Post-Breach: Preparing for a HIPAA Investigation

By Kelli Carpenter Fleming May 2019

Reprinted with Permission from the ***Birmingham Medical News***

The Office of Civil Rights ("OCR") is the federal agency that oversees compliance with the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations ("HIPAA"). In that regard, among other things, OCR conducts investigations following breach reports and imposes penalties and enters into corrective action plans as appropriate. In 2018, OCR imposed $28,683,400 in total settlements and judgments for HIPAA violations.

As with many governmental agencies these days, the manpower of OCR is limited, causing delays in investigations until years after the breach reports are filed. For example, in December 2018, we saw resolutions relating to breaches that were reported to OCR in 2013, 2014, and 2015, at least 3 years prior. This delay in enforcement by OCR makes documentation and preparation immediately following a breach extremely important.

Oftentimes, when a HIPAA breach occurs, providers are focused on providing the required notifications to both patients and OCR and then quickly move on. However, in light of the fact that an investigation may ensue years later, there are certain additional steps that providers should take to put themselves in a better position to respond to the investigation and to minimize the harm.

- **Mitigate and Cure the Breach.** When it comes to a resolution with OCR, taking steps to mitigate and cure patient harm is received favorably. For example, providers should offer credit monitoring services when appropriate. Under certain circumstances, providers should consider reporting the incident to the FBI and the police. Actions like these show OCR that you are taking the matter seriously and are responding appropriately to mitigate the harm to your patients.

- **Revise Policies and Procedures.** Following a breach incident, review your HIPAA policies and procedures and update as necessary in light of the incident. For example, if the incident involved a cyber-attack with infiltration by way of remote access, review how authorized individuals remotely access your system and add another layer of security (e.g., change passwords and require two-factor authentication). If the incident involved patient information that was removed from the physical premises, review your policies regarding when such removal is appropriate, who can remove patient information from the premises, what form the patient information takes when it is removed, and how to track patient information that has been removed and subsequently returned.

- **Training.** Following a breach incident, conduct training specifically aimed at the cause of the incident. For example, if the incident involved improper disclosure to the media, conduct training on what can and cannot be disclosed without patient authorization.

- **Document, Document, Document.** I cannot stress how important documentation is when responding to an OCR investigation, as employees depart and recollections fade over

time. As with a lot of things, when an investigation ensues, you will need to prove that you acted and responded appropriately, and the documentation serves as critical proof. In that regard, I suggest that providers complete a HIPAA Breach Assessment, which documents the who, what, when, where, and why of the breach incident. In addition, you should retain copies of the breach notification letters that were mailed to patients, as well as the breach report that was filed with OCR and any police/FBI reports that were filed. If the breach involves a cyber-attack, maintain documentation of the IT Report and security logs, reports, and scans. Document any and all steps you take to mitigate the harm, retain copies of all policies in effect at the time the incident occurred (as well as any new policies that were implemented in response to the incident), and document all training. All documentation should be retained for at least six (6) years.

When a breach incident occurs, if you can take appropriate steps to respond to the incident and to document what transpired, you will be all the more prepared for an investigation by OCR....when it eventually occurs several years later.

For more information, please contact:

Kelli Carpenter Fleming
Partner, Birmingham Office
P. (205) 458-5429
E. kfleming@burr.com

Kelli Fleming practices with Burr & Forman and works exclusively within the firms Health Care Industry Group.