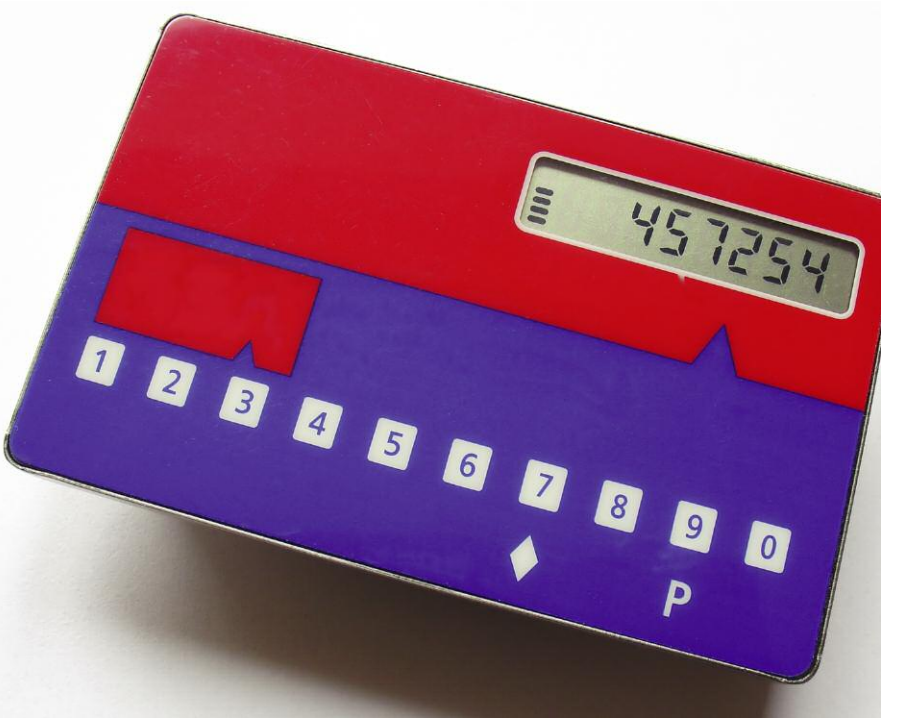
Biometrics as an Assistive Technology

Judith Katz

Part 2 in this series presents an overview of today's most common data-capture technologies and focuses on the particular value that biometrics deliver when integrated with applications designed to monitor and aid assisted living residents.



Technology's role in residential care settings continues to grow at a rapid pace. According to a 2005 Polisher Research Institute study (funded by the US Department of Health and Human Services), "Technology can potentially improve the efficiency of care delivery while enhancing the quality of that care and improving individuals' quality of life."

High-tech advancements that monitor and assist elderly residents are increasingly making their way into progressive assisted living (AL) facilities as competition drives development and affordability of sophisticated software and sensors. When integrated into systems that identify, track, and monitor individuals, data-capture technologies enhance responsiveness, fostering a greater sense of independence and well-being among AL residents. Four of the leading data-capture technologies are discussed in this article, including card-based, direct entry; proximity device; and biometric recognition systems.

Card-based Systems

These systems use plastic, credit card–style cards that differ based on the type of data they use and in how those data are stored on the card.

- *Magnetic-stripe cards* use a strip of coated magnetic recording tape encoded with the owner's credentials that are written onto the card during the personalization or enrollment process. The information, contained in 2 to 3 tracks, is composed of thousands of tiny, iron-based magnetic particles combined in a plastic film that, when swiped through the narrow slot of a terminal, are read by the scanner.
- *Barcode credentials* contain a series of lines that vary in width and distance from one another. Their readers use a laser beam sensitive to the reflected light of the lines. The reflections are translated into digital data that integrate with the computer for storage and/or decision making.

Direct Entry Systems

The cards of these systems assign an alphanumeric personal ID code to represent and identify a specific individual. These systems may require keying the personal identification number (PIN) into a terminal, inserting the card into a scanner that reads the coded data, or both. The data from each method of entry are compared to determine a match between them.

Radio Frequency Identification Smart Cards

These cards (RFID) contain a microchip with an integrated circuit ca-

pable of processing and storing thousands of bytes of electronic data. Smart card systems typically do not require PINs or other credentials because the copying of a microchip is both extremely difficult and rare.

Biometric Recognition Technology

This system addresses the challenges of authentication by using an individual's unique characteristic as his or her credentials or password. Regardless of the biometric trait being used, all recognition systems perform similarly. They begin by capturing an image of a physical trait and making a template for comparison to future samples. The ultimate goal is to resolve a pattern recognition problem to separate 2 classes—forgeries and originals.

Since the advent of computers, biometrics has moved from using one type of data—fingerprints—to using more than 10 types. Fingerprints continue to be among the most reliable and cost-effective recognition data, yet others, such as iris scans, retinal recognition, facial recognition, hand geometry, voice recognition, infrared imaging, keyboard dynamics, and handwriting dynamics, have also entered the field. And like fingerprints, these biometric characteristics are now analyzed through sophisticated sensors.

The Pros and Cons

Microchip smart cards can provide levels of security that other card-based systems cannot. For example, cards that rely on barcodes can be easily replicated with little more than a copy machine. Duplication of magnetic stripes is somewhat more difficult, but still doable. And all plastic cards are susceptible to damage. Cracks or breaks can interfere with the ability of a scanner to read them, and like any accessory, cards can be shared, lost, or, of even greater concern, stolen. Yet, barcode and magnetic-stripe cards afford the convenience of being created onsite, thereby enabling immediate replacement.

Replication of proximity smart cards, tokens, or key fobs is generally not an issue, but the potential for loss, theft, or sharing is comparable to that of other systems that use such accessories. However, RFID technology is pricier than its less expensive card-system competitors, in part because of the complexity and efficiencies it delivers. For example, "contactless" smart cards allow credentials to be read from a distance, providing an efficient way for authorizing a large group of individuals quickly. They are also effective where hands-free "log in" is important.

Convenient; impossible to share, forget, or lose; and nearly impossible to replicate, biometric systems are rated among the most secure data-capture technologies. Compared to passwords, coded-cards, or RFID-devices, "body part passwords" typically afford a superior level of security. Consequently, the digitization of "scannable" biological characteristics is part of a booming industry that the International Biometric Group projects will double to more than $7 billion by 2012.

Convenient; impossible to share, forget, or lose; and nearly impossible to replicate, biometric systems are rated among the most secure data-capture technologies.

But just as every human has flaws, so too does every biometric trait. For example, wet, dirty, or cracked skin can prevent a "proper read" of fingerprints. Voice recognition results can be obstructed by background noise, and incidents of computer-replicated voices have been reported to be able to "fool" the system. Some complain that the technology is too invasive, and express fears that fingerprints may be recreated and shared with law enforcement bureaus. However, in reality, software applications encrypt the biometric data into a mathematical algorithm. This format is incompatible with the automated fingerprint identification system (AFIS), the fingerprint matching standard of law enforcement and government agencies. Others object to lasers being beamed into the eyes during iris or retinal scans.

Decisions about which technology to use are contingent on several common factors: the targeted application, the needed security level, the cost of the technology, the cost of integrating it with existing software, the degree of user acceptance, and the technology's scalability for use with future applications. But, with continuous performance improvements and cost reductions in data-capture technologies, biometric recognition-based applications continue to be a worthwhile investment.

Biometric Access Control

Providing secure access points to and within an AL facility delivers many value-added benefits. It affords management the control to monitor and manage who is permitted access to the facility and individual rooms. This added level of security protects against criminals who may target AL facilities for access to drugs or because they consider elderly residents easy targets.

By making "you the password," biometric-access applications deliver a critical advantage over competing technologies. They eliminate the need to remember a password, bring along a card, or struggle to find and use key cards or key fobs—all of which can be stressful events for aging adults who suffer with memory loss and physical frailties.

For example, with fingerprint-recognition technology, a resident

(continued on page 36)

Computerw347.html. Accessed September 18, 2007.

3. Leapfrog Hospital Quality and Safety Survey. Leapfrog Group Web site. www.leapfroggroup.org/for_hospitals/leapfrog_hospital_quality_and_safety_survey_copy. Accessed September 18, 2007.

4. HRSA awards $31.4 million to expand use of health information technology at health centers. August 27, 2007. US Department of Health and Human Services (HHS) Web site. http://newsroom.hrsa.gov/releases/2007/HITgrantsAugust.htm. Accessed September 18, 2007.

5. State of the Union Address by the President. January 31, 2006. Whitehouse Web site. www.whitehouse.gov/stateoftheunion/2006. Accessed September 18, 2007.

6. American Health Information Community. HHS Web site. www.hhs.gov/healthit/community/background. Assessed September 18, 2007.

7. Healthcare Financial Management Association. Overcoming Barriers of Electronic Health Adoption. February 2006; p8. HHS Web site. www.hhs.gov/healthit/ahic/materials/meeting03/ehr/HFMA_OvercomingBarriers.pdf. Accessed September 17, 2007.

8. Health Information Technology Summit: Remarks by Tommy G. Thompson, Secretary Of Health and Human Services. Washington, DC: The Willard Hotel. May 6, 2004. HHS Web site. www.hhs.gov/news/speech/2004/040506.html. Accessed September 18, 2007.

9. HHS. What benefits will consumers and others receive from the community (AHIC)? Last revised March 26, 2007. HHS Web site. www.hhs.gov/faq/technology/ahtic/923.html. Accessed September 18, 2007.

10. Quality affordable health care for all by the end of Barack Obama's first term in office. Obama '08 Web site. www.barackobama.com/issues/healthcare/. Accessed September 18, 2007.

11. Health IT Now! Coalition applauds health IT bill introduced by Senators Kennedy, Enzi, Clinton & Hatch. June 21, 2007. Health IT Now! Web site. www.healthitnow.org/. Accessed September 18, 2007.

12. Wide gap between vision for e-prescribing and reality in physician practices; physicians report major barriers to using advanced e-prescribing features. April 3, 2007 [press release]. Health Affairs Web site.www.healthaffairs.org/press/marapr0704.htm. Accessed September 18, 2007.

Matthew T. Corso, Esquire, is an attorney in the firm of O'Brien & Ryan, LLP, Plymouth Meeting, PA. Mr. Corso is an experienced civil litigator and handles claims for healthcare providers, particularly LTC providers, throughout Pennsylvania and New Jersey.

Brett M. Littman, Esquire, an associate with O'Brien & Ryan, LLP in Plymouth Meeting, PA, focuses his practice on the defense of LTC facilities in Pennsylvania and New Jersey.

Biometrics as an Assistive Technology

(continued from page 32)

has nothing to find or remember. A simple tap of his or her finger on a digital sensor achieves the identity authentication required to "unlock" a door. No cards or keys can be stolen, reducing theft or other criminal activities. Moreover, fingerprint-recognition technology also eliminates the inconvenience and expense of replacing locks. And with today's robust solutions, access-control applications can even be programmed to lock and unlock doors for specific people at certain times.

Entry systems that incorporate biometric-recognition technology provide:

- Special egress security to protect residents with dementia or Alzheimer's from accidentally leaving a room or facility
- Elevator control to restrict floor access for 'memory' or dementia residences on specific floors
- Easy access to resident apartments
- Elimination of credential-accessories that can be duplicated, shared, lost, or stolen
- Logs and management reports documenting the identity of persons and the times that access events took place
- Secure, authorized access to pharmaceuticals
- Identity authentication required in medication pass management
- Easy integration with software and discrete video and camera solutions

Staff Management with Biometric Applications

Managing employee time and attendance is another challenge that biometric solutions successfully address for AL facilities. These applications frequently replace electronic time clocks or paper forms that require employees to manually enter the times they begin and end a shift. These approaches are susceptible to a high rate of human errors and inaccurate reporting. Mistakes may occur in mathematical conversions and pay-period totals. Manually compiled forms also permit employees to round up their hours or enter personal or sick time as hours worked. Timecards are also susceptible to fraudulent reporting: Buddy-punching, when employees punch in or out for absent coworkers, is a common concern that finds organizations paying staff members for time they did not work. Biometric time tracking addresses these issues and is credited with reducing time-consuming tasks and costly administrative errors and for improving employee accountability, productivity, and morale.

MSP Real Estate Inc., which specializes in Section 42 Independent Senior Housing, owns and operates 200 units at 4 AL and memory-care facilities; 3 in Wisconsin and 1 in Minnesota. Its Heritage Assisted Living Communities employ 130 people. For nearly 6 years, employee time and attendance had been managed with a traditional time clock system, which, according to MSP President Milo Pinkerton, was inefficient.

"We were spending too much time on payroll preprocessing tasks," says Pinkerton. "So when I saw a biometric application at the Annual ALFA Convention, I was interested. It automated the totaling of employee hours—so no more errors or wasted time spent on manually adding up timecards. And, it accurately clocked employees' arrivals and departures simply by having them tap a fingerprint sensor when they'd arrive or leave."

Last year Pinkerton had the biometric time-tracking application installed at all 4 Heritage Living communities. It will also be installed at the 5th and newest facility scheduled to open later this year. ALC

Judith Katz is the CEO of Count Me In, LLC (www.countmeinllc.com), a developer of award-winning fingerprint-based software solutions.