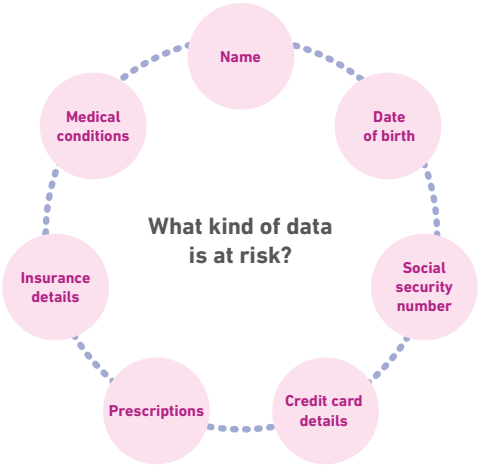
Is your patient portal as **secure** as it should be?

Patient portals allow consumers to view their medical records and lab results, arrange appointments, renew prescriptions, and in some cases make payments, all at the click of a button, day or night. Patient engagement goes up. Staff productivity goes up. Revenue cycles are more efficient. Health outcomes improve.

Unfortunately, what makes your patient portal valuable for patients is exactly what makes it attractive to cybercriminals. It's a one-stop shop for entire health records, and identity thieves can make a fast buck from stealing this data and selling it on.



Where are the weak points in portal security?

Many patient portals have surprisingly minimal security, with three main areas of vulnerability:

They rely on password-protection only.
Key-logging Trojan software allows fraudsters to steal a user's password, by lying dormant on the victim's computer and recording key-strokes when the target website's name is detected.

They have insufficient identity verification.
Even when a patient hasn't enrolled in the portal, fraudsters can set up a fake account using data obtained via "phishing" emails. The sign-up system has no way of knowing if this is the real person or not.

They fail to mask sensitive information.
Portals often show full insurance details without any encryption, opening the door for malicious software or "bots" to harvest medical identities and create very precise fraudulent claims.

"Healthcare-related data breaches are **10 times more frequent** than data breaches in the financial services sector, and medical identity theft accounts for **43 percent of all identity theft**."

How can you protect your patient portal?

To balance security and patient convenience, implement technology that uses a multi-layered solution with multiple measures, such as:

Sign-up screening that uses identity proofing to ensure users are who they say they are.

Log-in monitoring, using device intelligence to confirm the patient is using a cell phone or tablet your system recognizes.

Additional checks on particularly risky requests, such as downloading medical records or editing a patient's profile, with further out-of-wallet questions.

Rapid response and damage containment, so you can shut down the attack quickly and prevent further damage.

Promoting interoperability by enabling your systems to share data across different platforms in a safe and secure way, so it's only seen by the right people.

Find out more about how working with a trusted vendor such as Experian Health can help you implement state-of-the-art portal protection so you can minimize your risk and protect patient data at www.experianhealth.com/identityproofing

05/19 • 1060-EH