Healthcare is suffering from a patient identity crisis. Here's how we can cure it:

10% of patients are misidentified when their electronic health record is accessed. The most effective healthcare interventions don't treat symptoms, they treat causes. Patient identification errors are often caused by outdated patient lookup procedures during the registration processes that can be revolutionized to dramatically improve revenue cycle efficiency and patient safety.

Every hospital wants to improve the health of their patients and the health of their business. By improving your patient identification process, you can significantly improve patient safety, revive your revenue cycle efficiency, and increase your market share. Here's how you can identify, treat, and cure your patient identification crisis to improve the health of your hospital and increase the quality of care you provide:

Diagnosis
Patient Identity Crisis.

Prognosis
Left untreated, your patient identification crisis jeopardizes patient safety, negatively impacts revenue cycle efficiency, and reduces your profit margin and market share.

Risk factors
Your hospital uses an outdated oral or paper-based patient identification process that requires patients to share personal information, such as Social Security Numbers, with registrar staff during their visits.

Cause
Your patient identity crisis is caused by patient identification errors introduced at your registration desk. A study conducted at Johns Hopkins Hospital revealed that 92% of the patient identification errors resulting in duplicate health records were caused by inpatient registration mistakes.[1] These mistakes can be as simple as using a female patient's maiden name instead of her married name, or using other inconsistent naming conventions. According to the AHIMA, roughly 40% of duplicate health records have discrepancies caused by inconsistent records of patients' first and last names.[2] Identity fraud can also be traced back to fraudulent identity cards and shared insurance cares presented at the registrar desk.

1. Bittle MJ, Charache P, Wassilchalk DM. Registration-associated patient misidentification in an academic medical center: causes and corrections. Joint Commission Journal on Quality and Patient Safety/Joint Commission Resources. 2007;33:25–33

2. Technology Influence on Data Integrity & Impact on Patient Safety, Privacy & Security. AHIMA Convention Proceedings, September 2008

Due to the human error and insurance fraud risk inherent in manual patient identification registration processes, patients can be matched with the wrong records, or cannot be found within a hospital's database, causing overlays and requiring registration staff to create duplicate patient records. Such mismatched and duplicate health records provide incomplete and inaccurate medical histories that negatively impact revenue cycle efficiency, causing downstream effects of insurance denials and take backs. But, more importantly, patient identification mistakes jeopardize patient safety, significantly increasing the likelihood of medical errors and adverse events.

Prevalence

- Improving the accuracy of patient identification is The Joint Commission's #1 National Patient Safety Goal for hospitals.[3]

- Studies show that 10% of patients are misidentified during health record searches and that 9% of identification errors result in an adverse event.[4]

- The AHIMA reports that the average duplicate health record rate is between 8-12%.[5] And roughly 40% of all records have blank or default values in one of the key data fields of first name, last name, date of birth, gender, or Social Security Number.[6]

- The Advisory Board reports that the average 250-bed hospital lost more than $7M in 2013 because of inaccurate and incomplete documentation.[7]

- An estimated 2.3 million individuals were impacted by medical identity theft in 2014, an increase of 21.7% from 2013.[8] 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.[9] Based on this statistic, medical identity theft is estimated to cost the healthcare industry over $30 billion a year.

A study conducted at Johns Hopkins Hospital revealed that 92% of the patient identification errors resulting in duplicate health records were caused by inpatient registration mistakes.

3. Hospital National Patient Safety Goals 2016, The Joint Commission, 2016 http://www.jointcommission.org/assets/1/6/2016_NPSG_HAP.pdf

4. https://www.ecri.org/press/Pages/Patient-Identification-Errors.aspx

5. AHIMA MPI Task Force. "Building an Enterprise Master Person Index."Journal of AHIMA 75, no. 1 (Jan. 2004): 56A–D

6. Technology Influence on Data Integrity & Impact on Patient Safety, Privacy & Security. AHIMA Convention Proceedings, September 2008.

7. https://www.advisory.com/research/financial-leadership-council/multimedia/interactive/eight-ways-to-protect-your-margins

8. Fifth Annual Study on Medical Identity Theft, Ponemon, 2014

9. Ibid.

Patient identification errors undermine the efficacy of your substantial EHR and other MPI investments, which rely on accurate, clean data to treat patients effectively.

Symptoms

- **Medical errors:** patient safety is seriously jeopardized by patient identification errors. Patients who are inaccurately identified are treated on the basis of incomplete and inaccurate information, which exponentially increases the risk of serious patient harm, medical malpractice, and negative press coverage that impacts your organization's reputation. Preventable medical errors have been estimated to cause 440,000 patient deaths in the United States each year.[10] This statistic makes preventable medical errors the third most common cause of death in the United States.

- **Insurance denials:** insurance companies often catch patient identification errors after treatment, denying claims that are inadvertently submitted to the wrong insurance company, or purposely submitted fraudulently by patients who take advantage of the loopholes in traditional patient identification systems. Re-matching patients with the right insurance information after their visit elongates the revenue cycle. An elongated revenue cycle can ultimately reduce payments and negatively impact your bottom line.

- **Unrealized return on your EHR investment:** patient identification errors undermine the efficacy of your substantial EHR and other MPI investments, which rely on accurate, clean data to treat patients effectively. Without complete patient data integrity, these costly systems fail to provide the substantial treatment and safety benefits they promise.

- **Costly data cleansing processes:** cleansing master patient indexes for partial, duplicate, or overlapping health records is a costly and time-consuming endeavor that only treats the symptom of patient identification problems, not its root cause. Industry experts report that the average estimated costs associated with duplicate health records can be as much as $1,000 per record and $95 in labor costs alone just to correct a single duplicate record.[11]

10. A New Evidence-based Estimate of Patient Harms, "http://journals.lww.com/journalpatientsafety/Fulltext/2013/09000/A_New,_Evidence_based_ Estimate_of_Patient_Harms.2.aspx

11. Patient Safety and Risk to Rising Healthcare Costs Panel, HIMSS Conference, February 2014, Nancy Farrington, CHAM, MBA EMPI Administrator, Main Line Health System Robert Tennant, MA Sr. Policy Advisor, Medical Group Management Association Robert Halder, MD Retired, Rear Admiral USN; Executive Medical Consultant, LifeMed ID.

Treatment

Given the statistics, your hospital is almost certainly suffering from a patient identity crisis. To treat your patient identity crisis effectively, you have to intervene at the source of your patient identification errors: the patient registration process. Data cleansing measures only treat the symptoms of your patient identification problem, but the most effective healthcare interventions don't treat symptoms, they treat causes.

Legacy patient identification processes rely on probabilistic data-matching techniques that can be completely invalidated by a simple spelling mistake. The ONC's 2014 Patient Identification and Matching Final Report identified emerging technologies as promising solutions to patient matching problems.[12] Advanced biometric identification technologies provide a robust solution to patient identification problems. Biometric identification technologies 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.[13] Biometric technologies can also prove particularly useful in minimizing the risks of identity theft and related medical insurance fraud claims.[14]

In order to adequately treat and cure your patient identification problems an advanced biometric solution needs to:

✔ Minimize the opportunity for human error by providing a robust biometric alternative to paper and oral patient identification processes

✔ Ensure a 1:1 match between individual patients and their health records

✔ Minimize the likelihood of algorithmic error by using a strong, unique patient identification method

✔ Optimize interoperability and IT management by integrating directly with all major EHR, EMPI, HIS, and ADT systems

✔ Maximize patient adoption and ease of use by providing intuitive, non-intrusive design, and a pleasant patient experience

Data cleansing measures only treat the symptoms of your patient identification problem, but the most effective healthcare interventions don't treat symptoms, they treat causes.

12. Office of the National Coordinator, Patient Identification and Matching Final Report, 2014, http://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf

13. See Biometrics in Identity Management: Concepts to Applications, Shimon K. Modi

14. Biometric Technology Stomps Identity Theft, SANs Institute, http://www.sans.org/reading-room/whitepapers/authentication/biometric-technologystomps-identity-theft-126

Healthcare is suffering from a patient identity crisis. Here's how we can cure it:

Imprivata PatientSecure: The cure for your patient identity crisis

Imprivata PatientSecure is the leading positive patient identification solution for healthcare that improves patient safety and financial outcomes through biometric identification, medical record clean-up, improved patient matching, and workflow optimization. Imprivata PatientSecure pairs a patient's biometric with advanced patient matching software. This produces a unique biometric template that is a digital representation of the patient's unique biometric. During the initial Imprivata PatientSecure enrollment process, the solution associates this unique biometric template with the patient's health record in their healthcare provider's EHR. Once enrolled, returning patients simply provide their date of birth and have their biometric scanned.

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:

- **Minimizes the opportunity for human error** by providing a robust biometric alternative to paper and oral patient identification processes. Biometric solutions are a safe and accurate way to identify patients, streamline workflows, and eliminate human errors that result from traditional patient identification solutions.

- **Ensures a 1:1 match between patients' unique biometric and their individual health records** and integrates directly with existing EHR, EMPI, HIS, and ADT systems.

- **Minimizes the likelihood of algorithmic error** by using a strong, unique patient identification method, each patient's biometric is unique and stable over their lifetime, making recognition technology an ideal method for accurately identifying patients across a wide range of demographics

- **Optimizes interoperability and IT management** by integrating directly with existing EHR, EMPI, HIS, and ADT systems

- **Maximizes patient adoption and ease of use** by providing intuitive, non-intrusive design, and a pleasant patient experience. Imprivata PatientSecure has a high acceptance rate among patients because it is non-intrusive, stigma-free, and user-friendly.

Statistically, you're suffering from a patient identity crisis. Costly data cleansing processes only treat the symptoms of the crisis. Biometrics treat, and cure, the root cause of your patient identity crisis cause by replacing traditional oral and paper registration processes with a robust biometric alternative. To improve your patients' safety, increase your revenue cycle efficiency, streamline your registration process, and cure your patient identity crisis at its source, request a demo of Imprivata PatientSecure today.

Biometrics treat, and cure, the root cause of your patient identity crisis cause by replacing traditional oral and paper registration processes with a robust biometric alternative.

About Imprivata

Imprivata, the healthcare IT security company, enables healthcare globally to access, communicate, and transact patient information, securely and conveniently. The Imprivata platform addresses critical compliance and security challenges while improving 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
Uxbridge, UK
Melbourne, Australia
Nuremberg, Germany
The Hague, Netherlands

PS-WP-Patient-ID-Crisis-0717