Experian Health

The Pitfalls of Healthcare Portals

Why patient portals attract cybercriminals and how new industry solutions can help

An Experian Health white paper

Introduction

Online patient portals have been built to provide the ultimate self-service experience while engaging patients more fully in their care. Integrated into multiple internal systems, portals offer convenient access to personal information: Social Security number (SSN), date of birth (DOB), address, insurance information, prescription information and extensive medical records.

This one-stop shop for medical identities and health records is exactly what makes healthcare portals particularly attractive to cybercriminals. While lucrative for criminals, a portal compromise can be extremely costly to healthcare organizations, affecting finances and their reputation.

Given what's at risk, you would expect healthcare portals to be highly protected, but most are secured by little more than a password. This white paper will highlight some of the vulnerabilities of healthcare portal technology and will explain how innovations in the healthcare industry can help minimize potential exposure.

Healthcare technology transformation brings risk

Over the past several years, the U.S. healthcare ecosystem has embarked on an information technology (IT) transformation of unparalleled scope. Dentists, family practitioners, hospitals, pharmacy chains, medical labs and MRI facilities are migrating information to the Web. For consumers, patient portals play a significant role in reshaping the patient experience and engagement as part of the Affordable Care Act. While such IT advances can be highly beneficial, they also carry increased security, privacy and fraud risks.

The comprehensive data contained in healthcare portals is especially lucrative for fraudsters. While a stolen credit card number sells for a dollar, a full set of medical records can command hundreds of dollars in the underground market. The breadth of data offers fraudsters multiple opportunities to "cash in" using this personal information: name, DOB, SSN, credit cards and prescriptions. Fraudsters not only use personal information to purchase services or devices, but also to steal identities and affect consumers' credit.

Healthcare portals not only contain valuable information, but also often fail to mask sensitive information, which is conducive to large-scale, automated harvesting:

- Unlike banks, which typically mask bank accounts online by showing only the last four digits of an account number, most patient portals display full insurance details. Many also include front and back images of the patient's insurance card.
- A patient's "problem list" — a mandated component of any patient portal — offers an abstract of the patient's medical conditions. Fraudsters leverage uniform medical terminology dictated by standards such as ICD-9-CM and the SNOMED CT to develop

malicious software or "bots" that can run through patients' problem lists and classify each victim based on the type of fraudulent insurance claims their medical identity can support. This automation facilitates more precise fraudulent claims, thereby making the detection of treatment anomalies more difficult.

An environment conducive to password theft

Most healthcare organizations assume that passwords are sufficient protection for their portals. What they may not know is that the last 10 years have seen steady increases in the use of keystroke-logging Trojans, which enables fraudsters to steal users' passwords. While Trojan attacks traditionally have focused on banks, the attention has turned to healthcare portals.

Here's how they work. Keystroke-logging Trojans lay dormant on a victim's computer until the target Website's name is detected. Once the Website is detected, the Trojans "wake up" and record the victim's keystrokes as the username and password are entered.

Although it would seem that a credential compromise — sometimes called "account takeover" — impacts only patients who already are enrolled in a portal, portal security is of interest to all patients. Since a portal places medical records for all patients on the Web, fraudsters can put any patient at risk by enrolling in a portal with stolen personal information.

Breaches often involve a common provider of personal information such as name, DOB and address, which enables criminals to enroll victims in the portal, obtain full medical records and take the situation from bad to worse.

There is also a subtle social engineering vulnerability stemming from the number of portals soliciting patient enrollment. Providers are offering incentives for patients willing to enroll by sending out email invitations. Cybercriminals brand these emails with the portal vendor name, giving them an identical look and feel that can falsely lead patients to assume the email is credible, causing them to fall victim to password-stealing Trojans.

Portal security is a multilayered approach

As mentioned earlier, passwords easily can be stolen with keystroke-logging Trojans, with phishing emails or by other social engineering means, and they offer no backup plan. Once information is compromised, it is nearly impossible to distinguish between true patients and imposters. It is also difficult to assess the scope of the breach, to connect it to a common criminal or to quickly contain the damage. Given these limitations, healthcare organizations need to assess the level of authentication provided by passwords alone and consider their exposure should passwords be compromised. They also must evaluate whether they can recover gracefully from an attack.

How comfortable are you with the level of protection offered by passwords?

The answer to this question depends on the amount of risk you are willing to accept in potentially harming your patients and healthcare organization. Security guidelines seek to match the level of authentication to the level of risk. When a medical identity is stolen and used by another to receive treatment, medical records can become commingled and the result can be life-threatening. Given the potential impact on patients' quality of care, basic password protection appears to be insufficient.

The recommended approach is a multilayered solution that incorporates multiple measures, including the seamless integration of:

» device recognition,

» identity proofing analytics, and

» fraud management.

For example, the device submitting the password and claiming to represent the user can be analyzed for compatibility with the user, prior impersonation behavior and involvement in known crimes, as can identity proofing and knowledge-based authentication measures. This heightened situational awareness is of particular value for healthcare organizations faced with protecting a variety of new and evolving patient-facing products and services.

Key considerations for portal security

Enrollment screening
Leveraging identity proofing and device technology to detect fraud at the point of enrollment.

- **Identity proofing** to authenticate patients and ensure they are who they say they are. Leverage out-of-wallet questions such as the city of a person's birth, the make or model of his or her car, or previously held addresses to challenge suspicious applicants.
- **Device intelligence** to evaluate a patient's device attributes which assess the likelihood that patients are who they claim to be.

Login monitoring
Leveraging technology to monitor the devices submitting login requests to answer questions such as:

- Has this device been used by this patient before?
- If not, is this the type of device configuration that you would expect this patient to have?
- Has this device been seen representing, and potentially impersonating, multiple patients?
- Has this device been associated with previous fraudulent activities?

Logins that exceed a risk threshold can then be challenged with generated out-of-wallet questions to verify their validity.

Additional monitoring of risky requests
Some portal activities — for example, a request to download medical records or make edits to a patient's account profile — carry increased risk. As with login monitoring, these activities can be monitored and challenged using out-of-wallet questions. Placing additional controls for higher-risk activities balances user experience and portal security.

Rapid response and damage containment capabilities
Attacks on portals can be automated and can happen just as quickly as a data breach, but they may be more damaging due to the exposure of sensitive medical information. To prepare for portal attacks, organizations should implement measures that provide early visibility into which patients have been compromised, what data has been accessed and what steps need to be taken.

Monitoring Internet Protocol (IP) addresses isn't enough. The practice of linking by IP addresses has been done for so long that most savvy fraudsters change their IP addresses frequently to avoid detection. Monitoring for devices that impersonate multiple patients during login or enrollment can help detect attacks in progress, especially when the device's configuration is incompatible with that of the patient it is impersonating.

Secure your portals, secure your reputation

The broad deployment of healthcare portals and the lucrative nature of the data they hold nearly ensure that they will be targeted increasingly by cybercriminals in coming years. Currently, healthcare-related data breaches already 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. Early awareness of attack attempts — both successful and unsuccessful — will provide security teams with the knowledge necessary for developing fact-based security strategies. Utilizing new technology offers multiple linking and search tools for correlating devices and impersonated identities and linking their activities to help safeguard your patients and your organization.