STRATEGIC MANAGEMENT SERVICES

Office for Civil Rights Issues 2021 Annual Reports to Congress

Natalie S. Lesnick | February 2023

2021 marked a 25 percent increase in HIPAA and HITECH violation complaints over 2020, according to OCR's 2021 Annual Reports to Congress on HIPAA Compliance and Breaches of Unsecured Protected Health Information. OCR reported that 26,420 of the 34,077 complaints received were resolved. Seventy-eight percent of these complaints were resolved prior to an OCR investigation, and 13 percent of OCR investigations resulted in Resolution Agreements and Corrective Action Plans with monetary settlements totaling $815,150. OCR also received 609 notifications of breaches impacting 500 individuals or more – a decrease of 7% from those reported in 2020 – with many of these notifications stemming from successful hacking attempts.

Understanding government enforcement informs and assists compliance and privacy professionals in developing and strengthening compliance and privacy programs. Based on this most recent report, there is a continued need for covered entities to improve their compliance with the HIPAA Privacy and Security rules. Below are some ideas to develop and improve your privacy program.

1. *Get to Know Your Organization*. While you may qualify as a covered entity under HIPAA, knowing how each part of the regulation applies to your organization is important. Some areas may have a higher impact, while others may not. This does not mean ignoring or disregarding parts of the regulation but rather knowing how your organization is situated in the larger HIPAA regulatory landscape.
2. *Develop Privacy and Security Policies and Procedures*. There is a lot that goes into HIPAA Privacy and Security. Ensuring that employees have adequate written guidance to comply with HIPAA, written in a manner that is easy to understand and follow, is paramount. Written documentation may also act as evidence your organization is adhering to HIPAA and HITECH regulations.
3. *Conduct a Privacy and Security Risk Analysis/Assessment*. Similar to the first point, it is important to know what privacy and security areas are of the highest risk to your organization. Use your operational and business leaders to identify where your

organization's vulnerabilities lie by regularly conducting a privacy and security risk analysis or assessment.

4. *Require Privacy and Security Training for Employees*. HIPAA regulations are as complex as they are important, and an organization is only as safe as its weakest employee. Annual training keeps employees up to date with changing regulations and acts as a refresher for folks who need it. Also, periodic training is required under HIPAA and HITECH.
5. *Audit Your Controls*. Work with your information security team to ensure that your organization is conducting appropriate audits of your security measures regularly. Regular audits of your privacy and security practices can help ensure you catch vulnerabilities early and remedy potential gaps before
6. *Know What To Do In Case of a Breach*. Unfortunately, even after setting up your privacy program for success, breaches may occur. If your organization does experience a breach, it is important to have a plan in place to investigate and report as required.

For answers to compliance FAQs, see https://www.compliance.com/faqs/

Keep up-to-date with Strategic Management Services by following us on LinkedIn.

About the Author

Natalie Lesnick is a Consultant at Strategic Management Services, LLC. Ms. Lesnick has expertise in assessing provider compliance with the federal healthcare program rules and federal healthcare laws, including HIPAA and the Affordable Care Act.