Use of Biometrics to Increase Security and Privacy

Robb Linafelter, MHA, COE

In the film Minority Report, Tom Cruise passes by cameras in a mall and as they scan his retina, specific marketing messages are delivered to him. In the film Demolition Man, villain Wesley Snipes uses a “stolen” retina to escape from prison. While not as invasive as the use of retina scanners in these sci-fi classics, biometric scanning is no longer a sci-fi fantasy but a reality. The carry-out pizza counter service person uses a fingerprint scan to log on to the computer to confirm my order. Disneyworld scans the fingers of its guests to verify each day they enter one of the parks.

Now, biometrics are being used in the healthcare setting. Fingerprint scanning is used to log on to computers, to verify patients at admission, and in some settings, to verify patient identification before surgery or drug administration. In the future, biometrics will play an important part in the privacy and security of patient information. This column will define biometric scanning, its uses in healthcare, and how to overcome concerns regarding the use of biometrics.

Biometrics—Definition and Mechanics

Biometrics is the study and analysis of biological data. Biometrics uses computer technology to identify people based on physical or behavioral characteristics, such as fingerprints or voice scans (Small Business Encyclopedia, N.d.). In addition to fingerprints and voice, biometrics scans hands, faces, irises, retinas, or signatures. An early article on the use of biometrics published in Entrepreneur magazine reported that finger scanning accounts for 34% of biometric system sales, followed by hand scanning (26%), face scanning.

The technology is here, the costs are low, and as medical providers, we need solutions to capture patient information accurately and quickly.
(15%), voice scanning and eye scanning (11% each), and signature scanning (3%) (Campanelli, 2001).

Retinal scanning—which reads the blood vessels in the back of the eye and requires the user to be within six inches of the scanning device—is the most accurate system but also the least likely to enjoy widespread use because of people’s natural protectiveness of their eyes.

The first step in obtaining an individual’s information is in the enrollment phase. Biometric information is obtained from the individual and is stored either on a card or in a database in a template. Then, using a matching program, any subsequent inquiry regarding a person’s biometrics from the input mechanism is compared to the template in the database. Once matched, the needed approval is granted.

**Uses in Healthcare**

There are three issues that must be addressed when applying biometrics to healthcare: staff/physician sign-on, tracking of EMR exposure, and patient verification.

**Staff/physician sign-on.**

Probably one of the first uses of biometrics involves signing in to networks and patients’ electronic medical records. By using biometrics, most often a fingerprint scan, one can easily sign on to a network or into a patient chart without having to type in a user name and password. Many physicians find biometrics a relief for the multiple sign-ons and numerous passwords required to access most networks. The fewer keystrokes needed, the greater the physician satisfaction with your computer system.

**Tracking EMR exposure.**

Recent changes in the HIPAA (Health Insurance Portability and Accountability Act) through the HITECH (Health Information Technology for Economic and Clinical Health) Act require an accounting of access into a patient’s record (Porter, 2009). Using biometrics and giving access to the electronic medical record only to those who have a valid biometric sign-on, the EMR can easily track who has accessed the record.

**Patient verification.**

When I searched the database in my practice at Eye Surgical Associates, there were four Barbara’s, six Betty’s, and five Robert’s all with the same last name. The potential to access the wrong chart is certainly there. The use of a kiosk sign-in with biometric finger scans could save time at check-in and validate that you are seeing the right patient, as well as decrease potential abuse of seeing a fraudulent patient. The government’s impending Red Flag Rules require patient validation before information can be given out. While not cost effective at this time, voice recognition biometrics would be able to solve this problem. Biometrics could also be used before administering any drugs to validate that you are administering them to the right patient.

**Overcoming Concerns about Biometrics**

Biometrics appears to be a best-in-class solution for patient privacy and security, so why have many healthcare providers not implemented a biometric solution?

**Accuracy of biometric scan.**

Concerns regarding rejection of an actual person or identifying the wrong person are valid. As technology has increased, these concerns are decreasing. Given the amount of information contained in a fingerprint, it is highly unlikely (estimated at 1 in 64 billion) that any two fingerprints would be identical and therefore impossible to tell apart (National Center for State Courts, N.d.).

**Invasion of privacy.**

There is some concern that the biometrics obtained will be shared with others outside the organization. Sharing the finger scan would be similar to sharing a password with an outside source. It would have no use to others because your finger scan is unique to the individual.

**Cost.**

Biometrics systems, which once cost tens of thousands of dollars to install, were originally used only by large corporations and the government. Less expensive systems, costing as little as a few hundred dollars per computer, are making the technology available to smaller businesses and individual consumers. Many laptop computers are now pre-installed with a touch scanning device.

**Summary**

The technology is here, the costs are low, and as medical providers, we need solutions to capture patient information accurately and quickly. Biometrics appears to be the solution to meet these challenges. At Eye Surgical Associates, we will be incorporating biometric finger scanning into our new electronic medical records implementation. If it works for Mickey Mouse, it should work for us.

---

**References**


Robb Linafelter, MHA, COE (402-484-9032; rlinafelter@lincsurgery.com), is the administrator of Eye Surgical Associates and the CEO of the Lincoln Surgical Hospital in Lincoln, Neb.