Published on *The National Law Review* https://natlawreview.com

The Office for Civil Rights Speaks: HIPAA Liabilities Contained (Except When They Aren't)

Article By:

Edward I. Leeds

After a quiet winter, the Department of Health and Human Services' Office for Civil Rights (OCR) revived with the spring, issuing a set of frequently asked questions and two recent announcements.

The FAQs address the situation where an individual requests a covered entity to disclose protected health information ("PHI") to an app. The covered entity must generally comply with the request, even if the app is unsecured. It may be prudent to advise the individual of concerns about the app, but the individual has the right under HIPAA to access most PHI held by a covered entity set and to direct where the covered entity should send that information.

In case of unauthorized access to PHI that has been transmitted to the app, the liability of a covered entity, or an electronic health records ("EHR") developer acting as a business associate for the covered entity, will be determined by the relationship with the app. If, for example, there is no relationship with the app developer and the app does not perform functions on behalf of the covered entity, the FAQs provide comfort that the covered entity, and EHR developer, will not be exposed to penalties under HIPAA in the event of unauthorized access to PHI that has been transmitted to the app.

Conversely, if a relationship exist, for example, the app developer serves as a business associate of the EHR developer or the app is performing functions for the covered entity, the EHR developer and covered entity may be exposed to liability. Covered entities should consider building appropriate contractual protections into their business associate agreements to safeguard against such liabilities.

Within two weeks of publishing the new FAQs, the OCR issued a notification that it is reducing the maximum penalties that will apply to certain types of HIPAA violations. For penalty purposes, the OCR breaks HIPAA violations into four categories based on the severity of the violation. Prior to the new guidance, only the minimum penalty per violation increased with severity. The maximum penalty that could be imposed was the same for each category: $1.5 million for any type of violation per year. Under the new guidance, the maximum remains at $1.5 million for the most serious category of violations, but is lowered significantly for other types of violations. Going forward, the maximum penalty will be:

- Where the entity did not know and by exercising reasonable diligence would not have known

of the violation, $25K per type of violation per year.

- Where the violation arises from reasonable cause, $100K per type of violation per year.
- Where the violation arises from willful neglect and is corrected, $250K per type of violation per year.
- Where the violation arises from willful neglect and is not corrected, $1.5M per type of violation per year.

However, the reduction in the maximum penalties does not necessarily translate to a significant reduction in what the OCR will seek in enforcement actions, at least not with respect to the resolution agreements that the OCR has historically announced. Those resolution agreements typically pertain to situations where the OCR finds serious, uncorrected violations, often of more than one type.

One week after this notification, the OCR seemed to signal that it will continue to seek large settlement amounts when it followed the notice of penalty reductions with an announcement of a $3 million settlement with Touchstone Medical Imaging, LLC for violations that exposed the PHI of more than 300,000 patients. Although the OCR reached this resolution agreement prior to issuing its notice of the reduction in penalties, it is unlikely that the reduction would have made any difference with regard to the Touchstone breach, where the OCR found several HIPAA violations, including issues with the timing and thoroughness of the health care provider's investigation of the incident, which in turn led to a delay in its provision of notice of the breach to affected individuals.

The practical changes that will come from the reduction in penalties remain to be seen. Covered entities and their business associates under HIPAA may take comfort that relatively minor violations that are quickly addressed will not result in multimillion dollar liabilities, but based on past settlement announcements, it seems unlikely that the OCR would enforce the HIPAA requirements so harshly. On the other hand, it appears as if the OCR will continue to seek substantial monetary penalties for significant, uncorrected breaches.

Copyright © by Ballard Spahr LLP

National Law Review, Volume IX, Number 133

Source URL:https://natlawreview.com/article/office-civil-rights-speaks-hipaa-liabilities-contained-except-when-they-aren-t