Growth of Biometric Technology in Self-Service Situations

● Josh Napua

While the healthcare industry has made great strides in ensuring patient safety, challenges still remain with medical identity theft and insurance fraud continuing to make headlines, leaving hospitals responsible and exposed. In recent years, new procedures and technologies have emerged to address these challenges and help healthcare facilities protect their patients' privacy and well-being. This paper introduces activities that utilize biometric technology to address issues such as medical identity theft and identity verification in the USA.

1. Introduction

The first step in patient safety is correctly identifying patients at the point of entry to the healthcare facility (including matching them to the correct medical records). As the mounting number of medical identity thefts has shown, however, conventional identification processes are no longer adequate and present numerous issues that continue to put patients' safety at risk.[1] These include simple clerical errors, technological failures, and even dishonest hospital employees trying to commit fraud.

Today, however, there is a new solution that surpasses all conventional patient registration and identification means. Through the use of cutting-edge biometric technology integrated with electronic medical record (EMR) and registration systems, healthcare institutions can meet the challenges associated with patient identification.

2. Medical identity theft

For most healthcare organizations, the top priorities include ensuring patient safety and preventing identity theft and fraud. Approximately 47 million people in the USA are uninsured, so medical identity theft and insurance card sharing have increased dramatically over the past several years. The Federal Trade Commission (FTC) has reported that between January 2002 and April 2006, 19 428 individuals filed complaints. In these cases, healthcare institutions are subject to great liability.

Healthcare providers must also comply with government regulations, including the Fair and Accurate Credit Transactions Act (FACT Act) amendments to the Fair Credit Reporting Act. One of the new rules, referred to as the Red Flags Rules, includes requirements for the development and implementation of an Identity Theft Program. These Red Flag Rules require measures to be in place to ensure that the social security number provided is not the same as that submitted by another person on the account of another patient and that the address and telephone number provided are not the same as or similar to those of another patient.

Managing medical records is a potential nightmare if proper controls are not in place to meet these Red Flag Rules, and the situation is only made worse by the possibility of mistaken

identity—when the registrar accidentally selects the wrong medical record for a patient.[2)]

3. Patient identity management

Proper patient identification is crucial to ensure that the right care is provided to the right person, and improper patient identification can have tragic consequences. This process is so important that the Joint Commission[3)] (a private third-party organization for assessing healthcare organizations) has made improving the accuracy of patient identification its number-one goal for the last five years. It is even an accreditation requirement for hospitals.

The first step to proper patient identity management is to ensure that registering patients are exactly who they claim to be. Errors often occur when patients have multiple names (e.g., their registered name, their given name in their native language, and an abbreviated name). Such patients will often give a different name on different visits to a hospital, resulting in the creation of duplicate records, which can hinder caregivers and threaten the patient's safety.

In addition, people frequently enter the emergency room without any form of identification, or they are unable to identify themselves owing to a traumatic condition. Furthermore, by nature, young children typically have difficulty identifying themselves. Existing identification processes include requiring a photo ID, but this is not always accurate because patients' appearances change quite frequently, especially in the case of growing children. Some facilities rely on social security numbers, but this practice is frowned upon by most, especially Medicare recipients, because of the inherit risk of identity theft. For example, just saying a social security number out loud could subject a healthcare facility to a complaint under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The second step to proper patient identity management is to correctly match patients' names to their medical records. Technologies such as Enterprise Master Patient Indexes can search out patient records on the basis of various search terms, including first and last names, social security number, and date of birth. Frequently, however, the system will not return any matches or will incorrectly match a patient to a record because of an insufficient query.

Accurate patient identification and medical record matching are vital to the patient identity management process, but the inherent drawbacks of existing methods and technologies for each process create an opportunity for next-generation solutions. Progress in biometric technologies is helping to satisfy this opportunity by simplifying the task of identifying patients accurately while improving patient registration processes.

4. Self-service: Patient Kiosk

Innovations such as Patient Kiosk[4)] with integrated Fujitsu PalmSecure[5)] technology are vital to ensuring that physician groups not only implement, but fully utilize electronic health records (EHRs), which is a key goal of the American Recovery and Reinvestment Act of 2009.[note 1)]

Once patient records in digital databases have been automated, the next major challenge will be securing them so that only the patient and those qualified medical caregivers have access to this private information. The latest patient self-service offering, Fujitsu Med-Serv 50/60

note 1) On February 17, 2009, President Barack Obama signed into law the American Recovery and Reinvestment Act of 2009—more simply known as the Federal Stimulus Package. The package includes a mix of government spending and tax measures totaling $789 billion intended to stimulate the economy through investments in infrastructure, unemployment benefits, transportation, education, and healthcare. It specifically allocates almost $23 billion to healthcare information technology and EHR adoption through the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Patient Kiosk (**Figure 1**), incorporates state-of-the-art biometric technology[6] and delivers real-time updates to databases for patient billing information, including the option to make co-payments using a credit card.

The system also seamlessly updates the patient's EHR by taking a photograph to verify his or her identity and documenting each visit to include the procedures undergone by the patient at that time. While the patient's medical record is being accessed, reminders can be sent to the kiosk screen for future annual exams and other periodic checkups.

As shown in **Figure 2**, the kiosk's PalmSecure palm-vein sensor, which can also be implemented in other hardware configurations, allows a patient to sign in at the healthcare provider's office by simply holding one hand close to the kiosk's touch screen, which then captures an image of the palm's vein pattern and encrypts it. The kiosk uploads data automatically, charges co-payments automatically, and records the patient's progress around the hospital in a session log for every nurse and doctor to see.

Figure 1
Med-Serv 50/60 Patient Kiosk.

Fujitsu is working with several medical centers, including a 24-location clinic network in Springfield, Illinois and George Washington University Medical Faculty Associates (MFA) to execute production rollouts of the kiosks.

One primary goal of the Springfield Clinic in installing the kiosks is to increase customer loyalty by improving the entire hospital experience. But there are real benefits for the clinic, too. Harried receptionists not only keep patients waiting, but also tend to forget to ask certain questions or omit important details. The likelihood of errors increases too. In the clinic's beta tests, the kiosks not only collected standardized information better than humans, but also persuaded patients to correct outdated data in a way that they are not generally inclined to do. Patients feel more in control using kiosks to keep their personal information up to date.

"Physician practices are always on the lookout for ways to lower costs while improving patient satisfaction, and the Patient Kiosk is the

Figure 2
PalmSecure technology.

answer," said James Hewitt, Chief Information Officer of Springfield Clinic, a 260-provider multispecialty physician group with 24 locations in Springfield, Illinois and the surrounding 14 counties. "Patients love the kiosk because they are in control." Springfield, which co-developed the healthcare solution with Allscripts to work on the medical kiosk from Fujitsu, deployed 50 of the kiosks in 2009.

The Allscripts Patient Kiosk was also deployed at MFA in Washington, DC, a 550-physician group made up of the faculty of the George Washington University School of Medicine. Stephen Badger, Chief Executive Officer of MFA, said "We're excited that the kiosk will offer our patients the ability to securely check in, using nothing more than their hand on the Fujitsu reader, pay their co-pay, update and correct any mistakes in their personal information, and get an alert about an overdue colonoscopy—all within about two minutes. It's what our patients want and it saves our practice time and money."

The Med-Serv 50/60 Patient Kiosks use Fujitsu PalmSecure palm vein biometric authentication technology to verify patient identity, speed up check-ins, update patient records, make co-payments, and improve patient satisfaction in an easy-to-use, private manner.

5. Biometric technologies

Implementing biometric technologies for patient identification can help healthcare organizations accelerate the registration process, save money by stopping medical record duplication, prevent medical identity theft, reduce expensive fraud by preventing insurance card sharing, and even save patient's lives by quickly and accurately identifying patients whose names are similar and cannot be easily identified through conventional means.

Biometrics comes in many different forms. The different technologies range from the very simple and fairly accurate (like fingerprints) to the highly accurate but expensive (like iris scanning). The various types of biometrics are shown in **Figure 3**, which gives their accuracies and compares them in terms of usability, which indicates how easy it is for general users to interface with the scanning device, whether a majority of users can enroll and use the technology, and whether the technology is nonintrusive for users.

Generally speaking, biometric technologies

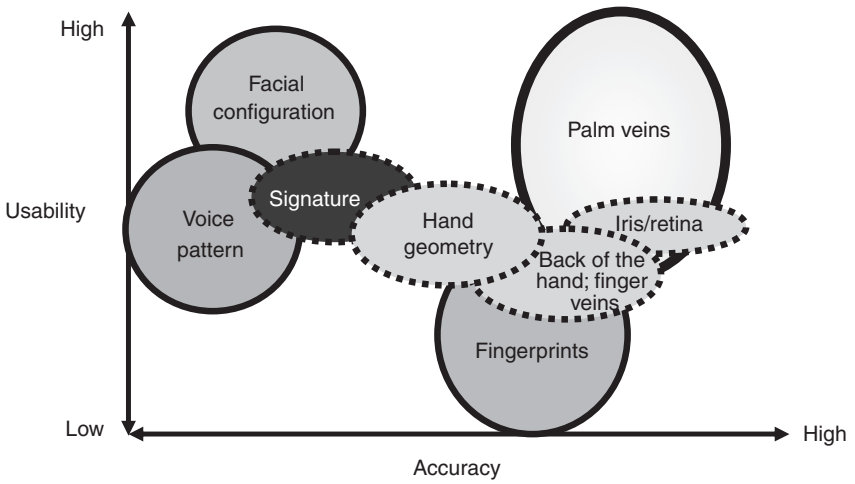

Figure 3
Comparison of PalmSecure and other biometric technologies.

are viewed as the most advanced, accurate, and secure means of identification. However, significant differences exist among the various form factors, which are important for any healthcare organization to understand when evaluating possible solutions.

Fingerprint identification, for example, has existed since the 19th century and is widely applied because the distinctive pattern of a person's finger minutiae serves as a unique identifier. However, the stigma associated with fingerprinting hinders voluntary, widespread use of fingerprinting. In addition, these patterns sometimes cannot be read if the person has surface damage to their fingers. Moreover, there are elderly people, workers in some types of jobs, and members of certain ethnic and demographic groups that simply cannot be identified using fingerprint scanning due to their low-quality fingerprints. Finally, this is not a hygienic solution as fingerprint scanners tend to accumulate germs due to repetitive contact over time. And this is not an entirely secure solution because the fingerprints residuals are easily left behind. However, PalmSecure contactless biometric technology generates rapid and highly accurate authentication that is virtually impossible to forge, leaves no biometric trace behind following authentication, and is not affected by the presence of hand lotions, chemicals, abrasions, skin conditions or cold environment effects compared to fingerprint identification.

Iris scanning is considered the most accurate biometric form factor available today. It involves scanning the vein pattern on the back of a person's retina. This pattern is unique and retains its pristine state because it is inside an enclosed space. This also makes retinal scanning very secure. However, there are significant usability issues associated with retinal scanning. The equipment is extremely expensive to implement, and like fingerprinting, iris scanning suffers from social resistance—many people do not like anything pointed at their eyes. Moreover, the scans take longer to complete and contact lenses or glaucoma may interfere, requiring re-scans.

It is vital to understand the drawbacks of these biometric solutions when they are being considered for a setting involving a large, demographically diverse user base, such as patients in a healthcare facility. In these situations, it is very important to ensure that the technology assures both a high level of accuracy and usability. In recent years, palm vein authentication has emerged as a biometric form factor that meets these requirements.

Palm vein biometrics involves shining near-infrared light at a patient's palm. The light penetrates the outer skin and reflects off the deoxygenated blood in the body. In simple terms, it illuminates a person's veins and produces a photograph of the vein pattern. This pattern represents a wealth of differentiation factors unique to the individual—palm vein authentication is approximately one hundred times more accurate than a fingerprint scan and as accurate as iris scanning.

The International Biometrics Group (IBG),[6] which evaluates biometric products through comparative testing, found that palm vein technology competes well with iris scanning technology in accuracy and demonstrated extremely low occurrences of both false positives and false negatives.

Palm vein biometrics ensures almost zero enrollment failure, essentially enabling any patient to use it. In addition, it is completely contactless—individuals simply hold their palm above the scanner for a brief moment (a second or less is sufficient)—so it is a far more hygienic option than fingerprinting and a more socially acceptable option than retinal scanning. The contactless reader provides ease of use with virtually no physiological restrictions. Moreover, it utilizes no trace technology so it leaves virtually no biometric footprint behind and it is therefore difficult to spoof, especially when compared with

Figure 4
Sensor unit for PalmSecure biometric authentication.

cheaper fingerprinting devices.

The Fujitsu PalmSecure vascular biometric authentication technology has been certified under the International Common Criteria[7] for Information Technology Security Evaluation as Evaluation Assurance Level 2. PalmSecure is the first vascular authentication solution to receive this certification, validating it as a superior form of biometric identification and security. The sensor unit for PalmSecure biometric authentication is shown in **Figure 4**.

Common Criteria are a set of established guidelines for evaluating and certifying the information security of information technology products and information systems. They are currently recognized in 26 countries, including the USA, the UK, Japan, Canada, Germany, France, and Spain. Achieving Evaluation Assurance Level 2 provides Fujitsu with a key security and competitive advantage in sales and business development efforts related to federal agencies as well as commercial enterprises seeking security products that comply with high-level industry and international standards. They also solidify PalmSecure's position as one of the industry's most secure biometric identification solutions.[3),8),9)]

6. Discussion

Medical identity theft and patient privacy remain critical concerns for healthcare organizations nationwide, and many are embracing advanced technologies to improve patient safety and, in turn, patient care. Patients are more technically savvy than ever and want to be assured that their medical records are accurate and protected. By capitalizing on the latest healthcare technology trends—the self-service kiosk and biometric identification—Fujitsu has implemented one of the first patient-oriented registration and check-in solutions for clinics and hospitals.

The combination of a biometric patient registration system and medical kiosk incorporates state-of-the-art PalmSecure biometric strong authentication, self-service check-in, credit card scanning, and patient information updating to revolutionize the patient registration process for physician practices. It is a one-to-one match between patients and their medical records, which not only prevents duplicate records from being created, but also prevents identity theft and insurance card sharing, helping healthcare organizations comply with the reporting needed for the FACT Act for Identity Theft.

Since November 1, 2008, the FTC has required healthcare providers to develop programs to safeguard against identity theft to comply with the Identity Theft Red Flag regulations as part of the FACT Act. Providers are required to implement policies and technologies to ensure that patients do not receive improper care and that they are not incorrectly diagnosed because their medical records have been compromised and/or are tainted with another patient's information. The Red Flag regulations also require providers to secure patients' medical records to prevent them from becoming victims of identity theft. The Patient Access Lifetime Match (PALM) patient registration and identification system used by ValleyCare Health System in Pleasanton,

California helps the hospital comply with these requirements by providing a highly accurate form of authentication that cannot be tampered with or bypassed.

7. Conclusion

This paper introduced activities that utilize biometric technology to address issues such as medical identity theft and identity verification in the USA. The self-service kiosk solution gives patients direct access and privacy to update their EHR data and the option to make insurance co-payments directly to the practice management system online. It not only improves patient safety associated with identification, but also increases the overall administrative efficiency of healthcare organizations and customer satisfaction. It protects patient privacy and safeguards EHRs while streamlining the registration process, meeting compliance requirements, and, most importantly, providing the highest-quality care and service possible to patients.

Josh Napua
Fujitsu Frontech North America Inc.
Mr. Napua received a B.S. degree in Electrical Engineering from the University of Denver and an MBA from Stanford University. As the Vice President of the Advanced Technology Group, he is responsible for developing solutions in the U.S. healthcare and security markets by using Fujitsu technologies and working with strategic application partners. Before joining Fujitsu, he was CEO of Wyle Systems in Irvine, California in 1996. From 1999 to 2003, he was President of Applied Computing Solutions at Avnet, Inc. in Phoenix, Arizona. He began consulting with Fujitsu in 2005 and assisted in the development channel and software partner strategies.

References

1) P. Dixon: Medical Identity Theft: The information crime that can kill you. World Privacy Forum 2006.
2) C. Nichols et al.: Medical Identity Theft. American Health Information Management Association (AHIMA), 2008.
3) Joint Commission. *http://www.jointcommission.org/*
4) Patient Kiosk. *http://www.allscripts.com/products/patient-access/kiosk.asp*
5) PalmSecure. *http://www.fujitsu.com/us/services/biometrics/palm-vein/*
6) International Biometric Group. *http://www.biometricgroup.com/*
7) Common Criteria. *http://www.commoncriteriaportal.org/*
8) N. K. Ratha et al.: Advances in Biometrics: Sensors, Algorithms and Systems Springer, 2007.
9) M. Watanabe: Palm vein authentication technology and its applications. *http://www.biometrics.org/bc2005/Presentations/Conference/1%20Monday%20September%2019/Poster%20Session/Watanabe_1568964435_BioSymposium_2005.pdf*