following the departure of a staff member, healthcare providers within the group should also be alert for unusual reports from patients about contacts from the former employee or

unknown telephone numbers. In the event that the group discovers an indication of an improper access or acquisition of PHI, including information which may still be in the possession of the now-former employee, the group should initiate its incident response policy for investigation into the matter.

Hackers are not the only source of privacy and data breaches. Medical groups must have safeguards in place to reduce the risks of privacy and security incidents caused by current employees, as well as staff members that are leaving the employment of the group, regardless of the reason.

If you experience a cybersecurity or other HIPAA-related incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak with the Claims department.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage® account here.

[1] Many state medical boards have rules addressing patient notification of a physician's departure from a group. For example, in Tennessee, the applicable rule provision addressing records of physicians upon departure from a group provides that "the responsibility for notifying patients of a physician who leaves a group practice whether by death, retirement or departure shall be governed by the physician's employment contract." The rule also provides criteria regarding which patients must be notified, and the content of the notification. Physicians should be familiar with the relevant provisions for patient notification in their employment agreements. Likewise, groups should know how to properly execute these provisions in the event of a physician departure, while also remaining mindful of their obligations under the HIPAA Privacy and Security Rules for safeguarding PHI (which includes patient name and contact information).

[2]. These instances may constitute a security incident. For obligations related to responding to such an incident, see the article, "Obligations of Medical Practices in Responding to Data Security Incidents (Not Just Data Breaches)." Even for those situations not constituting a security incident, such as incidents involving paper form PHI, the requirements are similar in the context of the HIPAA Breach Notification Rule's presumption that any an acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule is (with few exceptions) presumed to be a breach.

[3]. Employees should also understand that devices they personally own but are managed by the group will be remotely erased in the event the device is lost or stolen.

---

change over time.