UNDERSTANDING THE DIFFERENCES BETWEEN PATIENT IDENTIFICATION TECHNOLOGIES

A COMPREHENSIVE NEW EBOOK FROM RIGHTPATIENT®

RightPatient®

www.rightpatient.com

THE ACCELERATED RISE OF HEALTH INFORMATION TECHNOLOGY

Advances in health information technology (health IT) over the past few years have been developing at a breakneck speed. Passage of 2009's Health Information Technology for Economic and Clinical Health Act (HITECH) set the wheels in motion for an unprecedented explosion to promote and expand the adoption of health information technology and laid the foundation for modern healthcare reform beginning with the widespread adoption of interoperable electronic health record (EHR) systems. The philosophy was to encourage full scale implementation of EHR systems by healthcare providers through financial incentives by demonstrating "Meaningful Use" that reflected significant improvements in care. In addition, Health Information Exchanges (HIEs) emerged as a new tool and a byproduct of EHR systems which help to mobilize healthcare information and electronically share it across often disparate healthcare organizations with a region, community, or hospital system.

Since then, the health IT landscape has grown exponentially as vendors have stepped in to fill the technological void of evolving healthcare entities – designing and developing applications, systems, and tools that directly or indirectly work with EHR and HIE systems to improve their utility and ability to improve overall population health. One of the most important (and often over looked) components to ensure the success of most health IT investments is the ability to accurately identify a patient. As with any industry, there are choices on what type of patient identification solutions to adopt – each carrying specific advantages but only one able to meet the rising demand of ubiquitous patient identification at each and every touchpoint of modern clinical care.

SYSTEM
ACCURACY
PROCESS
DATA INTEGRITY
CONSISTENCY
CONTENT
RELIABILITY

Patient Identification in Healthcare

Patient identification continues to be a topic of debate in the healthcare industry and one that refuses to go away, largely due to a confluence of roadblocks that illustrate the challenges:

- A lack of industry standards governing the demographic information captured from each patient
- A lack of consistency in how information is collected
- Public perception that they are not obligated to present any type of government approved identification at the time of service

Despite the healthcare industry's inability to reach a consensus on what type of mandated patient identification standards should be implemented along with most healthcare providers continuing to capture "business as usual" demographic information, the need to design and develop electronic patient identification systems that support patient safety and ensure patient data integrity (especially across HIEs) continues to surface and many new solutions have sprouted up in the market to address patient identification needs.

Patient Data Integrity Dependent on Accurate Patient Identification

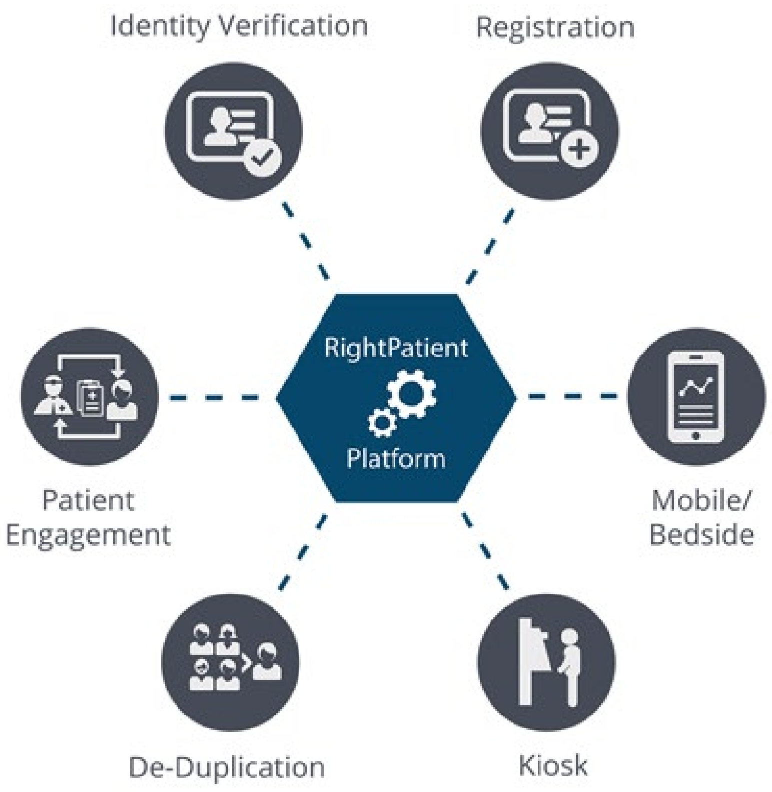
Establishing and maintaining patient data integrity is considered by many to be the holy grail of fluid, accurate, effective, and trustworthy EHR systems and Integrated delivery Networks (IDNs). As more hospitals and healthcare systems migrate to computerized physician order entry (CPOE) and EHRs, and more HIEs are built to coordinate care across networks, many are raising concerns about how to effectively manage data integrity to ensure it is kept free from corruption, modification or unauthorized access. The accuracy and trustworthiness of patient data within an EHR system is of course, a precursor to confident participation in HIEs.

The proliferation of healthcare EHRs and the transition of data across HIEs opens the door to data corruption, and as these systems become larger and more complex, vulnerabilities grow. In most other industries, data integrity is just as important, but corruption errors can be rectified and mistakes fixed. In healthcare, it often becomes a matter of life or death.

THE GROWING DEMAND FOR PATIENT ID AT NEW TOUCHPOINTS

Effective patient identification in healthcare requires a comprehensive strategy to establish authentication strategies at every touchpoint

The digitization of healthcare has created unprecendented demand for patient identification platforms that provide accurate authentication for a multitude of touchpoints to ensure that no matter where a patient interacts with the healthcare system, their identity is accurately identified. Accurate patient identifciation is the foundation to protect patient safety and guard against the perils of identity theft and fraud which directly endangers patient lives and lowers the integrity of medical data.



Increasing patient safety initiatives will always be a major focus in the healthcare industry. As the digital age ushers in new technology (mobile and patient portals for example), that threaten to derail otherwise aggressive and successful patient safety policies, it is critical that the industry implements patient identification enterprise solutions that will help to maintain a symbiotic relationship between adopting new patient tools to access and receive care and preserving safety protocols. Effective and sustainable patient identification solutions must rise up to meet the growing demand to protect patients at each and every step of their care, including new touchpoints resulting from the accelerated rise in health information technology.

As more patients are gaining access to healthcare and interacting with providers in different ways, it is critical that paitent identification solutions must be comprehensive enough to handle the evolving market in all these different ways and at the very least provide an integrated, secure patent identification platform across the multitude of patient touchpoints that respects privacy and helps comply with HIPAA guidelines to ensure the safe transmission and collection of health data.

MODERN PATIENT IDENTIFICATION SOLUTION OPTIONS

The key for any healthcare facility is to invest in a ubiquitous patient identification platform.

As with any new technology, it behooves healthcare providers to exercise proper due diligence and take the time to ask the right questions – questions that hit at the core of the patient identification technology's abilities and limitations including the capacity to evolve to meet increasingly complex and dynamic needs where accurate, safe, and secure patient identification is required such as mobile devices, patient kiosks, and home health environments. Healthcare providers must ensure that any patient identification technology investment ensures seamless authentication across any medium or touchpoint to generate clean data, lower costs, and secure patient trust – even if those touchpoints have not yet been invented!

The key for any healthcare facility is to invest in a ubiquitous patient identification platform. One that uses a combination of various human identity variables to ensure seamless patient ID regardless of the setting and has the utility for application in any authentication scenario.

In the era of rising consolidation and establishing economies of scale to help keep costs low and quality care high, why would you want to invest in a patient ID technology that is limited to only one setting and can't be used as a ubiquitous, flexible system to cover all patient touchpoints?

ARE SMART CARDS A VIABLE OPTION FOR PATIENT IDENTIFICATION IN THE U.S.?

Fast paced industry requires new patient identification tools

It has often been said that there aren't many working environments that are as fast-paced, dynamic, and decision-specific as today's modern hospitals where both medical and non-medical staff juggle attention and priorities to synch with patient flow depending on the severity of their conditions.

The fast paced world of healthcare is a key reason why improving patient identification accuracy has been #1 on The Joint Commission's National Patient Safety Goals since 2003 that encourages hospitals to research modern patient identification technologies that can address problems that arise when patients are misidentified in a clinical setting and provide a multi-factor authentication environment (i.e. – using at least two patient identifiers before providing care, treatment, or services).

In the spirit of meeting the challenge to provide modern patient identification tools that healthcare providers can use for accurate identification beyond simple demographic qualifiers, new tools are available in the market that help to increase identification accuracy and raise patient safety levels. What's important to remember is that new technologies come with limitations that healthcare providers should evaluate before making the decision to invest.

Smart cards for patient identification in healthcare

Among the multiple modern patient identification technologies that healthcare providers are evaluating is the use of smart cards. Smart cards can serve different functions and are usually programmed with multiple identification credentials including individual biometric characteristics, such as a fingerprint. Although smart cards have the ability to uniquely identify a patient in a healthcare setting, their limitations render them an impractical identification technology for the U.S. healthcare market.
Our experience with biometric technology has shown that in certain settings, the use of smart cards for patient identification is a viable option for the healthcare industry, but concerns over a lack of infrastructure, expense, privacy, the absence of industry standards for functionality and security, combined with the short shelf life of the technology do not render smart cards a viable long term solution.

The effective use of smart cards for patient identification in healthcare is largely dependent on the deployment environment. Take for example our work with smart cards in the country of Haiti to help monitor and track AIDS patients, ensuring medication adherence and accurate disease management. We embarked on this project through a strategic partnership with the Centers for Disease Control and Prevention (CDC), carefully studying environmental, demographic, and societal conditions that could negatively or positively affect the deployment and then made the decision that smart cards were the most viable option for patient identification based on:

- Low patient sensitivity to personal data (including a biometric profile) stored on the smart card
- Third party funding for the cost of the card absolving patients from the expense of producing and replacing the cards
- The absence of a need for hospital infrastructure to support the cards – all administrative and data processing are covered by third parties
- Our long history engineering biometric identification deployments based on human factor engineering and subsequent assessment that smart cards are not a viable alternative for long term patient identification

Market Factors Dictate Smart Card Applicability

The use of smart cards for patient identification in the U.S. market is affected by market environments that render their applicability questionable. For example, U.S. healthcare patients have a higher degree of sensitivity to personal information being stored on any credentialing document due to fears about the information being lost, stolen, or shared with any third party. Since smart cards for patient identification in healthcare carry this type of sensitive information, they can be interpreted as a threat to privacy, potentially exposing the patient to theft and fraud based on illegal use of their personal information.

Smart cards used for patient identification also carry an inherent replacement cost if the cards are lost or stolen that is the patient's responsibility to pay. This characteristic of smart cards can be potentially unfavorable if a patient on a limited budget is required to order another card and is forced into doing so only because their healthcare provider requires the card to render care.

Then there is the issue of smart card longevity. Despite the fact that they are a viable short term alternative for patient identification in healthcare, market forces are dictating the use of smart phones as the future of personal credentialing and identification. As the market inches closer to making smart phones ubiquitous personal identification tools, eventually smart card applicability and relevance will precipitously decline. This would prove to be an unfortunate circumstance for any healthcare facility that invested in the technology only to see its usefulness dissipate.

The effective use of smart cards for patient identification in healthcare is largely dependent on the deployment environment. Take for example our work with smart cards in the country of Haiti to help monitor and track AIDS patients, ensuring medication adherence and accurate disease management. We embarked on this project through a strategic partnership with the Centers for Disease Control and Prevention (CDC), carefully studying environmental, demographic, and societal conditions that could negatively or positively affect the deployment and then made the decision that smart cards were the most viable option for patient identification based on:

- Low patient sensitivity to personal data (including a biometric profile) stored on the smart card
- Third party funding for the cost of the card absolving patients from the expense of producing and replacing the cards
- The absence of a need for hospital infrastructure to support the cards – all administrative and data processing are covered by third parties
- Our long history engineering biometric identification deployments based on human factor engineering and subsequent assessment that smart cards are not a viable alternative for long term patient identification

Market Factors Dictate Smart Card Applicability

The use of smart cards for patient identification in the U.S. market is affected by market externalities absent from third world environments that render their applicability questionable. For example, U.S. healthcare patients have a higher degree of sensitivity to personal information being stored on any credentialing document due to fears about the information being lost, stolen, or shared with any third party. Since smart cards for patient identification in healthcare carry this type of sensitive information, they can be interpreted as a threat to privacy, potentially exposing the patient to theft and fraud based on illegal use of their personal information.

Smart cards used for patient identification also carry an inherent replacement cost if the cards are lost or stolen that is the patient's responsibility to pay. This characteristic of smart cards can be potentially unfavorable if a patient on a limited budget is required to order another card and is forced into doing so only because their healthcare provider requires the card to render care.

Then there is the issue of smart card longevity. Despite the fact that they are a viable short term alternative for patient identification in healthcare, market forces are dictating the use of smart phones as the future of personal credentialing and identification. As the market inches closer to making smart phones ubiquitous personal identification tools, eventually smart card applicability and relevance will precipitously decline. This would prove to be an unfortunate circumstance for any healthcare facility that invested in the technology only to see its usefulness dissipate.

ARE BARCODED WRISTBANDS ABLE TO KEEP PACE WITH THE EVOLVING DYNAMICS OF PATIENT IDENTIFICATION?

A Staple Technology for Patient Identification

A “barcode” is defined an optical machine-readable representation of data relating to the object to which it is attached. Tracing their history back to the late 1960’s and first used commercially in the retail industry in 1974 on a pack of Wrigley chewing gum, barcodes first became a commercial success when they were used to automate supermarket checkout systems and have since become the de facto identification standard in the healthcare industry ranging from patient identification for fast access to patient data including medical history, drug allergies, etc. to medication management, playing a key role on streamlining everyday processes to keep patients safe and increase operational efficiencies.

For a long time, the use of barcodes for patient identification have been a driving force in reducing occasional human errors that can result in dangers to patient safety by allowing practitioners the ability to quickly scan a wrist bracelet for fast identity authentication. Despite their history of being a viable technology to better identify patients in healthcare settings, barcodes are slowly becoming antiquated, unable to keep pace with the natural evolution of patient access to healthcare services and the growing need for healthcare organizations to adopt more ubiquitous patient identification solutions that meet the demands of new patient touchpoints quickly materializing in the modern healthcare ecosystem.

Limitations and Challenges of Barcoding

Despite their long run as the most popular form of patient identification in healthcare, the limitations and challenges of using barcodes in modern healthcare systems presents significant and perhaps insurmountable obstacles to healthcare organizations that still rely on them. In reality, the shifting sands of patient identification in the healthcare industry have evolved to the point where not only are barcodes quickly becoming antiquated because if their inability to meet modern demands of patient touchpoint authentication but some say that their continued use can even be considered dangerous.

One of the core problems for barcoding systems is their inability to act as a comprehensive patient identity platform that covers a wide variety of settings including patient portals, smart devices, and kiosks – all relatively new patient touchpoints that have materialized over the past few years due to the rapid digitalization of the healthcare industry. Let's break down some of the key limitations of barcoding that relegates the technology as a staple patient identification platform:

- **Damaged barcodes** – Important to keep in mind that a barcode reader is only as good as the back end system that supports it. Damaged, smudged, tampered, wrinkled, dirty, or poorly printed barcodes can result in the inability to accurately identify a patient before care is rendered. In an emergency situation where fast, accurate patient identification may be needed, damaged barcodes could present a serious limitation.

- **Pricing** – Barcoding systems require not only a significant upfront investment in new equipment including scanners and printers, but they also require ongoing capital expenditures on system maintenance and repair.

- **Application Settings** – Barcodes only work when utilized in healthcare settings where patients are physically present. The rapid digitization of the healthcare industry has introduced a host of new patient touchpoints that require use of a patient identification technology that uses a combination of various human identity variables to ensure seamless authentication across any medium or touchpoint.

Barcoding is limited in that it doesn't have the capability to be applied across all systems that can now affect patient identification. Kiosks, patient portals, mobile devices are all examples of new touchpoints where barcodes can't be applied.

- **Fraud** – Barcoded wristbands are highly susceptible to being swapped, shared, stolen, or forged. Not to mention the human error that can play in if hospital staff simply misidentifies at patient during registration and issues them a wristband under another patient's name or electronic medical record. Relying on identification documentation that authenticates based on what you have sets a dangerous precedent because it perpetuates the possibility of fraud.

BIOMETRICS - THE MOST ADVANCED PATIENT IDENTITY MANAGEMENT SOLUTION

Increasing patient safety initiatives will always be a major focus in the healthcare industry. As the digital age ushers in and establishes new patient touchpoints and the need to share data across disparate healthcare providers to manage both individual and population health rises, there has long been a cry from the industry to implement stronger and more flexible patient recognition platforms. In the absence of a national patient identifier, any type of industry standards on patient demographic data capture or how data is collected, and continued public perception that they don't have to present identification when accessing healthcare, the time seems ripe for a technology such as biometrics to fill the void that exists to provide more modernized, accurate, advanced patient identification solutions.

Protecting patients from the dangers associated with misidentification across increasingly complex healthcare information landscapes has pushed the implementation of modernized identification and data integrity platforms to the forefront of priorities for the industry. Effective patient ID platforms such as biometrics have the ability to cover each and every touchpoint of internal healthcare information systems and can easily be customized to meet new demands that arise as we continue to see the market evolve. Biometrics has emerged as an advanced patient identity management solution easily capable of rising to the demand to establish more secure, accurate, and ubiquitous authentication and data integrity solutions.

The problem is, not all biometric patient identification solutions are built the same and can offer ubiquitous authentication at each and every patient touchpoint throughout the continuum of care or provide back end patient matching capabilities that truly prevent duplicate medical records and medical identity theft – two extremely egregious potential threats to patient safety and data integrity. The question then becomes - How can you tell if your investment in a biometric patient identification platform will ensure the flexibility and scalability to meet the demands of the modern healthcare ecosystem and support patient safety with a true de-duplication mechanism and medical identity theft protection? Next generation biometric patient identification platforms should contain the following characteristics:

BIOMETRICS - THE MOST ADVANCED PATIENT IDENEITY MANAGEMENT SOLUTION

1. **Reliability** –Traditional patient identification solutions typically rely on a patient presenting something they know (e.g – a date of birth or address) or something they have (e.g. – an insurance card or driver's license). The problem that arises is that these identification methods are highly susceptible to theft and fraud so they can no longer be considered a safe and secure way to identify patients. Biometrics offers a more secure alternative by instead identifying patients by their own physiological or behaviorial characteristics, or "what they are" which is nearly impossible to fake or forge and offers a much more reliable way to identify patients.
2. **Flexibility** – A biometric patient identification solution should support the use of multiple modalities and devices (i.e. – fingerprint, finger vein, palm vein, iris, facial recognition) to ensure that a healthcare facility is never locked into a single modality or device and can always leverage the best biometric technologies as they continue to evolve. Biometrics has the ability to quickly adapt to rapidly changing environments and continually meet existing and new demands of patient authentication if you are careful to select a solution that is built to be flexible and adaptable to the rapidly shifting healthcare landscape.
3. **Longevity ("future proof")** – Healthcare facilities should not only seek to invest in technologies that will address their patient identification needs in the present, but have the ability to easily be adaptable to new scenarios that arise in the future. An investment in biometrics addresses not only the intricacies of patient identification that currently exist, but helps to "future proof" the investment by providing the flexibility to be used in any context, to maximize return on investment.
4. **Scalability** – As we move rapidly into the world of electronic health records, the ability to easily share healthcare information across a health information exchange (HIE) or Integrated Delivery Network (IDN) enables providers to enable safer and timelier care. A properly configured biometric patient identification system can easily scale for use across an HIE or IDN, ensuring clean records regardless of compliance issues or data entry errors. The ability to quickly and seamlessly scale up a patient identification solution helps to create and maintain the highest possible levels of data integrity.

BIOMETRICS - THE MOST ADVANCED PATIENT IDENTITY MANAGEMENT SOLUTION

5. **One-to-many Identification** – Investment in a biometric patient identification solution requires that the system perform one-to-many (1:N) identification which compares the captured biometric template against all stored templates. No other information or credentialing (for example, asking for a DOB before scanning a biometric credential) is required besides the biometric scan. This biometric matching type answers the question, “who are you?” 1:N matching is a true de-duplication mechanism and the only way to prevent duplicate medical records and improve patient data integrity.
6. **Mobile** – The dynamic nature of patient identification for a variety of healthcare settings necessitates a flexible biometric patient authentication solution that can be utilized with a mobile device within the clinical setting and offers real-time, accurate results. Healthcare providers need that flexibility to instantly identify a patient at bedside or at any point along the care continuum to ensure the right care is administered to the right patient.

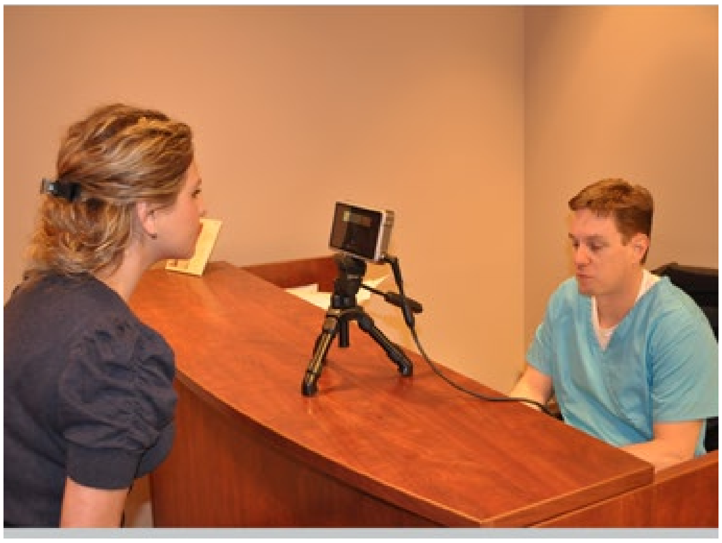
Biometric patient identification solutions must be able to provide the utility to verify a patient’s identity bedside, in home health, ER, and other mobile environments including patient self-driven interactions (e.g. – using facial and/or voice recognition for patient portal access or authentication over the phone). Investing in a biometric patient identification platform that covers these points is the only way to retain high levels of data integrity as the increase in mediums to access and deliver care has become more complex requiring comprehensive identity platforms that expand across each and every patient touchpoint. Any viable biometric patient identification solution should provide the unique ability to provide an integrated, secure patient identification platform across a multitude of patient touchpoints that respects privacy and helps comply with HIPAA guidelines to ensure the safe transmission and collection of health data.

BIOMETRICS IS THE MOST ADVANCED PATIENT IDENTITY MANAGEMENT SOLUTION

Patient safety will always be the end goal

At the core of any patient identification strategy is the need to protect patients from the harm that could result through misidentification. The dangers of duplicate medical records, overlays, and medical ID theft place patients at risk and are a key motivation for healthcare facilities to adopt more stringent patient ID protocols to increase safety.

As the digital age ushers in new technology (mobile and patient portals for example) that threaten to derail otherwise aggressive and successful patient safety policies and disrupt data integrity, it is critical that the healthcare industry implements patient identification solutions that will help to maintain a symbiotic relationship between adopting new tools to access and receive care, and preserving safety protocols. A biometric patient identification solution should provide the modern technology needed to meet the new demands to protect patients at each and every step of their care.



Industry Experience is Essential to Deploy Effective Solutions

Active in the biometrics industry for over a decade, our experience ranges from large to small scale deployments with millions of end users and thousands of deployments all over the world. Our unique use of human factor engineering which is:

"closely studying the intersection of people, technology, policy, and work across multiple domains using an interdisciplinary approach that draws from cognitive psychology, organizational psychology, human performance, industrial engineering, and economic theory to design and implement biometric systems that are acceptable and successful in a commercial environment."

This concept helps position us as an experienced biometrics identity management firm empowered with the knowledge and experience to determine which applications of patient identification technology will be most effective based on market environments. It is our opinion that although smart cards and barcoding play an important role in the identification industry, their use in healthcare is hampered by several factors that characterize them as impractical.

RightPatient®

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

1.770.393.0986
sales@rightpatient.com
www.Rightpatient.com

@rightpatient
M2SYS
RightPatient