The stage is set for increased HIPAA enforcement actions

Since the HIPAA Privacy Rule first required compliance in 2003, enforcement of the privacy and security obligations has been very limited. In recent years, enforcement has increased, but there remains only a handful of actions. Now, with the implementation of new HIPAA privacy, security and breach notification requirements, the expansion of HIPAA enforcement authority, the upcoming departure of the head of the primary HIPAA enforcement agency, and potential enforcement 'competition' from the FTC, Kirk J. Nahra, a Partner with Wiley Rein LLP in Washington, asks what can we expect in HIPAA enforcement in the years ahead?

In the beginning, there was the HIPAA statute, the Health Insurance Portability and Accountability Act of 1996. This statute spawned the HIPAA Privacy Rule (compliance required by 2003) and the HIPAA Security Rule (with compliance in 2005). The HIPAA law focused on 'portability' - the idea that individuals could take their health insurance coverage from one employer to the next, without having pre-existing health conditions acting as an impediment to job transitions. Congress added to this law the requirement for the creation of privacy and security rules. However, its tortured statutory history led to one key component of these rules: the limits on the applicability of these rules to 'covered entities' - such as doctors, hospitals and health insurers. The law mandated the rules, but restricted their application to those covered entities only. That meant that a large number of entities that obtained or used healthcare information were not within the scope of these rules, and were not subject to enforcement under HIPAA. The rules created contractual obligations for service providers to these covered entities - called business associates - but the HIPAA enforcement agency (the US Department of Human Services Office for Civil Rights) had no direct jurisdiction over these 'business associates.'

Part two of the HIPAA era is now in place, following additional action by Congress and the regulatory agencies. Following passage of the Health Information Technology for Economic and Clinical Health Act in 2009, the Department of Health and Human Services released an 'omnibus' regulation implementing changes to the HIPAA Privacy, Security and Enforcement Rules, along with an important regulation relating to notification of individuals in the event of a security breach. These new regulations - which were published on 25 January 2013 and required compliance by 23 September 2013 - set the stage for this examination of where HIPAA enforcement will go next.

Key developments

Expect more enforcement

We have seen predictions of more HIPAA enforcement for many years. It likely will be true soon, even though this enforcement increase is several years later than expected. Enforcement is creeping up, although slowly. There is pressure from other HHS agencies on OCR, including from the HHS Inspector General's Office which, in a recent report, criticised OCR for its enforcement activity. And, now that the full HITECH rules are in effect, OCR has the full range of enforcement and increased penalties to work with. This does not mean that we should expect enforcement to rise to the level of other healthcare initiatives, but we can anticipate a continuing and steady rise. Presumably, OCR will continue its overall philosophy, where enforcement typically is predicated either on significant problems or longstanding and unrepaired problems.

Business associate challenges

At the same time, enforcement also is likely to rise because there are now far more entities subject to enforcement. The entire service provider community - the full range of HIPAA 'business associates' - now face enforcement. But there is a substantial dilemma for any enforcement agency in this context. The rules are the same for covered entities and business associates, when HIPAA applies to the BA community (mainly the full security rule and portions of the privacy rule that are incorporated into business associate agreements). However, it is also clear that for many business associates, application of these principles in full simply may be unfair or inappropriate. The textbook model is a service provider where the firm services many industries, with healthcare constituting only a small portion. It may be appropriate to hold these businesses to the privacy components of these rules, as these providers should not be doing too much with health information other than providing services.

However, the issue of security rule compliance is much more complicated. Many of these businesses have large and sophisticated information security programs. But these programs are built for overall security protection, and typically were not built specific to the HIPAA details. How will OCR draw these lines? Will BAs be forced to reinvent their security programs to meet HIPAA

standards even if these standards are not necessarily better, just different? And what about the wide variety of service providers who may provide services to many industries and may have no idea that they have even accessed or obtained PHI? The application of the HIPAA rules to downstream contractors makes this problem even more acute (raising the possibility that a contractor is unaware of their obligations). So, HHS will need to tread carefully in its enforcement activities related to business associates.

New leadership

Another key challenge for the HHS Office for Civil Rights is the likely need for a near term selection of a new leader. The current OCR Director, Leon Rodriguez, has been nominated to a different government post. Rodriguez has been a smart, responsible and effective leader in his tenure at OCR. He has been vocal about what the agency expects, as well as being reassuring about the agency's mission and overall enforcement approach. While it is unlikely that a new leader will bring about a substantial change in direction (for budgetary reasons), a new agency head always means change.

FTC challenges

Last, healthcare companies also must worry about the expanding presence of the Federal Trade Commission as an enforcement agency. The FTC traditionally has played a role in the US as a 'default' privacy and security regulator, stepping in, in limited circumstances, where it views consumer rights as being violated. These steps typically have involved companies who otherwise are unregulated under US law on privacy and security issues. The FTC's approach is being challenged in court by one of the targets of its data security efforts, Wyndham Hotels. In a separate case, the FTC is being challenged for its data security enforcement activities against an entity covered directly by the HIPAA Rules. The FTC has defended its efforts by saying that it is enforcing consumer rights under its own authority, not enforcing HIPAA, but this action leads to the possibility that the FTC believes it can act against any covered entity or business associate also subject to the HIPAA rules if the FTC views consumer rights as being adversely effected. While they have not made this position clear, this seems to open up the FTC as an entirely separate agency for enforcement of privacy and security principles against healthcare companies, even if they are covered by HIPAA.

Healthcare companies also must worry about the expanding presence of the Federal Trade Commission as an enforcement agency.

Where are your biggest risks?

So, with these changes and evolutions on the horizon, where do companies need to pay the most attention in evaluating their privacy and security activities?

- Security breaches: The clearest path to HIPAA enforcement involves security breaches. There simply are too many breaches in the HIPAA environment. Now that many security breaches require notification to consumers and HHS, there is a steady stream of enforcement possibilities for the agency related to security breaches. Effective mitigation of security problems is always a smart step.
- Breach notification: The new breach notification rules are likely paths to enforcement. Companies need to make sure they are conducting appropriate risk assessments, and making smart decisions about when notification is appropriate or required.
- Security policies and procedures: HHS places an extraordinary emphasis on its review of policies and procedures in its investigations. HIPAA covered entities should have their policies and procedures in place, since these have been required for several years. However, this is a good time to re-evaluate these requirements. Business associates must meet this requirement for the first time, and it is clear that many are lacking in the appropriate documentation.
- Marketing activity: One of the key privacy rule changes resulting from the HITECH law involves additional restrictions on marketing activities where these activities involve remuneration. These restrictions are causing concern in the healthcare industry.
- De-identification: Lastly, there is a renewed focus on the efforts of covered entities and business associates to 'de-identify' health information. There is significant attention being paid to this issue, because of the substantial financial transactions involving de-identified information and the substantial opportunities to use de-identified information for useful purposes.

Conclusion

The healthcare industry faces significant upheaval because of the new changes to the health care privacy and security rules. At the same time, the opportunities to use and benefit from healthcare information have never been greater, and the areas of potential security concern grow with each new technological opportunity that makes the sharing of healthcare information easier. Healthcare companies and their service providers must make sure they stay on top of developments and ensure that they have a proactive and ongoing means of protecting themselves against realistic enforcement activity.

Kirk J. Nahra Partner
Wiley Rein LLP, Washington DC
knahra@wileyrein.com
Follow Kirk on Twitter @KirkJNahrawork