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]

Confidentiality of substance use disorder patient records, 42 C.F.R. Part 2

Rulemaking is underway to substantially revise 42 C.F.R. Part 2 (Part 2 Rule), the federal confidentiality rule governing certain substance use disorder information, concerning enforcement.

The Part 2 Rule was first promulgated in 1975, and in its over 45 years, we are not aware of a single enforcement action. The statute authorizing the Part 2 Rule originally provided fines of up to $500 for the first offense and up to $5,000 for each subsequent offense.[16] A 1992 law changed the penalties, providing that a person who violates the statute or regulations "shall be fined in accordance with Title 18, United States Code."[17] However, Title 18 never set forth applicable fines, leaving ambiguous what penalties, if any, could be imposed for violations of the Part 2 Rule. Additionally, only U.S. attorneys could enforce the Part 2 Rule (other than the Food and Drug Administration and then Substance Abuse and Mental Health Services Administration's authorities over methadone and opioid treatment programs, respectively, representing only a fraction of Part 2 programs). Additionally, without a breach notification requirement, violations of the Part 2 Rule often are unknown to the patient or law enforcement. All these factors—ambiguity over penalties, a low priority among U.S. attorneys, and a lack of transparency for violations—seemingly have contributed to the lack of enforcement actions since the Part 2 Rule's inception.

This dearth of enforcement may be coming to an end, however. In 2020, Section 3221 of the Coronavirus Aid, Relief, and Economic Security Act included an overhaul of the Part 2 Rule.[18] From a policy perspective, the biggest change to the Part 2 Rule is that a patient can provide general consent for the use and disclosure of the patient's substance use disorder records for treatment, payment, and healthcare operations. Once disclosed, under such consent, the recipient can redisclose the records as permitted for PHI under HIPAA rather than having to maintain the Part 2 Rule's more stringent confidentiality obligations. This partially addresses calls to better reconcile the Part 2 Rule and HIPAA. But this policy change may have less consequence than the changes to enforcement of the Part 2 Rule, as Section 3221 applies the HIPAA breach notification obligations and HIPAA's criminal and civil penalties to the Part 2 Rule.

On December 2, 2022, HHS issued a notice of proposed rulemaking to implement Section 3221's required changes to the Part 2 Rule.[19] The comment period ended on January 31, 2023. We do not know when a final rule will come, although I would not expect it before 2024 based on HHS' busy docket.

When finalized, the changes to the Part 2 Rule will likely reinvigorate its enforcement prospects. The breach notification requirement will increase transparency and scrutiny of violations. The clarified criminal penalties will make it easier to prosecute, although I would not expect DOJ to bring criminal prosecutions in any but the most egregious of cases. Most importantly, HHS will be able to bring civil penalties more readily, likely doing so in conjunction with enforcement of HIPAA violations.

It has always been extremely challenging for healthcare providers to comply with the Part 2 Rule, especially since the transition to electronic health records (EHRs). EHR systems often do not include functionality that allows healthcare providers to fully lock down substance use disorder records in compliance with the Part 2 Rule. For example, we have heard anecdotes of substance use disorder care being marked as confidential; however, related information still shows up in problem lists, medication lists, and appointment calendars accessible across a health system. Historically, the risk of these data leaks has been mitigated by the lack of enforcement. Once the proposed changes are finalized, healthcare providers may find themselves relying on HHS' enforcement

discretion when they suffer violations due to technical limitations of their EHR systems.

The Information Blocking Rule

The 21st Century Cures Act (Cures Act) Information Blocking Rule became "applicable" on April 5, 2021.[20] Yet, there currently are no mechanisms in place to enforce the rule. The Cures Act provides that the HHS Inspector General may impose civil monetary penalties of up to $1 million per violation of the Information Blocking Rule against health information technology developers of certified health information technology (HIT developers) and health information exchanges and health information networks (HIEs/HINs).[21] HHS Office of Inspector General (OIG) published a notice of proposed rulemaking for HIT developers and HIEs/HINs on April 24, 2020.[22] In the proposed rule, OIG indicated that conduct prior to its final rule's effective date (60 days after publication) would not be subject to penalties. As of the writing of this article, a final enforcement rule for HIT developers and HIEs/HINs has not yet been published, although the HHS regulatory agenda targeted March 2023.[23]

For healthcare providers, the Cures Act provides that, upon the OIG determining that a healthcare provider committed information blocking, the OIG will refer the provider to the appropriate agency to be subject to "appropriate disincentives using authorities under applicable Federal law, as the Secretary sets forth through notice and comment rulemaking."[24] HHS has not yet issued a notice of proposed rulemaking regarding what disincentives will apply to healthcare providers for information blocking. Accordingly, we do not know how HHS will enforce the Information Blocking Rule against healthcare providers or even which agency will be responsible for its enforcement. In the absence of a proposed enforcement rule, it likely will be years before a final rule and enforcement of the Information Blocking Rule against healthcare providers begin.

The Federal Trade Commission (FTC)

HHS is not the only federal agency with authority to bring enforcement actions with respect to health information privacy and security. The FTC has two statutory authorities that are applicable to this space.

First, under Section 5 of the FTC Act, the FTC can bring enforcement actions for unfair and deceptive trade practices.[25] For example, in January 2021, the FTC entered into a consent order with Flo Health, alleging that the company shared personal health information with third parties, violating its privacy policy.[26] The FTC has brought actions over the years against pharmacies, labs, billing companies, health information technology companies, and other entities also subject to HIPAA as covered entities or business associates.[27] Of note, the FTC generally does not have authority under Section 5 to bring actions against nonprofit entities.

Second, the FTC has a breach notification rule (Health Breach Notification Rule) governing personal health records.[28] The rule was promulgated under the HITECH Act, but we are not aware of any enforcement actions to date. The FTC's Health Breach Notification Rule does not apply to HIPAA-covered entities or to entities acting as business associates subject to HIPAA. In September 2021, the FTC published a statement regarding the scope of the Health Breach Notification Rule, clarifying that: (1) "personal health records" broadly include health and wellness apps to the extent that they collect health information from one source and information from any other sources (e.g., a fitness app that syncs with a consumer's fitness tracker and collects other information directly from the consumer), and (2) a "breach" includes any unauthorized access to a personal health record, including sharing such information without an individual's authorization—it is not limited to "cybersecurity intrusions or nefarious behavior."[29] It seems likely the FTC will seek to enforce the Health Breach Notification Rule based on this "clarified" scope.

State laws

Finally, a growing number of states are enacting general privacy laws governing personal information. As of January 2023, California, Colorado, Connecticut, Utah, and Virginia have enacted general privacy laws, and many other states have legislation in the works.[30] So far, all these state laws exempt PHI governed by HIPAA, and Connecticut, Utah, and Virginia laws exempt HIPAA-covered entities and business associates entirely. But some healthcare entities may find that certain personal information that is not PHI, such as employee personal information or certain website visitor information, is subject to these new state laws. It is too early to tell what enforcement will look like under these new laws, including whether it may reach healthcare entities.

Conclusion

In sum, there is an unprecedented amount of federal and state activity surrounding health information privacy. Each new law brings new potential risks for healthcare entities to navigate. Compliance officers, privacy officers, and privacy counsel can rest assured that they will have plenty to keep them busy in 2023 and the years to come.

Takeaways

- U.S. Department of Health & Human Services (HHS) Office for Civil Rights continues to prioritize enforcing the HIPAA right of access, so covered entities should ensure strong practices and training in this area.
- HHS is amending 42 C.F.R. Part 2, the rule governing the confidentiality of substance use disorder records, to provide for breach notification and increased enforcement mechanisms.
- There continues to be no enforcement mechanisms in place for the 21st Century Cures Act Information Blocking Rule with respect to healthcare providers.
- The Federal Trade Commission has clarified the scope of its Health Breach Notification Rule to broadly govern health and wellness apps.
- New state general privacy laws tend to exempt protected health information governed by HIPAA but govern other personal information such as employee data.

1 U.S. Department of Health & Human Services, Office for Civil Rights, "Lab Pays $16,500 Settlement to HHS, Resolving Potential HIPAA Violation over Medical Records Request," news release, January 3, 2023, https://www.hhs.gov/about/news/2023/01/03/lab-pays-16-thousand-5-hundred-dollar-settlement-to-hhs-resolving-potential-hipaa-violation.html.
2 U.S. Department of Health & Human Services, Office for Civil Rights, "Enforcement Highlights," last reviewed January 13, 2023, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (indicating 129 financial enforcement actions through December 31, 2023, which does not include the January 3, 2023 case).
3 U.S. Department of Health & Human Services, Office for Civil Rights, "Enforcement Highlights."
4 "Resolution Agreement," U.S. Department of Health & Human Services and Patricia King MD & Associates, August 20, 2020, https://public3.pagefreezer.com/content/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/sites/default/files/king-md-ra-cap.pdf; "Resolution Agreement," U.S. Department of Health & Human Services Office for Civil Rights and Anthem, Inc., October 15, 2018, https://www.hhs.gov/sites/default/files/anthem-ra-cap.pdf.
5 U.S. Department of Health & Human Services, Office for Civil Rights, "Resolution Agreements: Resolution Agreements and Civil Money Penalties," last reviewed February 2, 2023, https://www.hhs.gov/hipaa/for-

professionals/compliance-enforcement/agreements/index.html.
6 U.S. Department of Health & Human Services, Office for Civil Rights, "Enforcement Highlights."
7 Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended, 87 Fed. Reg. 19,833 (April 6, 2022), https://www.federalregister.gov/documents/2022/04/06/2022-07210/considerations-for-implementing-the-health-information-technology-for-economic-and-clinical-health.
8 U.S. Department of Health & Human Services, Office for Civil Rights, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," last reviewed December 1, 2022, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.
9 University of Texas M.D. Anderson Cancer Center v. U.S. Department of Health & Human Services, U.S. Court of Appeals, Fifth Circuit, 985 F.3d 472 (2021).
10 Massachusetts Office of the Attorney General Maura Healey, "Home Health Care Company To Pay $425,000 Following Data Breach Impacting Thousands of Massachusetts Residents," news release, November 3, 2022, https://www.mass.gov/news/home-health-care-company-to-pay-425000-following-data-breach-impacting-thousands-of-massachusetts-residents; Letitia James, New York Attorney General, "Attorney General James Announces $600,000 Agreement with EyeMed After 2020 Data Breach," news release, January 24, 2022, https://ag.ny.gov/press-release/2022/attorney-general-james-announces-600000-agreement-eyemed-after-2020-data-breach; New Jersey Division of Consumer Affairs, Office of the Attorney General, "New Jersey Health Care Providers Will Adopt New Security Measures and Pay $425,000 to Settle Investigation into Two Data Breaches, news release, December 15, 2021, https://www.njconsumeraffairs.gov/News/Pages/12152021.aspx; New Jersey Office of the Attorney General, "Acting AG Bruck Reaches Settlement with Two Printing Companies over Improper Disclosures of Protected Health Information," State of New Jersey, Department of Law & Public Safety, news release, November 10, 2021, https://www.njoag.gov/acting-ag-bruck-reaches-settlement-with-two-printing-companies-over-improper-disclosures-of-protected-health-information/.
11 Circuit Court of the State of Oregon for the County of Multnomah, "In the matter of Avalon Healthcare Management, Assurance of Voluntary Compliance," December 22, 2022, https://www.doj.state.or.us/wp-content/uploads/2022/12/AVC_Avalon_2022.pdf; Utah Office of Attorney General, "Assurance of Voluntary Compliance," December 5, 2022, https://attorneygeneral.utah.gov/wp-content/uploads/2023/01/Assurance-of-Voluntary-Compliance-Avalon-and-Utah-Signed-1.pdf.
12 U.S. Department of Justice, U.S. Attorney's Office for the Western District of Tennessee, "Five Former Methodist Hospital Employees Charged with HIPAA Violations," news release, November 10, 2022, https://www.justice.gov/usao-wdtn/pr/five-former-methodist-hospital-employees-charged-hipaa-violations.
13 U.S. Department of Justice, U.S. Attorney's Office for the District of New Jersey, "Doctor Admits Criminal HIPAA Scheme for Wrongful Disclosure of Protected Patient Health Information to Pharmaceutical Sales Representative," news release, October 7, 2022, https://www.justice.gov/usao-nj/pr/doctor-admits-criminal-hipaa-scheme-wrongful-disclosure-protected-patient-health.
14 U.S. Department of Justice, U.S. Attorney's Office for the Southern District of Iowa, "Des Moines Man Sentenced to 27 Months in Prison for Criminal HIPAA Violations," news release, June 29, 2022, https://www.justice.gov/usao-sdia/pr/des-moines-man-sentenced-27-months-prison-criminal-hipaa-violations.
15 U.S. Department of Justice, U.S. Attorney's Office for the District of Massachusetts, "Florida Man Sentenced in Multi-Million-Dollar Medicare Fraud Scheme," news release, February 17, 2022, https://www.justice.gov/usao-ma/pr/florida-man-sentenced-multi-million-dollar-medicare-fraud-scheme.
16 Confidentiality of Alcohol and Drug Abuse Patient Records, 40 Fed. Reg. 27,802, 27,803 (July 1, 1975).
17 ADAMHA Reorganization Act, Pub. L. No. 102-321 § 131, 106 Stat. 323, 369 (1992).
18 CARES Act, Pub. L. No. 116-136 § 3221, 134 Stat. 281, 375 (2020).
19 Confidentiality of Substance Use Disorder (SUD) Patient Records, 87 Fed. Reg. 74,216 (Dec. 2, 2022),

https://www.federalregister.gov/documents/2022/12/02/2022-25784/confidentiality-of-substance-use-disorder-sud-patient-records.
2045 C.F.R. § 171.101(b).
2142 U.S.C. § 300jj-52(b)(2)(A).
22 Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules, 85 Fed. Reg. 22,979 (April 24, 2020), https://www.federalregister.gov/documents/2020/04/24/2020-08451/grants-contracts-and-other-agreements-fraud-and-abuse-information-blocking-office-of-inspector.
23 U.S. Department of Health & Human Services, "Amendment to Civil Monetary Penalty Law Regarding Grants, Contract, and Information Blocking," 0936-AA09, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=0936-AA09.
2442 U.S.C. § 300jj-52(b)(2)(B).
2515 U.S.C. § 45.
26 "Decision and Order," Before the Federal Trade Commission In the matter of Flo Health, Inc., Docket No. C-5747, June 17, 2021, https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_decision_and_order.pdf.
27 Federal Trade Commission, "Privacy and Security Enforcement," accessed February 13, 2023, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.
2816 C.F.R. Part 318.
29 Federal Trade Commission, "Statement of the Commission On Breaches by Health Apps and Other Connected Devices," September 15, 2021, https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.
30 California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 to 1798.199.100; Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 to 6-1-1313; Connecticut Data Privacy Act, Conn. Pub. Act 22-15; Utah Consumer Privacy Act, Utah Code Ann. §§ 13-61-101 to 13-61-404; and Virginia Consumer Data Privacy Act, Va. Code Ann. §§ 59.1-575 to 59.1-584.