Health Information Compliance Alert

Toolkit: Don't Delay on Reporting HIPAA Breaches

Tip: Make timely breach reporting a practice priority.

With all that's going on in healthcare, you may have forgotten about HIPAA breach reporting. Unfortunately, the pandemic hasn't stopped privacy issues, data security incidents, or mobile device meltdowns; in fact, it has magnified them.

What do these things have in common? They often lead to HIPAA breaches for covered entities (CEs) that need to be reported. And the sooner you alert the Department of Health and Human Services (HHS) Secretary to the loss of protected health information (PHI) the better - don't stew over the breach or you will suffer the consequences.

Refresher: "According to the Privacy Rule, a breach is any acquisition, access, use, or disclosure in violation of the privacy rule - and that covers a lot," says **Jim Sheldon-Dean,** founder and director of compliance services at Lewis Creek Systems, LLC in Charlotte, Vermont.

If you uncover a HIPAA breach in your office, know that there are different timelines for reporting to HHS. The larger the breach the shorter the turnaround time to let the feds know the details.

Here's a basic breakdown of what you need to remember when reporting the violation to HHS.

Breaches that include more than 500 individuals:

- As a CE, you "must notify the Secretary of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach," notes the HHS Office for Civil Rights (OCR) breach notification guidance.
- Your breach notification must be filed electronically; plus, the data you submit and all information on the required forms must be complete and cover all aspects of the breach.
- You must notify the media - and similarly to alerting the Secretary, you must let the press know ASAP.
- You need to let the individuals know that their PHI was breached through first-class mail or in email within 60 days of the breach - if the impacted party has previously agreed to receive correspondences electronically, the OCR says.

Breaches that include fewer than 500 individuals:

- As the CE, you need to alert the HHS Secretary of the breach within 60 days of the calendar year in which the breach occurred. "For small breaches discovered in 2020, the deadline for reporting is March 1, 2021," remind attorneys **Laura Dona** and **Madison Pool** with Arnall, Golden, Gregory LLP in online legal analysis.
- You need to submit your forms electronically. However, even if your HIPAA breaches are on different days and concern different issues, you can still submit them on the same day.
- The individuals whose PHI was affected by the breach must be notified by first-class mail or email, too - within 60 days of the breach.

No matter the size or scope of the incident, all HIPAA breaches are reported through the OCR breach portal at https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true.

Remember: "Each breach must be reported, even if it affected as few as one individual," warn Dona and Pool.

Tip: Even a small practice can make an impact with HIPAA protocols by stopping breaches before they start and setting up BA agreements that are compliant. The initial task of creating resources and office compliance protocols can be daunting, but it's essential that you educate your staff and your BAs, setting up a breach management plan.

"The portal permits a business associate [BA] to report its own breach on behalf of the applicable covered entity, but the reporting obligation ultimately rests with the covered entity," acknowledge Dona and Pool. However, as the CE, you may want to "retain the reporting responsibility" to avoid problems, delays, and fines, they suggest.

Resource: Review OCR guidance on breach reporting at www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.