

Forbes

INNOVATION

Improving Medical Record Errors Through Technology

WES WRIGHT, FORBES COUNCILS MEMBER

Chief Technology Officer at Imprivata, a healthcare IT security company.

If you're not a professional actively working in the healthcare industry, you probably don't realize how important medical records are — or how dangerously unreliable they can be. According to Black Book Research covered in Becker's Hospital Review (registration required), "The average cost of repeated medical care due to inaccurate patient identification with a duplicate record, for example, is roughly \$1,950 per inpatient stay." That's a pretty high number — but duplicate medical records also mean your provider receives incomplete or inaccurate medical information about you. Even worse, bad information can be used to make critical medical decisions about patient care.

People who aren't in healthcare often don't even realize this problem exists. They have complete trust that, when they go to a healthcare facility, a check on their medical records will reliably deliver their actual medical information. But it doesn't always.

Patient matching problems often start at the front end of the patient onboarding process — incorrect identification at registration is a common cause. Reducing data entry errors at this stage requires better processes during the initial patient interaction. It's worth remembering that healthcare is moving from a transactional

event to more of a relationship with outcome-based results for many organizations and programs, such as Medicare. In this context, addressing the causes of such problems is critical to ensuring patient care.

Several technologies are helping with patient identification and medical records challenges. More traditional solutions such as the enterprise master patient index (EMPI) are well known. EMPI is a software that sits on top of different systems; it attempts to provide a unique identifier or resolve duplication at the back end. When a patient goes to a hospital and provides their name, confusion may occur between that point and, for example, the emergency room. If such confusion occurs, EMPI will resolve those records by looking at that data and clarifying.

Identity-proofing is another well-known patient identification technology. How do hospitals truly know that a patient is actually the person they claim to be? Experian and LexisNexis are perhaps the best-known providers of identity-proofing solutions, though the market has seen many new entrants of late.

Why exactly is patient identification so critical? As the CTO of a company that provides positive patient identification solutions, I believe it's because our doctors

and nurses can only provide effective care if they know the correct treatment to provide. Patient identification deals with this issue while avoiding the requirement that patients provide exhaustive identification every time they seek any type of medical care.

The finance industry provides a good comparison. Digital identity plays a crucial role in the financial world and was integrated into various transactions years ago. Consumers have since grown accustomed to using more complex passwords, as well as two-factor authentication (such as when the bank texts you a code to confirm your identity before you can continue with a virtual service). Unfortunately, other sectors, namely healthcare, still often lag behind in the adoption of digital identity.

In the financial services sector, digital identity is well established. Banking customers are familiar with the process of producing a bank card and providing that as proof of identity. It's straightforward and easy — and it works. The threat of identity theft still exists, of course, but solutions like these can help.

The healthcare industry, however, has yet to follow this approach to digital identity. Biometric solutions such as iris and palm vein scanning can also come into play here. These emerging technologies,

offered by companies like mine and Aware, provide the flexibility for providers to reliably connect patients to their medical information at the various touch points across the healthcare continuum.

If we see a greater shift toward value-based care, the emphasis will become more about the relationship than the transaction. What does it look like when patients find medical errors in their chart? Would you trust a bank if it somehow misplaced your funds? In one 2020 study, 1 in 5 patients found an error in their ambulatory visit note. Errors like these can significantly affect how hospitals interact with their patients. Healthcare organizations need to develop strategies for protecting their data and ensure its sanctity.

Despite greater adoption of the latest health IT solutions, too many health delivery organizations continue to use outdated identification methods, such

as matching a patient's Social Security number or address. These processes are prone to errors because they involve manual data entry and can result in patient misidentification. This in turn, can lead to patient safety issues, not to mention negative implications for healthcare organizations.

In my experience, Covid-19 has exacerbated digital identity management challenges with the rise of telehealth. New devices are now being used from a variety of locations to enable providers to continue delivering care during lockdowns and ongoing quarantines. This reality makes it more critical than ever for healthcare to look for areas where they can improve their current digital identity management practices.

Digital transformation is happening at warp speed and will continue to evolve quickly for the foreseeable future. Healthcare leaders need to adapt to this

new world and rethink their approach.

Although the financial industry has set a good standard for digital identity, the healthcare ecosystem is arguably more complex. There are different roles, and the industry must comply with HIPAA standards. While some strategies for security and privacy may cross over well from finance, HIT leaders likely know that what works in the banking sector may not transfer to their world. Healthcare requires a specialized plan to address the industry's unique challenges. To succeed with digital identity, the healthcare industry and technology providers will need to develop solutions that meet the needs of providers and can protect medical data every step of the way on a patient's healthcare journey. Having a modern solution in place could position healthcare for digital identity success during the pandemic and beyond.