PNPL

PANEL OF NATIONAL PATHOLOGY LEADERS

Topic of Interest for Members

Micro Highlight #7

HIPAA Breach Reporting – March 1st Deadline

for release – Tuesday, February 18, 2022

The March 1st **HIPAA Breach Report** deadline is quickly approaching for breaches of unsecured protected health information (PHI) involving fewer than 500 individuals. In addition to sending notification letters to individuals affected by a data breach, which must be done within 60 days of the discovery of the breach, HIPAA requires healthcare providers to report breaches of PHI to the Department of Health and Human Services' (DHHS) Office for Civil Rights (OCR). All HIPAA breaches involving fewer than 500 individuals that occurred in 2021 must be reported no later than 60 days from the end of the calendar year. Breaches involving 500 or more individuals must be reported to DHHS and to the media at the same time that the affected individuals are notified.

To help you navigate this reporting process, PNPL has consulted with **Dena M. Castricone, CIPP/US, CIPM**, of DMC Law, LLC. She recommends 5 important considerations for drafting an effective breach report, which can be found in her article "Drafting an Effective HIPAA Breach Report":

1. **Draft the breach report soon after completing the investigation.** While breaches involving fewer than 500 patients do not need to be reported to DHHS until 60 days after the end of the calendar year, it is best to craft the narrative portions of the report while the details of the incident are fresh in your mind.

2. **Use the Reporting Form Template.** The breach report has many elements and must be filed electronically. It is useful to print the reporting form template on DHHS's website to use as a guide in preparing to file the report. The report requires the following information:

   a. Number of individuals affected by the breach
   b. Breach start and end date
   c. Type of breach
   d. Location of the breach
   e. Type of phi involved
   f. Brief description of the breach
   g. Safeguards in place prior to breach
   h. Notice of breach
   i. Actions taken in response

   While all elements are important, the three discussed below are vital.

3. **Craft an Effective Description of the Incident**. The brief description section is the sole narrative-only component of the report, and it provides a critically important opportunity for you to demonstrate that your organization knows how to handle a breach. The relevant facts derived from the investigation should drive the narrative. Avoid commentary and judgmental statements. Be clear on the timeline and the results of the investigation. Finally, note the steps taken to mitigate risk and to ensure that a similar event will not occur in the future. The description should leave no unanswered questions and should convince DHHS that your organization understands its obligations under HIPAA and that there is no need for it to get involved.

4. **Accurately Note the Safeguards in Place.** After the brief description section, the on-line form presents a list of five possible safeguards in place prior to the breach. Those options are:

   a. None
   b. Privacy Rule Safeguards (training, policies and procedures)
   c. Security Rule Administrative Safeguards (risk analysis, risk management)
   d. Security Rule Physical Safeguards (facility access controls, workstation security)
   e. Security Rule Technical Safeguards (access controls, transmission security)

   For obvious reasons, selecting "None" will raise a red flag. Check all that apply. If you have a comprehensive HIPAA compliance program, then you should be able to check all the Privacy and Security Rule boxes.

5. **Detail the Actions Taken in Response**. The final section on the form provides a list of 14 post-breach actions including revised policies and procedures, trained staff, and implemented new technical safeguards. The 15th option is "other" and provides the opportunity to describe the "other" actions taken. It is best to check all those in the list that apply.

   Additionally, because none of the options in the list will comprehensively describe the steps you've taken, also check "other." Then use the narrative opportunity to provide details about the steps taken. This is important even if you mentioned those steps in the brief description. As with the brief description, the goal is to reassure DHHS that your organization handles breaches appropriately and understands the importance mitigation and prevention efforts.

   Take the time to describe your breach response efforts in the report. Avoiding further inquiry or an investigation is the goal. Once an investigation is underway, OCR can and will turn over many rocks and it almost always finds something, even things unrelated to the reported breach.