Protecting Patient Portals

Easy access to EHRs is a dream come true… for hackers.

As more and more patient records move to Web-based portals, your personal health information has never been closer—*but to whom?*

The frightening truth is that breaches of highly sensitive patient information are likely to keep rising as hackers find new ways to attack vulnerable patient portals.

Just how vulnerable are they? Consider that the clear majority of today's patient portals are secured by nothing more than a simple user name and password—which all but guarantees the likelihood of health records being hacked.

Security in name only.

Many vendors, in a misguided effort to strengthen their portal defenses, will move toward impossibly complex password requirements and frequent password changes.

But these "security" efforts frequently produce the opposite effect by encouraging users to either write down their passwords or use common mnemonic devices like "P@$$word!"

Worse yet, there is now evidence to suggest that cumbersome (and still ineffective) security measures are keeping patients from using these portals altogether—which is bad news for the cost reductions and efficiency gains your online system promised to deliver.

You are the security you've been seeking.

Security experts in the healthcare industry recommend that patient portals be protected by biometric-based multi-factor authentication.

It sounds like a mouthful, but it's really pretty simple. Multi-factor means using two or more different authentication types: like something you have (a key), something you know (a password), and something you are (a "biometric" such as your face, voice, or fingerprint).

With a biometric-based platform like Daon's IdentityX, doctors and patients can access highly secured portals using only their smartphones—no passwords required.

Depending on the sensitivity of the information requested, the portal might ask for 1, 2, or 3 factors. Best of all, the user gets to decide which combination of factors is most convenient.

ABOUT PATIENT PORTALS

Patient portals are secure, HIPPA-compliant websites that give patients access to their personal health information, also known as Protected Health Information or PHI. Though functionality varies from vendor to vendor, most portals enable patients to view their electronic health records and results of medical checkups, share medical histories with their care providers, manage appointments, review invoices and payments, and many other actions that save time and money for both the patient and caregiver.

Protecting Patient Portals

| Device Key | Face | Voice | Fingerprint | Passcode/PIN |
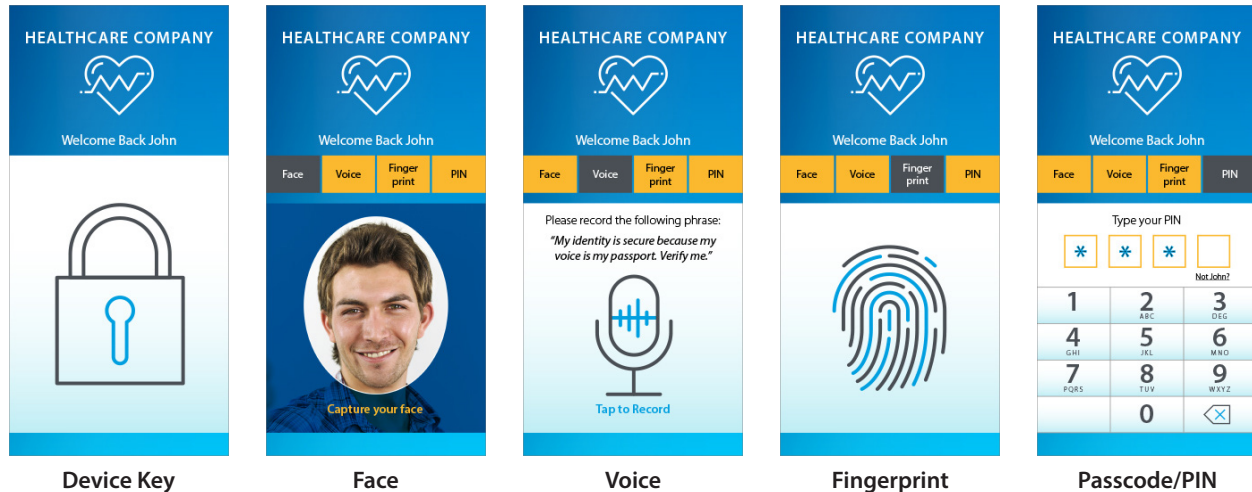
Worried about future-proofing?
IdentityX also supports cutting-edge behavioral biometrics and emerging biometric factors like palm recognition.

Getting patients on board.

One of the benefits of biometric-based authentication is that patients can sign up, get verified, and receive their credentials without ever setting foot in an office.

With digital onboarding through IdentityX, patients simply use their smartphones to snap an image of their government-issued photo ID. The photo is then processed to ensure its authenticity, or it's compared to a "live selfie" of the patient in order to verify a match. Once completed, IdentityX uses the patient data to query a wide range of 3rd party databases—confirming the patient's identity with a remarkably high level of assurance.

Take it *from* the bank.

Believe it or not, the financial, insurance, and technology industries have been reaping the benefits of biometric-based multi-factor authentication for years:

- Dramatically reduced identity theft and fraud—in many cases, zero evidence of fraud loss since deploying biometrics
- Increased use of digital channels—resulting in operational cost reductions
- Fewer "password reset" calls to Customer Support
- Higher reported user satisfaction

So why not derive those same benefits from a patient portal or other Electronic Health Records system?

It's time for patients to stop choosing between security and convenience.

You can have both.

Ready to see how IdentityX saves you time, dollars, and peace of mind? Visit **www.daon.com/healthcare**