Liability for Health Care Providers Under HIPAA and State Privacy Laws

Ashley Huddleston[*] *& Ronald Hedges*[**]

I. INTRODUCTION

As technology continues to evolve and more of the health care industry moves away from paper charts and records to electronically stored records, so do the state and federal privacy laws that protect that information. "Health care providers, insurers, and other related entities collect massive amounts of personal information from patients that is now stored electronically."[1] If an entity fails to secure the data properly, the data becomes vulnerable to compromises that can expose victims to financial damage and "personal distress from exposure of their highly sensitive information."[2] Thus, there have been major developments in

[*]Managing Associate, Dentons US LLP in the Litigation and Dispute Resolution practice. She represents clients in a wide variety of business matters involving contract disputes, accounting malpractice, and other commercial matters in both state and federal courts. *See* https://www.dentons.com/en/ashley-huddleston.

[**]Senior Counsel, Dentons US LLP in the Litigation and Dispute Resolution practice. He has extensive experience in e-discovery and in the management of complex litigation and has served as a special master, arbitrator and mediator. *See* https://www.dentons.com/en/ronald-hedges.

[1] *See* Cheryl L. Anderson, *Data Breaches and Electronic Personal Health Information (ePHI): What Is Injury-in-Fact and Does HIPAA Set a Negligence Standard of Care?*, 39 J. LEGAL MED. 263, 263 (2019).

[2] *Id.*

the last twenty or so years to ensure that patients' data is protected to the greatest extent possible to prevent such technological compromises.

With the increase in regulation, however, comes an increased risk of liability for health care facilities and providers. This Article looks at HIPAA and the protection that it provides for individuals' data, as well as three robust state laws that seek to accomplish the same goal—the California Consumer Privacy Act, New York's Stop Hacks and Improve Electronic Data Security Act, and Illinois's Biometric Information Privacy Act. Finally, this Article examines liability for health care providers given the recent litigation developments.

II. HIPAA BACKGROUND

On August 21, 1996, President Bill Clinton signed the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[3] HIPAA was created

> to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in the health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term case services and coverage, to simplify the administration of health insurance, and for other purposes.[4]

HIPAA covers three groups, known as "covered entities": (1) health plans; (2) health care clearinghouses; and (3) certain health care providers who transmit health information in electronic form in connection with certain transactions.[5] HIPAA has two parts—The Privacy Rule[6] and the Security Rule.[7] The Privacy Rule generally regulates the use and disclosure of health information that identifies patients who are the subject of that information.[8] The Security Rule

[3] Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

[4] *Id.*

[5] 42 U.S.C. § 1320d–1(a). ("Any standard adopted under this part shall apply, in whole or in part, to the following persons: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1320d–2(a)(1) of this title.").

[6] 45 C.F.R. §§ 164.500-.534 (2019).

[7] *Id.* §§ 164.302-.318.

[8] *Id.* § 160.103 (defining "protected health information" to mean "individually identifiable health information").

specifically addresses security "standards for protecting certain health information held or transferred in electronic form."[9]

A. *The Privacy Rule*

"The purpose of the Privacy Rule is to establish minimum Federal standards for safeguarding the privacy of individually identifiable health information."[10] "A major goal of the Privacy Rule is to assure that individuals' health information is properly protected, while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being."[11]

"The Privacy Rule regulates all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral."[12] This information is known as "protected health information" or PHI.[13] The Privacy Rule protects both obvious and more subtle identifiers that may be used to glean someone's identity. For example, the Rule protects straightforward identifiers such as name, address, social security number, phone number, and photo; and subtle identifiers such as zip code, treatment date, and employer.[14]

The covered entities regulated under the Privacy Rule include most health plans, health care clearinghouses, and healthcare providers who transmit health information in electronic form in connection with certain transactions.[15] The term "health plan" is defined broadly under the Rule.[16] "Health plans include health, dental, vision, and prescription drug insurers, health maintenance organization ("HMOs"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home and fixed-indemnity

[9] U.S. DEP'T OF HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA SECURITY RULE (2013), https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

[10] U.S. DEP'T OF HEALTH & HUM. SERVS., PROTECTING PERS. HEALTH INFO. IN RESEARCH: UNDERSTANDING THE HIPAA PRIVACY RULE 2 (2003) [hereinafter UNDERSTANDING THE HIPAA PRIVACY RULE], http://privacyruleandresearch.nih.gov/pdf/HIPAA_booklet_4-14-2003.pdf.

[11] U.S. DEP'T OF HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 1 (2003) [hereinafter SUMMARY OF THE HIPAA PRIVACY RULE], https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[12] *Id.* at 3.

[13] *Id.* (citing 45 C.F.R. § 160.103).

[14] 45 C.F.R. § 164.514(b) (listing elements of health information that must be removed to de-identify information).

[15] 42 U.S.C. § 1320d-1(a) (applying the Act to most health plans, healthcare providers, and other covered entities).

[16] *See id.* § 1320d(5).

policies)."[17] "Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans."[18] There are certain exceptions to those organizations that are defined as a health plan.[19] Health care providers include all "provider[s] of services" (e.g., hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility) and "provider[s] of medical or other health services" (e.g., non-institutional providers such as physicians and dentists), and any other person or organization that furnishes, bills, or is paid for health care.[20] "Health care clearinghouse" refers to any "public or private entity" that "[p]rocesses or facilitates the processing of health information received from another entity in a nonstandard format . . . into . . . a standard transaction."[21] Examples include billing services, community health management information systems, and repricing companies. "The Privacy Rule also protects individually identifiable health information when it is created or maintained by a person or entity conducting certain functions on behalf of a covered entity—a business associate."[22]

A covered entity or business associate may not use or disclose PHI except either as the Privacy Rule requires or permits, or as the individual who is the subject of the information authorizes in writing.[23] The Privacy Rule requires disclosure in two instances: (1) when the patient who is the subject of the PHI requests access to his or her own healthcare information; and (2) when the Secretary of Health and Human Services is undertaking a compliance investigation or review or enforcement action.[24] There are six other categories of permissive uses and disclosures under the Privacy Rule:

---

17 SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 11, at 2.

18 *Id.*

19 The following are excepted from the definition of health plans:

> a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government-funded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps programs; and (2) those programs whose principal activity is directly providing health care, such as a community health center . . . . Certain types of insurance entities are also not health plans . . . .

Id.

20 42 U.S.C. § 1320d(3); *id.* § 1395x(r)–(u).

21 45 C.F.R. § 160.103 (2019).

22 UNDERSTANDING THE HIPAA PRIVACY RULE, *supra* note 10, at 7.

23 45 C.F.R. § 164.502(a) (2019).

24 *Id.* § 164.502(a)(2).

1. To the individual. A covered entity may disclose PHI to the individual who is the subject of the information.[25]
2. "For treatment, payment, or health care operations."[26] A covered entity may use and disclose protected health information for its own treatment,[27] payment,[28] and health care operation activities.[29]
3. Inadvertent disclosures. The Privacy Rule does not require that every single incidental use or disclosure of PHI be eliminated. Covered entities may inadvertently disclose PHI when the disclosure occurs during another permitted or required use or disclosure.[30]
4. When authorized in writing. Covered entities may disclose PHI as authorized in writing by the individual.[31]
5. Agreed to disclosures. Covered entities may use and disclose PHI for a number of tasks once they have obtained the agreement of the individual.[32] These include listing the individual as a patient in a health care facility directory, informing the individual's visitors and clergy members that the individual is a patient in the facility, and disclosing PHI to family and friends of the individual who are involved in the individual's care or payment.[33] For example, this would "allow[] a pharmacist to dispense filled

---

[25] *Id.* § 164.502(a)(1)(i).

[26] *Id.* § 164.502(a)(1)(ii).

[27] "Treatment" is defined as:

> [T]he provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; a consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Id. § 164.501.

[28] "Payment" is defined as "activities undertaken by . . . a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan" and activities of "[a] health care provider or health plan to obtain or provide reimbursement for the provision of health care." *Id.*

[29] "Health care operations" is defined as a list of the covered entity's functions. 45 C.F.R. § 164.501.

[30] *Id.* § 164.402. The definition of "breach" excludes inadvertent disclosures.

[31] *Id.* § 164.502(a)(1)(iv).

[32] *Id.* § 164.502(a)(1)(v); *id.* § 164.510.

[33] *Id.* § 164.510.

prescriptions to a person acting on behalf of the patient."[34]

6. Public Interest and Benefit Activities. The Privacy Rule permits the use and disclosure of PHI, without an individual's authorization or permission, for twelve national priority purposes.[35] The disclosures are permitted, but not required, by the Privacy Rule in recognition of the important uses made of health information outside of the health care context.[36] These activities include participating in public health activities to prevent or control disease;[37] reporting abuse, neglect, or domestic violence;[38] complying with health audits and investigations;[39] judicial and administrative proceedings;[40] assisting law enforcement;[41] facilitating the donation and transplantation of cadaveric organs, eyes, and tissues;[42] research;[43] to prevent or lessen a serious and imminent threat to a person or the public, where such disclosure is made to someone they believe can prevent or lessen the threat;[44] certain essential government functions;[45] and to comply with workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.[46]

B. *The Security Rule*

The other major provision of HIPAA, the Security Rule, specifically addresses electronically stored health information and became effective in 2005.[47] The Security Rule, like the Privacy Rule, applies to covered entities. The main difference between the two rules is the

[34] SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 11, at 6.

[35] 45 C.F.R. § 164.512.

[36] *See* SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 11, at 8.

[37] 45 C.F.R. § 164.512(b).

[38] *Id.* § 164.512(a), (c).

[39] *Id.* § 164.512(d).

[40] *Id.* § 164.512(e).

[41] *Id.* § 164.512(f).

[42] *Id.* § 164.512(h)

[43] 45 C.F.R. § 164.512(i). The Privacy Rule defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." *Id.* § 164.501.

[44] *Id.* § 164.512(j).

[45] *Id.* § 164.512(k).

[46] *Id.* § 164.512(l).

[47] *See id.* §§ 164.302–.318.

coverage—the Security Rule's scope is more limited because it outlines separate measures that covered entities must take to ensure the security of electronically stored PHI.[48] The Security Rule does not mandate that all covered entities undertake the same methods for protecting patients' electronic PHI. Instead, the Security Rule is mindful that covered entities vary in size and resources, so measures that may be appropriate for one may be insufficient for another.[49]

The Security Rule has four general requirements that covered entities must adhere to:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.[50]
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.[51]
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.[52]
4. Ensure compliance with this subpart by its workforce.[53]

There are three types of safeguards that covered entities and business associates must implement: administrative,[54] physical,[55] and technical.[56] "A covered entity or business associate must review and modify the security measures implemented . . . as needed to continue

[48] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003).

[49] *Id.* (The "entities affected by this regulation are so varied in terms of installed technology, size, resources, and relative risk, that it would be impossible to dictate a specific solution . . . that would be useable by all covered entities."). In deciding what security measures to use, a covered entity or business associate must take into account four factors: "(i) the size, complexity, and capabilities of the covered entity or business associate; (ii) the covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities; (iii) the costs of security measures; and (iv) the probability and criticality of potential risks to electronic protected health information." 45 C.F.R. § 164.306(b)(2).

[50] 45 C.F.R. § 164.306(a)(1).

[51] *Id.* § 164.306(a)(2).

[52] *Id.* § 164.306(a)(3).

[53] *Id.* § 164.306(a)(4).

[54] *Id.* § 164.308.

[55] *Id.* § 164.310.

[56] 45 C.F.R. § 164.312.

the provision of reasonable and appropriate protection of electronic PHI."[57]

Administrative safeguards include implementing "policies and procedures to prevent, detect, contain, and correct security violations."[58] Among other implementation specifications, covered entities must "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic [PHI] held by the covered entity or business associate,"[59] and must "[i]mplement security measures sufficient to reduce risks and vulnerabilities . . . ."[60] Other administrative safeguards include the development of a workforce security plan designed to ensure that only those employees who need electronic PHI can access the information,[61] the implementation of a security training program for workers,[62] and the development of a procedure designed to respond to security incidents and threats.[63]

The physical safeguards section of the Security Rule requires that covered entities implement policies to limit physical access to their electronic PHI and storage facility, while also ensuring that authorized personnel have access to it.[64] Covered entities must create and implement policies and procedures that specify the functions and manners in which those functions are to be performed for specific workstations that can access electronic PHI.[65] Policies and procedures must also be created and implemented to "govern the receipt and removal of hardware and electronic media that contain electronic [PHI] into and out of a facility, and the movement of these items within the facility."[66]

Technical safeguards require covered entities to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic [PHI] to allow access only to those persons or

---

57 *Id.* § 164.306(e).

58 *Id.* § 164.308(a)(1)(i).

59 *Id.* § 164.308(a)(1)(ii)(A).

60 *Id.* § 164.308(a)(1)(ii)(B).

61 *Id.* § 164.308(a)(3)(i).

62 45 C.F.R. § 164.308(a)(5).

63 *Id.* § 164.308(a)(6).

64 *Id.* § 164.310(a)(1).

65 *Id.*. § 164.310(b). "Workstation" is defined as "an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment." *Id.* § 164.304.

66 *Id.* § 164.310(d)(1). For further information about the physical safeguards under HIPAA, see HIPAA SECURITY SERIES, SECURITY STANDARDS: PHYSICAL SAFEGUARDS, DEP'T OF HEALTH & HUM. SERV. (2007), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf.

software programs that have been granted access rights."[67] The implementation specifications require that covered entities assign a unique name or number to authorized users to track user identity,[68] and there must be procedures for obtaining necessary electronic PHI during an emergency.[69] Further, covered entities must "[i]mplement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic [PHI],"[70] and procedures must be developed to ensure that electronic PHI is neither altered nor destroyed.[71]

C. *Enforcing HIPAA*

If a person believes that his privacy rights have been violated or that a covered entity has not implemented or has breached appropriate security measures, the person cannot directly sue the covered entity or business associate. Instead, the individual must file their complaint with the United States Department of Health and Human Services (HHS) through the Office for Civil Rights (OCR).[72]

OCR enforces the Privacy and Security Rules in several ways: (1) "by investigating complaints filed with it;" (2) "conducting compliance reviews to determine if covered entities are in compliance;" and (3) "performing education and outreach to foster compliance with the Rules' requirements."[73] "OCR also works with the Department of Justice to refer possible criminal violations of HIPAA."[74]

Once OCR receives a complaint, they investigate to determine if a violation has occurred, and if they determine there was a violation, the Secretary of HHS informs the covered entity of noncompliance.[75] The Secretary may attempt to resolve the matter by informal means, which "may include demonstrated compliance or a completed corrective action plan or other agreement."[76] If the matter is not resolved by informal means, the covered entity will have "an opportunity to submit

[67] 45 C.F.R. § 164.312(a)(1).

[68] *Id.* § 164.312(a)(2)(i).

[69] *Id.* § 164.312(a)(2)(ii).

[70] *Id.* § 164.312(b).

[71] *Id.* § 164.312(c).

[72] *Id.* § 160.306(a); *see also* HHS, HIPAA ENFORCEMENT, DEP'T OF HEALTH & HUM. SERV., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html.

[73] DEP'T OF HEALTH & HUM. SERV., HIPAA ENFORCEMENT PROCESS (2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html.

[74] *Id.*

[75] 45 C.F.R. § 160.306(c); *Id.* § 160.312(a).

[76] *Id.* § 160.312(a)(1).

written evidence of any mitigating factors or affirmative defenses."[77] If the covered entity does not take satisfactory action to resolve the matter, the Secretary may impose civil fines that are tiered in their severity according to certain factors outlined in the statute.[78] If the Secretary determines that a person knowingly violated HIPAA, the person accused of committing the offense may be subject to criminal prosecution, including imprisonment.[79]

III. STATE DATA PRIVACY LAWS

In addition to the protection afforded by HIPAA, many states have passed their own data privacy statutes. This Part examines three such laws and outlines how they differ from HIPAA.

A. *The California Consumer Privacy Act*

The California Consumer Privacy Act (CCPA) was enacted by the California legislature in 2018 to give "consumers more control over the personal information that businesses collect about them."[80] The CCPA applies to businesses that collect and sell California consumers' personal information or disclose that information for a "business purpose."[81] This means that companies who sell goods or services to California residents, even if the business is not physically located in California, must comply with the requirements of the CCPA. A business is defined under the CCPA as a for-profit legal entity "that collects consumers' personal information or on the behalf of which such information is collected and that . . . determines the purposes and means of the processing of consumers' personal information, that does business in the State of California."[82]

---

[77] *Id.* § 160.312(a)(3)(i). The evidence must be submitted to the Secretary within 30 days of receipt of such notification.

[78] *Id.* § 1320d-5 (2018).

[79] *Id.* § 1320d-6.

[80] CAL. OFF. OF THE ATT'Y GEN., CALIFORNIA CONSUMER PRIVACY ACT (CCPA) (2021), https://oag.ca.gov/privacy/ccpa.

[81] *Id.*

[82] CAL. CIV. CODE § 1798.140(c) (West 2021). To fall within the scope of the CCPA, the business must also meet one of the following three criteria: (a) have $25 million or more in annual revenue; or (b) possess the personal data of more than 50,000 "consumers, households, or devices"; or (c) earn more than half of its annual revenue selling consumers' personal data.

The law provides Californians with the right to access the data companies collect on them,[83] a right to have that data deleted,[84] a right to know which categories of third parties the companies are sharing data with or selling data to,[85] and a right to opt out of such sales.[86] In contrast to HIPAA, a consumer may bring a private right of action if a company fails to take reasonable safeguards to prevent a data breach,[87] and the Attorney General may impose civil penalties as well.[88]

Despite the broad reach of the CCPA, the law does not govern the collection, use, disclosure, or protection of protected health information governed by HIPAA.[89] But the exemption does not cover all personal information collected by healthcare and life sciences businesses. First, "protected health information" collected by a "covered entity" or "business associate," as HIPAA defines those terms, are exempt from CCPA's reach.[90] Therefore, a company's status under HIPAA and the reason the company collects data will determine whether the company qualifies for the CCPA's HIPAA exemption. The CCPA further exempts a "covered entity" governed by HIPAA "to the extent the . . . covered entity maintains patient information in the same manner" as PHI under HIPAA.[91]

The CCPA limits consumers' actions to security breaches that are attributable to a business's "violation of the duty to implement and maintain reasonable security procedures and practices."[92] It also prohibits consumers from using the CCPA's provisions to "serve as the basis for a private right of action under any other law."[93] Litigation in California is still attempting to define the parameters of the private cause of action under CCPA,[94] but private causes of action provide an avenue for relief to aggrieved individuals. Conversely, it increases the exposure for health care providers who fail to comply with the state's privacy statute.

---

83 *Id.* § 1798.100.
84 *Id.* § 1798.105.
85 *Id.* § 1798.110(a)(4).
86 *Id.* § 1798.120.
87 *Id.* § 1798.150.
88 CIV. §§ 1798.155 (b)–(c)
89 *Id.* § 1798.145(c)(1).
90 *Id.* § 1798.145(c)(1)(A).
91 *Id.* § 1798.145(c)(1)(B).
92 *Id.* § 1798.150(a).
93 *Id.* § 1798.150(c).
94 Mark Smith, *Analysis: Unlocking CCPA's Private Cause of Action*, BLOOMBERG L. (May 11, 2020), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-unlocking-the-ccpas-private-cause-of-action.

The CCPA went into effect on January 1, 2020. The CCPA's implementing regulations were approved in August 2020, but the California Attorney General proposed modifications to the regulations in October and December 2020. To complicate matters for businesses further, California residents voted in November 2020 to approve another privacy law, the California Consumer Privacy Rights Act (CPRA), which further expands consumer privacy rights. One notable addition is the Right to Rectify, which requires that businesses use "commercially reasonable efforts" to correct personal information upon receiving a verifiable consumer request. The CPRA provisions are set to take effect on January 1, 2023.

B. *New York's SHIELD Act*

On July 25, 2019, New York Governor Andrew Cuomo signed the "Stop Hacks and Improve Electronic Data Security" (SHIELD) Act, which requires businesses to implement security programs to reduce risks of a data breach affecting New York residents' private information.[95] The bill was introduced to ensure that New York's data breach notification laws "keep pace with current technology."[96] The bill broadens the scope of information covered under the preexisting data breach notification law,[97] updates the notification requirements where there has been a breach of data, and broadens the definition of a data breach to include an unauthorized person gaining access to information.[98] It also requires reasonable data security, provides standards tailored to the size of a business, and provides protection from liability for certain entities.[99] Despite the expanded definition of what information must be protected, the New York SHIELD Act and HIPAA differ as to the number of data elements that qualify as a data breach.

The SHIELD Act requires that any "person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information."[100] The SHIELD Act is similar to HIPAA in that it deems a business in compliance with the "reasonable safeguards"

95 *See* N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019).

96 Sponsor's Memorandum in Support of Senate Bill S5575B, *available at* https://www.nysenate.gov/legislation/bills/2019/s5575.

97 The SHIELD Law significantly expanded the previous privacy statute's definition of "private information." *See* N.Y. GEN. BUS. LAW § 899-aa (1)(b) (McKinney 2019).

98 *Id.* § 899-aa(1)(b)(ii)(c).

99 *Id.* § 899-bb (McKinney 2020).

100 *Id.* § 899-bb(2)(a).

requirement if the business employs three categories of safeguards: administrative, technical, and physical.[101]

The reasonable administrative safeguards relate to the administration of the data security program. The administrative safeguards include designating "employees to coordinate the security program," identifying "reasonably foreseeable internal and external risks," assessing the existing safeguards to control the risks identified, training the workforce about the security program, and selecting and contracting with service providers who can maintain appropriate safeguards.[102]

Technical safeguards focus on the technology that a business uses to provide its service or content to its customers. The technical safeguards include conducting risk assessments of network, software design, "information processing, transmission, and storage;" implementing measures to detect, prevent, and respond to system failures; and testing and monitoring the effectiveness of controls.[103]

Finally, physical safeguards concern the physical storage and disposal of customer records. Physical safeguards include conducting risk assessments "of information storage and disposal;" implementing measures to detect, prevent, and respond to intrusions; and implementing protections "against unauthorized access to or use of private information during or after the collection, transportation, and destruction or disposal of the information."[104]

All businesses, regardless of size, are required to disclose data breaches affecting private information of New York residents. But companies that meet the definition of "small business"[105] may modify the nature and extent of the security program that it must maintain.[106] The "reasonable administrative, technical, and physical safeguards" may be shaped based on "the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."[107]

---

101 *Id.* § 899-bb(2)(b)(ii).

102 *Id.* § 899-bb(2)(b)(ii)(A).

103 BUS. § 899-bb(2)(b)(ii)(B).

104 *Id.* § 899-bb(2)(b)(ii)(C).

105 "Small business" is defined as "any person or business with (i) fewer than fifty employees; (ii) less than three million dollars in gross annual revenue in each of the last three fiscal years; or (iii) less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles." *Id.* § 899-bb(1)(c).

106 *Id.* § 899-bb(2)(c).

107 *Id.*

A covered entity or business associate as defined under HIPAA needs to be conscious of the SHIELD Act. If a covered entity must provide a notice of a breach of the security of its systems to an affected person under the HIPAA breach notification rule, the SHIELD Act does not require additional notification.[108] But the breaching business must also notify the New York State Attorney General of the breach within five business days of notifying HHS.[109]

The SHIELD Act is enforced by the New York State Attorney General, who can take action in court if a business violates certain parts of the Act.[110] The Attorney General must then act "within three years after either the date on which the [A]ttorney [G]eneral became aware of the violation, or the date" on which notice was sent to individuals, whichever comes first.[111] There is, however, no private right of action under the SHIELD Act.[112] Additionally, where a business has failed to properly notify people affected by a data breach, the Attorney General may impose a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification, provided that the latter amount shall not exceed $250,000.[113]

C. *Illinois' Biometric Information Privacy Act*

In 2008, Illinois passed the Biometric Information Privacy Act (BIPA) in response to the growing use of biometrics in the business and security screening sectors.[114] The Legislature focused specifically on finger-scanning technology that was, at the time, a new type of payment technology.[115] Biometrics, the Legislature recognized, "are unlike other unique identifiers that are used to access finances or other sensitive information."[116] Unlike other unique identifiers, biometrics cannot be changed and, thus, "once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[117]

---

108 *Id.* § 899-aa(2)(b)(ii).

109 BUS. § 899-aa(9).

110 *Id.* § 899-aa(6)(a).

111 *Id.* § 899-aa(6)(c).

112 *See* Abdale v. North Shore Long Island Jewish Health Sys., 19 N.Y.S.3d 850, 857 (2015).

113 BUS. § 899–aa(6)(a).

114 740 ILL. COMP. STAT. 14 / 5 (West 2008).

115 *Id.* 14/5(b).

116 *Id.* 14/5(c).

117 *Id.*

BIPA protects biometric identifiers and biometric information.[118] Biometric identifiers are defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[119] Biometric information is defined as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier," and "does not include information derived from items or procedures excluded under the definition of biometric identifiers."[120] Unlike HIPAA, BIPA permits any person aggrieved to bring an action in court and to recover for each violation liquidated damages of $1,000 or actual damages, whichever is greater, for negligent violations, and liquidated damages of up to $5,000 or actual damages, whichever is greater, for intentional or reckless violations.[121]

There has been a slew of litigation in Illinois attempting to define the parameters of BIPA. In one landmark case, *Rosenbach v. Six Flags Entertainment Corp.*,[122] the Illinois Supreme Court held that a person need not have sustained actual damage to have standing to sue under BIPA. The plaintiff's complaint alleged that the defendants violated the provisions set forth in section 15 of BIPA when it collected her son's thumbprint without following the statutorily prescribed protocol.[123] The existence of the violations was not contested, but the defendants argued that no further damage to the plaintiff's son was alleged, and she

---

118 *Id.* 14/10.

119 *Id.* The definition of "biometric identifiers" excludes a slew of identifying things.

> Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

120 740 ILL. COMP. STAT. 14 / 20.

121 *Id.*

122 129 N.E.3d 1197, 1206 (Ill. 2019).

123 *Id.* at 1203.

thus could not sustain a cause of action.[124] The court ruled in favor of the plaintiff and held that a procedural violation of the law is sufficient in and of itself to support a private right of action under BIPA.[125] The court reasoned that "when a private entity fails to comply with one of section 15's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach."[126]

Without the requirement to show actual damage, health care providers face an increased risk of liability for technical violations of BIPA. Given the Legislature's intent to protect what it deems the most sensitive personal information, it is not surprising that the Illinois courts took a broad view of the statute.

IV. LIABILITY FOR HEALTHCARE PROVIDERS.

HIPAA lacks a private right of action[127] and preempts any state law that is contrary to HIPAA unless the state law is "more stringent" than HIPAA for privacy protection.[128] But some courts have used HIPAA as a guide for importing federal privacy standards into state court actions that allege privacy violations under state law. That is, HIPAA's lack of a private right of action did not prohibit state courts from using HIPAA's requirements as the standard for reasonable care under common law principles. This means that HIPAA's requirements can easily become the subject of a lawsuit, as there are many common law causes of action that can be used to bring lawsuits for privacy and data security breaches.

In 2014, the Connecticut Supreme Court held in *Byrne v. Avery Center for Obstetrics and Gynecology, P.C.* that "[a]ssuming, without deciding, that Connecticut's common law recognizes a negligence cause of action arising from health care providers' breaches of patient privacy in the context of complying with subpoenas, we agree with the plaintiff and conclude that such an action is not preempted by HIPAA and, further, that the HIPAA regulations may well inform the applicable

124 *Id.* at 1204.

125 *Id.* at 1206.

126 *Id.*

127 Warren Pearl Constr. Corp. v. Guardian Life Ins. Co., 639 F. Supp. 2d 371, 377 (S.D.N.Y. 2009) (collecting federal court cases recognizing that no private right of action exists under HIPAA).

128 45 C.F.R. § 160.203 (2019) ("A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law.").

standard of care in certain circumstances."[129] A plaintiff filed a lawsuit against a medical facility where she received medical care for allegedly disclosing her medical forms improperly under HIPAA. She filed a lawsuit for breach of contract, negligently releasing her medical file without authorization, negligent misrepresentation of the medical center's privacy policy, and negligent infliction of emotional distress.[130] The court held that "to the extent it has become common practice for Connecticut health care providers to follow the procedures required under HIPAA in rendering services to their patients, HIPAA and its implementing regulations may be utilized to inform the standard of care applicable to such claims arising from allegations of negligence in the disclosure of patients' medical records."[131]

In another noteworthy case, the Vermont Supreme Court in *Lawson v. Helpern-Reiss*, looked to HIPAA to inform a common law standard of care related to breach of confidentiality of the plaintiff's medical records.[132] The plaintiff brought a complaint against a medical center and charge nurse based on the unauthorized disclosure of her personal information that was obtained while she was being treated in the emergency room for a laceration to her arm.[133] She alleged that she incurred damages as a result of the nurse's negligent disclosure of information in violation of the standard of care applicable to medical providers, inadequate training, and failure to develop policies regarding the disclosure of information obtained during medical treatment.[134] The plaintiff sought a common law remedy because neither Vermont law nor HIPAA provides a private right of action for damages incurred as a result of a medical provider's unauthorized disclosure of medical information.[135] The court found that Vermont recognized a duty of confidentiality between medical providers and patients, so recognizing a common law private right of action for damages arising from a medical provider's unauthorized disclosure of information obtained during treatment aligned with the public policy.[136] The court further concluded that in adopting a common law private right of action, HIPAA was a framework that served to inform the standard of care and exceptions with respect to the duty of confidentiality.[137]

---

129 102 A.3d 32, 41–42 (Conn. 2014).
130 *Id.* at 36–37.
131 *Id.* at 49.
132 212 A.3d 1213, 1217 (Vt. 2019).
133 *Id.* at 1215–16.
134 *Id.*
135 *Id.* at 1217.
136 *Id.* at 1218–19.
137 *Id.* at 1220–21.

The speculation following *Byrne*—the first case by a state supreme court to import the HIPAA requirements as a standard of care—was that the courts would be inundated with lawsuits for HIPAA-based negligence claims. In fact, at least seven other states have indicated that HIPAA may inform a standard of care in negligence actions.[138] Once again, health care providers need to be aware of the laws of the state in addition to the HIPAA regulations because wrongful disclosure of information obtained during medical treatment may give rise to claims for damages resulting from the disclosure, in addition to any federal or state government investigation.

[138] Austin Rutherford, *Byrne: Closing the Gap Between HIPAA and Patient Privacy*, 53 SAN DIEGO L. REV. 201, 216 (2016).