COSMOS
Navigate the Compliance Universe

Compliance Today - April 2023

Adam Greene (AdamGreene@dwt.com, linkedin.com/in/adam-greene-dwt/) is Partner at Davis Wright Tremaine LLP, Washington, DC.

Current trends in health information privacy and information blocking enforcement

by Adam Greene

For health information privacy professionals, 2023 promises to be a busy year. In this article, we will look at the expanding number of laws governing personal information maintained by healthcare entities and their service providers, focusing on past and future enforcement trends for these laws.

HIPAA

The primary enforcement trend with HIPAA continues to be the U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR) enforcement of the individual's right of access outlined in 45 C.F.R. § 164.524. On January 3, 2023, OCR announced its 43rd financial enforcement action under its HIPAA Right of Access Initiative.[1] For perspective, OCR has brought 130 financial enforcement cases in total. Right-of-access cases over the past three years represent about a third of all cases brought since the Privacy Rule's initial compliance date almost 20 years ago.[2] There is no indication that OCR is taking its foot off the gas with respect to its HIPAA Right of Access Initiative. Accordingly, we expect enforcement of HIPAA's right of access to continue to be a top priority. Covered entities should review their policies, procedures, documentation, and training concerning the right of access and consider auditing how effective their processes work in practice.

After 130 financial enforcement actions, the average amount has been just over $1 million per resolution agreement or civil monetary penalty.[3] The lowest amount in a case was $3,500 for a right-of-access case, and the largest was $16 million for a breach involving approximately 80 million individuals.[4] Generally, right-of-access cases tend to resolve with substantially lower amounts than breach cases. Additionally, OCR often resolves enforcement actions with larger covered entities and business associates at significantly higher amounts than smaller entities.

Besides the HIPAA Right of Access Initiative, in 2022, OCR also brought financial enforcement cases with respect to providers impermissibly disclosing protected health information (PHI) online in response to negative reviews, improper disposal of PHI in publicly accessible garbage containers, a breach by hackers that OCR seemingly attributed to the covered entity's failure to conduct an accurate and thorough risk analysis, and a dentist impermissibly disclosing patient information to a campaign manager and marketing company for purposes of his state senate campaign.[5]

While the financial enforcement actions garner the headlines, they actually represent a very small fraction of OCR's resolutions. In contrast, as of December 31, 2022, OCR had resolved approximately 30,000 cases requiring corrective action and about 53,000 cases by providing technical assistance.[6]

In 2022, OCR also issued a request for information related to two statutory provisions related to enforcement: (1) a 2021 statutory provision requiring HHS to consider "recognized security practices" that HIPAA-covered entities and business associates adequately demonstrate were in place for the previous 12 months when HHS makes determinations regarding fines; and (2) a 2009 provision of the Health Information Technology for Economic and Clinical Health (HITECH) Act requiring HHS to establish a methodology for the distribution of a percentage of a HIPAA penalty or settlement to an individual harmed by the noncompliance.[7] At this time, we are awaiting proposed and final rules on both of these upcoming regulatory changes, and it may be years before they are finalized. Of the two regulatory changes, we believe the distribution of penalties to harmed individuals will be particularly noteworthy, as it may lead to an increase in the volume of complaints to OCR, cause greater friction between OCR and complainants when OCR chooses not to pursue financial enforcement, and set precedent for other breach laws for determining who qualifies as a "harmed individual" for purposes of a privacy violation.

OCR also recently published guidance on the applicability of HIPAA to the use of online tracking technologies by HIPAA-covered entities and business associates on their websites.[8] Pursuant to this guidance, certain information that a regulated entity collects about website visitors will constitute PHI, so the entity is limited in its use and disclosure. This would include the need to put in place a business associate agreement with a third-party service provider who receives such website PHI for purposes of advertisement tracking or website analytics. While OCR has not yet brought an enforcement action concerning website visitor data, this has become an area of significant class-action litigation. OCR's guidance should be treated as a shot across the bow, indicating that they may bring enforcement actions in the future for such data.

One area of enforcement that OCR has not addressed is the Fifth Circuit's 2021 decision in *University of Texas M.D. Anderson Cancer Center v. HHS*.[9] In that decision, M.D. Anderson challenged HHS's decision to seek civil monetary penalties for certain security incidents as arbitrary and capricious because it did not similarly penalize other entities with similar incidents. The court agreed with the covered entity, vacating the proposed penalties. The decision calls into question HHS's historical approach to enforcing HIPAA: resolving the vast majority of cases with technical assistance or corrective action while only bringing financial enforcement actions in a small minority of cases without articulating exactly why such cases are distinguishable from all others. One of the biggest enforcement questions in the years to come is whether the Fifth Circuit's decision will ultimately lead to a fundamental change in how OCR enforces HIPAA. So far, it seemingly has not.

OCR, however, is not the only HIPAA enforcer. The state attorneys general can also bring civil actions, and the Department of Justice (DOJ) can bring criminal prosecutions. We continue to see occasional enforcement action from both categories of enforcers.

With respect to state attorneys general, we have seen enforcement actions from Massachusetts, New Jersey, and New York over the past few years.[10] Oregon and Utah jointly settled a suit in 2022 requiring a healthcare management company to comply with HIPAA, although they actually alleged violations of state laws rather than HIPAA in their settlement documents.[11] In general, this has not been a very active area of enforcement, usually about three to five enforcement actions per year.

Similarly, we occasionally see a few criminal prosecutions under HIPAA. In November 2022, five former hospital employees were charged with violating HIPAA by disclosing patient names and contact information to a third party who sold the information to personal injury attorneys and chiropractors.[12] In October 2022, a former physician pleaded guilty under HIPAA to wrongfully disclosing patient information to a pharmaceutical sales representative.[13] In June 2022, a man in Iowa was sentenced to 27 months in prison for criminal HIPAA violations related to obtaining and disclosing a patient's mental health condition and medications for personal

gain and malicious harm.[14] In February 2022, a Florida man was sentenced to three years of probation for kickback and HIPAA violations for selling Medicare patient data as part of a false claims scheme.[15]