Kentucky Law Journal

Volume 106 | Issue 4 Article 12

2018

New Frontiers in Medical Privacy: Protecting the Biometric Data of Patients in the Healthcare Industry

Jordan T. Shewmaker
University of Kentucky

New Frontiers in Medical Privacy: Protecting the Biometric Data of Patients in the Healthcare Industry

Jordan T. Shewmaker[1]

"Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules—not just for governments but for private companies."[2] – Bill Gates

TABLE OF CONTENTS

TABLE OF CONTENTS 813
INTRODUCTION 815
I. USE OF BIOMETRIC DATA IN HEALTHCARE 816
A. *What is Biometric Data?* 817
B. *Use of Biometric Data in the Healthcare Industry* 818
C. *Benefits and Disadvantages: Accuracy and Efficiency Versus Privacy Interests* 820
II. FEDERAL REGULATION OF BIOMETRIC DATA IN THE HEALTHCARE INDUSTRY 822
A. *Health Insurance Portability and Accountability Act* 822
B. *Health Information Technology and Economic Clinical Health Act* 825
C. *Genetic Information Nondiscrimination Act of 2008* 826
III. STATE EFFORTS TO REGULATE THE USE OF BIOMETRIC DATA AND PATENT PRIVACY PROTECTIONS 827
A. *State Law Private Right of Action for Wrongful Use of Protected Health Data* 827
B. *State statutory Protection of Biometric Data* 829
IV. THE CASE FOR INFORMED CONSENT, LIMITED USE, AND REGULATION OF STORAGE METHODS 831
A. *Informed Consent Before Capture of Biometric Information* 831

---

[1] Editor-in-Chief, Volume 106, KENTUCKY LAW JOURNAL. Centre College, B.A. 2014. University of Kentucky College of Law, J.D. 2018. The author would like to thank the entire editorial staff of the KENTUCKY LAW JOURNAL for their assistance and dedication to the JOURNAL. Additionally, the author would like to thank his family and friends for their unwavering support and patience.

[2] Bill Gates, Interview by Steven Levy with Bill Gates and Bill Clinton, in N.Y.C., N.Y. (Sept. 23, 2013), *in* Steven Levy, *Bill Gates and President Bill Clinton on the NSA, Safe Sex, and American Exceptionalism*, WIRED (Nov. 12, 2013, 6:30 AM), https://www.wired.com/2013/11/bill-gates-bill-clinton-wired/ [https://perma.cc/L9SR-YZTR] (last visited June 12, 2018).

B. Limits on the Use of Biometric Information and Retention Schedules 833
C. Standards for the Storage of Biometric Data 834
CONCLUSION 835

INTRODUCTION

As you walk into your physician's office, praying that you can get some relief for the flu-like symptoms that have been plaguing you for a week, the receptionist greets you like always. You try to muster a hoarse greeting to the receptionist and pull out your wallet, eager to pay your co-pay and sit down. But the receptionist pulls out a thin pad and asks you to put your fingertip on the pad. Unsolicited, the receptionist explains, "This is a new thing we're doing, we are using your fingerprint for check-in instead of signing-in." You mechanically comply, placing your finger on the pad, hoping that your nose will stop running long enough for your fingerprint to be captured. Besides, you are hoarse and feel that if you stand at the reception desk any longer that you may faint.

Your doctor visit goes well. Luckily no flu, just a bad sinus infection. But you unfortunately cut your thumb a few weeks later and require stitches. At the hospital, you are asked to put your (uninjured) finger on the same thin pad that you saw at your physician's office. Then, the receptionist says, "Thank you, I just pulled up all your information, you're all set." Initially, you appreciate the efficiency and speed of the new check-in process. But later you get an unsettling feeling that you may not know the entire story. You wonder, how did the hospital get access to my fingerprint scan that I gave the doctor a few weeks ago? When the receptionist says she "has all [my] information," what exactly does she mean? How does that little fingerprint machine work anyway?

Immediately, Orwellian visions of the worst spiral through your brain. Who else can my doctor share my fingerprint with? Why wasn't I informed of this new method for check-in? Can I refuse? Can they sell my information to the government, telemarketers, or other companies?

The foregoing fictional account of registration at healthcare facilities may not be common, but it is concerning. Health care providers have begun experimenting with biometric identification[3] to check patients into healthcare facilities and identify patients while providing medical care. At first blush, the use of fingerprints or other biometric information to identify a person may not seem like an issue. Besides, you use your fingerprint to access your iPhone. Even so, while efficient and accurate, the collection, storage, and use of biometric information poses serious privacy concerns that must be addressed to ensure the data security of healthcare patients. Furthermore, patients should be informed of the exact purpose and time

[3] The terms "biometric information" or "biometric data" refer to unique physical or behavioral characteristics that can be used to identify a person. Biometrics also refers to biometric recognition methods, such as the use of fingerprints, iris scans, or facial recognition to determine an individual's identity. Biometrics Research Group, *What is Biometrics?*, MICH. STATE U., http://biometrics.cse.msu.edu/ [https://perma.cc/BWW7-V2B8] (last visited June 12, 2018). Throughout this Note, "biometrics" will refer to the use of recognition methods that use unique physical characteristics to identify a person.

parameters of the use of their biometric data so they can make informed care decisions.

This Note examines current federal statutory and regulatory protections for the use and collection of biometric information in the healthcare industry, and argues for increased privacy protections pertaining to how patients' biometric data is collected and stored. This note proceeds in four Parts. Part I provides an explanation of what biometric data is and how it is used in the healthcare industry. Part II includes a survey of existing federal regulation of personal health information, including biometric data. Part III provides examples of state statutory regulation of collection and storage of biometric data by private companies. Part IV argues that patients in the healthcare industry should be warned of potential risks of the use of biometric identifiers and should be provided information about steps taken to maintain security of stored biometric data.

I. USE OF BIOMETRIC DATA IN HEALTHCARE

Health care providers have turned to biometric data to accurately identify patients and prevent fraud.[4] Even so, opponents and privacy experts express concern that biometric information can be stolen, a concern that is intensified due to the immutable nature of biometric characteristics.[5] Legal ambiguities about patient privacy rights when biometric information is used only to identify patients—as opposed to biometric data that is linked to a patient's health record—further complicate the ongoing privacy debate.[6]

---

[4] *Biometrics as a Security Measure in Health Care*, AM. SENTINEL U.: THE SENTINEL WATCH (Jan. 8, 2014), http://www.americansentinel.edu/blog/2014/01/08/biometrics-as-a-security-measure-in-health-care-2/ [https://perma.cc/YD2C-FAHE] (last visited June 12, 2018).

[5] *See* Sci. Am. Eds., *Biometric Security Poses Huge Privacy Risks*, SCI. AM. https://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks/ [https://perma.cc/QNW2-DLM9] (last visited June 12, 2018) [hereinafter *Biometric Security*].

[6] See *infra* Parts I and III for a discussion about privacy laws and issues concerning the collection and storage of biometric data.

A. What is Biometric Data?

Initially, a cursory explanation of biometric data and biometric recognition technology is necessary to understand the privacy concerns surrounding the use of biometric data in the healthcare industry.[7] Generally, collection of biometric data can be categorized as: "(1) invasive, such as a blood sample, taken to collect a person's DNA; (2) minimally or non-invasive, such as a finger print or iris scan; or (3) collected without the subject's knowledge, such as photographs taken from a distance or DNA collected from discarded biological material."[8] Most commonly, minimally or non-invasive methods , such as fingerprint scans, iris scans, or facial recognition, are used to capture biometric information.[9] Additionally, palm vein and finger vein location can be used as a unique biometric identifier.[10]

To collect a person's biometric data through non–invasive means, a collection device, generally a camera or mobile scanner, is used to capture a representation of the biometric characteristic.[11] Most biometric recognition technology stores a mathematical representation of the biometric characteristic, comprised of ones and zeros, which represent unique characteristics of a human being, in lieu of an actual picture of a person's fingerprint or iris.[12] Subsequently, the unique mathematical representation of a biometric characteristic can be used as a key to identify a person.[13]

Most individuals are familiar and comfortable with biometric recognition technologies; for instance, anyone who owns an Apple iPhone 5s or later model can unlock the phone using a fingerprint scanner.[14] Biometric recognition technologies are also prevalent in United States border security efforts, in post–arrest booking procedures, and during criminal background checks.[15]

---

[7] This explanation of biometric data collection and storage is intentionally simplistic. Obviously, the capture and storage of biometric data is much more complex than is represented in this note. For a more detailed explanation of biometric data collection methods and the accuracy of biometric data see Anil Jain et al., *Biometric Identification*, COMM. OF THE ACM, Feb. 2000 at 91.

[8] Jennifer Lynch, *From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond*, IMMIGRATION POLICY CENTER 4 (May 2012), https://www.eff.org/document/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond [https://perma.cc/BMT5-YSTW] (last visited June 12, 2018).

[9] *See id.*

[10] *See RightPatient Palm Vein Biometrics,* RIGHTPATIENT, http://www.rightpatient.com/palm-vein-biometrics-patient-identification/ [https://perma.cc/6246-3RJK] (last visited June 12, 2018).

[11] Lynch, *supra* note 9, at 4–5.

[12] *Id.* at 5.

[13] *Id.*

[14] *See Use Touch ID on iPhone and iPad*, APPLE INC. (Mar. 28, 2018), https://support.apple.com/en-us/HT201371 [https://perma.cc/GB2C-JGDL] (last visited June 12, 2018).

[15] *See* LYNCH, *supra* note 8, at 4.

B. Use of Biometric Data in the Healthcare Industry

The use of biometric data to identify patients is not unheard of in the healthcare industry. Biometric recognition technologies are employed by health care providers across the country to identify patients, to restrict access to certain areas, and to identify employees.[16] In fact, the use of biometric technology in the healthcare industry is quite varied: some hospitals use biometrics to identify patients,[17] some physician's offices use biometrics during the patient check–in process,[18] and some providers take fingerprints of infants and children for identification.[19]

For example, the use of biometric technologies can actually assist with HIPAA compliance by requiring employees to scan their fingerprint of retina before logging onto medical records software.[20] Additionally, biometric technologies can allow healthcare providers in remote or impoverished areas to collect the health information of patients without birth certificates or accurate forms of identification.[21] Biometric identification technologies can increase patient engagement in their healthcare plan by allowing secure remote access to patient health records and information.[22] Finally, biometric technologies may allow patients to check in at a self-help kiosk at a doctor's office or hospital, decreasing wait time, reducing staffing needs, and protecting patient privacy by preventing

---

[16] *See* Jess White, *More Hospitals Using Fingerprint Scans for Patient ID*, HEALTHCARE BUS. & TECH. (Nov. 27, 2015), http://www.healthcarebusinesstech.com/fingerprint-biometrics/ [https://perma.cc/G9N6-HDJ8] (last visited June 14, 2018); Biometric Research Group, Inc., *Biometrics and Healthcare*, BIOMETRIC UPDATE 7 (Jan. 2015), https://www.biometricupdate.com/wp-content/uploads/2015/02/Biometrics-in-Healthcare.pdf [https://perma.cc/Z83F-GTQN] (last visited June 28, 2018).

[17] *See* Alex Perala, *Adventist Health System Puts Faith in Biometrics*, FIND BIOMETRICS (Oct. 12, 2016) http://findbiometrics.com/adventist-health-system-biometrics-310126/ [https://perma.cc/X474-Y9H9] (last visited June 14, 2018).

[18] Natasha Singer, *When a Palm Reader Knows More Than Your Life Line*, N.Y. TIMES (Nov. 20, 2012) http://www.nytimes.com/2012/11/11/technology/biometric-data-gathering-sets-off-a-privacy-debate.html?_r=0 [https://perma.cc/7CYC-SP8R] (last visited June 14, 2018).

[19] *See* Prem Sewak Sudhish & Anjoo Bhatnagar, *Biometrics for Child Vaccination and Welfare: Persistence of Fingerprint Recognition for Infants and Toddlers*, MICH. STATE UNIV. (Apr. 15, 2015), https://arxiv.org/pdf/1504.04651.pdf [https://perma.cc/9X93-Y7WK] (last visited June 14, 2018).

[20] *See* Danny Thakkar, *Biometric Single Sign-On to Secure Healthcare Systems*, BAYOMETRIC, https://www.bayometric.com/biometric-single-sign-on-secure-healthcare-systems/ [https://perma.cc/FH5Y-NXC4] (last visited June 14, 2018).

[21] *Pocket-sized Fingerprint Scanner Could Solve Healthcare Bottleneck*, REUTERS (May 5, 2015), http://www.reuters.com/article/us-bangladesh-fingerprint-scanner-idUSKBN0NQ11L20150505 [https://perma.cc/E5LF-RXJG] (last visited June 14, 2018).

[22] *See Remote ID*, RIGHTPATIENT, http://www.rightpatient.com/rightpatient-remoteid/ [https://perma.cc/DX22-X4ME] (last visited June 15, 2018).

patients from having to divulge personal health information during the check-in process.[23]

Even so, the use of biometric technology for patient identification is a recent phenomenon and the use of biometrics is still not prevalent in healthcare across the United States.[24] Initially, medical providers must invest in technologies that can efficiently collect and securely store the biometric characteristics of patients. Additionally, specialized software is required to connect a patient's personal information such as an electronic health record ("EHR") with their biometric identifier.

Ultimately, the use of certain biometric recognition technologies to identify patients and employees, such as fingerprint scanning, is promising because collection can be done quickly, is minimally invasive, and biometric technology is unique to each individual.[25] Physical characteristics such as fingerprints, face structure, or voice tones cannot be easily duplicated, copied, or stolen like passwords or photo-IDs.[26] The use of biometric information also has many potential benefits such as preventing medication errors, reducing billing errors, identification of unconscious patients during medical emergencies, and promoting information exchange between health care providers.[27] Biometric technologies present great promise for the healthcare industry, especially in light of recent efforts to modernize healthcare records and expand the role of technology in the healthcare industry.[28]

---

[23] *See* Nicole Troxell, *Self-service Technology Doctors Up Health Care, Pt. I*, KIOSK MARKETPLACE (Aug. 25, 2014), https://www.kioskmarketplace.com/articles/self-service-technology-doctors-up-health-care-pt-i/ [https://perma.cc/394S-CK5G] (last visited June 15, 2018).

[24] *See Biometrics as a Security Measure in Health Care*, *supra* note 4 (noting that the biometric industry is "poised for explosive growth").

[25] *See Id.*

[26] *See Id.*

[27] *Id.*

[28] *See generally*, Off. Nat'l Coordinator for Health Info. Tech, *Meaningful Use and MACRA*, HEALTHIT.GOV, , https://www.healthit.gov/topic/meaningful-use-and-macra/meaningful-use-and-macra [https://perma.cc/NCV8-X6BL] (last visited June 16, 2016) (describing benefits, implementation, and incentives pertaining to the use of electronic health records); David Jackson, *Most Health Care Records Now Are Electronic*, USA TODAY (Sept. 23, 2013, 2:47 PM), http://www.usatoday.com/story/news/politics/2013/07/16/obama-electronic-health-care-record-keeping/2521217/ [https://perma.cc/K9W9-7249] (last visited June 16, 2018) (examining the nationwide shift to electronic medical records).

C. Benefits and Disadvantages: Accuracy and Efficiency Versus Privacy Interests[29]

The immutable nature of biometric identifiers is what makes them both attractive as an identification tool and worrisome from a patient privacy perspective. The unique nature of biometric data paired with the ease of collection and storage also raise significant privacy concerns about its use.[30] First, most forms of biometric data can be collected and stored easily, making it easy to collect biometric data without permission.[31] In fact, biometric technologies have been used by the FBI and law enforcement agencies to scan facial structures of Super Bowl attendees.[32]

Furthermore, the mathematical representation of stored biometric data can be hacked or stolen just like a password or credit card number.[33] But here, the unique nature of a person's biometric data enhances security concerns.[34] For instance, a stolen credit card number or bank account number can be remedied by issuance of a new account number. But if a person's unique biometric data representation is hacked or stolen, the representation cannot be changed since the biometric information cannot be changed.[35] In fact, theft of biometric data is unlike other forms of identity theft because biometric characteristics, unlike bank account numbers and social security numbers, cannot be changed. Commentators have warned that, "[i]t's easy to replace a swiped credit card, but good luck changing the patterns on your iris."[36] Thus, the ease of collection and storage of biometric data paired with the threat of theft or hacking of unique biometric information raises legitimate privacy concerns that must be addressed.

Most concerns about the use of biometric data in the healthcare industry stem from concerns that patient information biometric data could be hacked or stolen

---

[29] A great deal of case law and legal scholarship regarding biometric information has focused on the use of biometric identifiers in criminal law, anti-terrorism efforts, and border security. This Note does not focus on whether a person has a general privacy interest in biometric information. But many resources and cases do discuss the privacy interest in biometric information. *See, e.g.*, Birchfield v. North Dakota, 136 S. Ct. 2160 (2016); Maryland v. King, 133 S. Ct. 1958 (2013); Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 410–88 (2012).

[30] *See Biometric Security*, *supra* note 5; *Privacy Today: A Review of Current Issues*, PRIVACY RIGHTS CLEARINGHOUSE (Mar. 1, 2001), https://www.privacyrights.org/blog/privacy-today-review-current-issues [https://perma.cc/2U44-SNRZ] (last visited June 16, 2018).

[31] *See* Jain et al., *supra* note 7, at 94–98.

[32] Vickie Chachere, *Biometrics Used to Detect Criminals at the Super Bowl*, ABC NEWS (Feb. 13, 2001), http://abcnews.go.com/Technology/story?id=98871&page=1 [https://perma.cc/D2ZD-DY35] (last visited June 16, 2018).

[33] *See* William Abernathy & Lee Tien, *Biometrics: Who's Watching You?*, ELECTRONIC FRONTIER FOUNDATION (Sept. 14, 2003), https://www.eff.org/wp/biometrics-whos-watching-you [https://perma.cc/DBU5-3284] (last visited June 16, 2018).

[34] *Id.*

[35] *Id.*

[36] *Biometric Security*, *supra* note 5.

and then used to access sensitive health information.[37] Privacy concerns pertaining to healthcare information are enhanced by the prevalence of medical identity theft. According to the Ponemon Institute, medical identity theft rose around 22% in 2014, affecting an estimated 2.3 million Americans.[38] Medical identity theft can happen in several ways. For example, medical identity theft can occur when a person steals the personal identification of another to seek treatment such as surgery or to receive certain types of medication.[39] Moreover, identity theft can also occur when employees in the healthcare industry use patients' personal identification to bill for services that were not rendered or that were unnecessary.[40] Additionally, "[d]ata hackers and identity thieves will pay more for medical records than for any other form of personal information because such records contain data useful not only for individual identity theft but also for defrauding government health care programs."[41] Furthermore, recent high profile breaches of patient health data, such as the Anthem (Blue Cross) cyber-attack, demonstrate the potential liability issues for healthcare organizations who fail to adequately protect private health information.[42]

Ultimately, the potential benefits of using biometric information to identify healthcare patients and employees[43] must be weighed against the potential privacy and security concerns of using unique identifiers that cannot be changed if hacked. The use of biometric data raises legitimate security and privacy concerns. Examining the proper role of biometric technology in the healthcare industry is

---

[37] Christina Farr, *Would You Trust a Hospital to Scan Your Fingerprint?*, KQED (Nov. 23, 2015), https://ww2.kqed.org/futureofyou/2015/11/23/would-you-trust-a-hospital-to-scan-your-fingerprint [https://perma.cc/56B8-434F] (last visited June 17, 2018).

[38] Ponemon Institute, *Fifth Annual Study on Medical Identity Theft*, MED. IDENTITY FRAUD ALLIANCE (Feb. 2015), http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf [https://perma.cc/MM29-6VUS] (last visited June 17, 2018).

[39] *Medical Identity Theft: FAQs for Health Care Providers and Health Plans*, FED. TRADE COMMISSION 1 (Jan. 2011), https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf [https://perma.cc/649Q-EUHU] (last visited June 17, 2018).

[40] *Id.*

[41] NICOLE HUBERFELD ET AL., THE LAW OF AMERICAN HEALTHCARE 597 (Rachel E. Barkow et al. eds., 2017).

[42] *See Statement Regarding Cyber Attack Against Anthem*, ANTHEM (Feb. 5, 2015), https://www.anthem.com/health-insurance/about-us/pressreleasedetails/WI/2015/1813/statement-regarding-cyber-attack-against-anthem [https://perma.cc/3R9C-8UZ4] (last visited June 18, 2018); Reed Abelson & Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyber Attack*, N.Y. TIMES (Feb. 5, 2015), https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html?_r=0 [https://perma.cc/K3M4-9BWX] (last visited June 18, 2018).

[43] The analysis within this Note focuses exclusively on the collection of biometric data for identification of patients. While legal scholarship has discussed the use of biometrics to identify employees, this is an area where additional legal research is warranted. *See generally* William A. Herbert & Amelia K. Tuminaro, *Emerging Technology and Employee Privacy*, 25 HOFSTRA LAB. & EMP. L.J. 355 (2008); Grayson Colt Holmes, Note, *The New Employment Verification Act: The Functionality and Constitutionality of Biometrics in the Hiring Process*, 43 CONN. L. REV. 673 (2010).

crucial to ensuring a proper balance between patient privacy and accuracy and efficiency of healthcare delivery. Ultimately, now is the appropriate time to have a conversation about the advantages and disadvantages of biometric identification technology in the healthcare industry as more providers look to biometrics as a tool to increase the efficiency of healthcare delivery and secure patient data.

II. FEDERAL REGULATION OF BIOMETRIC DATA IN THE HEALTHCARE INDUSTRY

Numerous federal regulations protect electronically stored identifiable information in the health care industry but there is legal ambiguity about how these regulatory measures pertain to biometric data when used solely for the purpose of identifying a patient.[44] The three main federal regulatory schemes that protect the privacy of healthcare patients are the Health Insurance Portability and Accountability Act ("HIPAA"),[45] the Health Information Technology and Economic Clinical Health Act ("HITECH"),[46] and the Genetic Information Nondiscrimination Act of 2008 ("GINA").[47] Biometric data is protected health information ("PHI").[48] Even so, biometric data is only protected by federal law when used by certain entities for the provision and payment of healthcare services.[49] A basic understanding of current federal protections for biometric data is essential in examining the need for additional protections and safeguards for patient privacy.[50]

A. Health Insurance Portability and Accountability Act[51]

HIPAA empowers the United States Department of Health and Human Services to enact the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rules"), which sets national standards to protect certain

---

[44] Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, AM. B. ASS'N: BUS. L. TODAY, http://www.americanbar.org/publications/blt/2016/05/08_claypoole.html [https://perma.cc/7446-4SNS] (last visited Oct. 20, 2016).

[45] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.) [hereinafter HIPAA].

[46] Health Information Technology and Economic Clinical Health Act, Pub. L. No. 111-5, Title XIII, 123 Stat. 115 (2009) (codified in scattered sections of 42 U.S.C.) [hereinafter HITECH].

[47] Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110–233, 122 Stat. 881 (codified as amended in scattered sections of 26 U.S.C., 29 U.S.C. and 42 U.S.C.) [hereinafter GINA].

[48] *See* 45 C.F.R. § 160.103 (2016).

[49] *See* Claypoole & Stoll, *supra* note 44.

[50] Part I provides a summary of federal protections of biometric data in the healthcare context. For a discussion of the need for additional protections of patient privacy, see *infra*, Part III.

[51] For a detailed summary of HIPAA and other privacy protections in the healthcare industry, *see* HUBERFELD, *supra* note 41, at 597–638.

health information.[52] The Privacy Rules are extensive but do address the use and disclosure of patients' individually identifiable health information by covered entities[53] and business associates[54] that are subject to the Privacy Rules.[55] Ultimately, the rule seeks to strike a balance between protection of sensitive health information and allowing the free flow of health information between providers to improve the provision of care.[56]

The Privacy Rules define "individually identifiable health information"[57] and protect such information (protected health information) that is held or transmitted by covered entities and business associates.[58] Biometric identifiers clearly fall into the definition of individually identifiable health information since biometric data is received or captured by the healthcare provider for future identification purposes, is used for the provision of healthcare or payment for healthcare services, and can clearly identify a person.[59] Furthermore, "biometric identifiers, including finger and voice prints," are explicitly listed as identifiers that must be removed to de-identify[60] a health record.[61]

---

[52] *See* HIPAA, Pub. L. No. 104–191, 110 Stat. 1936; *see also* HUBERFELD ET AL., *supra* note 41, at 599–600; *Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [https://perma.cc/Y3ET-372P] (last visited June 19, 2018).

[53] "'Covered entity' means: (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 covered by this subchapter." 45 C.F.R. § 160.103 (2016).

[54] "Business associate" is defined in 45 C.F.R. § 160.103 and includes health information organizations, E–prescribing Gateways, and other persons and organizations.

[55] *See Summary of the HIPAA Privacy Rule*, *supra* note 52.

[56] *Id.*

[57] "Individually identifiable health information" is defined as:

> [I]nformation that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

45 C.F.R. § 160.103.

[58] *Summary of the HIPAA Privacy Rule*, *supra* note 52.

[59] *See* 45 C.F.R. § 160.103.

[60] A covered entity is permitted unrestricted use of a "de-identified" health record. A health record can be de-identified by:

> [E]ither: (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

Summary of the HIPAA Privacy Rule, *supra* note 52.

[61] 45 C.F.R. § 164.514(b)(2)(i)(P) (2016).

The Privacy Rules specify disclosures that are permitted and those that are not in order to protect the protected health information of patients.[62] Generally, covered entities are permitted to use and disclose protected health information without patient consent for treatment, payment, and health care operations[63] (such as, *inter alia*, business planning, reviewing quality and competence of health care professionals, and conducting quality assessment).[64] In such incidences of permitted disclosure, the covered entity "may obtain consent of the individual to use of disclose protected health information."[65] When disclosing health information for health care operations (and other uses not exempted by 45 C.F.R. § 164.502(b)(2)) a "minimum necessary" standard applies.[66] The minimum necessary standard requires that "a covered entity . . . make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[67]

Furthermore, covered entities can disclose protected health information for use in a hospital directory and to provide information to clergy so long as the patient is given the opportunity to object and consents or the covered entity reasonably infers, based on professional judgment, that the patient does not object to the disclosure.[68] When a patient is incapacitated or is not present, the covered entity may use professional judgment to determine if the disclosure is in the best interest of the patient.[69] Additionally, the Privacy Rules allow for certain incidental uses and disclosures that occur as a by-product of a permissible use so long as reasonable safeguards are taken to prevent such disclosures (such as talking quietly in common areas, locking file cabinets, and using passwords on computers).[70]

Additionally, covered entities may disclose protected health information without patient authorization as required by law;[71] for public health activities;[72] to

---

[62] *See* 45 C.F.R. §§ 164.502, 504, 506, 508 (2016); *see also* HUBERFELD ET AL., *supra* note 41 at 603–09; Leslie Francis, *Privacy and Health Information: The United States and the European Union*, 103 KY. L.J. 419, 428–31 (2015) (discussing HIPAA protections and disclosures of protected health information).

[63] "Health care operations" includes activities as defined in 45 C.F.R. § 164.501. 45 C.F.R. § 164.501(2)(1)–(6) (2016).

[64] 45 C.F.R. §§ 164.501, 506.

[65] 45 C.F.R. § 164.506(b)(1).

[66] 45 C.F.R. § 164.502(b) (2016).

[67] *Id.*

[68] 45 C.F.R. § 164.510 (2016).

[69] *Id.* § 510(b)(3).

[70] 45 C.F.R. §§ 164.502(a)(1)(iii), 530(c) (2016); *Incidental Uses and Disclosures*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/incidental-uses-and-disclosures/index.html?language=en [https://perma.cc/8VDN-DQBE] (last visited June 20, 2018).

[71] 45 C.F.R. § 164.512(a) (2016).

[72] 45 C.F.R. § 164.512(b). Public health activities encompass a broad category of uses of protected health information such as certain disclosures to public health authorities, employers, and schools. *Id.*

assist victims of abuse, neglect, or domestic violence;[73] and for law enforcement purposes,[74] among other uses.[75] Law enforcement can request protected health information to identify criminal suspects and is not subject to the minimum necessary standard.[76]

Finally, some disclosures require prior authorization from the patient.[77] Patient authorization is required for the disclosure of psychotherapy notes, marketing purposes, and sales of protected health information.[78] A valid authorization requires a specific description of the information to be disclosed, the name of the person or entity authorized to make the requested disclosure, a description of each purpose of the requested use or disclosure, an expiration date for the use or disclosure, and the patient's dated signature.[79] Additionally, the patient must be given notice that he or she has the right to revoke the authorization in writing at any time and the authorization must be written in plain language.[80]

Ultimately, biometric information is protected by HIPAA as individually identifiable health information. Even so, the Privacy Rules allow covered entities to disclose this protected health information in certain limited circumstances, which raises concerns about data security and patient privacy. Even though covered entities are limited in use and disclosure of protected health information, there are many permitted disclosures that do not require patient consent or authorization. Thus, under the current law, patients' biometric information can be collected, stored, and used by covered entities without the informed consent of the patient or disclosure of how the biometric data will be protected or limited in use.

B. Health Information Technology and Economic Clinical Health Act

HITECH was enacted as part of the American Recovery and Reinvestment Act of 2009.[81] Generally, HITECH promotes investment in electronic exchange of health information and encourages the expansion and "meaningful use" of electronic health records (EHRs).[82] Additionally, HITECH provides additional privacy protections for protected health information. For instance, HITECH requires that providers notify patients if their personal health information and identification is breached.[83] But HITECH allows for delayed notification of

---

[73] *Id.* § 512(c).
[74] *Id.* § 512(f).
[75] *Id.* § 512.
[76] 45 C.F.R. §§ 164.512(f), 502(b)(2).
[77] 45 C.F.R. § 164.508 (2016).
[78] *Id.* § 508(a).
[79] *Id.* § 508(c)(1).
[80] *Id.* § 508(c)(2)–(3).
[81] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111–5, 123 Stat. 115.
[82] HITECH, Pub. L. No. 111–5, 123 Stat. 226, 246–58 (2009) (codified at 42 U.S.C. §§ 300jj–32–38).
[83] *Id.* § 13402.

disclosure of protected health information when used for law enforcement purposes: "[i]f a law enforcement official determines that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security."[84] Thus, HITECH allows for unauthorized disclosures of protected health information for law enforcement purposes.

In addition to notification requirements, HITECH provides additional security protections. First, HITECH deputizes state attorneys general to pursue privacy actions and obtain damage awards on behalf of citizens whose data has been breached.[85] Furthermore, HITECH codifies the Office of the National Coordinator for Health and Information Technology (ONC), which was originally established by executive order.[86] ONC has the authority to establish programs that promote the efficient use of electronic information technology for the provision of healthcare.[87]

HITECH is an important piece of the healthcare privacy puzzle because it provides additional protection and enforcement measures for health information.[88] While the law does not directly address or even use the term biometric data, it does require notification if a patient's stored biometric data is breached. Additionally, under HITECH, state attorneys general can bring civil actions against covered entities if protected health information, including biometric identifiers, is breached or disclosed in an unauthorized manner.[89] Finally, the ONC is well-situated to examine the effective use and implementation of biometric identification technology in the healthcare industry writ-large.[90]

C. Genetic Information Nondiscrimination Act of 2008

Generally, GINA regulates the collection and use of genetic information, particularly by employers and health insurance plans, in order to avoid discrimination based on a person's genetic information.[91] For instance, GINA prohibits a group health plan from requesting, requiring, or purchasing a person's genetic information prior to his or her enrollment.[92] Additionally, GINA specifies that genetic information is protected health information under HIPAA and defines the term genetic information.[93] Thus, GINA provides meaningful protections for

---

[84] *Id.* § 13402(g).

[85] *Id.* § 13410(d).

[86] *Id.* § 3001; *see also* Exec. Order No. 13335, 3 C.F.R. 2004 Comp. at 160 (2005).

[87] American Recovery and Reinvestment Act § 3001(b).

[88] *See* HUBERFELD ET AL., *supra* note 41, at 609–10.

[89] *Id.* § 13410(d).

[90] *Id.* § 3001.

[91] GINA, Pub. L. No. 110–233, 122 Stat. 881 (codified as amended in scattered sections of 26 U.S.C., 29 U.S.C. and 42 U.S.C.).

[92] *Id.* § 101(d).

[93] *Id.* §§ 105(a), 201(4).

employees and other persons pertaining to the use of their genetic information for attaining health insurance.

GINA does not address biometric identifiers and does not provide additional protections for the use of biometric data in the healthcare industry.[94] Biometric data is certainly "genetic" in the sense that it has immutable characteristics like DNA and is inherited from parents. Still, GINA's protections are aimed at genetic testing of DNA specifically, and do not address protections for the most common type of biometric identifiers such as fingerprints or palm vein location.

Ultimately, biometric data is considered protected health information. Various regulatory schemes, namely HIPAA and HITECH, govern the collection, use and distribution of biometric data. Furthermore, these regulatory schemes allow the Office for Civil Rights of HHS (OCR) to be more proactive in ensuring compliance with federal privacy standards and reacting to noncompliance through civil fines and other remedial measures.[95] Nevertheless, privacy advocates argue that additional measures are needed to increase protections for the use of biometric data in the healthcare industry.[96]

III. STATE EFFORTS TO REGULATE THE USE OF BIOMETRIC DATA AND PATIENT PRIVACY PROTECTIONS

In addition to federal controls, some states regulate the collection and storage of biometric data. Notably, both Illinois and Texas have enacted legislation to regulate private entities' collection of biometric data.[97] Furthermore, although HIPAA does not contain a private right of action for individuals harmed by security breaches, some state courts have found that HIPAA does not preempt state laws that allow private right of actions under preexisting state law. This section will briefly discuss state protections for protected health information and health privacy.

A. State Law Private Right of Action for Wrongful Use of Protected Health Data

HIPAA does not contain a private right of action for individuals who are harmed by data breaches or wrongful disclosures of protected health information. In fact, a provision of HIPAA clearly states that HIPAA preempts any contrary state law.[98] But there are exceptions to federal preemption.[99] For example, a state law is not preempted when it "relates to the privacy of individually identifiable

---

[94] *See* GINA.

[95] *See generally* HUBERFELD ET AL., *supra* note 41, at 611–20.

[96] *See Biometric Security*, *supra* note 6.

[97] *See* Illinois Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 (2008) [hereinafter BIPA]; TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

[98] 42 U.S.C. § 1320d–7 (1996); 45 C.F.R. § 160.203 (2016).

[99] 45 C.F.R. § 160.203.

health information and is more stringent than a standard, requirement, or implementation specification adopted under [HIPAA regulations]."[100]

45 C.F.R. § 160.202 defines when a state law is more stringent than a federal law.[101] For instance, a state law is more stringent when, "for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission."[102]

Even so, some state courts have found that a private right of action does not exist because HIPAA preempts state law.[103] Also, civil litigation about Facebook's collection of biometric data,[104] in violation of some states' laws, has revolved around whether the plaintiffs suffered an actual injury due to the violation.[105] Thus, state law right of actions for breaches or misuse of patients' biometric data may not be available because state law protections do not exist or because they are preempted by HIPAA. Even if state laws are not preempted by HIPAA, plaintiffs may have a difficult time demonstrating an actual injury when their biometric data is taken without their consent without clear state statutory protections in place. Ultimately, while state law can provide a right of action for aggrieved plaintiffs, it is important that clear standards on the appropriate use, capture, and storage of biometric data are in place with accompanying penalties for violators.

Obviously, technological advances generally outpace regulatory action by legislatures and administrative agencies. Even so, the fact that it is difficult for legislatures to stay abreast of the latest technological advances in healthcare data capture is no excuse for inaction. The model biometric identification statute in Part IV provides important protections for patients while still being broad and flexible enough to allow for innovation and experimentation with new data capture methods in the healthcare industry.

---

[100] *Id.* § 160.203(b).

[101] 45 C.F.R. § 160.202 (2016).

[102] *Id.*

[103] O'Donnell v. Blue Cross Blue Shield of Wyo., 173 F. Supp. 2d 1176 (D. Wyo. 2001); Bonney v. Stephens Mem'l Hosp., 17 A.3d 123 (Me. 2011); Young v. Carran, 289 S.W.3d 586 (Ky. Ct. App. 2008).

[104] In re Facebook Biometric Info. Privacy Litig., F. Supp. 3d 1155 (N.D. Cal. 2016)

[105] *See* Derek J. Sarafa et al., *Use of Biometric Information as a Basis for Civil Liability*, LAW 360 (May 20, 2015, 10:14 AM), http://www.law360.com/articles/654052/use-of-biometric-information-as-a-basis-for-civil-liability [https://perma.cc/8S6U-WSAE] (last visited June 22, 2018).

B. State Statutory Protection of Biometric Data

Additionally, some states have enacted legislation to regulate the collection and use of biometric information.[106] Illinois regulated the use of biometric data in passing the Illinois Biometric Information Privacy Act (BIPA).[107] BIPA was passed in response to legislative findings that "[m]ajor national corporations have selected . . . locations in [Illinois] as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias."[108] Additionally, the Illinois legislature recognized the unique privacy risks presented by use of biometric data. "Biometrics . . . are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[109] Finally, the legislature found that "[a]n overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information."[110]

In response, BIPA requires private entities[111] who capture biometric information to develop a written policy that is publicly available, "establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."[112] Before biometric data can be captured, BIPA requires private entities to inform persons that their biometric information is being captured, inform persons how long their information will be stored and how it will be used, and obtain written consent to capture and use biometric data.[113] Furthermore, BIPA restricts the sale of biometric information, prohibits unauthorized disclosures, and requires that private entities in possession of biometric data "store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry" and treat stored biometric information

---

[106] *See* BIPA, 740 ILL. COMP. STAT. 14 (2008); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

[107] *See* BIPA.

[108] *Id.* § 5(b).

[109] *Id.* § 5(c).

[110] *Id.* § 5(d).

[111] ""Private entity' means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof." *Id.* § 10. Private hospitals, medical providers, and insurance companies are clearly private entities for the purpose of the act. But public hospitals or research hospitals affiliated with public universities may not be covered as private entities under BIPA.

[112] *Id.* § 15(a).

[113] *Id.* § 15(b).

with the same care that the entity treats other confidential information.[114] Finally, BIPA creates a private right of action, allowing injured parties to seek liquidated or compensatory damages.[115]

Additionally, Texas implemented protections for biometric data in 2007.[116] Like BIPA, the Texas statute regulated the collection, use, and possession of biometric information for commercial use.[117] Instead of providing a private right of action, however, Texas provides a $25,000 civil penalty for violations of the act that can be enforced by the Texas Attorney General.[118]

The increased protections for biometric data in Illinois and Texas passed without one dissenting vote in the legislatures of both states.[119] Additionally, it appears that increased privacy protections for the collection and use of biometric data is not a partisan issue. When BIPA passed the Illinois state legislature, both chambers of the state legislature were controlled by Democratic majorities.[120] In contrast, when Texas implemented increased protections for biometric data, both chambers of the state legislature were controlled by Republicans.[121] This suggests that support for increased protection of biometric information is politically popular and enjoys bipartisan support.

State efforts to regulate the collection, use, and storage of biometric data provide consumers and patients with important privacy protections. Even so, state protections do not always provide a private right of action to harmed individuals and may not protect patients at public hospitals if state regulations only apply to private entities.

---

[114] *Id.* § 15(c)–(e).

[115] *Id.* § 20.

[116] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

[117] *Id.*

[118] *Id* § 503.001(d).

[119] S. JOURNAL, 80 Leg., Reg. Sess., at 2056 (Tex. 2007), http://www.journals.senate.state.tx.us/sjrnl/80r/pdf/80RSJ05-15-F1.PDF#page=6 [https://perma.cc/CKP8-85LA] (last visited June 25, 2018); H. JOURNAL, 80 Leg. Reg. Sess., at 2667 (Tex. 2007), http://www.journals.house.state.tx.us/hjrnl/80r/pdf/80RDAY65FINAL.PDF#page=27 [https://perma.cc/C6NQ-KFFD] (last visited June 25, 2018); S. 95–S.B. 2400, Reg. Sess., at 38 (Ill. 2008), http://www.ilga.gov/legislation/votehistory/95/senate/09500SB2400_04162008_038000T.pdf [https://perma.cc/BHP6-U4YH] (last visited June 25, 2018); H. 95-S.B. 2400, Reg. Sess., at 71 (Ill. 2008), http://www.ilga.gov/legislation/votehistory/95/house/09500SB2400_05302008_077000T.pdf [https://perma.cc/HTT6-ANZY] (last visited June 25, 2018).

[120] *Partisan composition of State Legislatures 2002-2014*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/documents/statevote/legiscontrol_2002_2014.pdf [https://perma.cc/F2BJ-WLM2] (last visited June 25, 2018).

[121] *Id.*

IV. THE CASE FOR INFORMED CONSENT, LIMITED USE, AND REGULATION OF STORAGE METHODS

Existing federal and state privacy regulations exemplify how government can incentivize and expand the use of new technologies, such as biometric data, while also protecting the privacy interests of consumers and patients. Ultimately, while federal and state regulations provide some protections for the use of biometric data, additional protections are needed to ensure that patients' biometric information is captured responsibly, used appropriately, and stored safely. This section argues that the federal government should increase patient participation in healthcare decisions by implementing regulations that will require informed consent prior to capture of a healthcare patient's biometric information. Additionally, this Note advocates for regulations that limit the use of biometric information without authorization from the patient. Finally, this Note supports federal implementation of standards to require the responsible storage of biometric information.

Due to existing federal regulatory schemes and the national standard of care, the federal government is best situated to implement responsible standards that will promote efficient uses of biometric technology while ensuring patient privacy and data security.[122] In lieu of federal action, however, states may pass legislation that promotes responsible and efficient use of biometric information using BIPA as a guide.[123]

A. Informed Consent Before Capture of Biometric Information

Patients should be informed about biometric information, the intended use of their information, and have the opportunity to object to collection and use of their biometric information before it is captured to be used by medical professionals. The most effective way to accomplish this goal is to acquire signed consent from a patient before capturing biometric information. To some critics, this measure may sound like unnecessary paper-pushing in a healthcare industry that is already known for duplicitous paperwork and disclosures. But signed authorizations allowing healthcare providers to collect and store biometric information has a dual benefit for patients and providers alike. Initially, patients can be informed that their biometric information is being captured, providing an opportunity to think about the potential risks and ask questions before data is collected. After authorization is granted, healthcare providers can reduce their exposure to litigation costs if the patient willingly consented to the capture and use of biometric information.

---

[122] *See generally*, HIPAA, Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.); Peter Moffett & Gregory Moore, *The Standard of Care: Legal History and Definitions: The Bad and Good News*, 12 W. J. EMERGENCY MED. 109, 109–12 (2011) (discussing the legal history and meaning of national standard of care).

[123] *See generally*, BIPA, 740 ILL. COMP. STAT. 14 (2008) (presenting a model for state regulation of the collection, use, and storage of biometric data).

First, many patients will be familiar with the use of fingerprints and other biometric information as an identification tool from watching crime shows,[124] James Bond films,[125] and from using biometric identification technology on their cell phones.[126] Even so, the term biometric technology is not a layman's term and many medical patients will not understand how their biometric information is used, captured, or stored. More importantly, most patients will not understand or consider the serious privacy concerns associated with using their biometric information. The fact that patients know that fingerprints and other biometric information can be used as an identification tool does not completely alleviate privacy concerns with the use of a patient's biometric information. A patient may understand that their fingerprint can be captured but may not grasp the potential risks of storage of their biometric data or the probability that their immutable biometric information may be stolen and used by hackers and thieves.

Some may argue that when a patient puts their finger on a pad to collect their fingerprint that they are impliedly consenting to the use of their biometric information. Most patients, however, will not understand that they can refuse the use of their biometric information as an identification method and may feel that they will be denied care if they refuse or hesitate when asked to check-in using their fingerprint. In fact, Joel Reidenberg, a professor at Fordham University School of Law, has stated: "if [medical providers] are not informing patients [collection of their biometric data] is optional, then effectively it is coerced consent."[127] If a patient refuses the use of biometric identification, the healthcare provider can simply use another identification method such as an identifying bracelet, social security number, name, or any existing method of identifying patients in a healthcare setting. Additionally, some privacy experts and patient advocates argue that a sign, informing patients that collection of their biometric data is optional, may be sufficient.[128] Although a sign is not the most effective method for providing notice, it is better than no notice being provided to patients before their biometric information is captured and stored.

Additionally, some may question whether patients will actually refuse to allow healthcare providers to use biometric identification. There are documented cases of patients expressing regret or discomfort with the use of their biometric identification in the healthcare setting.[129] Furthermore, the fact that patients will

---

[124] Shows such as *Castle*, *Law and Order*, and *Forensic Files* regularly use fingerprints to identify fabricated and real crime suspects. *See Castle* (ABC Studios 2009–2016); *Law and Order* (Wolf Films 1990–2010); *Forensic Files* (Medstar Television 1996–2011).

[125] For instance, in *Skyfall*, James Bond uses a handgun that only functions when gripped by James Bond, most likely because it responds to Bond's unique biometric information. *See* SKYFALL (Eon Productions 2012).

[126] *See Use Touch ID on iPhone and iPad*, *supra* note 14.

[127] Singer, *supra* note 18.

[128] *See id.*

[129] *See id.*

not refuse the use of their biometric identification in the healthcare setting is no justification for inaction or failure to provide proper notice. Significant privacy concerns surrounding the use of biometric data as an identification tool in the healthcare industry necessitate proper notice and consent before the initial capture and use of patient biometric information.

Regardless of the exact method, whether on a consent form, by oral statement, or by a posted sign, patients should be clearly and unequivocally told that their biometric information is being captured and that they can opt-out of such identification methods. Furthermore, patients should be informed of alternative identification methods that exist and that the level of care they receive will not be impacted if they opt-out of the use of biometric identification. Ultimately, giving patients a choice in whether their biometric information is captured protects the privacy of patients and hospitals by giving the patient a say in how their healthcare is delivered from an administrative standpoint.

B. Limits on the Use of Biometric Information and Retention Schedules

In addition to having the opportunity to opt-out of biometric identification methods, patients should be clearly informed on how their healthcare provider will use their biometric information and how long their information will be stored. Patients can only provide proper authorization for medical providers to use their biometric information when they are aware of how that information will be used, are told that it will be stored, and know the period in which their information will be stored.

Limits on the use and retention of biometric information provide the most robust privacy protections for patients. Biometric information that is stored for a long period of time is more susceptible to hacking and data breach. Thus, medical providers should take steps to limit the storage and use of biometric information, especially when a doctor-patient relationship no longer exists.

First, medical providers should provide patients with information on how biometric identification technologies will be used in the delivery of healthcare services. Will the biometric information be used only at check-in to identify the patient? Will biometric information be used by nurses to identify patients before dispensing medicine and other care? In consenting to the capture of biometric data, is the patient also consenting to their data being shared with other covered entities and medical providers? Regardless of how the information is being used, it is important that the patient is aware of the parameters of use of their biometric data. For instance, a patient may feel comfortable with nurses taking their fingerprint on a portable scanner before giving them medicine in the hospital but may not be comfortable with the hospital sharing their biometric identifiers with other medical clinics in the area to reduce check-in times, increase security, or standardize check-in procedures.

Second, medical providers should provide clear notice on how long they intend to retain a patient's biometric information by establishing a retention schedule and

should have a policy for permanently eliminating the biometric data when a provider-patient relationship no longer exists. BIPA provides a good example of a retention provision. Under BIPA, a private entity must establish a retention schedule and must have a procedure to permanently destroy biometric information when the original purpose for using the information has been satisfied or within three years of the last interaction between the individual and the private entity.[130] At the very least, medical providers should permanently erase a patient's stored biometric data when that patient changes medical providers.

C. Standards for the Storage of Biometric Data

Finally, regulatory or statutory protections should require that medical providers treat stored biometric data with the same standard as other protected health information is treated within the medical field. Furthermore, law should impose civil liability upon medical providers who negligently store the sensitive biometric data of patients.

Ultimately, patient choice, limited use, retention schedules, and standards for storage are all measures that ensure patients can provide informed consent for the use of their biometric data and that said data will be stored with the utmost care. True, these measures may increase the opportunity costs for medical providers who seek to reap the benefits of biometric technologies in delivering medical care. Even minor data breaches, however, can have negative consequences for health care patients.[131] Thus, patients clearly have an interest in insuring that their biometric data is used responsibly and stored securely.

Furthermore, health care providers have a vested interest in insuring that they get proper authorization to use and take steps to protect protected health information. Not only is protecting patients' health information the right thing to do, it also allows hospitals to protect themselves from civil liability which has become an expensive line item in healthcare providers budgets through judgment awards and insurance premiums.[132] Even in lieu of federal or state regulation of biometric identification, there are best practices for medical providers and patients

---

[130] BIPA, 740 ILL. COMP. STAT. 14/15(a) (2008).

[131] *See, e.g.*, Charles Ornstein, *Small Violations of Medical Privacy Can Hurt Patients and Erode Trust*, NPR, Dec. 10, 2015, Morning Edition, http://www.npr.org/sections/health-shots/2015/12/10/459091273/small-violations-of-medical-privacy-can-hurt-patients-and-corrode-trust [https://perma.cc/6PPQ-NANG] (last visited June 30, 2018) (providing examples of small breaches of protected health information that harmed patients).

[132] *See, e.g.*, Jess White, *Recent Settlements Show Cost of HIPAA Violations*, HEALTHCARE BUS. & TECH. (Apr. 27, 2016), http://www.healthcarebusinesstech.com/hipaa-settlements/ [https://perma.cc/U4P6-VH97] (last visited June 30, 2018) (providing examples of costly settlements resulting from HIPAA violations).

to ensure the responsible use and security of biometric information.[133] Thus, patients, medical providers, privacy advocates, and policy makers all have a stake in ensuring that the privacy of patients is protected, medical care is delivered in a cost-effective, efficient manner, and that informed consent is gained before capturing, using, or storing biometric information.

CONCLUSION

Ultimately, the use of biometric identification technology presents great promise for use in the healthcare industry to increase the accuracy and efficiency of healthcare delivery and protect patient privacy. Even so, the immutable nature of biometric information enhances the privacy and security fears concerning data breaches and misuse. Thus, federal and state regulatory efforts must attempt to strike a responsible balance between effective sharing of health information and patient privacy concerns.

Currently, federal regulations, especially HIPAA and HITECH, regulate the use of biometric information as protected health information by covered entities. Additionally, some states have recognized security concerns with the commercial use of biometric data and have enacted more stringent protections for the use of biometric information. Even so, additional protections are needed to ensure that patient privacy is protected and to limit the civil liability of medical providers. Thus, federal regulators should enact common sense measures such as patient choice, limited use, retention schedules, and standards for storage which impose minimal additional financial and administrative costs om medical providers while greatly enhancing patient privacy and autonomy. In the meantime, medical providers should continue to follow best practices by requiring informed pre-authorization from patients before collecting, using, and storing patients' biometric information. Action at the federal level is preferable as it will provide a national standard for the capture, storage, and use of biometric information. In the meantime, states can enact legislation to provide enhanced privacy protection to patients and provide clear standards to protect healthcare providers. Ultimately, government should move to enact responsible regulation of biometric information before the use of biometric identification becomes more prevalent in the healthcare industry.

---

[133] *IBIA Privacy Best Practice Recommendations for Commercial Biometric Use*, INT'L BIOMETRICS & IDENTIFICATION ASS'N (June 2014), https://www.ntia.doc.gov/files/ntia/publications/ibia_statement_to_ntia_-_best_practice_recommendations_6-17-2014.pdf [https://perma.cc/9KNK-YBRA] (last visited June 30, 2018).