Published on *The National Law Review* https://natlawreview.com

Don’t Forget About These Three HIPAA Compliance Requirements

Article By:

Hannah R. Demsien

Amy C. Ciepluch

Given all the focus on new group health plans requirements like the No Surprises Act and Mental Health Parity Regulations in the last few years, it can be easy to lose track of compliance with long-standing requirements. We are here this month to remind you of three key requirements under HIPAA (the Health Insurance Portability and Accountability Act of 1996). HIPAA requires that group health plans and health insurers (HIPAA Covered Entities), protect the privacy and security of an enrolled individual’s Protected Health Information (PHI). HIPAA requires that Covered Entities implement safeguards to protect PHI, adopt written privacy and security policies and procedures outlining the measures they have put in place to protect PHI, and give individuals certain rights with respect to their own PHI, among other requirements. In the event PHI is improperly shared or accessed by third parties, Covered Entities must take steps to mitigate the breach of PHI.

Large breaches of PHI have been climbing over the past few years. The number of individuals impacted by large breaches as reported to the Department of Health and Human Services (HHS) has risen from 15,210,437 in 2018 to 134,787,438 in 2023.[1] The majority of these breaches were caused by hacking or other information technology incidents.[2] The Office of Civil Rights (OCR), which is responsible for HIPAA enforcement within HHS, entered into eight civil settlements in connection with HIPAA violations in 2023, the largest of which involved a $4.75 million settlement payment in addition to a corrective action plan and further monitoring of the violating entity by OCR.[3] While most HIPAA enforcement actions are against health care providers, in recent years there have been several large settlements with health plans. In light of increasing cybersecurity incidents and scrutiny by OCR, Covered Entities need to make sure that their HIPAA compliance measures are up to par.

While there are several categories of compliance requirements under HIPAA, there are three areas that OCR has recently highlighted in its enforcement efforts. Plan sponsors, health insurers, and other service providers involved in the administration of group health plans should review their HIPAA compliance operations in these areas considering this recent OCR activity.

Conducting a Risk Analysis

HIPAA requires Covered Entities to conduct a risk analysis of their systems that contain electronic PHI, and OCR investigations often find this analysis lacking.[4] Plan sponsors, health insurers, and other service providers involved in the administration of group health plans should ensure that they conduct risk analyses on a regular basis and when implementing new technologies and business operations. OCR has made available a recording of a recent best practices webinar regarding the HIPAA risk analysis requirement here.

Individual Access Rights

OCR noted an uptick in complaints from individuals that Covered Entities were not providing them with access to their PHI.[5] Under HIPAA, Covered Entities generally must provide an individual with access to inspect and copy their PHI that is held by the Covered Entity within 30 days of a request for access by an individual.[6] Plan sponsors, health insurers, and other service providers involved in the administration of group health plans should have a policy in place to timely process requests from individuals.

Covered Entity Employees and PHI

Only employees who need access to PHI as a part of their job or who assist in the administration of the group health plan should have access to PHI.[7] This group of employees should receive training regarding HIPAA requirements and the Covered Entity's security measures to protect PHI.[8] As a best practice, Covered Entities should consider providing employees with general information security training covering topics like phishing, password security, and social engineering. Covered Entities should limit access to PHI to appropriate personnel and have a process for reviewing employee access to PHI. Inappropriate access to PHI by employees outside of those who need PHI as a part of their role within an organization is a way that breaches of PHI may occur. Appropriate and practical training regarding how to maintain the privacy and security of PHI can help prevent breaches of PHI.

Conclusion

Many Covered Entities implemented their HIPAA compliance practices in 2013 when certain group health plan requirements were amended, but they have not reassessed their practices since then. As a best practice, Covered Entities should review their HIPAA compliance practices on a regular basis and ensure that their actual operations align with HIPAA requirements. Given the changes in technology and the rise of cybersecurity incidents since 2013, plan sponsors, health insurers, and other vendors should also take a close look at their existing practices to make sure they hold up to current technology standards. OCR has several resources available to help with this technical assessment, including a Security Risk Assessment Tool available here.

---

[1] Slide 10 from OCR's February 27, 2024 OCR Update and 2024 Priorities presentation, located here. All references to Slides in this Article are to slides from this OCR presentation.

[2] Slide 11.

[3] Slide 14.

[4] 45 CFR § 164.308.

[5] Slides 4 and 18.

[6]45 CFR § 164.524.

[7]45 CFR § 164.504.

[8]45 CFR § 164.530 and 45 CFR § 164.308.

National Law Review, Volume XIV, Number 108