Health IT OUTCOMES

Guest Column | November 18, 2016

The Role of Mobility And Digital Automation in Patient Engagement

By Pem Guerry, executive vice president, SIGNiX and Sam Johnson, president and CEO, RELATIENT

Healthcare is a heavily documented business. From patient management to compliance upkeep, paper shuffling plays a major role in the day-to-day activities of organizational staff and clinicians alike.

Think about the typical patient experience: appointment notices arrive in the mail and then new patient intake forms, health history forms, and a number of waivers are filled out on a clipboard minutes before the appointment. Doctors review materials with patients in the room, take notes in charts, hand off prescriptions, present lab and imaging requests to other providers (among other clinical processes), and later the billing process begins.

This, of course, is just a high-level overview. The bottom line is this: while paper has been a mainstay in the industry, manual processes can actually restrain patient engagement and hurt the patient experience. There's not a central portal where patients can access — from anywhere — their medical, appointment and billing information. There's no streamlined automation that moves processes forward. And medical staff will spend time manually inputting notes and information into digital platforms, adding time spent on administrative work instead of clinical care.

As value-based healthcare drives the need for enhanced engagement and streamlined experiences, elements of digital automation (like e-signatures, e-documents and e-prescribing) are rising in importance. In fact, according to **VDC Research**, enhancing the patient experience is the leading driver for clinicians to invest in digital healthcare and technologies.
In order to move the needle on patient experience and engagement, mobile adoption in the health space must meet three primary thresholds — usability, privacy, and trust.

continued on next page

PATIENT ENGAGEMENT, CONT'D

Usability

Healthcare mobility is in a transition state — no longer nascent, but not yet ubiquitous. As the pendulum shifts toward broader use, it must be palatable for staff and patients alike so that adoption actually occurs.

The good news is that the mass consumerization of mobile communication technology, like smartphones and tablets, makes using these devices, even for healthcare administrative purposes, familiar.

Still, there can be a complicated web of mobile applications, portals and APIs if tech architecture isn't designed to work cohesively together. When digital programming is integrated into a single user interface and automated workflows are established, the technology becomes more efficient and valuable for both patients and providers.

Instead of the paper-based example from above, integrated mobile technology could automatically notify patients of an appointment on a mobile device, provide an e-forms engine for patients to fill out forms online, leverage a secure and compliant e-signature engine for those forms to be signed online and sent back to the provider and file the forms automatically via an enterprise content management system. One seamless workflow for the patient and provider that removes hassle and speeds up processes.

The more powerful the technology, the fewer the touches.

Privacy

While technology must be easy to use, it cannot undermine a patient's or a provider's personal or proprietary information. Still, legal compliance with some technologies will require judgment calls from IT staff.

For instance, the Health Insurance Portability and Accountability Act (HIPAA) does not require a specific type of electronic signature technology for documents with patient health information. But that's not to say that every electronic signature platform is designed to mitigate the risk of a data breach.

Regardless of the technology used for engagement purposes, healthcare providers are wise to consider the following to improve privacy:

- **Two-factor identity authentication.** Identity authentication technology is crucial when sending or accessing sensitive information across mobile channels. And the ideal is to require two different methods of identification (**two-factor authentication**), which provides an

continued on next page

added layer of security against a privacy breach. In fact, this is where the industry is headed as a whole. Two-factor authentication in non-federal acute care hospitals has increased 11 percent each year since 2010, according to the ***Office of the National Coordinator for Health Information Technology***.

- **File control.** As documentation enters the mobile space, it's essential for IT staff to consider all external parties using and keeping copies of those digital files. Some outside providers may need to keep documents on their servers so legal evidence can be accessed. Others don't, incorporating the legal validity into the document itself, which gives the document owner the authority to determine how it is stored. Some providers may also have the ability to use, and then digitally shred, documents. It's important to track the life cycle of any digital file accessed or sent via the cloud, determine which parties control what and understand where potential privacy vulnerabilities may lie.
- **Vendor site security.** Security and privacy are only as strong as your network's weakest link. When contracting with software providers, it can be a good idea to perform a security audit—not just of their technology, but also of their site, to make certain that every aspect of your technology platform is as secure as it can be.

Trust

Because of the importance of privacy, leveraging technology within a sensitive space like healthcare will require trust from users.

Once security protocols have firmly been established, it's the more "superficial" details of the technology that can lead to trust and adoption. Seemingly minor elements like aesthetics and branding can play a significant role in building confidence among users.

When technologies can be white labeled and take on the branding of a hospital or health organization — it removes the hesitancy a user may face if she is suddenly introduced to a new vendor she's never interacted with before. The familiar interface reinforces the same spirit of protection that the doctors provide. For that reason, it also provides another level of accountability for the patient's data — it has the provider's brand, which in essence, is a stamp of approval.

Trust is the keystone of technology adoption in healthcare. Once it is assured, patients and staff are psychologically ready to make the best use of mobility and automation — meaning patient experiences and engagement can flourish.

About The Authors

Pem Guerry is Executive Vice President at SIGNiX, a digital signature solutions provider that makes signing documents online safe, secure, and legal for any business. SIGNiX offers the

continued on next page

PATIENT ENGAGEMENT, CONT'D

only independently verifiable, cloud-based digital signature solution, which combines workflow convenience with superior security. Learn more about what makes SIGNiX different at www.signix.com.

Sam Johnson is President and CEO at RELATIENT, the only web based and mobile-first Patient Relationship & Engagement engine that allows provider groups, hospitals, and health systems to automate global outreach to their patient population with compliant and proven strategies. Improve compliance, reduce readmission, promote health, lower risk, and collect balances with a platform designed for today's mobile user. Learn more about RELATIENT at www.relatient.net.