# Risks Abound
## Safeguarding Health

*by* | **Katherine R. Kratcha** and **Sarah A. Sargent**

# d:
# Plan Data

The privacy and security of health information has become an area of increased focus for regulators following the Supreme Court ruling in *Dobbs* as well as several large data breaches. Health plan sponsors should take note and review their plans for compliance with HIPAA and other rules.

benefits MAGAZINE

Over the last year, the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules (and the use of medical information in general) have received a significant amount of attention from both the public and regulators. In part, concerns around the privacy of medical information began to increase after the Supreme Court issued its decision to end the constitutional right to abortion in *Dobbs v. Jackson Women's Health Organization*.[1] In the wake of *Dobbs*, many consumers and government officials questioned how companies tracked and gathered online medical information. In addition to the privacy concerns raised post-*Dobbs*, several recent large vendor data breaches involving medical information have ensured that the security of medical information remains a top concern for organizations and regulators. This heat, light and attention on the privacy and security of medical information has resulted in notable updates in the past year to which every HIPAA-covered entity and plan sponsor should pay attention.

## A Brief Privacy and Security Rules Overview

As a quick overview, the HIPAA Privacy and Security Rules establish standards for how covered entities, such as group health plans and their vendors, should handle protected health information (PHI).[2] For example, the Privacy Rule requires covered entities to provide privacy notices to individuals describing how the entity will use and disclose the individual's PHI and the individual's rights over their PHI.[3] The Privacy Rule also dictates when a covered entity or *business associate* (a vendor of the covered entity) may share PHI with third parties. If a covered entity shares PHI with a vendor, the vendor must commit to comply with the Privacy and Security Rules in a contract.[4] The Security Rule requires covered entities to maintain certain cybersecurity standards, such as maintaining written security policies and regularly reviewing security practices.[5] The Security Rule also dictates when covered entities must provide individuals with notices of a data breach.[6]

## Enforcement and Consequences of Noncompliance

If an entity does not comply with the Privacy and Security Rules, it could face an investigation or enforcement action from the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Penalties include civil fines, criminal fines and criminal charges.[7]

OCR investigations typically start with a complaint or a breach report, although the agency also has the authority to initiate compliance reviews on its own. OCR investigates all reported breaches that involve 500 or more individuals[8] and also may investigate other reported breaches.

OCR generally prefers to enter into settlement agreements rather than impose civil penalties so that it may require the entity to prove its compliance during an oversight period—generally for three years—in addition to paying a settlement amount. Covered entities and business associates tend to prefer settling as well since the settlement amounts are lower than the civil money penalties that OCR would otherwise pursue and the entity is not usually required to admit a violation.

If OCR does impose civil penalties, the amounts range from $100 to $50,000 per violation.[9] Annual limits of approximately $25,000 to $1.5 million (adjusted annually for inflation) apply for all violations of the same requirement.[10] The penalties are tiered depending on culpability, ranging from whether the entity did not know and reasonably would not have known of the violation to whether the violation was due to willful neglect and not quickly corrected.

If a person knowingly discloses or obtains individually identifiable health information in violation of the HIPAA rules, OCR will refer the case to the Department of Justice for criminal investigation. As of July 31, 2023, OCR had made 1,862 such referrals.[11] Potential criminal penalties include a fine of up to $50,000, imprisonment of up to one year, or both, or higher fines and prison terms for offenses that involve false pretenses or the intent to sell, transfer or use PHI to gain an advantage or cause harm.[12]

In addition, the Department of Labor (DOL) has begun asking questions and requesting documents on health plans' cybersecurity and information security in investiga-

## learn more

**Education**

**HIPAA Security E-Learning Course**

Visit *www.ifebp.org/elearning* for more details.

**33rd Annual Health Benefits Conference and Expo (HBCE) January 29-31, 2024, Clearwater Beach, Florida**

Visit *www.ifebp.org/hbce* for more information.

tions. Many of these requests are consistent with DOL guidance from April 2021 regarding cybersecurity for plans subject to the Employee Retirement Income Security Act of 1974 (ERISA). This guidance focused on retirement plans but is widely applicable to all ERISA plans.

## takeaways

- Common online tracking technologies are, in the view of the Department of Health and Human Services Office for Civil Rights (OCR), causing breaches of the Health Insurance Portability and Accountability Act (HIPAA) and have resulted in lawsuits. Health plans and business associates need to know whether their websites or mobile apps use tracking technologies and what protective measures are needed.
- Large HIPAA breaches involving hacking and information technology (IT) incidents are becoming more common and affecting greater numbers of plans and individuals.
- The prevalence of large breaches is making careful contracting by plan sponsors all the more important to protect against a breach and minimize costs.
- Employee Retirement Income Security Act (ERISA) plan sponsors also should use the Department of Labor's April 2021 guidance to evaluate and bolster their plans' cybersecurity.

## HHS Guidance on Online Tracking

One notable 2023 HIPAA update follows the fallout from OCR's December 2022 guidance on the "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates."[13] The 2022 guidance clarified that the use of online tracking technologies, such as the Meta pixel, Google Analytics or other website cookies, could result in the impermissible sharing of PHI. For example, if a patient's IP address was shared with Google such that Google knew the patient logged into a specific hospital's patient portal or made an appointment with a provider, then such disclosure would be impermissible under the Privacy Rule unless the hospital had a business associate agreement with Google. Thus, the mere knowledge that an individual visited a particular website could be considered PHI. In addition, OCR stated that such impermissible disclosures may require covered entities to notify individuals of a data breach pursuant to the Security Rule.

After the guidance was issued, some health care providers did notify individuals of a data breach related to the use of online tracking technologies. Quickly after the guidance and notifications, a number of providers were also sued in class action lawsuits related to the impermissible sharing of PHI via online tracking technologies.[14] The lawsuits allege that the providers violated the Privacy Rule by sharing IP addresses with Meta, Google or other similar technology providers without a business associate agreement or any other basis that permitted such disclosures. While many of the original lawsuits are still pending, the number of tracking-related lawsuits continues to increase as plaintiffs' attorneys can easily see what tracking technologies a covered entity's website uses and can allege such disclosures are impermissible. Many entities are frustrated by the outcome of the OCR bulletin, and even the American Hospital Association called for OCR to finalize the amendment to the Privacy Rule and clarify that a mere IP address is not PHI.[15]

To avoid these lawsuits, plans should first investigate whether and how their websites or mobile applications use tracking technologies. An example would be a health plan web page that requires a user to log in and uses website analytics tools, such as Google Analytics, to track how a user navigates the website. If tracking technologies are used, then plans should have a detailed understanding of what information is being collected and shared with technology vendors. If PHI could be shared with a vendor, then a business associate agreement must be in place with the vendor. Plans should be cautious if they rely on vendors to manage tracking technologies since many vendors do not fully understand the latest OCR guidance on tracking technologies. Thus, plans should ensure that they receive correct information during these investigations and perform their own analysis of any technologies.

## The Impacts of Large Vendor Data Breaches

A second notable 2023 update comes from the lessons learned from some of the large vendor data breaches that have impacted covered entities and plans recently. One such large vendor data breach was the 2020 ransomware attack against Blackbaud, Inc.—a software provider that hosted a large amount of PHI and donor information for thousands of organizations. After notifying its customers of the breach, Blackbaud faced an organized investigation by various state attorneys gener-

al and a number of lawsuits, including by its customer Trinity Health and its insurer Aspen American Insurance Company.[16] In the lawsuit, Trinity alleges that Blackbaud violated the parties' agreement, breached fiduciary duties, negligently misrepresented its security practices, and was negligent and grossly negligent. Trinity seeks reimbursement for the costs it incurred due to the data breach, such as costs related to mailing notices, providing credit monitoring and legal fees. However, the court held on May 31, 2023 that only the contract-related claims could move forward because there is no common law duty to protect the public from data breaches and Blackbaud did not owe any fiduciary duties to Trinity.[17] The lawsuit is ongoing, but the initial decision from the court shows the importance of fulsome privacy and security provisions in vendor contracts.

Without a well-negotiated contract, a plan could bear the brunt of costs related to a data breach and face an uphill (and expensive) battle in court to try to recover from the responsible vendor. For key vendors with access to PHI, whenever possible, plans should include the following in the contract (or business associate agreement).

- Specific security requirements above and beyond mere compliance with law
- Detailed reporting requirements related to data breaches
- An obligation to effectuate notice at the direction of the plan or to reimburse the plan for any incurred notification costs
- A provision requiring the vendor to indemnify the plan for any costs related to a data breach
- An exclusion from the limitation of liability for any costs related to data breaches

## Notable Enforcement Updates

Sponsors of group health plans governed by ERISA also will need to keep two eyes out for enforcement, especially if they have been affected by a data breach. DOL has begun asking for information on health plans' cybersecurity posture in its investigations, and OCR is reorganizing to more effectively handle its caseload.

DOL appears to be using its cybersecurity guidance from April 2021 as a road map in investigations for health plans, similar to its approach with retirement plans. DOL guidance came in three publications: "Tips for Hiring a Service Provider," "Cybersecurity Program Best Practices" and "Online Security Tips." DOL began asking questions regarding retirement plans' cybersecurity in investigations soon after it published its guidance in 2021. Now, recent investigations indicate that the Department has gained enough experience with cybersecurity to start questioning fiduciaries of health plans as well. Although the DOL guidance generally is addressed to retirement plan sponsors and service providers, the fiduciary principles that it is based upon apply to all ERISA plans.

In addition to increased DOL enforcement, OCR hopes to increase enforcement of the HIPAA Privacy and Security Rules. OCR is reorganizing into three new divisions: Enforcement, Policy and Strategic Planning.[18] The agency is also renaming the Health Information Privacy Division to the Health Information Privacy, Data, and Cybersecurity Division (HIPDC) to better reflect its cybersecurity work. HIPDC will support the three new divisions in addressing health information privacy and cybersecurity.

The name of the new enforcement division makes its mission clear; OCR intends for the division to more effectively respond to complaints and drive greater enforcement of the law. OCR is trying to keep up with the continued growth in breaches and especially large breaches—those affecting 500 or more individuals. The 2023 OCR *Annual Report to Congress* regarding breaches of unsecured PHI offers the following statistics.[19]

- Between 2017 and 2021, the number of breaches affecting fewer than 500 individuals increased 5% and the number of breaches affecting 500 or more individuals rose 58%.
- Ninety-three of these reported large breaches in 2021 were from health plans, affecting over 3 million people.
- Hacking or information technology (IT) incidents accounted for 75% of large breach reports in 2021 and for 95% of the total number of people affected by large breaches of PHI.
- Hacking and IT incidents caused only 1% of smaller breaches (those affecting fewer than 500 individuals) reported in 2021 but affected a disproportionate number of individuals (24%) among those breaches.

In addition, OCR received more than 33,000 complaints in 2022 alleging HIPAA violations.[20]

The new policy division staff will work to increase implementation of HIPAA Privacy and Security Rules. Even though these rules are not new, many covered entities and business

associates could still use the help. In its most recent report to Congress, OCR identified a number of areas under the Security Rule that need improvement.[21] OCR thinks the following HIPAA Security Rule standards need better compliance.

- Conducting risk analyses, implementing security risk management measures and regularly reviewing system activity
- Implementing audit controls to catch and review malicious activity
- Allowing only those with proper access rights into systems containing electronic PHI

## Conclusion

Covered entities and plan sponsors faced a variety of cybersecurity and privacy challenges this year, ranging from breach reporting and litigation over online tracking technologies to dealing with large breaches with service providers and facing additional scrutiny by federal agencies. Breaches and cyberthreats are not likely to decline in 2024. Plan sponsors should take the time to consider their plans' security and make any necessary changes for their protection.

## Endnotes

1. 142 S. Ct. 2228 (2022).
2. Privacy Rule, 45 CFR Part 160 and Subparts A and E of Part 164; Security Rule, 45 CFR Part 160 and Part 164, Subparts A and C.
3. 45 CFR §164.520.
4. 45 CFR §164.502.
5. 45 CFR §164.308.
6. 45 CFR §164.404.
7. 42 USC §320d-6; 42 USC §1320d-5.
8. www.hhs.gov/sites/default/files/breach-report-to-congress-2021.pdf. Covered entities under HIPAA must notify affected individuals, the Secretary of the Department of Health and Human Services (HHS) and, in some cases, the media, after discovering a breach of unsecured protected health information (PHI) or learning of one by a business associate. If a breach involves 500 or more individuals (a "large breach"), the covered entity needs to notify HHS when it notifies the affected individuals—within 60 days of discovery—under 45 CFR § 164.408(b). Covered entities must report breaches involving fewer than 500 individuals to HHS annually by March 1 (February 29 in a leap year), under 45 CFR §164.408(c).
9. 42 USC §1320d-5(a)(1).
10. Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties, 84 FR 18151, 18153, www.federalregister.gov/d/2019-08530.
11. www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.
12. 42 USC §1320d-6.
13. HHS, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited August 1, 2023).
14. See generally, *Kurowski v. Rush System For Health*, No. 22-5380, 2023 WL 4707184 (N.D.Ill. July 24, 2023). *Horton v. Willis-Knighton Medical Center*, No. 23-314 (W.D.La. filed March 8, 2023). *Stewart v. Advocate Aurora Health*, No. 22-5964 (N.D.Ill. Filed Oct. 28, 2022).
15. Melinda Reid Hatton, "American Hospital Association, Letter to OCR on HIPAA Privacy Rule, Online Tracking Guidance" (May 23, 2023), www.aha.org/lettercomment/2023-05-22-aha-letter-ocr-hipaa-privacy-rule-online-tracking-guidance.
16. *Aspen American Insurance Company v. Blackbaud, Inc.*, No. 22-44 (N.D.Ind. May 31, 2023).
17. The court held that the negligent misrepresentation claim could not move forward because it was barred by the economic loss doctrine.
18. www.hhs.gov/about/news/2023/02/27/hhs-announces-new-divisions-within-office-civil-rights-better-address-growing-need-enforcement-recent-years.html.
19. www.hhs.gov/sites/default/files/breach-report-to-congress-2021.pdf.
20. www.hhs.gov/about/news/2023/02/27/hhs-announces-new-divisions-within-office-civil-rights-better-address-growing-need-enforcement-recent-years.html.
21. www.hhs.gov/sites/default/files/breach-report-to-congress-2021.pdf.

bios

**Katherine R. Kratcha** is an attorney with the law firm of Reinhart Boerner Van Deuren s.c. in Milwaukee, Wisconsin. Her practice centers on advising health and welfare plan sponsors, including employers, boards of trustees for multiemployer plans and associations. Kratcha holds a J.D. degree from the University of Wisconsin Law School. She can be reached at kkratcha@reinhartlaw.com.

**Sarah A. Sargent** is a certified information privacy professional (CIPP)/U.S. and CIPP/E certified attorney at Godfrey & Kahn S.C. in Milwaukee, Wisconsin. She specializes in cybersecurity and data privacy, specifically with respect to domestic and international compliance planning and data breach response. Sargent holds a J.D. degree from the University of Iowa College of Law. She can be reached at ssargent@gklaw.com.

pdf/1123