Healthcare Organizations, Is Your Patient Portal Secure?

By Michael R. Bertoncini and Valerie K. Jackson

August 1, 2019

Healthcare organizations' traditional cybersecurity measures are insufficient against today's cyberattacks, according to a report from LexisNexis® Risk Solutions and the Information Security Media Group released in July 2019.

Even as healthcare organizations embrace new technologies (such as patient portals), the report shows that organizations' cybersecurity measures for these technologies are behind the times.

Risk: Patient Portal

A patient portal is a secure online website that allows patients to access their electronic health record from any device with an internet connection. Patients also may request prescription refills, schedule appointments, and securely message providers in some of these portals.

This increased access for patients also increases the risk that someone other than the patient will gain unauthorized access to the portal, and to the patient's electronic protected health information (ePHI).

Target: Healthcare Organizations

Healthcare organizations continue to be heavily targeted by cyberattacks for their valuable patient records and ePHI. Approximately 25 million patient records have been breached just halfway through 2019, eclipsing by more than 66% the number of patient records breached in all of 2018. While a Social Security number may sell for $1.00 on the black market, patient records can fetch $1,000, which explains why healthcare organizations are a frequent and lucrative target for hackers.

Healthcare organizations, therefore, are challenged to provide patient portals that balance patients' desire for ease of use with the duty to prevent unauthorized access to patient records.

Survey and Report

To learn more about how healthcare organizations are meeting the challenge, LexisNexis® Risk Solutions, in collaboration with the Information Security Media Group, conducted a survey in spring 2019 asking healthcare organizations about their cybersecurity strategies and patient identity management practices. The results of the survey, which included responses from more than 100 healthcare organizations, including hospitals and physician group practices, were published in a report, "The State of Patient Identity Management."

The report concluded that healthcare organizations still maintain high levels of confidence in their cybersecurity preparedness, despite most surveyed organizations using only traditional authentication methods to secure access to patient portals, which are no match for today's cyberattacks.

More than half of survey respondents (58%) reported that the cybersecurity of their patient portal was above average or superior when compared to other patient portals. Only 50% of respondents were confident that their current authentication methods could prevent unauthorized access to patient portals. The vast majority of respondents reported they continue to use traditional authentication methods, such as username and password (93%), knowledge-based authentication questions and answers (39%), and email verification (38%).

Significantly, less than two-thirds of respondents reported using multifactor authentication. Multifactor authentication verifies a user's identity in two or more ways, using:

1. Something the user knows (*e.g.,* passwords and security questions);
2. Something the user has (*e.g.,* mobile phone and hardware that generates authentication code); or
3. Something the user does or is (*e.g.,* fingerprint, face ID, and retina pattern).

The report concluded that traditional authentication methods "cannot be relied upon for any confident level of cybersecurity." Usernames and passwords can be weak or stolen, the report pointed out. Knowledge-based questions and answers are vulnerable to social-engineering threats. Answers to common questions such as "What is your mother's maiden name?" or "Where did you attend high school?" are

Meet the Authors

Michael R. Bertoncini

Principal
Boston
617-305-1270
Email

Valerie K. Jackson

Associate
Boston
617-305-1269
Email

Practices

Privacy, Data and Cybersecurity

Industries

Healthcare

easily attainable through social media, like Facebook. Additionally, the number of high-profile security breaches in healthcare already may have made legitimate authentication credentials available for misuse by hackers. Others also have made similar findings. For example, the Patient Portal Identity Proofing and Authentication Guidance from the Healthcare Information and Management Systems Society (HIMSS) Identity Management Task Force found that "[d]ue to the increased sophistication that attackers have developed, the traditional approaches to authentication are no longer adequate and more sophisticated methods are now necessary."

While multifactor authentication is an improvement over traditional authentication methods, the report noted it is still "the bare minimum of what organizations must employ to prevent unauthorized access to data." According to the HIMSS Guidance, "there is no excuse today for any healthcare organization not to implement two factor authentication for access to PHI as the default."

Cybersecurity and Authentication Measures for Healthcare Organizations

While the HIPAA Security Rule does not require multifactor authentication, it requires covered entities and business associates to use security measures that reasonably and appropriately implement its standards and implementation specifications.

Generally, the HIPAA Security Rule requires covered entities and business associates to:

1. Ensure the confidentiality, integrity, and availability of all ePHI the covered entity or business associate creates, receives, maintains, or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.

The Person or Entity Authentication standard of the HIPAA Security Rule requires covered entities and business associates to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. However, this standard has no implementation specifications. Covered entities and business associates, therefore, have the flexibility of using a range of security measures that reasonably and appropriately implement the HIPAA Security Rule standards. Entities may take into account certain things about their organization, including:

1. Size, complexity, and capabilities;
2. Technical infrastructure, hardware, and software security capabilities;
3. Costs of security measures; and
4. Probability and criticality of potential risks to ePHI.

Given the relentless cybersecurity threats to healthcare organizations, the sensitivity of patient's ePHI, and the inadequacy of traditional authentication methods, multifactor authorization may be considered a reasonable and appropriate way to implement the HIPAA Security Rule Person or Entity Authentication standard.

While healthcare organizations challenged with safeguarding ePHI are not required to adopt any particular cybersecurity framework or authentication method under HIPAA, hardening cybersecurity and implementing multifactor authentication for access to patient portals can go a long way in complying with the HIPAA Security Rule.

Finally, a failure to implement reasonable and appropriate cybersecurity measures could not only lead to a healthcare data breach, but it also could result in a covered entity or business associate being fined by the Department of Health and Human Services Office for Civil Rights.

To learn more about how Jackson Lewis can assist healthcare organizations with HIPAA compliance and data security, please contact a Jackson Lewis attorney.

*The National Operations Center serves as the firm's central administration hub and houses the firm's Facilities, Finance, Human Resources and Technology departments.