HIPAA Settlements in April and May Highlight Key Compliance Concerns for OCR

06.16.2017

After a break in March with no new settlement agreements, OCR returned in April and May with quite a few. The Health Care Data Aware Blog already posted about a $400,000 OCR settlement released April 12, 2017, which can be read here. This post will provide insight into the remainder of the settlements from these two months.

On April 20, 2017, OCR announced a $31,000 settlement with the Center for Children's Digestive Health (CCDH) in Illinois. Several aspects of this settlement make it notable:

- Although the majority of settlements begin with a breach and subsequent notice to OCR, CCDH became the subject of a compliance review after OCR investigated one of its business associates, FileFax, Inc., a record storage company.
- A failure to produce a Business Associate Agreement (BAA) covering the entire period that CCDH disclosed to FileFax was the key violation resulting in a settlement – although FileFax received protected health information since 2003, there was no BAA on record until 2015.
- Every record turned over to FileFax before FileFax signed the BAA was considered the result of an impermissible disclosure, affecting over 10,000 patients.

Just a few days later, on April 24, OCR issued a press release announcing a $2.5 million settlement with CardioNet Inc. ("CardioNet"), a company that provides remote health monitoring services. This settlement, the first with a "wireless health services provider," shows that:

- Using mobile devices to maintain PHI can be risky, as CardioNet discovered when an employee's laptop was stolen from a vehicle. Many breaches of PHI arise from lost or stolen mobile devices, and entities should put strict procedures in place to monitor their movement and use, in accordance with the Security Rule, and utilize any guidance on mobile devices provided by OCR and the Office of the National Coordinator for Health Information Technology (ONC).
- Entities must adopt the policies they create and put them into practice. Here, CardioNet had a draft set of policies and procedures, but had not yet finalized them.
- Like many other settlements, the failure to perform a risk analysis and implement subsequent risk management measures were alleged violations contributing to the amount of the settlement. Under the Security Rule, routine risk analyses are a required standard with which all covered entities and

business associates must comply. *See* 45 C.F.R. 164.308(a)(1)(ii)(A).

Another settlement over $2 million was announced on May 10, 2017, with Memorial Hermann Health System (MHHS) in Texas. MHHS agreed to pay $2.4 million to settle alleged HIPAA violations arising from the issuance of press releases and further third party disclosures related to one patient. The lessons to be drawn from this settlement are that:

- Identifying a patient to the media requires HIPAA authorization. This settlement was the result of a compliance review initiated due to media reports naming a patient without obtaining proper authorization. It is important to remember that an authorization must meet specific requirements set forth in the Privacy Rule and cannot be an oral or implied consent. *See* 45 C.F.R. 164.508.
- Documentation is critical. Another alleged violation cited in the Resolution Agreement is MHHS' failure to record sanctions imposed on employees who impermissibly disclosed the patient's name and information. Records generated for HIPAA compliance purposes generally must be kept for a 6-year period. *See e.g.,* 45 C.F.R. 164.530(j).

The most recent OCR settlement published was a $387,200 settlement with St. Luke's-Roosevelt Hospital Center Inc. ("St. Luke's") due to improper disclosures of two patients' highly sensitive PHI, including HIV, sexually transmitted disease, and mental health diagnoses, by the St. Luke's clinic specializing in the treatment of patients with HIV or AIDS. The settlement was the result of an investigation that began in 2015 after a complaint was filed with OCR. The most important "take-aways" from this settlement are:

- OCR will account for the sensitive nature of PHI when negotiating a settlement. In its pressrelease, OCR states that "In exercising its enforcement authority, OCR takes into consideration aggravating factors such as the nature and extent of the harm caused by failure to comply with HIPAA requirements," and called the release of this information "egregious" in the Resolution Agreement.
- The releases in question were to third parties (an employer and an organization where the patient was a volunteer) against the express wishes of the patients. Covered entities must put proper processes and policies in place to ensure that all uses and disclosures of PHI comply with the Privacy Rule, including the handling of patient requests for additional privacy protections. *See* 45 C.F.R. 164.522.

OCR has published nine settlements already in 2017, and there is no indication that its enforcement activity will slow. With each new settlement announced from OCR, we learn a little bit more about OCR's enforcement concerns and considerations. To the extent that a covered entity or a business associate sees in these settlements areas where its own compliance can be strengthened, it should do so, before it becomes the subject of an OCR investigation.

Related People