

It's Your Fault! Breach Notification in the Age of Electronic Health Information Exchange

By Adam H. Greene, Davis Wright Tremaine LLP

You are traveling on a family trip to a national park in a remote part of the country that you previously only dreamed of visiting. Unfortunately, a tumble leaves you visiting that scenic area's closest emergency department. Within moments of first seeing you, the treating physician can instantly pull up your past medical records, identifying some relevant medication allergies and past conditions. Or you are visiting a new specialist for the first time. In addition to asking for your medical history, she can see past x-rays, CT scans, and MRIs, allowing her to identify whether something of note has changed over the years. These are just some of the myriad of use cases that make nationwide health information exchange (HIE) so exciting. Through increased interoperability and connectivity, patients, health systems, and health plans have the opportunity to realize improved health care and reduced health care costs.

To quote the immortal words of Ben Parker, however, with great power comes great responsibility. An HIE corollary may be that with great access to medical records comes great temptation. The benefits of HIE come with a dark side. A doctor in Minnesota can look up the medical information of a high school crush in New Mexico. A nurse in New York can seek to look up a celebrity's medical records in California. A billing agent in Florida can use HIE to try to locate an ex-girlfriend who is hiding from him due to past physical abuse. A physical therapist in Texas could look up reproductive health care records of his daughter in Colorado for purposes of bringing litigation against her mother and the treating physician under Texas law.

Accordingly, any health care organization that is participating in HIE, or looking to expand its HIE footprint through participation in the nationwide HIE framework known as the Trusted Exchange Framework and Common Agreement (TEFCA),¹ must balance the significant patient benefits of increased HIE participation with the increased risk of patients' information becoming breached.

Breach Notification Laws: Blame the Victim?

In 2002, California enacted the nation's first breach notification law.² The legislation's focus was to allow victims of identity theft to receive notification so that they could act quickly to minimize the damage.³ After Californians began receiving breach notices, other states followed suit and enacted their own breach notification laws.

In general, these state breach notification laws require an entity that maintains computerized data containing personal information to notify affected individuals, sometimes regulators, and sometimes others (such as credit reporting agencies) if an unauthorized person gains unauthorized access or acquisition of the personal information.⁴ Breach notification laws do not place obligations on the persons who committed the unauthorized access or acquisition. The unauthorized persons are often bad actors and presumably cannot be trusted to comply with the law and provide

appropriate notifications. Prosecutors potentially can bring criminal enforcement actions against such bad actors. Instead, the victim of the unauthorized access or acquisition—the organization that maintained the computerized data—must incur the costs and reputational harm of providing the breach notifications.

Sometimes a breach may occur because an organization maintained inadequate safeguards for the personal information. Other times, however, an organization may have reasonable safeguards and nevertheless experience a breach. None of the state breach notification laws make an organization's notification obligations contingent on whether it acted reasonably to safeguard the personal information.

In 2009, Congress added breach notification requirements to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) through the Health Information Technology for Economic and Clinical Health (HITECH) Act.⁵ Pursuant to the HITECH Act, the U.S. Department of Health and Human Services (HHS) issued an interim final breach notification rule in 2009 and a final rule in 2013 at 45 C.F.R. pt. 164 subpt. D.⁶ The HIPAA Breach Notification Rule requires a business associate to report a breach of unsecured protected health information (PHI) to a covered entity, and requires a covered entity to notify affected individuals, HHS, and (if more than 500 affected individuals in a state or jurisdiction) the media.⁷ The rule defines a “breach” as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule that compromises the security or privacy of the PHI, with certain exceptions.⁸ As with state breach notification laws, the HIPAA Breach Notification Rule requires a regulated entity to provide breach notification without regard to whether the entity was in any way at fault for the breach.

Breaches Caused by Other Entities

In 2008, before the HITECH Act and its corresponding Breach Notification Rule, the HHS Office for Civil Rights (OCR) issued a series of guidance documents focused on how HIPAA's Privacy Rule applies to HIE. In a document on “Accountability,” OCR provided guidance on liability for impermissible disclosures in HIE, stating that: “a covered entity is not liable for a disclosure that is based on the non-compliance of another entity within the health information exchange, as long as the covered entity has complied with the Privacy Rule.”⁹

After the HITECH Act and Breach Notification Rule, however, OCR has not updated the above guidance to reflect which entity has breach notification obligations in HIE. For example, while a covered entity may not be liable for a disclosure that is based on the non-compliance of another entity within the HIE, OCR has not formally clarified whether the covered entity whose PHI was inappropriately accessed has the breach notification obligations (despite having done nothing wrong and not being liable for the disclosure).

In the absence of OCR guidance on this point, there is a significant risk that OCR or another regulator (e.g., a state attorney general) will take the position that the breach notification obligations fall on the regulated entity whose PHI was inappropriately

accessed in an HIE, even if the inappropriate access was by the workforce member of another regulated entity.

In 2024, this issue was highlighted with respect to TEFCA in a public dispute between Epic, the electronic health record vendor, and Particle Health, a health tech company that aggregates health information for its customers.¹⁰ Epic alleged that three Particle Health customers were making questionable use of patient data through TEFCA for purposes unrelated to patient care or treatment. For example, one of the customers in question provides legal professionals with access to real-time medical records. While Epic and Particle Health publicly disputed the matter, health care providers whose records were accessed by the customers in question were left to investigate and determine whether they had breach notification obligations under HIPAA and state laws. All because they chose to participate in TEFCA and make their patients' records more readily available for treatment and other permissible purposes.

TEFCA's Privacy and Security Safeguards

To be fair, privacy and security considerations were top of mind during TEFCA's drafting.

Before delving into TEFCA's privacy and security requirements, an overview of its structure is helpful. TEFCA is overseen by a recognized coordinating entity (RCE). The HHS Office of the National Coordinator of Health Information Technology (ONC)¹¹ selected a nonprofit entity called the Sequoia Project to act as the RCE.¹² Organizations that facilitate HIE apply to the RCE to become qualified health information networks (QHINs). Once an applicant completes the onboarding process, they can participate as a Designated QHIN. As of March 24, 2025, there are eight Designated QHINs, such as eHealth Exchange, Epic Nexus, and CommonWell. The QHINs enter into the Common Agreement (a portion of TEFCA) with the RCE. The Common Agreement Exhibit 1 requires QHINs to flow down certain standard terms to "participants." A participant could be an end user, such as a health care provider, or could be an intermediary, such as a commercial or regional HIE or an electronic health record vendor. If the participant is an intermediary, then it must flow down Common Agreement Exhibit 1's terms to its subparticipants (who themselves could be intermediaries and have further subparticipants).

The end user of data—a participant or subparticipant—may be a HIPAA covered entity or business associate. Alternatively, a participant or subparticipant may fall outside of HIPAA, such as a health care provider who does not electronically conduct HIPAA-covered transactions (or a company that purports to provide medical care as part of supporting class action attorneys' tort cases).

TEFCA requires most participants that are not subject to HIPAA to comply with relevant HIPAA Privacy Rule requirements and the Security Rule as if the participants were HIPAA covered entities.¹³ Additionally, TEFCA requires participants to report security incidents upstream to a QHIN, participant, or subparticipant and also to report security incidents downstream to affected subparticipants.¹⁴ For example, if a regional HIE connects to TEFCA through a QHIN and experiences a security incident, then the

regional HIE is a “participant” and must notify the upstream QHIN and the affected downstream subparticipants (e.g., health care providers participating in the regional HIE).

The RCE has adopted a standard operating procedure (SOP) governing TEFCA security incident reporting. Under the SOP, a party must report a security incident upstream and downstream as soon as reasonably practicable, but no more than 72 hours after discovery of the incident. Additionally, a QHIN must report a security incident to the RCE and to all other QHINs likely impacted within the same time frame. In the above example, the regional HIE would need to report the incident to its QHIN and to affected subparticipants (e.g., health care providers) as soon as reasonably practicable, but no more than 72 hours after discovery. Upon receiving notice from the regional HIE, its QHIN would need to report the incident to the RCE and to other QHINs likely impacted as soon as reasonably practicable, but no more than 72 hours after receiving the notification from the regional HIE.

While the above represents relatively stringent security incident reporting requirements, TEFCA more or less punts on the question of who has breach notification obligations to affected individuals and regulators. For example, the Common Agreement Exhibit 1 provides:

Nothing in this Section 8.3 shall be deemed to modify or replace any breach notification requirements that You may have under the HIPAA Rules, the FTC Rule, or other Applicable Law. To the extent You are already required by Applicable Law to notify Upstream QPS or a Subparticipant of an incident that would also be a TEFCA Security Incident, this section does not require duplicative notification.

Accordingly, participants and subparticipants must determine whether breach notifications fall on them or another entity under applicable law. If a participant’s PHI is impermissibly accessed by another participant, then TEFCA includes contractual reporting requirements among the participating TEFCA entities, but does not address which entity (e.g., the participant whose patients’ data was inappropriately accessed or the participant responsible for impermissibly accessing data) is responsible for breach notification to affected individuals and regulators under applicable laws.

Guidance Sought on More Equitably Assigning Breach Obligations

In 2024, in the wake of the dispute between Epic and Particle Health regarding access to records through TEFCA, a number of hospitals sought guidance from OCR and ONC regarding which entity has breach notification obligations when a patient’s records are inappropriately accessed through HIE.¹⁵ The letter advocated for treating the breach as attributable to the bad actor—the entity that accessed records through HIE for an impermissible purpose—rather than the entity whose records were inappropriately accessed. The entity that disclosed records through HIE arguably made a permissible disclosure as it had every reason to believe that its disclosure was for a permissible purpose pursuant to the HIE contract. Accordingly, the disclosing entity arguably did not

make an impermissible disclosure and, therefore, would not have a reportable breach. In contrast, the letter sought guidance clarifying that the bad actor made an impermissible use of PHI and, therefore, would have breach notification obligations under HIPAA (if the bad actor is subject to HIPAA). To address participants that are not subject to HIPAA, the letter advocated for ONC to revise TEFCA to require such a participant to contractually agree to comply with certain HIPAA Breach Notification Rule requirements in the event that the participant inappropriately accesses PHI through the HIE. As of this writing, OCR and ONC had not formally responded to the letter.

California's Mandatory Data Exchange Framework

As HIE increasingly occurs at a nationwide level, the issue of who is responsible for breach notification is a national problem. But nowhere is the issue more acute than in California. This is because of the conflux of two issues.

First, California has adopted the California Data Exchange Framework (DxF), which requires general acute care hospitals, physician organizations and medical groups, skilled nursing facilities, health care service plans and disability insurers, clinical laboratories, and acute psychiatric hospitals to exchange health information in real time for treatment, payment, and health care operations.¹⁶ It also allows voluntary exchange by social service entities, community-based organizations, and other entities that may not be covered by HIPAA. The DxF's policies and procedures require participants to report breaches of data to other participants who have been impacted and to California's Center for Data Insights and Innovation.¹⁷ Similar to TEFCA, the DxF's Data Sharing Agreement and policies and procedures do not, however, address which participant is responsible for notifying affected individuals under applicable law when one participant inappropriately accesses another participant's patient data. While required by law, there currently are no apparent penalties for failing to participate in the DxF.

The second issue that is somewhat unique to California is its Confidentiality of Medical Information Act (CMIA), CMIA's private right of action, and its nominal damages. The CMIA restricts a provider of health care's and certain other regulated entities' use and disclosure of medical information.¹⁸ A patient whose medical information has been used or disclosed in violation of CMIA and who has sustained economic loss or personal injury may recover compensatory damages, punitive damages of up to \$3,000, attorney's fees of up to \$1,000, and the costs of litigation.¹⁹ Additionally, an individual may bring an action against a person or entity who has negligently released medical information in violation of the CMIA for nominal damages of \$1,000 without the need for the plaintiff to have suffered or have been threatened with actual damages.²⁰ Based on this statutory framework, a class action alleging the negligent release of 1,000 patients' medical records can seek "nominal" damages of \$1 million without the need to demonstrate any actual harm from the release of information.

Accordingly, California health care providers are stuck between a rock and a hard place. They are statutorily required to make their patient data available for health information exchange. But, if another HIE participant inappropriately accesses their patients'

records, then they may have to provide breach notification to affected individuals. This may lead to allegations that they negligently released medical information, with a class action seeking \$1,000 per affected patient. A health care provider has a strong case that releasing medical information through DxF, because it is required by law, cannot possibly be negligence. Nevertheless, they still would face the costs and uncertainty of litigation. Many health care providers may choose to settle rather than incur the cost and risk of going to trial on a multi-million-dollar lawsuit.

The HIE Risk-Benefit Analysis

Where does this leave organizations that are considering participating in or expanding their participation in HIE, including TECCA?

There are significant benefits to providers, plans, and patients through HIE participation, such as improved health care, reduced health care costs, and reduced duplicative paperwork and tests. Additionally, participating in TECCA makes compliance with the 21st Century Cures Act Information Blocking Rule easier. Specifically, a regulated actor is not information blocking if it makes available access to electronic health information through TECCA and denies a request for an alternative means of access (other than a request for access through a standardized application programming interface, or API).²¹ Additionally, an organization may be statutorily required to participate in HIE (such as pursuant to California's DxF).

An organization must weigh these benefits (and statutory requirements) against the increased risk of breaches of PHI. The more an organization's PHI is available to others through HIE, the greater the risk that others will abuse such access.

If a breach occurs, an organization can take the position that the breach notification obligations fall on the participant whose workforce member inappropriately accessed the patient data. But there are numerous challenges with this approach. First, a regulator may disagree with this position, viewing that the breach notification obligations fall on the affected provider. Second, the bad actor may disagree with this position and the affected provider may have little leverage to convince the bad actor otherwise. Third, impacted patients likely will not be familiar with the bad actor, so they may disregard a breach notification from the bad actor.²² Accordingly, if an organization learns that its patient data has been accessed inappropriately through HIE, it can take the position that the bad actor is responsible for providing breach notification, but this position involves regulatory risk and patients may not learn of the breach and take appropriate action (either because the bad actor refuses to accept breach notification responsibility or because patients disregard a breach notification from an unknown entity).

If the affected provider takes on providing breach notification, then there may be limited recourse against the bad actor for the resulting cost due to a lack of contractual privity between HIE participants. While the affected provider could seek damages under some common law theory or by asserting a claim against an HIE intermediary that sits between the participants, the likelihood of success would be highly uncertain. Organizations should carefully evaluate their insurance policies to understand the extent

that their costs are covered for an HIE breach and should be prepared for increased policy premiums if they regularly make insurance claims for HIE breaches.

Based on the above, organizations that choose to participate in HIE should expect to experience a greater number of breach events and should be prepared, unfortunately, to incur the resulting cost and reputational harm. Whether the benefits of HIE outweigh this increased breach risk is a clinical and business decision that every health organization should carefully consider.

BIO

Adam H. Greene, JD, MPH, (AdamGreene@dwt.com), a partner in the Washington, DC, office of Davis Wright Tremaine LLP, is a nationally-recognized authority on HIPAA and other health information privacy and security laws. Adam primarily counsels health care systems and technology companies on compliance with the HIPAA and state privacy, security, breach notification requirements and the information blocking rule. Adam is a former regulator at the U.S. Department of Health and Human Services, where he was responsible for determining how HIPAA rules apply to new and emerging health information technologies and where he was instrumental in the development of the HIPAA enforcement process.

PG THANKS

This Feature Article is brought to you by the **Health Information Technology Practice Group: Elizabeth Hodge**, Akerman LLP (Chair); **Jody Erdfarb**, Wiggin and Dana LLP (Vice Chair); **Jennifer Kreick**, Haynes and Boone LLP (Vice Chair); **Heather Deixler**, Latham & Watkins LLP (Vice Chair); **Adam Greene**, Davis Wright Tremaine LLP (Vice Chair); and **Leeann Habte**, Best Best & Krieger LLP (Vice Chair).

¹ TEFCA, Assistant Secretary for Technology Policy, <https://www.healthit.gov/topic/interoperability/policy/trusted-exchange-framework-and-common-agreement-tefca> (last reviewed Dec. 4, 2024).

² SB 1386, 2001-2002 Leg. (Ca. 2002), codified at CAL. CIV. CODE § 1798.82.

³ *Id.* at § 1(e).

⁴ See, e.g., CAL. CIV. CODE § 1798.82.

⁵ Pub. L. No. 111-5, § 13402, 123 Stat. 115, 260-63 (2009), codified at 42 U.S.C. § 17932.

⁶ Breach Notification for Unsecured Protected Health Information Interim Final Rule, 74 Fed. Reg. 42740 (Aug. 24, 2009); Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566 (Jan. 25, 2013).

⁷ 45 C.F.R. §§ 164.404-.408.

⁸ 45 C.F.R. § 164.402.

⁹ The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Accountability, OCR, <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/accountability.pdf> (last visited Feb. 26, 2025).

¹⁰ H. Landi, *Epic, Particle Health dispute exposes broader challenges with sharing patient data, health IT experts say*, FIERCE HEALTHCARE, Apr. 15, 2024, <https://www.fiercehealthcare.com/health-tech/epic-particle-health-dispute-exposes-broader-issues-accessing-and-sharing-patient-data>.

¹¹ ONC is now the Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology and now goes by ASTP. For purposes of this article, we will continue to refer to the organization as ONC.

¹² HHS, *ONC Awards The Sequoia Project a Cooperative Agreement for the Trusted Exchange Framework and Common Agreement to Support Advancing Nationwide Interoperability of Electronic Health Information*, Sept. 3, 2019, <https://public3.pagefreezer.com/browse/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/about/news/2019/09/03/onc-awards-the-sequoia-project-cooperative-agreement.html>; The Sequoia Project, *ONC Awards The Sequoia Project 5-Year TEFCA RCE Contract*, Aug. 28, 2023, <https://sequoiaproject.org/onc-awards-the-sequoia-project-5-year-tefca-rce-contract/>.

¹³ Exhibit 1 to the Common Agreement for Nationwide Health Information Interoperability §§ 7 and 8, https://www.healthit.gov/sites/default/files/2024-11/Common_Agreement_2.1.pdf.

¹⁴ *Id.* at § 8.2.

¹⁵ Letter to Melanie Fontes Rainer and Micky Tripathi, Aug. 6, 2024.

¹⁶ CAL. CIV. CODE § 130290.

¹⁷ CalHHS Data Exchange Framework Policy and Procedure: Breach Notification (OPP-3), Dec. 11, 2023, https://www.cdii.ca.gov/wp-content/uploads/2023/12/CalHHS_Breach-Notification-PP_Final_v1.0.1_12.11.23.pdf.

¹⁸ CAL. CIV. CODE §§ 56 to 56.37.

¹⁹ CAL. CIV. CODE § 56.35.

²⁰ CAL. CIV. CODE § 56.36(b)(1).

²¹ 45 C.F.R. § 171.403.

²² To address this issue, the bad actor's breach notification could potentially name the affected provider so that the patient recognizes the legitimacy of the notification, although this leads to reputational harm to the affected provider.