THE
NATIONAL LAW REVIEW

HIPAA and Health Care Data Privacy - 2018 Year-in-Review

Friday, January 4, 2019

Today, we're looking back at HIPAA and other privacy and security developments in 2018. This past year saw continued HIPAA enforcement (including the largest ever fine for a HIPAA breach), reminders from the OCR on best practices for HIPAA compliance, and updates to state and international privacy and security laws. We'll also look ahead to 2019, which could bring several significant changes to HIPAA, such as reducing the burdens for sharing patient information in order to promote care coordination and better patient outcomes. Here we go!

Article By Mintz
Health Law Practice Health Care Advisory

Communications, Media & Internet
Health Law & Managed Care
All Federal

HIPAA Enforcement

HIPAA enforcement continued in 2018, with the HHS Office for Civil Rights (OCR) announcing a total of eight resolution agreements related to breaches and HIPAA violations by covered entities and business associates. Though there were fewer resolution agreements than in 2017, 2018 brought us the largest fine since OCR began enforcing HIPAA (Anthem's payment of $16 million in October).

With this year's resolution agreements (all of which are available here) we see many of the same enforcement themes we have seen in previous years, including:

- the importance of conducting an accurate and thorough risk assessment;
- the necessity of business associate agreements; and
- the need to be good at the "basics" of HIPAA compliance.

For instance, as we previously discussed, a Florida physician group shared protected health information (PHI) with a medical billing services vendor without first entering into a business associate agreement (BAA). The issue of not having a BAA in place with vendors has been a costly oversight for many providers over the past few years. Similarly, disclosing PHI to news media is also a recurring issue and one that appeared again in 2018, this time implicating a physician practice. In that case, one of the practice's physicians disclosed PHI to a reporter at a local television station in response to a public patient complaint. The disclosure led to a $125,000 penalty.

Another lesson from 2018 is that HIPAA still applies at the end of relationships – whether that is the closure of a business or the termination of an employee. Only a few weeks ago we saw a resolution agreement entered into by Pagosa Springs Medical Center in Colorado for failure to cut off a former employee's access to PHI. The beginning of 2018 started with a parallel situation, whereby a receiver appointed to liquidate assets of Filefax, Inc., a medical records storage and maintenance company, had to pay $100,000 for potential HIPAA violations. This case is a reminder that HIPAA obligations continue throughout the lifecycle of a business, including those that file for bankruptcy.

OCR Announcements

OCR continued its regular monthly newsletter and often promoted back-to-basics principles. OCR reminded

health care providers about the importance of using simple measures to ensure HIPAA compliance, including:

- Using simple, physical safeguards to protect PHI, like locked cabinets and privacy screens;
- Assessing and mitigating information security risks; and
- Securely disposing and destroying electronic devices and media after they are no longer needed.

In June, OCR also issued new interim guidance on individual authorizations for the use and disclosure of PHI for future research, as mandated by the 21st Century Cures Act.

In October, OCR and the HHS Office of the National Coordinator for Health Information Technology (ONC) updated the Security Risk Assessment Tool to help covered entities and business associates complete their risk assessments.

It's Not Just HIPAA—2018 Brought the GDPR and New State Data Breach Laws

As if HIPAA compliance weren't challenging enough, 2018 brought two big updates for the compliance obligations of healthcare entities that handle personal information. First, on May 25, 2018, the European Union's General Data Protection Regulation (GDPR) went into effect. Though many U.S.-based healthcare entities are not directly subject to the GDPR, for those that are, coming into compliance was (and continues to be) a major feat.

This year also saw South Dakota and Alabama finally enacted state data breach notification laws, meaning that all 50 states now have their own form of data breach notification laws. These laws vary in the types of personal information they cover, their application to HIPAA-regulated entities, and the notification obligations of an entity that has experience a data breach. Any entity handling personal information, whether or not regulated by HIPAA, should be aware of these laws.

What's Ahead for 2019

We may see some action in 2019 toward lessening the burdens of sharing patient information when such sharing is necessary for patient care.

Earlier this year, Congress attempted but failed to enact a bill aligning 42 CFR Part 2's notoriously rigorous standards with HIPAA. The draft legislation would have permitted providers to share information about patients subject to 42 CFR Part 2 for the purpose of treatment, payment, and operations, similar to HIPAA. The purpose of the legislation was to promote patient treatment and outcomes for substance abuse disorders, particularly in light of the opioid epidemic. However, after Congress failed to pass the legislation, HHS announced that it planned to release a notice of proposed rulemaking on the topic in March 2019.

In addition to possible changes to 42 CFR Part 2, HHS issued a request for information to identify HIPAA regulations that care coordination and value-based payment systems, both of which require sharing of patient information.

Finally, HHS may change the way it handles monetary penalties or settlements resulting from data breaches. HHS plans to issue a request for information on a proposal to share a percentage of money paid by health care organizations through civil monetary penalties or monetary settlements with the individuals directly affected by the data breach.

Source URL: https://www.natlawreview.com/article/hipaa-and-health-care-data-privacy-2018-year-review