EM Connections

Euclid Managers Compliance Resources

March 21, 2024

HHS Delivers Reports to Congress on HIPAA Compliance

On February 14th, 2024, the Department of Health & Human Services' (HHS) Office for Civil Rights (OCR) issued two reports regarding Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance and enforcement during the 2022 calendar year. The reports focused on *Privacy, Security, and Breach Notification Rule Compliance* and *Breaches of Unsecured Protected Health Information*.

These reports are an annual requirement per the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. They seek to help regulated entities (such as most health care providers, health plans, and healthcare clearinghouses) and any of their business associates in their HIPAA compliance efforts by sharing steps taken by OCR to investigate complaints, breach reports, and compliance reviews regarding potential violations of the HIPAA Rules. The reports include important data on the number of HIPAA cases investigated, areas of noncompliance, and insights into trends such as cybersecurity readiness.

As a refresher, the HIPAA rules provide the minimum required privacy and security safeguards for protected health information (PHI), and give individuals rights with respect to that information, such as the right to access their health information.

The HIPAA Privacy Rule protects the privacy of the health information of individuals while permitting important uses and disclosures of the information, such as for treatment of an individual, payment for health care, and for sharing of information to the friends and family involved in the care of an individual. Covered entities and their business associates may not use or disclose PHI, except either as the Privacy Rule permits or requires.

The HIPAA Security Rule establishes standards to protect electronic PHI (ePHI) created, received, maintained, or transmitted by covered entities and their business associates. The Security Rule requires numerous safeguards to ensure the confidentiality, integrity, and availability of ePHI.

The HIPAA Breach Notification Rule requires HIPAA covered entities to notify affected individuals, HHS, and, in some cases, the media, following the discovery of a breach of unsecured PHI. Business associates are also required to notify covered entities following the discovery of a breach.

The 2022 Report to Congress on *Privacy, Security, and Breach Notification Rule Compliance* addressed the complaints of HIPAA violations reported to the Secretary and the actions taken in response to those complaints. Specifically, the report identified the number of complaints received, the method by which those complaints were resolved, the number of compliance reviews initiated by OCR, and the outcome of each review. Examples of their findings include:

- Receipt of 30,435 new complaints alleging violations of the HIPAA Rules
- OCR resolved 32,250 complaints alleging violations of the HIPAA Rules

- OCR resolved 17 complaint investigations with Resolution Agreements and Corrective Action Plans with monetary settlements totaling $802,500, and one complaint investigation with a civil money penalty in the amount of $100,000.
- OCR completed 846 compliance reviews and required the entities to take corrective action or pay a civil money penalty in 80% (674) of these investigations. Three compliance reviews were resolved with monetary payments totaling $2,425,640.

The second report to Congress, which addressed *Breaches of Unsecured Protected Health Information*, identified the number and nature of breaches of unsecured PHI that were reported to HHS during calendar year 2022 and the actions taken in response to those breaches. It also highlighted the constant need for regulated entities to improve compliance with the HIPAA Security Rule requirements, including:

- Risk analysis and risk management;
- Information system activity review;
- Audit controls;
- Response and reporting; and
- Person or entity authentication.

Hacking and other IT incidents remained the largest category of breaches that occurred in 2022, comprising 77% of the reported breaches. Network servers continued to be the largest category by location for breaches involving 500 or more individuals, at 58% of reported large breaches.

So, what do these reports to Congress have to do with employers and their health plans? As you may have guessed, these findings speak to the importance of compliance, especially when it comes to employees' private information. These reports underscore the importance of considering what employers are doing to protect their companies from intended or unintended hacks, security breaches, and possible violations. They are reminders of the precautions employers should take, update, and implement as part of fulfilling governmental requirements. Finally, they are vivid reminders that HHS and other agencies do receive inquiries and complaints regarding security issues, and employers do not want to become the subject of such an inquiry.