By Lauren A. Suttell

Your Employee Caused a HIPAA Breach – Now What?

Insider breaches account for the majority of healthcare data breaches and security incidents.[1] So it should come as no surprise to you when you find out that one of your staff members faxed the wrong patient information, your receptionist opened spam email and hackers accessed your server, one of your clinicians lost his or her cell phone or laptop, or one of your physician employees shared patient information at a cocktail party last weekend.

But now what do you do?

The approach in each instance should be threefold – investigate, mitigate, and enforce. Hopefully, you have an incident response plan that spells out in detail the steps required to investigate the who, what, when, where, why and how of the incident. You should take appropriate steps to mitigate the harm (actual or potential) posed by the incident. And hopefully your employee handbook, policies and agreements set out the potential repercussions for the particular employee involved. If these steps are transparent and widely known within your organization, you will have a greater chance of detecting the incident and there will be no surprises for you or the employee involved (or your other employees who are watching the events unfold with great anticipation).

The appropriate consequences for an employee's breach will depend on the nature of the violation. Before passing judgment, your investigation should determine what happened, why and how it happened, and ultimately, whether HIPAA was violated. It may be appropriate to suspend the employee or place them on leave (with or without pay) pending the investigation.

Generally, an unintentional acquisition, access or use of patient information by an employee that was made in good faith and within the scope of his or her authority would not be a breach under HIPAA and would probably not result in any discipline.

At the very least, a breach should result in additional training for the employee involved, and potentially the entire workforce. Egregious and intentional violations may warrant termination. It is not illegal to terminate an at-will employee for a HIPAA violation. Recently, Lowell General Hospital fired an employee who accessed medical records without authorization or any legitimate reason for doing so. The Kansas Department for Aging and Disability Services terminated an employee who sent an unauthorized email with patient information to a group of its business associates. A diagnostic laboratory in Florida terminated an employee who disposed of patient records in a dumpster, rather than following company protocol that required such documents be securely shredded before disposal.

If the employee involved is a licensed professional, you may need to determine whether the circumstances warrant or require reporting to the state licensing board. Even if you do not report the employee's conduct, the state licensing board may investigate and impose sanctions on your employee anyway. In fact, in early 2018, a nurse had her license to practice suspended for twelve months by the New York State Education Department Office of the Professions after she disclosed patient information to her new employer and the new employer used such information to contact the patients about switching providers.

Special care and attention may be necessary if the employee has an employment agreement or is an independent contractor. An employment agreement or independent contractor agreement may set out the specific grounds for and procedures that must be followed in advance of termination. These agreements should be carefully reviewed with counsel before taking any remedial action against the individual.

Things may become more complicated if the individual is a partner of a medical practice (regardless of whether or not there is an employment agreement). Ownership of the practice does not (and should not) make an individual immune to consequences of a HIPAA violation, but it may be more difficult to expel such an individual from the practice if the underlying ownership documents do not adequately address the situation. The practice, its owners and counsel should review any employment agreement with the owner and any shareholders agreement, operating agreement, or partnership agreement to determine whether expulsion from ownership is possible and, if so, how it must be accomplished.

Lastly, you should also consider and weigh the degree of internal confidentiality versus transparency of the circumstances and consequences of a particular breach. The disciplinary actions taken in every incident set the tone within your organization, define your compliance culture, and establish expectations (or lack thereof) for future conduct. If repercussions are inequitably dealt (whether across clinical versus non-clinical or partner versus non-partner lines) this could create division within your organization and suggest to some that they are "immune" from harsher penalties than others.