

PATIENT AND STAFF IDENTIFICATION

Understanding Biometric Options

By Evan Smith

Accurate patient identification is critical to achieving the benefits of electronic medical records and to ensuring patient safety. There is also an increasing need for positive staff ID to protect patient privacy and track e-prescribing. This paper analyzes identification problems and evaluates available biometric solutions.

Health Care Identification Problems

Patient ID. Electronic medical record (EMR) systems are powerful tools for improving care, but their power also expands opportunities for error. As EMRs and Health Information Exchanges (HIEs) are installed, more

patient information is stored and retrieved, in more discrete access events, in more records, from more locations, by more people. The goal is a single record for each patient identified in a master patient index (MPI), with perfect integrity for each record. As systems expand, the number of records with similar names and birthdates increases. Given these factors, errors will inevitably increase unless administrators take proactive steps to create a 100% accurate link between the patient and the MPI record.



Front-line caregivers must have confidence that they can rely on the accuracy of electronic patient records. Minimizing record matching errors is a key factor in determining whether these new systems will be reliable and useful, or create more problems than they solve.

Staff ID. Better control of staff log-in processes is needed to protect the privacy of patient records and provide an undeniable audit trail for e-prescriptions and other order entries.

ID Problems and Electronic Medical Records

Four categories of problems occur when inaccurate patient identification methods are used with EMRs:



Duplicate records. If an arriving patient is not matched to an existing record, a new record is often opened. Medical staff cannot see potentially critical information in the patient's previous record and must order duplicate tests and spend time on diagnosis that might have been avoided with better record finding.

Data Filing Errors. Vital signs, lab results, medical notes and diagnoses may be filed in the wrong patient record by an attending staff member, lab or other entity. Each time this happens, two records are corrupted. One record has misleading information relating to another patient, and another record omits potentially critical patient care information. Each corrupted record may cause a medical error.

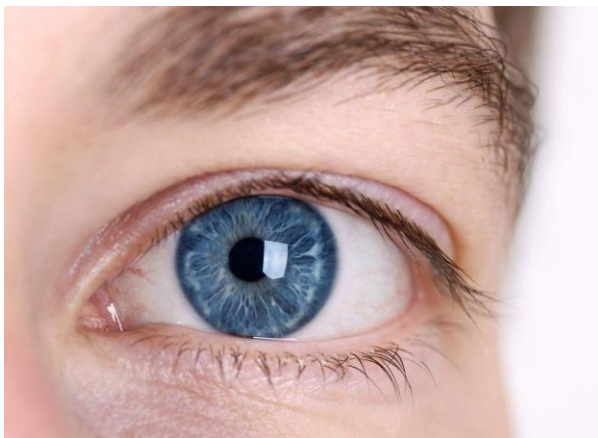
Relying on the Wrong Record. Bringing up the wrong record, and relying on the information in the record for diagnosis or treatment, may result in a medical error.

Benefits Fraud and Identity Theft. Misrepresentations of identity are increasing, and the known incidents represent only a fraction of the true volume of fraud. Accurate patient identification can stop identity theft and the use of others' benefits before they happen, and improve collections.

These errors have a profound personal and financial impact on families, health care facilities, and the economy. Studies indicate that hospital medical errors kill 48,000 to 98,000 Americans each year. Many of these errors are caused by mistaken ID or inaccurate recordkeeping. Monetary costs are high. For example, the average remedial treatment cost for a “wrong medication error” is \$4,700 per adverse event. Better approaches are clearly needed.

Approaches to Identification

There are three ways to determine a person’s identity:



- **What they carry** – medical ID cards, ID bracelets, driver’s licenses and implanted chips.
- **What they say** – interview and software-assisted record location process. (What’s your name and date of birth?)
- **Who they are** – positive biometric ID based on unique physical features of the human body.

The first two (traditional) methods immediately fail if the patient does not offer accurate information that matches his existing record. The weakness of these methods enables fraud and identity theft. Further, human and system record locating errors occur regularly *even when the patient is honest, cooperative and mentally sharp*. The third method, biometric ID, is the only approach that can identify people with virtually zero errors.

Why Use Biometrics?

Correctly matching patients to their records and treatment orders is an essential step in preventing medical errors. Because of the significant potential for harm when an ID error occurs, there is no acceptable error rate. Patients expect a high level of attention and accuracy in maintaining and accessing their records, including deploying the best

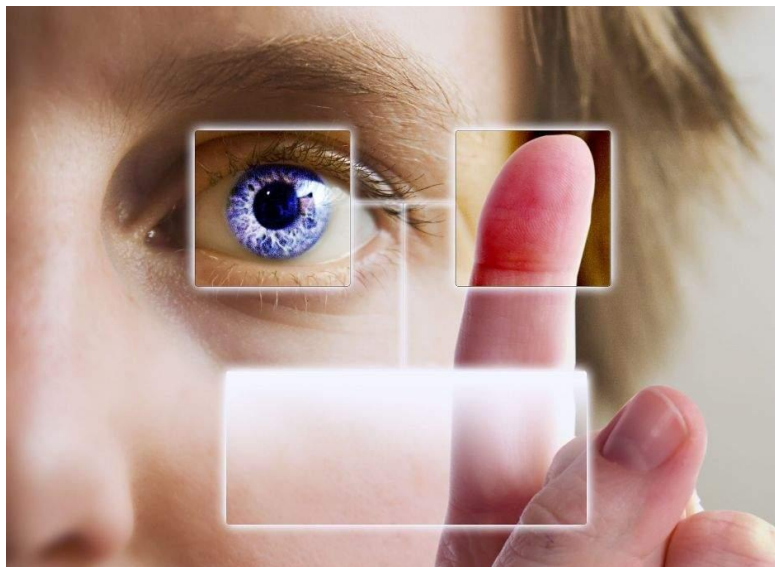
available technology. ID errors will increasingly be viewed as careless and unacceptable, particularly when patient harm results.

Privacy considerations and new government mandates create new requirements for accurate staff identification. Traditional approaches involving two-factor authentication, complex passwords, and items that must be carried will work for occasional remote access, but are too cumbersome for daily clinical use at shared computers. Biometrics deliver better security *and* instant log-in for busy clinicians.

Comparing Biometric Technologies

Fingerprints, iris and facial are the three most prominent commercially available biometric technologies. Palm vein recognition, a new and relatively untested technology, is also advertised for healthcare applications.

Each technology has different features and limitations. To select the one that's best for a particular application, biometric experts start by identifying the performance issues that are critical for the application. In



patient identification, there are eight key categories:

- *Accuracy*
- *Search Capability*
- *Reliability*
- *Patient Comfort/Safety*
- *Privacy Protection*
- *Staff ID Capabilities*
- *Ease of Interfacing*
- *Cost*

Let's look at each of these categories and the capabilities of the competing biometrics.

Accuracy. Patient ID applications require zero-error accuracy. The maximum accuracy of each biometric is limited by the uniqueness of the feature used for identification. A single fingerprint can be used to verify an otherwise-established identity, but accurately finding an identity in a

large database requires multiple fingerprints. Facial technology is limited by the relatively small number of distinguishing facial features and is incapable of the accuracy required for patient care. Palm-vein vendors claim high accuracy, but these claims are based on their own testing under lab conditions, or studies by their paid consultants.

The iris is the most accurate of the biometrics. No two irises on the planet are the same--even identical twins have different iris patterns. The abundance of detail in the iris, its variability and lack of genetic dependence all make iris identification far more accurate than either fingerprints or facial. The capabilities of iris identification have been scientifically verified in reliable, independent long-term tests by the U.S. National Institute of Standards and Technology (NIST), U.S. Department of Defense and similar United Kingdom government studies.

Search Capability. An ideal clinical biometric system will instantly identify a patient and retrieve his record. The uniqueness of the iris, coupled with the speed of the iris identification matching algorithms, makes it possible to complete a “one-to-many” search of millions of records in seconds. This means a patient can walk up to a counter or sit down in an exam room, look at the camera without providing any other information, and the correct medical record will always be instantly retrieved and displayed. Competing technologies do not have the same search capabilities. They add verification steps to the familiar manual lookup process, rather than simplifying and expediting patient intake.

Reliability. Patients, insurers and other stakeholders may question the administrator’s choice of technologies. Biometrics selected for clinical use should have capability reports from large-scale, independent U.S. government studies that justify reliance on the technology. Fingerprint and iris technologies meet this government testing requirement, but palm-vein does not.

In addition to government lab testing, a proven track record in real-world operations is essential for biometrics in critical health care applications. Fingerprint, facial, and iris systems are all long-available commercial technologies with well-understood performance characteristics. In addition to more recent patient ID installations, iris identification has been used in high security applications around the world for over ten

years with zero errors. The Immigration Services of the United Kingdom and Canada, among others, have adopted iris identification for critical functions like passport control.

Fingerprint systems have been tested for patient identification, although with limited success. Palm-vein technology lacks the decades-long field performance record of the mainstream iris and fingerprint biometrics.

Patient Comfort and Safety. In a clinical setting, patient comfort and preventing disease transmission are both key considerations. Fingerprinting requires touching a sensor that requires sterilization each time it is used. Palm-vein vendors claim that their scanners are “non-contact,” but careful examination of these statements is recommended. Independent reports about actual hospital installations confirm that the patient’s hand must be placed on a support or “cradle” positioned above the scanner for correct operation,¹ and the cradle must be sterilized after each use.



The digital cameras used in iris systems do not touch the patient, so there is no risk of disease transmission and no additional sterilization step is needed. Iris ID systems also provide excellent patient comfort. The digital cameras do not use a flash or any other irritating or harmful illumination. The patient just looks at the camera and their identification is complete.

Privacy Protection. Clinical biometric systems must preserve and protect patient privacy. If a significant number of patients refuse to use a system, it will not deliver the desired benefits.

Fingerprinting is unavoidably a “big brother” method. The primary worldwide use of fingerprinting is for criminal investigation and immigration enforcement. People leave fingerprints everywhere they go, and fingerprint records can be used to identify them without their

¹ See e.g. http://www.sciencedaily.com/videos/2007/1009-high_tech_patient_id.htm which includes a video showing how the patient places his hand on the palm-vein scanning cradle.

knowledge. For these reasons, many patients object strongly to being fingerprinted. Fingerprint pattern information collected for clinical ID purposes, by its very nature, can be useful in criminal investigations. It is therefore possible for the police, FBI or INS to issue subpoenas for clinical fingerprint data and use these records against patients. Medical facilities must comply with court orders and cannot assure patients that their fingerprint data will not be used by government agencies.

In contrast, iris and palm-vein systems store pattern data extracted from an image taken at enrollment. This pattern data is a collection of ones and zeros that has no value for criminal or immigration investigation. The intentional or unintentional release of this data would not compromise personal privacy because the stored data is only useful when installed in the clinic's system and used by the software that matches the pattern data to a patient looking into the clinic's scanner. Iris systems designed for medical applications identify people only when they give their consent by looking at the camera, and cannot be used with long-range cameras.

Staff ID Capabilities. Clinicians must be accurately identified for e-prescribing, electronic records access, and establishing patient care audit trails. An ideal clinical ID system serves both staff and patient identification needs. The advantages of the iris in terms of speed, accuracy, and search capability make it the best available tool for fast log-in and single-sign-on (SSO). The same iris cameras used to identify patients can instantly log-in a staff member with no keyboarding. The reliable iris technology links the staff member to their electronic session activities and to the procedures they perform with no room for denial. In addition to being less accurate and less capable, palm-vein and finger technologies are less convenient. In a clinical environment fingers, palms, and facial features are often covered by gloves and masks, while the iris remains uncovered.

Ease of Interfacing. Clinical ID applications require an architecture that enables rapid interfacing of the biometric system to existing clinical software applications. All of the major biometric vendors provide interfaces, so interfacing is not a major distinguishing feature. However, the ease and convenience of that interfacing should be evaluated.

Some of the available iris systems were designed specifically to rapidly add biometric ID capabilities to electronic medical record systems. In these systems, two interface methods are available. A universal interface can be used “out of the box” with almost any Windows-based application. Software Development Kits (SDKs) are available to users and medical software providers who wish to tightly integrate the system with clinical software. The SDK provides a simple Windows-standard interface allowing the clinical software to control and activate the identification service as desired. When the ID service is activated by the calling program, within a few seconds the patient is identified and the patient’s unique identifying number is returned to the calling program. The EMR or other clinical software product then uses the patient number to retrieve and display the patient’s record.

Cost. The commercial iris, vein, and fingerprint systems each include software, hardware, and interface components, so looking at the cost of one piece does not tell the whole story. The appropriate basis for cost comparisons is “total cost of ownership,” taking into account acquisition costs, periodic maintenance costs, installation and training, and per-patient sterilization costs. Today, there are commercial iris, vein, and fingerprint systems with closely competitive total costs of ownership. Today, each of the available biometrics is affordable for patient ID applications.

It should be noted that for many years, iris identification systems were very expensive and were used mainly in national security applications. However, the same technology is now available in a package that is cost effective for daily medical use. One commercially available iris system uses cameras that cost less than \$150 each.

Choosing the Best Solution

This table summarizes biometric performance relative to the eight key criteria discussed in the previous section. Facial recognition is omitted from the table because it lacks the accuracy needed in patient ID applications.

Selection Criteria	Iris	Finger	Palm Vein
Most accurate biometric	<input checked="" type="checkbox"/>		
One-to-many ID capability (large database search)	<input checked="" type="checkbox"/>		
Reliability – long track record, validated by U.S. government studies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Protects privacy – doesn't perform "big brother" operations	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Patient Safety/Hygiene: comfort, zero contact	<input checked="" type="checkbox"/>		
Accurate staff ID while wearing gloves/masks	<input checked="" type="checkbox"/>		
Interface Capacity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Affordable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Fingerprint technology requires touching a sensor, and is unavoidably a "big brother" biometric that will draw significant objections in some patient populations.

Palm vein technology claims to be non-contact, although these claims are contradicted by press reports and the statements of hospital administrators using these products. Palm-vein cannot perform instant one-to-many searches in large databases, and does not have the proven track record and government study validation of the other biometrics.

Iris identification easily meets each of the biometric selection criteria for clinical applications. It is the most accurate biometric. Its superior one-to-many search capabilities in large databases

and its ability to identify patients and staff members without any contact are significant advantages in patient ID applications. Iris systems also speed staff ID for e-prescribing, fast log-in, and procedure tracking, and can be used while wearing gloves and masks.

Based on this analysis, iris technology is the most appropriate biometric for clinical identification.

Conclusions

- People can be identified by what they carry, what they say, or who they physically are. However, only systems that rely on unique physical characteristics (biometrics) can identify people without errors.
- A zero error rate is the appropriate standard, both for identifying staff and for matching patients to medical records.
- The latest iris identification systems significantly outperform other ID products in terms of accuracy, large-database search capability, reliability, patient comfort and safety, and privacy protection. Cost, however, is competitive with the other biometrics.
- Iris identification systems are an excellent tool for identifying staff members. Iris ID enables fast log-on with no keyboarding and provides an undeniable audit trail linking the staff member to actions taken.
- Iris identification is a cost-effective, clinically advantageous way to significantly increase record locating accuracy at facilities using electronic medical record systems. Patients will benefit from a system that ensures accurate storage and retrieval of critical information. Hospitals, clinics, and insurance providers will benefit through reduced fraud, improved billing and collections, streamlined patient flow and better staff utilization.

For more information about biometric identification technologies for healthcare applications including clinical iris identification systems, contact:

Eye Controls, LLC ▪ 22 Baltimore Road ▪ Rockville, MD 20850

info@eye-controls.com ▪ 877-4-IRIS-ID ▪ www.eye-controls.com