My first real experience with biometrics

Family, Parenting

My first real experience with biometrics occurred when my son purchased a new cell phone nearly two years ago. During the initial setup, he selected an iris scan as his passcode. I was a little surprised by thetechnologyand skeptical of the convenience and security. My first question to him was, " What if someone needs to get in your phone?". He quickly replied, " That is what the security feature is for, so they can't get in. If I want them in it, I'll open it and hand it to them." He is an active duty Navy sailor. He explained to me that he felt more secure knowing that no one could break into his phone because of this passcode.

I observed him over the next two weeks while he was home on leave. Each time he accessed his phone, he simply looked into the screen and instantly he had access. He has shared that when others see that his passcode is an iris scan, they realize they cannot hack into the phone. Most never attempt anything at this point. Those that do are not successful. To this day, he has not had any security issues with his phone.

Watching the success and ease at which biometrics worked with a cell phone, I moved to a biometrics passcode when I purchased a new computer earlier this year. My new computer came with FastAccess Facial Recognition. After initial setup which included some training to recognize my face, I no longer had to enter a password or PIN.

. There are advanced features that turn off the webcam, enable parental controls, and enable an automatic login feature that make FastAccess safe and user-friendly. When someone else tries to access my computer, access is denied because FastAccess does not recognize them. I've been told for many years that my daughter could pass as my twin, but the computer knows better, it would not unlock for her. Lighting can affect the process, the system does not work in poor lighting conditions.

In these cases, I am prompted for a second form of authentication, a PIN or password. Other than this, I have been very pleased with not having to use a password to access my system and knowing my data is secure. Now that I was familiar with biometrics in " my" environment, I wanted to learn more about biometrics in the area ofhealthinformation, an area I have worked in for nearly thirty years.

According to Whitman and Mattord (2018), biometric access control refers to physiological characteristics used to authenticate identification that has been provided. This control relies on recognition, comparing an actual image to a stored image. Fingerprints, palm prints, hand geometry, facial recognition, retinal prints, and iris patterns are types of biometric authentication technologies.

The three characteristics in humans that are generally considered unique are the fingerprints, the retina, and the iris (pp 334-335). Iris recognition provides the highest level of accuracy of all biometric markers. According to Katz, the algorithms used in iris recognition are so accurate " that the entire planet could be enrolled in an iris database with only a small chance of false acceptance or false rejection" (2002).

Concerns in the area of biometrics are " false negative" and " false positive". When an individual has a false negative their identity is registered within the system but for some reason, the system does not recognize them. A false positive is the larger concern. This rating means the individual is not registered within the system, yet the system is recognizing them as another registered user and providing access to them based on that recognition.

Facial recognition technology opens the door to many possibilities in healthcare, particularly in the area of health information management. This technology has been widely discussed as part of the national patient identifier initiative. Facial recognition is a preferred technology over other biometric techniques because it does not require direct contact with the patient and it is easily deployed.

Some of the uses for facial recognition in the health information management area allows for authentication of proper security clearance for employees to grant or deny access within the EHR to staff without a password or PIN. By authenticating your employee, you are maintaining the confidentiality of the protected information. The same technology can be used to verify or authenticate the identity of a provider when they access controlled substances.

Facial recognition is the preferred technology because " some areas within a hospital zones require clinicians to wear surgical gloves and masks, thereby prohibiting the use of fingerprint authentication" (Callahan, 2017). Another option is a feature where " a patient's image can bring up their file in the EHR using facial recognition software" (McCleary, 2016).

This security feature allows the healthcare provider to compare their patient to the stored patient image. Authenticating the patient allows you to maintain the integrity of your data, minimize medical mistakes and improve patient safety. Additional bonuses will be cost savings by reducing fraud, and improved protection or security of confidential patient heath information.

There are yet additional benefits of facial recognition to the medical arena. One benefit is the prevention or reduction of medical identity theft. Medical identity theft occurs when someone uses another individual's information to obtain medical services for personal or financial reasons. If the individual presenting for treatment had to be identified by facial recognition, their identity would be authenticated or denied. This could prevent someone from trying to use your insurance benefits or obtain access to your demographic or financial information. Again, this protects the security of confidential patient data.

Facial recognition is also an important authentication feature in the healthcare field to establish the identity of patients, particularly those that are unresponsive. Early identification of these patients in emergency situations within an integrated EHR can give healthcare providers instant health information about medical conditions, medications, and allergies. Facial recognition provides a better alternative for identification than fingerprinting for burn victims those patients who have experienced amputations. Some genetic conditions allow diagnosis via facial recognition according to a study at the National Human Genome Research Institute.

One provider of facial recognition software, Nextgate, " claims to simplify registration, flag fraudulent activity, and eliminate the creation of duplicate records" (McCleary, 2016). We may be able to eliminate duplicate records if this software meets its expectation. Duplicate records are a data quality issue that result in compromised " patient safety, medical care, data accuracy, and reimbursement" (Harris and Houser, 2018).

Duplicate records occur for a variety of reasons, primarily human error due to transposing of letters and/or numbers during data entry, the use or non-use of middle names, and abbreviations. As we see more and more organizations merge or become part of a larger healthcare organization, the opportunity for duplicate medical records increase. " Duplicate records have caused negative outcomes in the discovery phase of the litigation process because there will be discrepancies with diagnoses, medications, and allergies" (Harris and Houser, 2018). Maintaining a single, confidential patient record ensures the availability and integrity of the patient data.

Organizations are beginning to turn to biometrics to eliminate their duplicate records. The three possible methods include iris, palm vein, and fingerprint scanning. Iris scanning is the preferred method because it " supports hospital infection control initiatives and is very effective in preventing duplicates as there is a low occurrence of false positives and extremely low (almost zero percent) false negative rate" (Harris and Houser, 2018).

With iris scanning, the technology never has to touch the patient whereas, palm vein and fingerprint scanning technology requires a physical contact between the patient and the technology. This increases the opportunity for infections to be spread.

Organizations with an advanced enterprise master patient index (EMPI) are those that often contain patient information for multiple locations within one health system. The EMPI integrates data from the various systems forming an " overarching technology umbrella, resolving and synchronizing data issues and providing a single patient view that can be accessed across the enterprise. The EMPI resolves data quality issues and synchronizes back to enable accurate patient identification and matching that minimizes duplicates records" (Harris and Houser, 2018). The EMPI provides a level of confidentiality and security throughout the organization.

When biometrics are implemented at the registration process and integrated into the EHR, health information professionals and providers can view and authenticate the patient information while working with the patient and within the EHR. Members of a data integrity team can verify patient records are properly integrating into the EHR as the patient moves through the health system. In areas where a facial recognition or fingerprint cannot be captured but a barcode can be scanned, the integration provides the patient's image for a comparison prior to medication administration or other service. This form of authentication provides an added security and safety feature.

While all of this technology sounds like a win for the patient and the healthcare system in general, we must also consider the law. According to Hedges, three states (Illinois, Texas, and Washington) now have legislation that regulate how biometric information is collected and used. More states are expected to follow suit.

The Illinois Biometric Privacy Act (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." (Hughes, 2018). BIPA does not include information captured in a healthcare setting or collected for treatment, payment, or healthcare options under HIPAA. It is uncertain how the Department of Health and Human Services will address biometric information at this time. One area that healthcare organizations should start to consider is how their business associates may interact with any biometric information they collect.

The changing pace of technology is trying to keep up with the pace of today's security challenges. It seems as if each day we hear of another security breach or security issue almost daily. There are tools for the health information professional to address or combat areas information security issues. Two of the most powerful tools are iris scanning and facial recognition. These tools can authenticate employee and patient identification. By authenticating the employee, you maintain confidentiality of information. By authenticating the patient, you maintain patient safety and the integrity of your data.