Choosing The Most Effective Biometric Modality for Patient Identification in Healthcare

Assessing the characteristics and capabilities of biometric hardware

RightPatient®

www.rightpatient.com

Executive Summary

The journey to implement a biometric identification system will require healthcare organizations to evaluate several different biometric modalities and reach an educated decision on which one or which combination may be the most effective based on the unique demographics of their patient population. Evaluating the effectiveness of a biometric hardware modality can be difficult however without a thorough understanding of device characteristics and limitations.

The goal of any biometric patient identification solution is to enroll as many patients as possible and the only true way to create incremental value over time is to deploy a single hardware modality or multiple modalities that have the best chance of achieving high levels of patient acceptance, have the ability to quickly scale, can identify patients with 100% accuracy regardless of their physical condition, and can be used to accurately identify patients at ANY point along the care continuum.

Over 13 years of experience in global biometric identification projects in a multitude of verticals encompassing a wide range of physical environments has taught us that biometric hardware modalities are well suited for use in certain conditions, but may not be as effective when subjected to challenges unique to the vertical where they are being used.

Choosing a biometric hardware modality requires careful analysis of device attributes to maximize return on investment and patient participation. This white paper closely examines and evaluates biometric hardware modalities that can realistically be used for patient identification in healthcare including a detailed assessment of their unique characteristics to help you make an educated decision on which modality, or combination of modalities is the best choice for your healthcare organization.

Understanding the capabilities and limitations of biometric HARDWARE DEVICES is a key factor to a successful implementation of patient identification solutions. For example, did you know that photo biometrics does not require patient contact with a hardware device making it a hygienic patient ID technology that supports hospital infection control?

Table of Contents

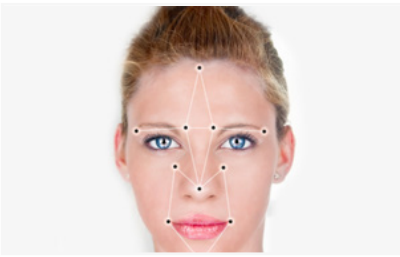
Finger Print Reader

Palm Vein Reader

Photo Biometrics

Finger Vein Reader

Voice Recognition



Facial Recognition

Introduction

More hospitals and healthcare organizations are investing in the use of biometrics for patient identification and with good reason. Biometrics are a proven patient identification technology that has the unique ability to significantly improve patient safety by:

- Preventing medical identity theft and fraud at the point of service
- Eliminating duplicate medical records and overlays
- Improving and sustaining patient data integrity across any network
- Safeguarding personal health information (PHI) access from any touchpoint
- Establishing a federated patient identification credential to solve patient data matching errors across distributed locations

The path to implementing a biometric identification system requires healthcare organizations to decide which hardware modality is the most effective to deploy based on their own unique needs and ability to offer accurate patient identification covering all touchpoints along the care continuum.

The problem is that most biometric patient identification software vendors only offer the choice of using one hardware modality, hampering the effectiveness of their solution to achieve the goal of improving patient safety and patient data integrity. Limiting hardware options can not only negatively affect system performance, but it also forces healthcare organizations to risk single vendor dependency without the option of expanding the solution deployment to cover mobile operating systems, patient portals, home health, and many new touchpoints that have recently manifested parallel to the rise in healthcare digitization. In addition, single hardware modality biometric vendors often rely on proprietary systems that lock you in to using one device and do not conform to industry data standards limiting deployment flexibility and hampering the ability to easily share clean data across networks – an important goal that directly affects the ability to improve population health and participate in a health information exchange (HIE).

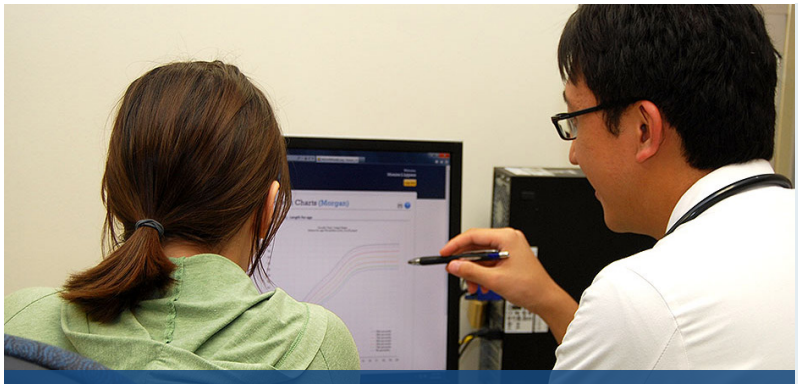
The problem is that most biometric patient identification software vendors only offer the choice of using one hardware modality, hampering the effectiveness of their solution to achieve the goal of improving patient safety and patient data integrity.

Why does hardware Variety matter?

Patient identification in healthcare used to be simple. A patient arrives at a hospital, doctor's office, or medical facility, provides their insurance card, driver's license, or other document to verify their identity and is then administered care. However, digitizing healthcare has exponentially increased access to a host of new patient touch points to access PHI which demands the same level of secure identification then a physical trip to a healthcare facility. Why?

Patients who now utilize fitness tracking devices, mHealth apps on smartphones, patient portals or other connected medical devices could potentially be at risk of privacy and security data breaches due to the fact that these new touchpoints still rely on antiquated identification credentials for secure access. User names and passwords are no longer sufficient or adequate security credentials that have the ability to secure and protect sensitive PHI. When we think about using biometrics for patient identification, most of us envision a patient providing their biometric credentials via a fingerprint, palm vein scan, or iris pattern at a registration desk within a healthcare organization because the use of biometrics in healthcare traces its origins to patient access for brick and mortar healthcare facilities.

The evolution of digitized healthcare has help to cultivate a bevy of new ways patients can access PHI and healthcare services – patient portals, mHealth apps, and mobile devices for example. In lockstep with the proliferation of these new patient touchpoints is the rising demand from patients to ensure their data and privacy is kept safe and intact when engaging with these new touchpoints and a raised consciousness of how healthcare data breaches endanger their health and well-being and reflect negatively on provider reputation.



A doctor assisting a patient with portal access

Digitizing healthcare has exponentially increased access to a host of new patient touchpoints to access PHI which demands the same level of secure identification as a physical trip to a healthcare facility.

Why does hardware Variety matter?

The use of biometrics to secure PHI data and patient privacy requires developing a security strategy that capitalizes on the flexibility of this technology to offer unprecedented identification accuracy. In an optimal setting, healthcare organizations can use multiple forms of biometrics to address the need for secure patient identification not only on a physical trip to the doctor's office, but also at any point along the care continuum. This requires deployment of more than one biometric modality to meet the unique identification needs of each patient touchpoint.

For example, if hospital A sought to deploy biometrics for patient identification at every touchpoint where patients could either access PHI or receive medical services, they may want to consider this strategy:

- Iris recognition biometrics to identify a patient during an office or hospital visit
- Facial recognition biometrics to secure a patient's identity prior to using a mobile device or mHealth app to access PHI or receive telehealth services
- Voice biometrics for secure patient identification via telephone communications to access PHI

The reality of deploying biometrics for patient identification is that a combination of modalities is required to successfully address the challenge to secure PHI and ensure a patient is who they claim to be, regardless of where they are along the care continuum.

With that backdrop, let's closely examine the characteristics of current biometric modalities that are available for patient identification in healthcare and in what environments they can actually be deployed.

Next-generation photo biometrics cameras offer highly innovative and intuitive patient positioning to achieve 100% identification accuracy

Which biometric patient identification hardware is best for you?

A digital disruption is playing out in healthcare, as witnessed by the emergence of new business models and technology that will change the nature of patient interactions, alter consumer expectations, and ultimately improve health outcomes. As consumer health platforms support more patient touchpoints, there is a growing need to implement stricter identification protocols so patients feel at ease that their medical identities are protected and their sensitive PHI data is not accessed by unauthorized individuals.

In healthcare, mandates are steered towards making information more, not less accessible, adding urgency to adopt stronger identification technologies that have the ability to verify a patient's identity no matter where they may be. The idea is not to limit or shield off information, but aggregate it more and make it more available across all aspects of workflow from hospitals to insurance carriers to health information exchanges.

Benchmarking the value of a biometric patient identification solution includes assessing its flexibility to offer more than one modality to help meet the shifting demands of accurate patient identification across every touchpoint along the care continuum.

Biometric hardware modalities each possess their own unique strengths and attributes that differentiate their capabilities. The key to determining which biometric modality or combination of modalities would provide a holistic approach to accurate patient identification across the entire care continuum is a thorough assessment of infrastructure, work flow, patient demographics, reliability, accuracy, and form-factor.

To help you decide how to choose which biometric modality or combination of modalities is the ideal fit, we created a comparison chart that includes a detailed list of hardware characteristics and capabilities, and where these modalities are best suited for deployment.

Biometric Modality	Characteristic	Deployment Options
Fingerprint	• Small form factor allows for easy distribution • Very fast matching speeds (100MM/sec) • 1:N scan* and identify (no need to enter D.O.B. or other credentials) • Relatively easy to use • Proven technology – in use for many decades • Not locked into any single device manufacturer – lowers long term risk • Non-proprietary technology: complies with industry data standards (e.g. NIST)	• Patient ID in person and at bedside • Patient ID for home health

Biometric Modality	Characteristic	Deployment Options
Finger vein	• Low social stigma • Device provides audio and visual result notifications • Small form factor allows for easy distribution • More difficult to forge than fingerprint since vein patterns are inside the body • Relatively easy to use • Doesn't rely on skin integrity (like fingerprint)	• Patient ID in person and at bedside • Patient ID for home health

Biometric Modality	Characteristic	Deployment Options
Facial Recognition	• Easy as taking a picture • No hygiene issues • Enrollment photos can be used for remote authentication (e.g. patient portal, mHealth apps, etc.) with multi-biometric platform • Does not require physical or even deliberate interaction • Can work with any standard	• Patient ID in person and at bedside • Patient ID for portal access • Patient ID on mobile devices • Patient ID for home health

Biometric Modality	Characteristic	Deployment Options
Palm vein	• Low social stigma • More difficult to forge or spoof than fingerprint since vein patterns are inside the body • Relatively easy to use • Doesn't rely on skin integrity (like fingerprint)	• Patient ID in person and at bedside • Patient ID for home health

Biometric Modality	Characteristic	Deployment Options
Iris (photo biometrics)	• Easy as taking a picture • No hygiene issues (non-contact) • 1:N scan and identify (no need to enter D.O.B. or other credentials) • Very fast matching speeds (up to 6MM/sec) • Very accurate – chance of two irises being identical is 10^{78} • Template exhibits long-term stability • Minimum enrollment age: 1 year • Simultaneous photo capture • Not locked into any single device or manufacturer – lowers long term risk • Works on one or both eyes • Non-proprietary technology: complies with industry data standards (e.g. NIST)	• Patient ID in person and at bedside • Patient ID for home health • Patient ID on mobile devices and smartphones (coming soon)**

***1:N biometric matching compares a captured patient template against all stored templates in a biometric database – the only way to ensure high levels of data integrity across an HIE or IDN**
****Iris recognition on smartphones is still in development for mainstream use**

The table above characterizes each biometric modality based on their unique abilities and practicality to be used in modern settings along the care continuum. What's clear is that no individual biometric hardware modality has the capability to be used at each and every point along the care continuum.

Instead, if the goal is to attain the highest levels of patient identification accuracy and patient data integrity, a combination of biometric hardware modalities simply must be deployed to realistically cover every touchpoint that a patient now has the ability to interact with if a healthcare organization is committed to ensuring privacy and reducing risk to improve safety.

CONCLUSION

Patient identification in healthcare is fundamentally different than years past. Healthcare digitization has opened a plethora of new touchpoints where patients can access PHI and receive care outside of the traditional brick and mortar environments. As a result, healthcare organizations must now strategize patient identification initiatives with a holistic mindset that covers these new touchpoints and sustains patient data integrity with flexible technology that combines speed and accuracy and protects patient privacy.

The goal of achieving 100% patient identification accuracy in healthcare can no longer be realized by relying on unreliable, antiquated authentication security protocols that open the door to data breaches and cyber attacks due to their inability to provide adequate protection against identity theft and fraud.

Increasing safety and reducing the risks that can lead to unintended medical errors caused by patient misidentification is an important goal and cannot be accomplished with biometrics by relying on a single biometric modality to cover all patient touchpoints. The savvy healthcare organization that invests in a biometric patient identification solution must understand that deploying a variety of biometric hardware modalities that contain attributes which match the unique requirements of each touchpoint is a necessity to ensure the highest levels of patient safety.

Additional resources

EBook

Understanding Patient Identification Solutions (What are the differences between biometrics, smart cards, and barcodes?) **http://bit.ly/1kaK3Wp**

White Paper

Eliminate Patient Fraud and Increase Patient Identification Accuracy with Vascular and Iris Recognition Biometric Identification Technology **http://bit.ly/1KXy0AP**

Blog

ww.rightpatient.com/blog/

References and copyright

This white paper was written, designed, and assembled by RightPatient®. Information contained in this white paper is the copyright of RightPatient®. This white paper is our opinion on how to understand biometric hardware modalities based on their unique characteristics backed by our 13+ years of knowledge and experience in global biometric identification projects. We did not reference any third party articles or research for this report because it is based on our own real world experience implementing biometric identification in a variety of markets. Please feel free to contact RightPatient® if you have any questions.

RightPatient®

1050 Crown Pointe Pkwy
Suite 850 , Atlanta,
GA 30338 USA

Phone - (404) 528-1270

Mail - info@rightpatient.com

Fax - 678-559-0219

RightPatient @rightpatient RightPatient RightPatient

RightPatient®

www.rightpatient.com