Improving patient care with positive patient identification
Patient identification errors jeopardize patient safety, impede patient engagement, and result in serious financial inefficiencies for healthcare providers.

Efficient, quality care starts with positive patient identification

Healthcare can only be effective if the right care is provided to the right patient, using the right patient information. Unfortunately, many healthcare organizations are saddled with cumbersome, manual patient identification processes. These front-end processes all too often result in patient identification errors that propagate throughout the entire care continuum. Patient identification errors jeopardize patient safety, impede patient engagement, and result in serious financial inefficiencies for healthcare providers. That's why improving patient identification is The Joint Commission's #1 National Patient Safety Goal for hospitals.

Ineffective processes create patient identification problems; effective technologies can, and should, address these problems

According to The ONC’s Patient Identification and Matching Final Report from 2014, patient identification errors are an inevitable by-product of healthcare's increasingly complicated technology environment. To address patient identification problems, healthcare organizations need to find effective technological solutions that do not add to the burden and complexity of their current IT environment – instead, they should simplify and optimize existing clinical and administrative workflow processes.

Patient identification errors exist because most healthcare organizations have yet to find an effective way to uniquely identify each patient at the point of care. However, some leading healthcare organizations are deploying positive patient identification solutions that use innovative biometric technologies such as palm vein biometrics to accurately and securely identify each patient and create a 1:1 match with their digital health record. Ideally, these systems seamlessly integrate with providers’ existing patient record databases.

Positive patient identification solutions can help healthcare organizations significantly reduce patient identification errors and achieve:

- Improved patient safety
- Decreased opportunities for patient identity theft and insurance fraud
- Increased revenue cycle efficiency
- Enhanced patient experience and satisfaction

This whitepaper examines how patient identification errors are created today, and offers suggestions and examples of how to avoid patient identification errors in the future. Additionally, it makes the case for deploying a positive patient identification solution and provides a checklist for choosing a positive patient identification solution that meets healthcare organizations’ needs.

---

**Patient Identification errors: an overview**

Patient identification processes that rely on photo ids, oral demographic data, and other personal information, such as Social Security Numbers, can be prone to transcription mistakes and record matching problems that cause the following patient identification errors:

**Duplicate medical records**

Duplicate medical records occur when a single patient is associated with more than one medical record. Oftentimes, duplicate medical records are partial duplicates that only capture a portion of a patient’s medical history.

**Overlays**

Overlays occur when one patient’s record is overwritten with data from another patient’s record, creating a combined, inaccurate record.

**Not all errors are mistakes**

Most of the time, patient identification errors are accidental mistakes caused by simple oral identification and transcription errors or database complexities. However, an increasingly high proportion of patient identification errors are deliberate. Identity thieves can easily take advantage of healthcare facilities’ current patient identification processes by supplying other peoples’ photo IDs, demographic data, or personal information — all of which can be easily stolen. Similarly, insurance card fraud can be deliberate, if patients’ intentionally share their insurance information with others, or accidental, if patients’ insurance information is stolen. This kind of accidental and intentional abuse of the patient identification system directly contributes to a systemic medical identity theft and insurance fraud industry that undermines the quality and integrity of healthcare services. An estimated 2.3 million individuals were impacted by medical identity theft in 2014, an increase of 21.7% from 2013. Unlike credit card fraud, victims of medical identity theft can suffer serious financial consequences. The average out-of-pocket cost of a single identity theft incident is $13,450. Based on this statistic, medical identity theft is estimated to cost the healthcare industry over 30 billion dollars a year.

Patient identification errors caused by identity theft, insurance fraud, duplicate medical records, and overlays can contribute to a number of problems, including:

**Ineffective patient care**

Patient identification errors seriously jeopardize patient safety. Studies show that 7-10% of patients are misidentified during medical record searches and that 6% of identification errors result in an adverse event. That means that 60 out of every 10,000 medical record searches results in a medical error

---

5. Fifth Annual Study on Medical Identity Theft, Ponemon, 2014
6. Ibid.
causing an adverse event. Preventable medical errors have been estimated to cause 440,000 patient deaths in the United States each year. This statistic makes preventable medical errors the third most common cause of death in the United States.

Duplicate medical records and overlays cause patients to be treated based on incomplete or inaccurate knowledge about their medical history or profile, resulting in potentially serious medical errors and complications. A duplicate medical record or overlay may not include the correct information about a patient’s blood type, allergies, or their diagnostic, medication, or family histories – all of which are critical for effective, safe treatment.

**Financial inefficiency and legal liability**

Correcting patient identification errors requires costly and time-consuming data-cleansing processes. The medical identity theft resolution process takes over 200 hours to complete, on average. Industry experts report that the average estimated costs associated with duplicate medical records can be as much as $1,000 per record and $95 in labor costs alone just to correct a single duplicate record. Duplicate medical records and overlays can also undermine the substantial investments hospitals make to support their EMR, EMPI, ADT, and HIS solutions by negatively impacting the ROI benefits these solutions offer.

The problems caused by patient identification errors, medical identity theft, and insurance fraud can also lead to costly insurance claw backs, damaging malpractice lawsuits, and can potentially harm hospitals’ Meaningful Use targets and HCAHPS scores, which can, in turn, negatively affect hospitals’ funding.

**Patient dissatisfaction and increased cost of care**

Patient identification errors can also result in unnecessary repeated tests, slower wait times, and incorrect or ambiguous diagnostic information. Duplicate medical records can also negatively impact communications between healthcare providers and their patients: duplicate medical records are associated with a higher risk of missing important laboratory results and a higher likelihood that patients are subjected to unnecessary testing. These issues can not only increase the cost of care, but weaken staff morale and negatively impact the public perception of a hospital, especially if the hospital receives low HCAHPS ratings based on negative patient experiences.

---

How patient identification errors are created today

Patient identification errors are a by-product of complex interactions between healthcare organizations’ patient registration, check-in, and digital healthcare information systems. These interconnected systems suffer from human, algorithmic, and technological weaknesses that combine to create the perfect conditions for patient identification problems.

The following statistics from the Harris County Hospital District in Texas illustrate the prevalence of shared patient data, and the complexities of finding unique identifiers for patients with similar demographic data:ⁿ¹³

- Number of patients in Harris County Hospital District's database: 3,428,925
- Number of times when two or more patients share the same last and first names: 249,213
- Number of times when five or more patients share the same last and first names: 76,354
- Number of times when two or more patients share the same last and first names, and date of birth: 69,807
- Number of patients named Maria Garcia: 2,488
- Number of patients named Maria Garcia sharing the same date of birth: 231

Similar demographic clusters and naming conventions occur in patient populations throughout the United States. For example, it is very common for fathers and sons in many cultures to share the same name, address, and other demographic information.

Human error

Many hospitals still use paper or oral registration processes that require patients to share their personal information with hospital registration staff. When a patient provides their personal information, hospital staff members enter the patient's information into a digital system in order to match the patient's information with their unique EMR. Small typos that cause date of birth or Social Security Number (SSN) errors, misspelled names, or mistyped addresses can match patients with the wrong medical records. A study conducted at Johns Hopkins Hospital revealed that 92 percent of the errors resulting in duplicate medical records were caused by inpatient registration mistakes.ⁿ¹⁴ These mistakes can be as simple as using a female patient's maiden name instead of her married name, or using other inconsistent

---

According to the AHIMA, roughly 40% of duplicate medical records have discrepancies caused by inconsistent records of patients’ first and last names naming or titling conventions. For example, a single patient could be accurately recorded as Maria Garcia, Maria L. Garcia, María de López García, and Maria Garcia Williams. Though technically accurate, these kinds of naming inconsistencies wreak havoc with healthcare organizations’ algorithmic processes for identifying patients. According to the AHIMA, roughly 40% of duplicate medical records have discrepancies caused by inconsistent records of patients’ first and last names.  

**Algorithmic error**

Enterprise master patient index (EMPI) systems are designed to maintain consistent patient records by using deterministic algorithms for patient identification purposes. Deterministic algorithms use a combination of demographic variables such as name, age, date of birth, gender, and Social Security Number, to attempt to identify patients. This type of matching method only works effectively if the variables are an exact match to a patient’s record. Small human typing errors can completely invalidate the efficacy of deterministic algorithms, thus compounding the negative effects of small patient registration errors introduced during in-patient check in processes. EMPI’s deterministic demographic matching processes are also particularly ineffective when patient populations share similar demographic characteristics, which is often the case for local hospital populations.

**Technological error**

Patient registration and check in processes often involve complex interactions with a suite of different healthcare technology systems. These technologies can include EMR, EMPI, ADT, and other HIS solutions. Oftentimes, these different systems do not integrate well together, and do not accurately match patients with their correct medical records across various record-keeping platforms. Interoperability problems with interconnected technological networks are particularly problematic for organizations with large patient databases and health networks, such as Integrated Delivery Networks (IDNs) and Health Information Exchanges (HIEs). Large networks experience more complicated interoperability problems than smaller networks, making it even more difficult for them to maintain Master Patient Index (MPI) integrity across their multiple interconnecting IT systems. The statistical likelihood of false positive and false negative matches also increases exponentially in larger patient information datasets.

---

How patient identification errors can be avoided in the future

Patient identification errors can only be avoided in the future by addressing the root causes of the human, algorithmic, and technological errors that contribute to patient identification errors today. The ONC’s 2014 Patient Identification and Matching Final Report identified emerging technologies (such as advanced biometric systems) as promising solutions to patient matching problems.¹⁶ According to their report, a number of key stakeholders in hospitals have identified biometric solutions as promising because they have the potential to reduce healthcare organizations’ reliance on demographic matching algorithms.

Innovative biometric patient identification technology can effectively address the human error and algorithmic error problems that oral and paper patient identification processes create. Biometric identification technology such as palm vein biometrics are more accurate than in-person identification processes; they minimize the potential for human errors caused by typos and transcription errors, and they reduce the statistical error rates of algorithms by providing more unique identifying factors than demographic data.¹⁷ Biometric technologies can also prove particularly useful in minimizing the risks of identity theft and related medical insurance fraud claims.¹⁸

Positive Patient Identification must be easy for providers to use and for patients to adopt

In order to address patient identification errors effectively, biometric technologies have to do more than simply identify patients accurately. They need to provide extremely high levels of interoperability, patient acceptance, and usability. Technologies such as palm vein biometric identification are widely used with proven adoption of over 95% by patients. Well designed patient identification technologies integrate directly with healthcare organizations’ existing digital record systems and automatically create a 1:1 match between individual patients and their unique medical records.

¹⁷. See Biometrics in Identity Management: Concepts to Applications, Shimon K. Modi
An effective positive patient identification solution will improve patient safety, patient engagement, and revenue cycle efficiency.

**Positive patient identification solution checklist:**
An effective positive patient identification solution will reduce patient identification errors by:

- **Minimizing the opportunity for human error** by providing a robust biometric alternative to paper and oral patient identification processes.
- **Minimizing the likelihood of algorithmic error** by using a strong, unique patient identification method.
- **Optimizing interoperability** by integrating directly with healthcare organizations’ existing technological systems and creating a 1:1 match between individual patients and their unique medical records.
- **Maximizing patient adoption and ease of use** by providing intuitive, non-intrusive design, easy IT management, and a pleasant patient experience.

By meeting these four conditions, an effective positive patient identification solution will improve patient safety, patient engagement, and revenue cycle efficiency.

**Why choose palm vein recognition technology?**
Palm vein biometric recognition technology is the most widely used positive patient identification technology because it is one of the safest, most accurate patient identification methods. Each patient’s palm vein pattern is unique and stable over their lifetime, making palm vein recognition technology an ideal method for accurately identifying patients across a wide range of demographics. Palm vein recognition technology pairs a biometric scanner with advanced patient matching software. A biometric scanner uses a near-infrared light wave (the same kind of light waves used by television remote controls) to capture the vein pattern in a patient’s palm. This scan produces a unique biometric template that is a digital representation of the patient’s unique vein pattern. During the initial enrolment process, the palm vein recognition technology solution associates this unique biometric template with the patient’s medical record in their healthcare provider’s EMR. Once enrolled, returning patients simply provide their date of birth and scan their palm. Palm vein recognition has a high acceptance rate among patients because it is non-intrusive, stigma-free, and user-friendly.
Introducing the Imprivata Positive Patient Identification Platform

Imprivata PatientSecure™ is a positive patient identification solution that uses palm vein biometric technology to accurately and securely identify patients and retrieve their digital health records across multiple clinical systems at any entry point of care. Imprivata PatientSecure creates a 1:1 match between patients’ unique palm vein scans and their individual medical records and integrates directly with existing EMR, EMPI, HIS, and ADT systems.

How Imprivata PatientSecure works

1. Biometric enrollment creates a 1:1 link to MRNs from multiple clinical systems
2. Securely and accurately identifies patients at any point of care directly from the registration screen
3. Retrieves the correct record from appropriate clinical systems

Imprivata PatientSecure palm vein recognition technology offers a powerful, user-friendly solution to hospitals’ patient identification problems. Each patient’s palm vein pattern is unique and stable over their lifetime, making palm vein recognition technology an ideal method for accurately identifying patients across a wide range of demographics. Palm vein identification also has a high patient success and adoption rate. Patients appreciate the non-intrusive palm scanning process that does not require them to share their SSN or other sensitive information with hospital staff.

Imprivata PatientSecure is the leading palm vein recognition solution in the healthcare industry and is currently being used to identify over 7 million patients across the United States. To learn more about why Imprivata PatientSecure is the positive patient identification of choice for over 350 hospitals, please visit www.imprivata.com/patientsecure.
About Imprivata

Imprivata (NYSE: IMPR), the healthcare IT security company, is a leading provider of authentication, access management, secure communications, and patient identification solutions for the healthcare industry. Imprivata products address compliance and security challenges while improving provider productivity and the patient experience.

For further information please contact us at:
1 781 674 2700
or visit us online at
www.imprivata.com

Offices in:
Lexington, MA USA
San Francisco, CA USA
Santa Cruz, CA USA
Tampa, FL USA
Uxbridge, UK
Paris, France
Nuremberg, Germany