Privacy and Security Risks with Biometrics

By Ron Hedges, JD

Collection and use of biometric information may be useful to healthcare providers looking for new and better ways to positively identify patients as well as fight fraud. Biometric technologies include facial recognition, retinal scanning, and palm-vein scanning, among others. Moreover, biometric technology might also enable healthcare providers to keep track of employees or visitors at facilities.

The task of managing greater volumes of patient data and ensuring the accuracy of these technologies will fall to health information management (HIM) professionals and their provider partners. All of this sounds good—assuming that the cost of installation and operation of the technology is affordable. But there are also risks and potential legal pitfalls to consider.

Regulation of Biometric Information

Three states have enacted legislation regulating the collection and use of biometric information: Illinois, Texas, and Washington. Other states are considering similar legislation.

Illinois' legislation is called the Biometric Privacy Act (BIPA).[1] BIPA defines biometric information to mean "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." It defines a biometric identifier to be "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. 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." In other words, BIPA's focus is on biological factors unique to a person.

BIPA requires a private entity to do several things before it can collect or "otherwise obtain" a person's biometric identifier or information. The entity must do all of the following:

- Advise in writing that the information is being collected or stored
- Inform in writing of the "specific purpose and length of term for which the information is being collected, stored, and used"
- Receive a written release

The entity must also "develop a written policy, made available to the public, 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 three years of the individual's last interaction with the private entity, whichever occurs first."

Significantly, BIPA created a private cause of action against entities that violate its terms and allows injured persons to recover money damages, injunctive relief, and attorneys' fees.

BIPA allows for civil actions to enforce its terms. Not surprisingly, more than one such action has been filed. A major issue in these actions has been what type of injury a plaintiff must allege to proceed. Is it sufficient to allege a violation of BIPA or must a plaintiff show some actual harm arising from the alleged violation? Courts have been divided on the answer. In *Rosenbach v. Six Flags Entertainment Corp*., an Illinois appellate court held that actual harm must be shown.[2] The Illinois Supreme Court has accepted an appeal from that holding. Until that court rules and definitively interprets BIPA there will be uncertainty.

The state of Washington took a somewhat different approach to biometric information in its H.B. 1493 legislation.[3] This legislation applies to the "enrollment" of a defined biometric identifier into a database for a commercial purpose. H.B. 1493 prohibits enrollment "without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use

of a biometric identifier for a commercial purpose." It exempts entities that collect and store biometric information for a "security purpose." H.B. 1493 does not include a private cause of action.

Texas is the third state with biometric-specific legislation, the Capture or Use of Biometric Identifier Act (CUBI).[4] CUBI defines a biometric identifier to be "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." CUBI provides that "a person may not capture a biometric identifier of an individual for a commercial purpose unless the person informs the individual before capturing the biometric identifier and receives the individual's consent to capture the biometric identifier." As with Washington's H.B. 1493, CUBI does not provide for private enforcement.

Biometric Information and Healthcare Providers

Significant data privacy and security concerns are everywhere, but especially in the healthcare industry. Recent examples of how these concerns are being expressed are the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act, two laws that further restricted unauthorized use of personal information. At the same time, biometric information offers a means by which healthcare providers presumably can improve both patient privacy and security.

Interestingly, BIPA, for example, excludes from its reach patient-related information: "Biometric identifiers do not include information captured from a patient in a healthcare 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," the law states. H.B. 1493 includes a similar exclusion. Therefore, healthcare providers should consider the collection and use of biometric information under the HIPAA Privacy and Security Rules. How the Department of Health and Human Services Office for Civil Rights will deal with biometric information is beyond the scope of this article. However, healthcare providers should keep various concerns in mind, such as:

- Although patient-related biometric information is outside the scope of BIPA and H.B. 1493, healthcare providers may be subject to these regulations when providers collect and use biometric information to, for example, identify employees.
- Regardless of the applicability of legislation, healthcare providers may be subject to liability imposed under the common law when providers collect or use biometric information. For an example of how the common law might impose liability, see the author's Legal e-Speaking blog post "You've Been Served: What's Next?"[5]

Beyond liability concerns, cost is always a factor for healthcare providers. Whenever a new technology is being evaluated by a provider, the cost of implementation and maintenance of that technology into an existing information governance or other framework must be considered. Another factor, depending on the information that the new technology might gather, is required compliance with HIPAA Privacy and Security Rules. That might entail working with entities that offer new technologies—and that means, among other things, entering into written business associate agreements.

This article began by recognizing that biometric information technology might be of great value. Entities must consider the expected benefits to be derived, possible risks, current law regulating the technology, and all costs before implementation and use.

Notes

1. Illinois General Assembly. Illinois Biometric Information Privacy Act. www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004.
2. *Rosenbach v. Six Flags Entertainment Corp.*, 2017 IL App (2d) 170317 (Ill. App. Ct. Dec. 21, 2017), leave to appeal allowed, 123186 (Ill. Sup. Ct. May 30, 2018).
3. Washington State House of Representatives. Biometric Identifiers. H.B. 1493. July 23, 2017. http://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/Session%20Laws/House/1493-S.SL.pdf.
4. Texas.gov. Texas Capture or Use of Biometric Identifier Act. https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm.
5. Hedges, Ron. "You've Been Served: What's Next?" *Journal of AHIMA* website. February 28, 2018. http://journal.ahima.org/2018/02/28/youve-been-served-whats-next/.

Ron Hedges (r_hedges@live.com) is a former US Magistrate Judge in the District of New Jersey and is a writer, lecturer, and consultant on topics related to electronic information. He is a senior counsel with Dentons US LLP.

Article citation:
Hedges, Ron. "Privacy and Security Risks with Biometrics" *Journal of AHIMA* 89, no. 8 (September 2018): 46–47.