HHS OCR announces results of most recent round of HIPAA audits

December 18, 2020

On December 17, 2020, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued its Industry Report on the HIPAA audits it conducted in 2016 and 2017. OCR found widespread noncompliance with most of the Privacy, Security, and Breach Notification Rule requirements that were reviewed in the audits.

OCR audited 166 covered entities and 41 business associates in this round of audits and focused on a narrow set of Privacy, Security, and Breach Notification Rule requirements. The business associates selected for the audit were chosen from lists provided by the audited covered entities.

Regarding the Privacy Rule, OCR focused on the Notice of Privacy Practices content, electronic notice requirements and the right of access. It found that 98 percent of the covered entities failed to provide all of the required content for the Notice of Privacy Practices, with many Notices missing required content related to individual rights. OCR also highlighted that many of the Notices were not written in plain language as required by the Privacy Rule. On a more positive note, OCR found that most covered entities that maintained websites about their customer services or benefits met the requirement to prominently post the Notice of Privacy Practices to those websites.

Meanwhile, 89 percent of covered entities failed to show that they were correctly implementing the individual right of access. Common issues included inadequate documentation of access requests, insufficient evidence of access policies, inadequate or incorrect access policies, lack of a clear reasonable cost-based fee policy or application of blanket fees in violation of the standard, and failure to maintain policies requiring a timely written denial and the basis for the denial.

The Security Rule audit focused on the requirements to conduct risk analysis and risk management. OCR found that only 14 percent of audited covered entities and 17 percent of audited business associates "substantially fulfilled" their regulatory responsibilities to safeguard electronic protected health information (ePHI) through risk analysis activities. The results were similarly bad on the risk management requirement, with 6 percent of covered entities and 12 percent of business associates fulfilling the requirement to implement appropriate risk management activities sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Finally, OCR examined covered entities' compliance with the breach notification timeliness and content requirements and business associates' compliance with the requirement to notify covered entities of breaches. While OCR found that most covered entities provided notice to individuals in a timely manner, 67 percent of the covered entities submitted notification letters to individuals that were missing required content such as a description of the protected health information (PHI) involved in the breach and steps the individual should take to protect themselves from harm. Only nine of the audited business associates reported ever having a breach, and OCR found that most of those provided the majority of the required information in a timely manner.

In the press release announcing the Industry Report, OCR Director Roger Severino stated, "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."

Authors