Health Information Compliance Alert

HIPAA Compliance: Pay Attention To 4 Key Areas That Will Rock Your HIPAA World

Get ready now for big changes to BAAs, enforcement, breaches and more.

Thanks to the recently finalized omnibus rule, you're in for a busy summer of revamping your HIPAA policies and procedures. Here's what you need to know to prioritize your work ahead.

The final rule brought together a slew of outstanding interim and proposed rules relating to HIPAA privacy, security and enforcement, most of which go into effect in September. Although the omnibus rule technically took effect on March 26, you'll have until Sept. 23 to come into compliance with most of its provisions, according to the law firm **Epstein Becker & Green** in a white paper.

Four major changes stand out the most in terms of what you'll need to do to stay in compliance: business associates (BAs), enforcement, marketing rule changes, and data breaches.

1. What's Changing for You & Your BAs

The omnibus rule makes significant changes to the definition of a BA, according to Epstein Becker & Green. The definition now includes the following types of entities as BAs:

- Health information organizations, e-prescribing gateways, and entities that provide data transmission services for protected health information (PHI) to a covered entity (CE) and that require access to PHI on a routine basis.
- Entities that offer personal health records to individuals on behalf of a CE; and
- Subcontractors that create, receive, maintain, or transmit PHI on behalf of another BA.

Traditionally, your BA's obligations were to comply with the BA agreement (BAA), which would dictate the requirements for using PHI with the CE, explains attorney **Wayne J. Miller, Esq.,** founding partner of the **Compliance Law Group** in Los Angeles.

New: But now that's changed. Not only does your BA need to comply with the BAA, but it will also be held liable under the law itself, Miller says. Another key change is a "trickle-down" effect that not only holds the BA directly liable for HIPAA violations, but also any subcontractors of the BA.

So even though the contractor or subcontractor with the CE is not actually a healthcare provider, they are now subject to direct enforcement actions and penalties if they're responsible for a HIPAA violation like a breach.

"Whatever obligations that this business associate takes on, they have to comply to the same extent ... of the law that the covered entity would," Miller states. The law also mandates that BAs provide PHI to the **Centers for Medicare & Medicaid Services** (CMS), patients and/or the CE, on request and pursuant to the law.

BAs also must participate in the breach notification process. If your BA has a breach on its side, the BA must notify you the CE properly and immediately. Additionally, BAs must now comply with the entire security rule, starting with the risk assessment, Miller says.

According to the final rule, the CE is responsible for reporting breaches on the BA or subcontractor level the BA isn't

necessarily obligated to report directly to patients or the government when a breach occurs. But the BA is responsible for reporting the breach to the CE, and this is where your BAA comes in.

You have 60 days maximum to report a breach to the government, and the clock starts ticking when you first discover the issue. You must build into your BA contract a far shorter timeframe for the BA to report any breaches to you so you can in turn report them to HHS and the affected patients.

Your responsibility: So along with these changes, CEs have more oversight responsibilities to ensure that their contractors are complying with all these new rules. You won't be directly responsible for the BA's compliance process, but you need to make sure that your BA is making appropriate strides to comply.

You also need to review your business relationships to ensure that you have BAAs in place including for those relationships with entities that now qualify as BAs under the new definition, states Epstein Becker & Green. And look over your current BAAs to ensure that they comply with the omnibus rule's requirements.

Bottom line: One thing that the final rule makes clear is that if the BA is really an agent of the CE, then the CE is responsible for the acts of the BA, Miller stresses. So you need the ability to oversee and audit the BA. And you may want indemnification provisions and warranties in your BA contract.

2. Brace Yourself for Heavier HIPAA Enforcement

Now the **HHS Office for Civil Rights** (OCR) will head all HIPAA enforcement activities. But OCR isn't necessarily where the enforcement ends, Miller warns. A HIPAA-related investigation could turn up concerns about improper payments, fraud and abuse, or Stark law violations. In these cases, you might also hear from the **HHS Office of Inspector General** (OIG).

Additionally, you could "hear from state agencies because they also have the authority to independently bring HIPAA actions as well as actions under their own state laws with respect to privacy and security of medical information," Miller notes.

The omnibus rule also increases the civil money penalties (CMPs) for HIPAA violations, raising the potential aggregate liability to $1.5 million. And a single event can produce multiple violations even for the simple fact that multiple patients are impacted by the event.

Example: If somebody stole a disk containing many patient names and health information, you could reach the $1.5-million penalty ceiling "based on the fact that each of the persons on that disk are potentially penalized or hurt by this mistake," Miller explains.

What's worse: And the $1.5 million isn't necessarily the end total penalty, "because there could be multiple different types of violations that can be identified even in a single event," Miller cautions. So say you had an unsecured disk that somebody stole, but you also didn't have policies and procedures in place, and you didn't mitigate the damages each of these could become a separate violation that could lead to additional penalties.

Another new responsibility you're facing is an "accounting of disclosures" requirement, which requires you to account for all disclosures of electronic PHI (ePHI), even if the disclosure isn't related to a data leak or breach.

3. Don't Let Your Marketing Cross the New Line

Marketing is another crucial area affected by the final rule. The rule attempts to greatly limit the situations in which you can do any sort of marketing without patient authorization.

The rule defines marketing in a very broad way by describing it as any communication that encourages the use of a

particular product or service, Miller says. Of course, there are exceptions. But if you're communicating via a letter, commercial, newsletter or other means regarding a product or service for which you're receiving financial remuneration from a third party, you must have patient authorization.

Example: A drug company wants you to market a new drug to your patients, and the company will pay you the cost of sending the marketing out to your patients. This is "a marketing event that requires prior authorization before sending it out to the patients," Miller states.

"So it's really important to look at ... the underlying facts of a particular communication as to whether or not you're now under the marketing rule, which basically is that if you're dealing with marketing (or what's defined as marketing), that needs prior authorization before you utilize PHI to disseminate that marketing," Miller explains.

As for the exceptions to this rule, you can send refill reminders to your patients without such authorization as long as the reminders contain no promotional language or materials for a particular third party, such as a drug or device company. Also, any face-to-face or other communications to promote general health or for patient education are excluded from the marketing rule if there's no payment by a third party involved.

Also: Another limited exception to the prior authorization mandate is if you're doing fundraising activities with your patients. If you want to fundraise with your own patients, you don't need prior authorization but you do need to provide patients with an opt-out choice to stop receiving those types of communications from you.

4. Follow New Procedures for Data Breaches

You already know that when a breach of unsecured data occurs, you must provide a notification. But the final rule changes what's considered a breach. Before, you could determine on your own whether a data leak actually constituted a significant breach, but now nearly all kinds of PHI leaks are breaches.

"You have to kind of assume you have a breach unless you can really prove ... by the facts that the data wasn't compromised in some way or that there was a low probability the data was compromised," Miller says.

And the more people who are affected by a data breach, the more people you have to notify, Miller notes. "And if you're talking about less than 500 [individuals] affected, you may have to make an annual notice to the department [HHS]."

Beware: Anything containing PHI that's unsecured is subject to the notification rule. This means any disk, email communication or other data that's not encrypted.