



© Sebastian Kaulitzki | Dreamstime.com

BUSINESS ASSOCIATE LIABILITY: HIPAA's New Hazard

By Steven Andersen

Think the Health Insurance Portability and Accountability Act is old news? Think again. Health care reform may have grabbed all the headlines this year, and companies will be sorting out the Patient Protection and Affordable Care Act for years to come. But in-house counsel who take their eyes off of HIPAA will get stung by new provisions soon to come online.

Enacted in 1996, HIPAA's regulations have rolled out in waves. Privacy rules went live in 2003, security requirements in 2005. At each step, companies had to change the way they thought about health care to be in compliance.

"One big challenge for in-house counsel was understanding that everybody's group health plan was a covered entity, and they had to do health plan compliance," says [Sarah E. Coyne](#), who chairs the health law group at [Quarles & Brady LLP](#). "It was a hard message to get out. The same concern applies to business associates, whether they're people in the business of shredding paper or making bicycle parts. They're not used to thinking of themselves as a regulated health care entity."

Every company had to create a compliance program and designate a privacy officer. In smaller companies, that usually meant an HR employee had to wear multiple hats and dance a complicated two-step with a lot of guidance from counsel. That is still a challenge, and it's not the end of the story. Yet another layer of businesses now have to come to terms with HIPAA's requirements.

Oblivious Business Associates

Buried deep in the 2009 financial stimulus package was a law that significantly reshaped HIPAA: the Health Information Technology for Economic and Clinical Health Act (HITECH).

"Most of the HITECH requirements became effective in February 2010," Coyne says. "One of the changes is that 'business associates' are now, for the most part, directly regulated by HIPAA, as opposed to just being contractually liable through their business associate agreements."

HIPAA's nomenclature can be opaque to the uninitiated, so it's critical to point out that the key phrase is "business associate."

Entities directly regulated by HIPAA fall into three broad categories: health care providers, health plans and health care clearinghouses, with mainstream companies covered under the health plan banner.

"Most companies with a health plan already are impacted by HIPAA," says [Kerry L. Moskol](#), a senior associate in Quarles & Brady's health law group. "Almost all of those companies have business associates, like third party administrators, who will be affected as well."

Business associates are entities that work with HIPAA-covered companies and come in contact with protected health information.

(Privacy, of course, is one of the prime functions of HIPAA, and protected health information constitutes just about anything identifiably related to an individual's treatment or payment for treatment.) Business associates who might see this type of data include billing services, accountants, auditors, outside administrators, IT contractors and law firms.

Understandably, there's considerable confusion on the matter. In response, on July 14, 2010, the Department of Health

HIPAA enforcement, which is already active, got a significant boost from HITECH.

"It's ratcheted up—hugely," Coyne says. "HITECH has a section called 'improved enforcement,' which was sort of an in-joke to us HIPAA geeks because it was only improved in the sense that it was more."

Additional enforcement parameters were codified in October. Not only have fines increased—companies can be on the hook for as much as \$1.5 million per year—the government has expanded the number

worried that a vast number of businesses out there have no clue and will never even think to think of it."

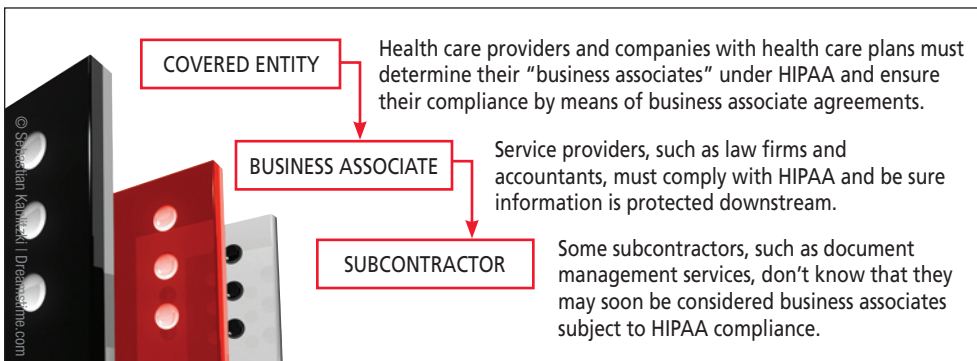
As companies await more guidance and finalized rules, the crux question is when to act. Full HIPAA compliance is an onerous process, and no one wants to waste time and effort needlessly. On the other hand, too much of a wait-and-see approach may not leave companies enough time to react. On this question, there is no one right answer.

A cleaning or maintenance subcontractor, for example, probably won't have to be HIPAA compliant, whereas most professional service providers almost definitely will. As a constant provider of legal services to HIPAA-covered entities, Coyne says her firm opted to proactively establish compliance under the best current understanding of the HITECH regulations. At the very least, she says, companies need to get a clear picture of how their protected information is shared, and with whom.

"Everyone needs to get a handle on what protected health information flows through their business," Coyne says. "They also need to run their business through the machinery of whether or not they are business associates of a covered entity or a subcontractor of a business associate of a covered entity. If these rules are finalized, they become a business associate, too."

The Cascade Effect

PENDING HIPAA REVISIONS EXPAND DOWNSTREAM LIABILITY



and Human Services announced a set of proposed modifications to HIPAA to clarify the regulation of business associates under HITECH. The comment period ended on Sept. 13, 2010. The new rules will go into effect 180 days after they are finalized, which likely will happen in the coming months.

Stiff Penalties

HIPAA regulations have a kind of cascade effect. Every regulated entity not only has to be in compliance, it must draft business associate contracts that ensure compliance downstream. Now business associates will also have an affirmative responsibility to require their own subcontractors to comply with HIPAA.

"Let's say an accountant has a data destruction service, and they run across protected health information that the accountant received from the hospital," Coyne says. "Whether or not there's actually a written contract in place, that data destruction service under these proposed rules would have affirmative HIPAA compliance obligations—and would never know it."

Ignorant or not, the consequences for companies that fail to make adequate compliance efforts can be swift and severe.

of agencies tasked with tracking down violations. Spontaneous audits may come from HHS's Office of Civil Rights, the Office of the Inspector General or even—because there are criminal as well as civil penalties—the Justice Department.

"This used to be a complaint-driven law, so you could be comfortable that unless someone complained, no one was going to come looking at your HIPAA compliance," Coyne says. "Now audits are coming from a number of arms of the government."

State attorneys general are also empowered to go after offenders, and a new penalty-sharing scheme gives whistleblowers a share of the penalty, a la the False Claims Act.

Take Action, but When?

Given the intensifying enforcement climate, companies that ignore HITECH liability do so at their own peril. Still, the current level of HIPAA awareness among business associates is spotty at best.

"Those who have regular relationships with the health care industry are used to running their business through the intense network of health law regulation, and they probably have this on their radar," Coyne says. "But with this hugely expanded scope, I'm

 Join the martindale.com® Connected conversation

Article Participants:

[Sarah E. Coyne](#) is the national chair of the health law group at Quarles & Brady. She is based in Madison, Wis., and can be reached at sarah.coyne@quarles.com. She is [Peer Review Rated](#).

[Kerry L. Moskol](#) practices in Quarles & Brady's health law group. She is based in Madison, Wis., and can be reached at kerry.moskol@quarles.com.

With 450 attorneys in seven offices, [Quarles & Brady LLP](#) offers clients a full spectrum of national corporate legal service. The firm's health law group provides comprehensive guidance on the complex and quickly evolving health care issues, including compliance with HIPAA and HITECH.