HIPAA ENFORCEMENT RELAXED, BUT NOT ABANDONED

Hodgson Russ Healthcare and Cybersecurity & Privacy Alert
August 14, 2020

As previously reported here, the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) announced in March 2020 that it would exercise discretion in enforcement actions related to HIPAA restrictions that might otherwise limit the good faith provision of telehealth services. But with the pandemic and the implementation of work-from-home policies, health care providers — so called "Covered Entities" — must be more vigilant than ever to employ commercially reasonable efforts to safeguard the protected health information (PHI) of patients.

One recent enforcement action is a case in point. On July 27, 2020, OCR announced a $1,040,000 settlement with Lifespan Health System Affiliated Covered Entity (Lifespan) to settle alleged violations of HIPAA's Privacy and Security Rules. The settlement followed Lifespan's self-disclosure to OCR of the theft of an employee's laptop from a locked car. The laptop contained the PHI of 20,431 patients across various affiliated provider facilities. The exposed PHI included patients' names, medical record numbers, demographic information, and medication information. OCR's investigation determined that there was systemic noncompliance with the HIPAA Rules including a failure to encrypt PHI on laptops after Lifespan determined it was reasonable and appropriate to do so. The investigation also found other controls lacking, including the absence of device and media controls, and the failure to have business associate agreements in place among healthcare provider affiliates. OCR Director, Roger Severino, touted the settlement stating, "[l]aptops, cellphones, and other mobile devices are stolen every day, that's the hard reality. Covered entities can best protect their patients' data by encrypting mobile devices to thwart identity thieves." In addition to the monetary settlement, Lifespan agreed to a corrective action plan that includes two years of monitoring. The resolution agreement and corrective action plan may be found at: https://www.hhs.gov/sites/default/files/lifespan-ra-cap-signed.pdf.

HIPAA's standards for the lawful use and disclosure of PHI can be onerous. Covered Entities must conduct annual audits to assess gaps in security, remediate those gaps in security, draft and revise policies and procedures to comply with HIPAA, train personnel, vet and manage vendors with access to PHI, and create processes to respond to and report breaches, among other things. And, under the best of circumstances, these requirements can lead to problems, exposing Covered Entities

Attorneys

Christine Bonaguide
David Bradley
Jane Bello Burke
Roopa Chakkappan
Reetuparna Dutta
Joshua Feinstein
Peter Godfrey
Charles H. Kaplan
Michelle Merola
Matthew Scherer
Gary Schober
David Stark

Practices & Industries

Cybersecurity & Privacy
Healthcare

to regulatory fines. Some of the more common enforcement actions arise out of failing to properly safeguard PHI, failing to enter into the appropriate business associate agreements and/or disclosing PHI in a way that is not allowable under the law.

The Lifespan settlement is an important reminder that Covered Entities need to be proactive about protecting PHI in order to avoid and/or mitigate the consequences of a breach. Regular assessments of your security procedures is not only prudent, it's the law. Contact Michelle Merola (518.736.2917), or any member of Hodgson Russ's Healthcare Practice or Cybersecurity and Privacy Practice to discuss how we can assist you with HIPAA-related compliance.

If you received this alert from a third party or from visiting our website, and would like to be added to any of our mailing lists, please visit us **HERE**.