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

OCR Releases Report Summarizing HIPAA Privacy and Security Compliance Failures

Article By:

Joseph J. Lazzarotti

Maya Atrakchi

In the final days of 2020, the Office for Civil Rights (OCR) at the U.S. Health and Human Service (HHS) released a HIPAA Audits Industry Report ("the Report"), that could be quite helpful to covered entities and business associates for tackling HIPAA compliance as we enter the new year. The Report examines OCR's findings from HIPAA audits the agency conducted during 2016-2017 of 166 healthcare providers and 41 business associates. The audits were intended to examine mechanisms for compliance, identify promising practices for protecting the privacy and security for health information, and discover vulnerabilities that may be have been overlooked by OCR enforcement activity. It is the OCR's hope that insights from the Report will enhance industry awareness of compliance obligations and assist the OCR in developing tools and guidance to assist industry compliance, self-evaluation, and prevent data breaches.

The Report looked at seven components of HIPAA compliance by covered entities:

Privacy Rule:

- notice of privacy practices/content requirements
- provision of notice – electronic notice (website posting)
- right of access

Breach Notification Rule:

- timeliness of notification
- content of notification

Security Rule:

- security management process – risk analysis
- security management process – risk management

For business associates, the Report examined three components:

Breach Notification Rule –

- notification by a business associate,

Security Rule –

- security management process – risk analysis and
- security management – risk management.

The Report applied a rating scale of 1-5 to covered entities, one being essentially full compliance and five being no evidence of a serious attempt to comply with the rules. Based on this scale and the results from the audits, the Report concludes covered entities generally demonstrated compliance in only two of the seven areas audited: 1) timeliness of breach notification and 2) prominent posting of the notice privacy practices on their websites. Here are some troubling data points from the Report:

- With regard to satisfying the content requirements for HIPAA notices of privacy practices, only 2% of covered entities fully met the requirements, and two-thirds failed to or made minimal or negligible efforts to comply.
- Almost all covered entities audited (89%) failed to show they were correctly implementing the individual right of access. Notably, right of access compliance is a specific enforcement initiative of the OCR, having announced 13 enforcement actions over the past two years. Compliance gaps included inadequate or incorrect policies and procedures for providing access, such as policies that incorrectly state that the entity could deny access to PHI or lack of policies for honoring requests for information to be provided to a designated third party.
- Approximately 70% of covered entities used breach notification letters that failed to satisfy regulatory content requirements, such as a description of the electronic personal health information (ePHI) breached and steps individuals can take to protect themselves from additional harm.
- As the OCR's previous audit (from 2012) found, covered entities struggled to implement the Security Rule's requirements for both risk analysis and risk management – the Report highlighted that only 14% of audited covered entities "substantially fulfilled" responsibilities regarding safeguarding of ePHI through risk analysis mechanisms, and only 6% of covered entities adequately fulfilled requirements to implement appropriate risk management mechanisms to reduce risks and vulnerabilities to a reasonable and appropriate level.

Business associates shared similar struggles with covered entities regarding implementation of security risk analysis and management requirements – only 17% of audited business associates "substantially fulfilled" requirements regarding safeguarding of ePHI through risk analysis, and only 12% of business associates fulfilled the requirement to implement appropriate risk management mechanisms. Moreover, while few audited business associates reported a breach of ePHI, those that did generally evidenced minimal or negligible efforts to address audited requirements.

On a positive note, the Report noted that a large majority of the covered entities and business associates shared their appreciation for the comments or findings, and already initiated steps to strengthen policies, procedures, and/or correct deficiencies. The Report also provides helpful easy-to-use tools and resources to assist organizations with compliance. For example, the Report highlights the Model Notices of Privacy Practices available on the OCR's website – covered entities may customize these models by entering their entity-specific information.

In the OCR's announcement of the Report, OCR Director Roger Severino emphasized,

The audit results confirm the wisdom of OCR's increased enforcement focus on hacking and OCR's Right of Access initiative. We will continue our HIPAA enforcement initiatives until health care entities get serious about identifying security risks to health information in their custody and fulfilling their duty to provide patients with timely and reasonable, cost-based access to their medical records.

Takeaway

The OCR was active in enforcing HIPAA regulations in 2020. In particular, there were thirteen settlements under the OCR's Right to Access Initiative which enforces patients' rights to timely access medical records at reasonable cost. In September of 2020 alone, the OCR announced settlements with five providers under that Initiative. OCR settlements have impacted a wide array of health industry related businesses including hospitals, health insurers, business associates, physician clinics, and mental health/substance abuse providers. Furthermore, 2020 saw more than $13.3 million recorded by OCR in total resolution agreements.

In addition, there was a significant amount of OCR issued guidance relating to HIPAA in 2020. In March OCR issued back-to-back guidance on COVID-19 related issues, first regarding getting protected health information (PHI) of COVID-19 exposed individuals to first responders, and next providing FAQs for telehealth providers. In July, the Director of the OCR issued advice to HIPAA subject entities in response to the influx of recent OCR enforcement actions – "When informed of potential HIPAA violations, providers owe it to their patients to quickly address problem areas to safeguard individuals' health information." In September, the OCR published best practices for creating an IT asset inventory list to assist healthcare providers and business associates in understanding where electronic protected health information (ePHI) is located within their organization and improve HIPAA Security Rule compliance, and shortly after issued updated guidance on HIPAA for mobile health technology. Finally, regulations have been issued to permit hospitals and health systems to donate cybersecurity technology to physician practices.

The Report combined with increased OCR enforcement activity and guidance, serves as a reminder of the seriousness in which OCR treats HIPAA compliance obligations, and healthcare organizations and their business associates need to address basic best practices as they enter 2021.

National Law Review, Volumess XI, Number 7