

HIPAA - Enforcement

written by Richard Leslie | May 24, 2016

Avoiding Liability Bulletin - June 2013

... According to statistics from the U.S. Department of Health and Human Services (HHS), of the complaints that have been received and resolved since the HIPAA (Privacy Rule) compliance date in April 2003, over sixty percent (60%) of the complaints have been closed because they were not eligible for enforcement. The Office for Civil Rights (OCR) within HHS receives and resolves complaints for violation of the HIPAA Privacy Rule. An example of a complaint not eligible for enforcement is a complaint alleging a violation by an entity not covered by HIPAA. Additionally, it is possible that the complaint would be closed because it was not filed in a timely manner (generally within 180 days of the alleged violation).

The compliance issue investigated the most was for impermissible uses and disclosures of protected health information. The most common types of covered entities that have been required to take corrective action to achieve voluntary compliance are private practices. Approximately twelve and one-half percent (12.5%) of complaints were investigated and resulted in a finding of no violation. Approximately twenty-six and one-half percent (26.5%) of the complaints were investigated and resolved by some kind of enforcement action, such as requiring changes in the privacy practices of the involved covered entities.

These statistics, along with other information I have read, indicate to me that fears of the OCR and HIPAA enforcement by "the feds" is somewhat overblown. Of course, many sole proprietors may not be a "covered entity" under the HIPAA regulations. If a complaint is filed with HHS against such persons, their response to an OCR inquiry would be that they are not a covered entity and therefore not bound by the "Privacy Rule." The OCR will typically ask the subject of the complaint to submit information regarding whether or not certain information (insurance-related transactions) is transmitted electronically. Assuming that there is nothing suspicious about the explanation given to OCR, a statement indicating that there is no electronic transmission should suffice. OCR can, of course, inquire further.

Even in cases where the provider is a covered entity under HIPAA, the OCR generally seeks voluntary compliance and usually pays more interest to larger organizations with systemic problems and those who knowingly or intentionally violate the regulations. With respect to sole proprietors who are covered entities, the statistics seem to indicate that there is not much to worry about - unless, of course, the provider is involved in some kind of intentional or reckless behavior with respect to compromising the privacy of the patient or the provider has not voluntarily or adequately complied with the Privacy Rule's requirements.

When OCR finds some kind of a defect in a provider's privacy practices, they typically seek voluntary compliance. OCR is not likely to impose substantial fines unless there is a serious or substantial violation found. They will usually seek voluntary compliance, some form of corrective action, or other agreement. In more serious cases, however, they may file a formal finding of violation. The person complained against can request a hearing before an Administrative Law Judge with Health and Human Services to contest the finding.