Articles + Publications | May 11, 2021

Facing Up to Tough Issues: Health Care Compliance Concerns with Facial Recognition Technology

WRITTEN BY

Sara B. Richman | Wynter L. Deagle | Kimberly Hughes Gillespie | Barak A. Bassman | Leah Greenberg Katz

Facial recognition technology (FRT) has become the new normal for many of us. We use it to unlock our phones or to sign into various apps. But unlocking our cell phones is just one of the many ways we may experience FRT; industries across the spectrum are using FRT for a variety of reasons. In a 2020 study,[1] the U.S. Government Accountability Office (GAO) found that companies use FRT to enhance security systems, authorize payments, and monitor attendance of students at school or employees at certain events.[2] Recently, FRT also has received the attention of the health care industry in which there may be unique potential legal and compliance considerations, which health care providers should carefully weigh before implementing and using FRT.

What is FRT?

FRT is a type of biometric technology that can "identify individuals by measuring and analyzing physical and behavioral characteristics … ."[3] The technology works by converting a photo or video of a person into a template or mathematical representation of a person's face. It then runs the template through an algorithm that matches it to other photos in a database and/or confirms the identity of the individual. FRT relies heavily on "machine learning," "a component of artificial intelligence in which an algorithm uses training data to identify patterns and predict an answer to a question … ." The GAO found that "[s]ince around 2013, the use of deep neural networks — a type of machine learning algorithm — has led to a dramatic increase in the accuracy of FRT. In a deep neural network, training data are used to identify patterns and become more accurate as the algorithm 'learns.'"[4] Since this development, FRT arguably has become more accurate and faster, which has led to increased use.

How is FRT Being Used in Health Care?

Reportedly, some hospitals use FRT to augment their security programs, which could offer protections to both patients and staff.[5] For example, FRT can be used to identify and notify hospital security staff when an individual enters its facility who is known for violent behavior, drug diversion, or fraud. And, FRT can be used to enhance a hospital's privacy program by replacing or adding to security measures, such as entering a password before accessing patient medical records.

FRT could also be used to expedite admission processes and to ensure the information a person provides to hospital staff is indeed accurate, thereby reducing medical identity theft. Moreover, when patients arrive in an emergency room unconscious, or otherwise not in a position to effectively communicate with staff, FRT could be used to identify the patient and quickly access his/her medical record. This would allow health care providers quicker access to information about a patient's known allergies, current medications, prior medical history, and

more, which could lead to improved patient care, safety, and outcomes.

Further, FRT has been credited with helping to diagnose patients after they arrive at the hospital. For example, FRT has helped identify certain genetic disorders and reportedly can be used to predict behavior, pain, and emotions associated with behavioral health disorders. Others believe that it could help identify and avoid procedural and patient errors.

What are the Potential Problems with FRT?

In its 2020 report, the GAO highlighted a number of potential challenges that need consideration when utilizing FRT. One of which is accuracy. Although they found that the accuracy of FRT had greatly improved in recent years, it is still not 100%, and perhaps more importantly, accuracy can vary significantly depending on the system being used. While the reasons for this are beyond the scope of this article, those looking to potentially use FRT should be mindful of this and do their due diligence before selecting a vendor to assist.

The second issue the GAO identified concerns an inherent bias in the systems across the board. Specifically, they found that the accuracy of FRT varied "widely by race, ethnicity, or country of origin, as well as by gender and age."[6] Generally, the systems more accurately identified white men. False positives were higher among women and people of color, with the highest false positive rate occurring among black women.[7] There was also a high false positive rate for the elderly and children.[8]

Lastly, while proponents argue that FRT can be used to enhance a hospital's privacy program by replacing or adding to security measures like having to enter a password before accessing patient medical records, this presents additional risk in the event of a data breach. Biometric information, unlike a password, is not something that is easily reset.

What are the Potential Legal Risks in the Health Care Setting?

In general, laws and regulations have not kept up with the developments and uses of FRT. A few states have attempted to regulate this area with Illinois being the first with its Biometric Information Privacy Act(BIPA) in 2008. Since then, other states (*e.g.,* Washington, Texas, California, and Vermont) have passed laws to address the collection, use, storage, sale, and/or security of biometric information (including FRT),[9] but these efforts vary considerably and draw debate over the right approach. According to the GAO, a few additional states have added biometric information to their breach notification laws, requiring companies or individuals possessing such information to safeguard the information and to notify individuals when their data has been accessed or acquired without authorization.[10] Obviously, health care providers will need to be knowledgeable about their particular state's laws and weigh the legal risks before utilizing FRT.

Although not a complete list, below find several possible legal issues a health care provider must evaluate when considering whether to utilize FRT.

***HIPAA*.** The Health Insurance Portability and Accountability Act (HIPAA) sets forth certain privacy and security standards regarding the handling and use of personal health information (PHI). Specifically, it outlines rules for how PHI can be used and/or disclosed by certain health care providers and requires protections to guard against

improper use or disclosure of PHI. Biometric identifiers, full-face photographic images (or any comparable images), and “any other unique identifying … characteristics” may be considered HIPAA-protected PHI. Therefore, health care providers subject to HIPAA and using FRT must be mindful to ensure compliance with HIPAA’s standards and rules.

BIPA. Generally, BIPA requires that any private entity in possession of biometric information (1) develop a written policy governing the collection, use, storage, and destruction of biometric information; (2) inform the owner of the biometric information in writing about the purpose for collecting the information and the length of time it will be stored, (3) obtain written consent for the collection and storage of the data, and (4) refrain from selling, leasing, trading, or otherwise profiting from that biometric information. A critical component of BIPA is its private right of action, which allows “any person aggrieved by a violation of [the] Act” to sue for steep liquidated damages: $1000 for each negligent violation, $5000 for each intentional or reckless violation, attorneys’ fees and costs, and injunctive or other relief. Since its passage, over 750 purported class actions have been filed — many of which settled for significant amounts — seeking damages for violations of BIPA. Accordingly, health care providers using FRT should ensure that they are complying with BIPA’s requirements for biometric information collected from individuals located in Illinois or Illinois residents.

***Informed Consent*.** When FRT is used in a clinical context, health care providers must be knowledgeable about their state’s rules around obtaining informed consent. For example, patients should be informed that their images are being collected and stored, the purposes for which that image might be analyzed, and how that information will be used in their clinical care. It is likely that some patients will not intuitively grasp how FRT can be used to assist a physician in making a medical diagnosis. In addition, to the extent FRT will be used as a diagnostic tool, providers should be familiar with and account for the risks of inaccuracy and bias.

***EMTALA*.** The Emergency Medical Treatment and Labor Act (EMTALA) requires all patients who present at an emergency department to be stabilized and treated regardless of their insurance status or ability to pay. Hospitals considering using FRT to help identify individuals entering their facilities and known for violent behavior, drug diversion, or fraud will need to be thoughtful about how they set up these programs, how they develop their policies and procedures, and how they train their employees. Regardless of whether an individual is identified via FRT to fall within one of these categories of concern, if he/she arrives in the emergency room seeking care, the hospital must ensure it continues to comply with all of its obligations under EMTALA. In other words, a patient cannot be turned away or not appropriately screened and stabilized simply because he/she has been identified as someone with a history of violence, drug diversion, fraud, or theft.

***Anti-Discrimination Rules*.** Hospitals and their caregivers have an array of legal obligations to ensure that patients are not treated differently based on age, race, ethnicity, religion, culture, language, physical or mental disability, socio economic status, sex sexual orientation, and gender identity or expression. For example, such requirements often are set forth in payor contracts and the conditions of participation in federal and state benefit programs. However, as noted above, there are concerns about bias in FRT algorithms. In addition, if a hospital utilizes FRT to identify patients with a history of violence, fraud, drug diversion, or theft, it must be careful not to apply those types of red flags in a discriminatory manner based upon ingrained biases or stereotypes. This may require planning on the front end when designing the program, putting in place proper policies and procedures, and conducting comprehensive and regular training for staff, including anti-bias training.

If your hospital wants to implement a program utilizing FRT, we highly recommend engaging qualified and knowledgeable legal counsel to help analyze the risks and navigate the legal landscape in this emerging area of the law.

---

[1] "Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses," GAO-20-522, July 2020.

[2] *Id*.

[3] *Id*. at page 4.

[4] *Id*. at page 7.

[5] Paresh Dave and Jeffrey Dastin, "Exclusive: Why a U.S. hospital and oil company turned to facial recognition;" *Reuters* (April 20, 2021) at https://www.reuters.com/world/middle-east/exclusive-why-us-hospital-oil-company-turned-facial-recognition-2021-04-20/.

[6] GAO-20-522; at page 25.

[7] *Id*. at page 26.

[8] *Id*.

[9] *Id*. at page 41-42.

[10] *Id*. at page 42 (These states include Arizona, Arkansas, California, Colorado, Delaware, Illinois, Iowa, Louisiana, Maryland, Nebraska, New Mexico, New York, North Carolina, South Dakota, Washington, Wisconsin, and Wyoming.).

RELATED INDUSTRIES + PRACTICES

- Advanced Technology: Leading-Edge Issues
- Health Care + Life Sciences
- Technology