HIPAA Covered Entity Settles Breach Notification Failure with OCR for $2.175 Million

December 26, 2019

The HHS Office for Civil Rights (?ÃÂ£OCR?ÃÂ¥), which is the agency responsible for enforcement of the HIPAA privacy, security, and breach notification rules (?ÃÂ£HIPAA Rules?ÃÂ¥), announced a recent $2.175 million settlement with a covered entity under HIPAA (the ?ÃÂ£Covered Entity?ÃÂ¥) for the Covered Entity?ÃÃs failure to properly notify HHS of a breach of unsecured protected health information (?ÃÂ£PHI?ÃÂ¥) as required by the HIPAA Rules, and other potential violations.

Background

OCR had investigated the Covered Entity in response to an individual complaint it received that alleged the Covered Entity had sent correspondence to the individual containing another person?ÃÃs PHI.

OCR?ÃÃs investigation determined that the Covered Entity had mailed correspondence containing the PHI of 577 individuals to the wrong addresses. In some of the correspondence, the PHI consisted of the names and account numbers of the individuals and their dates of medical service. The Covered Entity had reported this incident to HHS as a breach affecting only eight of the individuals because the Covered Entity concluded, incorrectly, that unless the disclosure included patient diagnosis, treatment information, or other medical information, no reportable breach of PHI had occurred.

OCR also determined that the Covered Entity failed to have a HIPAA business associate agreement in place with one of the entities that performed business associate services for the Covered Entity. In addition to the monetary payment, OCR?ÃÃs settlement agreement required the Covered Entity to undertake a corrective action plan that included two years of monitoring by HHS.

Practice Tip

The facts regarding this OCR settlement serve as a helpful reminder to employers sponsoring group health plans that are ?ÃÂ£covered entities?ÃÂ¥ under HIPAA. The definition of PHI subject to the HIPAA privacy and security rules may be broader than commonly understood by a plan sponsor. For example, in addition to details regarding an individual?ÃÃs medical diagnosis or treatment, PHI includes information related to the provision of health care to the individual and payment for the provision of health care to the individual. In the event of an impermissible disclosure of individualized health information relating to health plans, employers must maintain and consult their HIPAA-compliant policies and procedures to determine whether any breach notification requirements have been triggered.

OCR?ÃÃs Press Release and Resolution Agreement with the Covered Entity is available here