Show Me Some ID: Tips for Trusting Identity in the Era of Cybercrime and Fraud

Save to myBoK

By Mary Butler

Meet Maria, a fictional emergency department (ED) registration clerk who's been on the job at a big city trauma center for six months. When Maria starts her shift she gets an alert that the patient photo verification system for the ED's registration software—which connects to the ED's electronic health record (EHR)—was down for the day with a patch in the works. Maria doesn't sweat it since the photo feature went live only three months ago. She knows she can register patients without it for the night.

The first patient to come in on Maria's shift is a young woman presenting with lower abdominal pain which she believes is caused by a kidney stone. The woman has an insurance card that matches the name and address she gave, but she doesn't have a photo ID. Maria prints out a wristband, asks the patient to confirm the demographic information on it, and directs her to the waiting area.

A couple hours later a retired nurse in her 50s named Stephanie Baker comes in complaining of shortness of breath with pain in her arms—and a warning she may be having early heart attack symptoms. Rushing to get Baker help, Maria in her haste doesn't realize she chose the wrong Stephanie Baker (there are three in the hospital's database). Incidentally, Baker's latex allergy and history of adverse reactions to certain painkillers are not noted in the profile Maria clicked on.

The last patient Maria checks in is an infant with panicked parents. The baby had been born in the same hospital, but the parents decided on the child's middle name a week after the delivery. Seeing several records with the child's same first and last name, Maria opts to create a new record to be safe.

Later in the week Maria's supervisor tells her that she needs to be retrained. The kidney stone patient had used a stolen insurance card, likely to acquire prescription narcotics. The hospital would not be reimbursed for that encounter since it was fraudulent. Baker, the retired nurse, helped ED staff realize she had been registered improperly when she told her nurse about a latex allergy. This kind of error is known as an "overlay." Finally, the hospital's health information management (HIM) department identified the duplicate record Maria made for the infant she checked in.

As the volume of health data continues to balloon in coming years, HIM professionals will be charged with managing greater volumes of patient records and must ensure that each patient is properly identified and matched to his or her specific health information.

Fortunately, there are tools and best practices available to help every provider type. AHIMA has been partnering with standards development organizations, including Integrating the Healthcare Enterprise, to develop standardized ways of exchanging patient identification elements across organizations and health information exchanges (HIEs). AHIMA has also developed patient ID toolkits and Practice Briefs to meet the growing need for best practices.

The Office of the National Coordinator for Health IT (ONC) has also acted, mandated by the 21st Century Cures Act, to help protect patient health information. Finally, biometric technologies such as palm vein scanners, photographs, and retinal scans comprise some of the high-tech identification methods that are helping reduce human error.

High Costs of Patient Matching Errors

The misidentification of patients in clinical settings has untold financial impacts for an organization in uncompensated care as well as serious patient safety consequences, such as wrong-side surgeries and even death.

A Ponemon Institute survey, the “2016 National Patient Misidentification Report,” found that 86 percent of respondents say they have witnessed or know of a medical error that was the result of patient misidentification.[1] Additionally, difficulty finding charts or medical records and sorting through duplicates can contribute to errors, according to the survey respondents.

“On average respondents say that 35 percent of all denied claims result directly from inaccurate patient identification or inaccurate/incomplete patient information, costing the average healthcare facility $1.2 million per year,” according to the Ponemon survey, which questioned 503 nurses, physicians, and health IT practitioners in a range of facility types across the United States.

A 2008 RAND Corporation study found that missing information can lead to inefficiencies such as the cost of reordering diagnostic tests and delays and errors in treatment.[2] Such inefficiencies have been estimated to cost the healthcare system $8 billion annually. Duplicate records and the problems resulting from their creation can cost healthcare organizations as much as $96 per record, according to a Healthcare Financial Management Association article.[3]

“Fixing overlays and duplicates continues to be challenging,” says Beth Liette, MS, RHIA, senior director of HIM at Cincinnati Children’s Hospital Medical Center. “Fixing the cases can be pretty routine and take minutes or can take all day to sort out. The number of downstream systems that have to be touched has an impact upon the time involved. Overlays are much more time-intensive and if not caught before bills go out of the organization, they can be very challenging to correct. Once the incorrect data lands in the third party payer’s database, it can take persistence to get the data corrected.”

Jami Woebkenberg, RHIA, CPHI, MHIM, director of HIMS at Banner Health, says that for the most part facilities are getting better at properly identifying and matching patients thanks to new biometric identification methods and electronic master patient index software. But there is room for improvement, Woebkenberg notes, especially when identifying patients at the start of an encounter.

“For instance, my personal experience has been that when a patient has a visit at a provider’s office, the patient is asked each time for his/her identification and insurance card, if applicable,” Woebkenberg says. “While the name and personal information may be requested for matching in the hospital setting, a copy of the patient’s identification (state-issued ID) may not be provided—it could be the patient’s name and date of birth, Social Security number, or other information that could have been obtained by an individual who is not the person actually presenting for care. This can cause issues with medical identity theft, duplicate patients, overlays, all of which can also lead to patient safety and care issues.”

Individuals working as registrars typically are not HIM professionals, and, according to an ONC report, the average length of employment for a registrar is four months.[4] As a result, they often don’t receive adequate training after their initial introduction.

Liette says any facility that’s investigating duplicates and overlays should do a determination of the root causes of the error.

“Categories of root causes include, but are not limited to: human error, hardware and software design, internal forces such as vague or confusing policies/procedures, human/computer interface, and external forces such as the patient/parent or outside healthcare providers,” Liette says. “Investing in training, sharing audit results with affected staff, and ensuring that policies and procedures are clearly written and understood are several best practices to explore.”

Government’s Role in Patient Identification

The federal government, by way of ONC, was directed by the 21st Century Cures Act to work with federal partners including the National Institute of Standards and Technology (NIST) and the healthcare and health information technology (health IT) community to develop a “trusted framework” for interoperability. The Cures Act called for “a common method for authenticating trusted health information network participants; a common set of rules for trusted exchange,” and additional organizational and operational policies.

The resulting document, the draft “Trusted Exchange Framework and Common Agreement (TEFCA),” was released by ONC in January.[6] AHIMA submitted recommendations during the comment period, a number of which touched on the matter of standardizing patient identification.[7]

For example, in one section of the document about standardization titled “Patient Demographic Data For Matching” there’s a requirement (which AHIMA supports) to “help establish a floor in the exchange of certain data attributes and the standardizing of such data.”

AHIMA noted that it’s concerned “that the requirements may not be enough to accurately identify a patient and could result, particularly in the execution of a broadcast query, in multiple records being returned, thereby requiring a back-end reconciliation process. Compounding this problem is the fact that participants may have policies and procedures that vary in terms of how the data attributes are entered into the system to begin with. For example, differences may arise in data collection with respect to legal name versus nickname (i.e., Elizabeth Smith versus Betty Smith), hyphenated names or names with special characters, and/or differentiations in addresses (111 Crane Trail versus 111 Crane Trl).”

In additional comments, AHIMA directs ONC to look at recommendations set forth in “Health IT Safe Practices: Toolkit for the Safe Use of Health IT for Patient Identification,” a document developed by the Partnership for Health IT Patient Safety, a multi-stakeholder group that includes AHIMA.[8]

AHIMA and other patient safety advocates continue to urge Congress to reconsider legislation to permit federal discussions around implementing a unique patient identifier (UPI), aka a patient safety identifier. A UPI number, ideally, would be assigned to every American and would be used to help link an individual’s health information wherever they might go for care. UPIs have broad support from industry groups, HIM professionals, and health IT experts.

Legislators from both parties sent a letter to the Government Accountability Office (GAO) last fall urging the agency to study UPIs and other methods of increasing the accuracy of patient matching. The letter was signed by Sen. Elizabeth Warren (D-MA), Sen. Orrin Hatch (R-UT), Sen. Sheldon Whitehouse (D-RI), Sen. Tammy Baldwin (D-WI), and Sen. Bill Cassidy (R-LA).[9]

Although Congress still passed a bill in March with statutory language that prohibits the use of funds “to promulgate or adopt a final standard providing for… the assignment of a unique health identifier,” it does ask the Centers for Medicare and Medicaid Services (CMS) to study the issue. The bill contains report language that calls upon CMS to issue a report no less than 12 months after the date of enactment of the bill on the impact on care improvement, reduction in costs, estimated saved lives or reduction in errors, and improvements in patient safety if hospitals were required to use a patient matching system as a requirement for participation in the Medicare program.

Patient Identification Best Practices

Some of the most effective identification practices are simple and low-tech. Many facilities have full-time staff devoted to working on sorting out mismatches, with entire teams that work on master patient index (MPI) cleanup and data integrity. Two-factor authentication is still the best practice for verifying identity (i.e., name and date of birth) but isn’t always done or done right. Requiring a photo ID, such as a driver’s license or state identification card, is preferred in most cases but isn’t always available for populations such as children and seniors who don’t drive.

According to Grant Landsbach, RHIA, CHDA, MSHA, system manager for data governance and interoperability at SCL Health in Denver, CO, registrars should ideally use three or four factors or more for proper identification. Asking the patient to verbally state their name, address, and birthdate results in fewer errors than simply having them say “yes” or “no” to registrar-posed questions. Patients tend to be distracted when they register and have a tendency to automatically say “yes” to identifying statements made by the registrar. When possible, having a patient read for themselves and confirm the accuracy of the information printed on their wristband or on the computer screen is more effective, studies have shown, according to Landsbach.

SCL Health has recently added photo identification to its EHR and registration systems—a decision that has added a greater degree of certainty to matching patients. Like many other health systems, SCL Health considered palm vein scanners, thumb prints, and retinal scanners, but the cost of implementing any one of those technologies, building a database to store a separate data stream, and getting it to interface with existing software was too daunting. Plus, the patient photo capability already existed in SCL Health's EHR and the cost of mounting webcams at registration stations was miniscule compared to retinal and palm scanners.

Having the photo of a patient attached to their medical record solves a number of problems. Doctors and nurses will notice right away if the person they're treating doesn't look like the patient they're charting on; patients can be properly matched to their photos at the point of registration; and people knowingly committing medical ID fraud don't want their picture taken.

"Just the existence of the camera helps to limit fraud. Criminals don't want their photos in a database because they think police can get it. So it's a pretty strong deterrent because they don't know how we're going to use it," Landsbach says.

Of course, SCL Health has developed policies around patient photos. For example, they aren't used in emergent or behavioral health encounters that could escalate. And, to account for physical changes, office staff try to update each patient's photo once per year.

Another patient identification standby in healthcare is comparing patient signatures on consent forms. Landsbach says this method has fallen out of favor now that his organization has transitioned to electronic signature pads. Switching to electronic signatures has also saved HIM staff valuable time and resources spent on scanning and copying consent forms, Landsbach says.

Though comparing signatures hasn't disappeared as a practice. "Comparing signatures can be used as a screening tool when there already is a suspension or concern. The process is more difficult now since many of the consent authorizations are obtained by use of signature pads. If you have signed for a purchase using a signature pad, you have seen firsthand that your signature does not match your handwritten signature and [they] are often illegible," Liette says.

SCL Health has rolled out patient registration kiosks in one facility, set up very much like airport check-in terminals. The kiosks can take a person's photo, and use the photo on a person's ID or credit card to match it with other photos in a database. The kiosk also forces patients to authenticate their own demographic data and guide them through making a co-pay.

"It's so advanced that it can print out a copy of a patient's signed consent form. And if the patient forgets to pick up the paper, the machine is automatically set to shred it in two minutes," Landsbach says.

Ensuring Secure Release of Information

Registration isn't the only place where verifying a person's identity is paramount. The use of patient portals to help patients manage their own (or another's) care will only continue to grow and become a major responsibility of HIM departments.

"Facilities need to develop guidelines around enrollment for the portal including how and who proxy access may be granted to," Woebkenberg says. "For example, requiring the patient to electronically complete and sign an authorization form to request any additional records that may be needed and not included in the portal."

Pediatric facilities also have their own unique concerns. "HIM often assists with proactive auditing to determine [if] appropriate proxy access has been given to the parents. Legal guardianship might need to be reviewed to determine if the parent has parental rights to the medical record. Foster parents are usually not given access and proxy access is often given to the parent until the patient becomes a teenager (ages 12 and above) without the child consenting to the parental access," Liette says.

AHIMA's "Patient Portal Toolkit" recommends that access to the portal be "initiated during a patient visit or hospital stay, which allows the organization to establish its authentication process (verify user identity), ensure the patient has access to the training and other materials that can accentuate the use of the portal and explain how the portal can increase the patient's involvement in their care.[5]

Landsbach's organization is working with its EHR vendor and a commercial credit reporting and public records database to formalize how they authenticate patient portal users once they leave the care setting and start portal access.

"When they leave the hospital they'll get a packet that has an authentication code that's only good for a week or two because of the security risk. If they wait too long they'll have to call our technical center that will ask them a lot of questions based on public information records, such as ‘Have you ever driven a Suburu?’ or ‘Have you ever lived at this address?’ If the patient answers five questions correctly, it will let them into the portal,” Landsbach says.

Notes

1. Ponemon Institute. “2016 National Patient Misidentification Report.” December 2016. https://pages.imprivata.com/rs/imprivata/images/Ponemon-Report_121416.pdf.
2. RAND Corporation. “Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System.” 2008. www.rand.org/pubs/monographs/MG753.html.
3. Lusk, Katherine. “Duplicate Records Compromise EHR Investment.” Healthcare Financial Management Association. August 2009. www.justassociates.com/application/files/8014/9124/7591/HFM_August_2009_Children_Dallas_cost_of_duplicates.pdf.
4. AHIMA Work Group. “Best Practices for Patient Matching at Patient Registration.” *Journal of AHIMA* 87, no. 10 (October 2016): 74-81. http://bok.ahima.org/doc?oid=301906#.
5. AHIMA. “Patient Portal Toolkit.” October 2017. http://bok.ahima.org/PdfView?oid=301419.
6. Office of the National Coordinator for Health IT. “Draft Trusted Exchange Network.” January 5, 2018. www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf.
7. AHIMA. “AHIMA Comments on ONC Drafted Trusted Exchange Framework to Dr. Donald Rucker, National Coordinator, ONC.” February 20, 2018. http://bok.ahima.org/PdfView?oid=302447.
8. Partnership for Health IT Patient Safety. “Health IT Safe Practices: Toolkit for the Safe Use of Health IT.” February 2017. www.ecri.org/Resources/HIT/Patient%20ID/Patient_Identification_Toolkit_final.pdf.
9. United States Senate group. “Letter to Gene L. Dodaro, Comptroller General, US Government Accountability Office.” October 3, 2017. www.warren.senate.gov/files/documents/2017_10_03_GAO_Patient_Matching_Letter.pdf.

Mary Butler (mary.butler@ahima.org) is associate editor at the *Journal of AHIMA.*

Article citation:
Butler, Mary. "Show Me Some ID: Tips for Trusting Identity in the Era of Cybercrime and Fraud." *Journal of AHIMA* 89, no.6 (June 2018): 24-27.