Strategies for improving patient identification and patient record integrity

Ensuring the highest possible accuracy of patient identification seems so obvious an imperative that healthcare organizations can probably afford to put more emphasis on other areas. But patient misidentification has long been, and still remains, a challenging and highly problematic issue for healthcare IT professionals, clinicians, and administrators.

In fact, a recent webinar — sponsored by Imprivata — pointed out a raft of problems related to patient identity and the financial, legal, and operational implications of those challenges. For instance:

- Misidentification causes 30% of radiation, medication, and blood transfusion errors.
- The average medical record duplication rate is 10%, resulting in an average cost of $1,000 per duplicate record, as well as an additional $5,000 per overlay to cleanse the data record.
- The average hospital can lose between 1-4% of net patient revenue as the result of denial write-offs, which are often due to misidentification.
- A staggering 2.3 million patients are impacted by medical identify theft each year.

“It's really amazing that healthcare has made such great strides in moving to a digital world when it comes to their EMR,” said Justyna Evlogiadis, former senior product marketing manager at Imprivata. “Yet, patient identification is still a very manual, cumbersome process in hospitals, which leverages things like drivers licenses and passports—manual information, we call it.”

A recent report from the Ponemon Institute, a leading research organization that tracks security and risk sources across different industries, shed a bright
Now the focus needs to turn toward digital solutions, because traditional, largely manual and people-intensive solutions are no longer adequate.

light on the root causes and both clinical and financial impacts of patient misidentification. Ponemon's 2016 National Patient Misidentification Report, based on responses from more than 500 nurses, physicians, IT professionals, and financial executives, made some important discoveries:

- Registration mistakes are the primary root cause of patient misidentification. In fact, this finding was supported by both clinical audiences and financial executives responding to the survey.
- Numerous factors lead to patient misidentification, including the inability to find a specific chart or record; finding duplicate patient records during a search; pulling up the wrong record because a different record had the same patient name or date of birth; and the inability to match the right record to the right patient.
- An eye-opening 86% of respondents said they have witnessed a medical error from misidentification.

Capping it off, 65% of respondents said they believed denied claims from patient misidentification have had either a “very significant” or “significant” impact on the hospital’s accounts receivable.

Clearly, patient misidentification is a major challenge — one that has a demonstrably negative impact on healthcare organizations. But now the focus needs to turn toward digital solutions, because traditional, largely manual and people-intensive solutions are no longer adequate.

“These (traditional) processes can still result in patient misidentification due to duplicate and overlaid medical records, identity theft, and insurance card sharing, as well as simple clerical records,” according to Claire Reilly, a clinical workflow specialist at Imprivata and a 25-year emergency room nurse.

Reilly noted that modern solutions have to be driven by an understanding of where misidentification begins. These issues can range from confused patients or their inability to communicate; incorrect or outdated information on file; mistakes made by registrars due to time or training constrains; fraud and abuse; cultural variation in naming conventions; and lack of awareness by the general public.
Healthcare organizations should consider moving to a positive patient identification solution, which typically is paired with a hospital’s existing Enterprise Master Patient Index (EMPI) and is designed to work across multiple EMRs and enterprise healthcare applications.

A key element of the such as solution is biometrics. “When patients show up at your healthcare organization, as opposed to just handing over an ID or stating their date of birth, they simply provide a biometric,” said Evlogiadis. “That may be their palm vein, for instance. That’s positively going to identify them as themselves.” She added that biometrics can, and already are, being used not only in traditional registration settings, but also at self-service, check-in kiosks.

This approach, embodied in solutions such as the Imprivata PatientSecure® solution, is already paying dividends for large healthcare organizations. For instance, Carolinas HealthCare System (CHS) had a 5% duplicate medical record rate, due in large part to the fact that they had about 80 different healthcare IT systems feed patient data into their Health Information Exchange across multiple organizations. Adding an EMPI helped reduce that duplication figure slightly, but they still struggled as they acquired more hospitals, and patient registrations surged.

By adding biometrics, and implementing Imprivata Patient Secure, CHS was able to reduce duplicate medical records to 0.01%, and in the process, reduce check-in times by 75%.

In the end, successful adoption of a biometric-based program to slash patient misidentification problems requires an organization-wide approach to education, communication, and implementation. Internal employees must be well trained and fully aware not only of how to use the system, but also in how to communicate its value to colleagues and to patients. Organizations also need to use proven marketing and public relations techniques to connect with internal and external audiences. Finally, there needs to be a proven, documentable deployment methodology, spanning project readiness, configuration and validation, initial go-live, full deployment, and ongoing optimization.