Investigating and Settling Potential HIPAA Privacy and Security Violations

October 30, 2020

Since the beginning of 2020, the U.S. Department of Health and Human Services, Office for Civil Rights (?ÃÂ£***OCR***?ÃÂ¥) has announced six substantial settlements with HIPAA covered entities (either health care providers or health plans) for potential violations of the HIPAA privacy and security rules (?ÃÂ£***HIPAA Rules***?ÃÂ¥) related to safeguarding protected health information (?ÃÂ£***PHI***?ÃÂ¥). OCR is the federal agency responsible for enforcement of the HIPAA Rules. These settlements generally arose from investigations pursued by OCR following the receipt of a breach report by the covered entity and involved settlement payments ranging from $25,000 to $6.85 million (the second largest HIPAA settlement payment in OCR history). The settlements also imposed a corrective action plan on each covered entity, with two years of monitoring by OCR. Findings by OCR during its investigations included one or more of the following infractions by the subject covered entity:

- Neglected to implement HIPAA policies and procedures;
- Failed to conduct a risk analysis as required by the HIPAA security rules;
- Failed to have the necessary business associate agreements in place with business associates;
- Neglected to provide workforce members with HIPAA privacy and security training as required;
- Failed to encrypt electronic PHI on laptops after the covered entity determined it was reasonable and appropriate to do so;
- Failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; and
- Failed to implement information system activity review, security incident procedures, and information access controls.

These OCR settlements underscore the risks for covered entities under HIPAA, including employer-sponsored group health plans, for neglecting to make HIPAA compliance a top priority. Three of these six OCR settlements were related to a HIPAA breach caused by hacking or a cyberattack of the covered entity?ÃÃs information system. In one of its press releases, OCR commented that such attacks are now ?ÃÂ£the number one source of large health care data breaches.?ÃÂ¥ As the use of technology expands, hacking and cyberattacks are likely to become even more common. Thus, employers should be diligent with ensuring that PHI created or received by their group health plan is appropriately safeguarded in compliance with the HIPAA Rules. The settlement agreements are available **here**.

© 2026 Haynes Boone