Health Information Compliance Alert

Breaching the Cloud: Crucial Action Points You Must Follow

What are your responsibilities versus your BA's?

You have a lot of issues to consider for moving your medical information to cloud storage. Beyond the preliminary issues, you also need to be prepared for the worst case scenario: a breach of your patients' protected health information (PHI).

The biggest part of your responsibility when there's a breach -- an unauthorized access to unsecured data that compromises the security or privacy of PHI -- is a "notice requirement," says **Wayne J. Miller, Esq.**, founding partner of the **Compliance Law Group** in Los Angeles. Under the Health Information Technology for Economic and Clinical Health (HITECH) Act, you must issue this notice to alert any individuals to the unauthorized access to their PHI.

In some cases, you have to notify only the patients affected by the breach. But in other cases where a breach affects or may potentially affect a large number of people -- typically 500 or more -- your notice requirement becomes far more onerous, Miller explains. With such large numbers, you would need to also notify the **Department of Health and Human Services** (DHHS), possibly posting on DHHS's website, and even alert the media.

Consider More Stringent State Laws

Under federal law, the notice requirement mandates that you provide written notification within 60 days of the breach. But you must look at your own state laws regarding such breaches, because these laws will preempt federal law when they're more stringent, Miller notes. And in some cases, state laws are far more stringent than federal law. For example, under California law, the breach notice period is just five days.

When you're developing your Business Associate Agreement (BAA) and working with your cloud-storage vendor, you must keep these notification requirements in mind. So if your notice period is 60 days, be sure that your BAA has a breach-reporting requirement of within 30 days, Miller advises.

Who Does What?

Aside from nailing down the notice requirement timeline, you have an even bigger job in preparing for a breach. You must ensure your policies and procedures -- and your training -- include clear directions to all your staff on what constitutes a breach and who should be contacted (even on nights and weekends), according to Washington, D.C.-based **Ober Kaler Attorneys at Law**.

Beyond these issues, you must detail what steps you and your cloud-storage vendor should take "immediately to ensure all data breaches are properly reported and addressed promptly," state Ober Kaler principal **James B. Wieland** and associate **Joshua J. Freemire** in a recent blog post at oberhealthinformationtechnology.com. Your BAA should specifically address each of these items in terms of what the vendor must do in response to a breach or suspected breach, as well as what your responsibilities are as the covered entity (CE).

CPT® 2023 American Medical Association. All rights reserved.