APPSIAN SECURITY

EXECUTIVE BRIEF

Data Privacy: How to Enable Healthcare Workers While Strengthening Security

Greg Wendt • Executive Director, Security

Did you know HR data and not patient data yields the highest ROI for cyber criminals? Here's why hospitals need to focus on data privacy and protection beyond patient ePHI, and ensure their security technology protects employees' personally identifiable information.

As COVID-19 continues to challenge healthcare organizations around the country, hackers are increasingly targeting healthcare employees. Whether via phishing or ransomware attacks, cybercriminals continue to bombard overloaded IT systems in search of electronic personal health information (ePHI).

Overworked and understaffed healthcare IT departments work to defend their systems, networks and applications, but fewer resources mean greater risk. Amidst the current chaos, healthcare organizations need to focus on data privacy and protection, beyond patient ePHI and ensure their security technology provides the necessary protection for employee personally identifiable information (PII) as well.

Putting the processes in place to protect HR data

Many healthcare organizations assume that patient data, as covered under HIPAA, is the primary target of hackers. However, cybercriminals operate with the objective of attaining as much valuable data as possible. This data is usually in the form of employee HR data like direct deposit, social security and any other information that would enable identity theft. Consequently, HR data tends to yield the highest ROI as cybercriminals re-directing payroll from HR systems to offshore accounts is a common occurrence.

As non-essential staff move off-premises and work remotely, healthcare IT departments must be aware the increased threat of remote access will only exacerbate an organization's risk. Cybercriminals gaining access to data via privileged credential theft, such as IT/HR/Finance administrator accounts, can allow them to move inside business applications with ease.

This new landscape means least privilege process controls must be incorporated as part of a healthcare organization's overall data privacy and protection strategy. Limiting access according to the principle of least privilege means ensuring that users access only the data and resources needed to complete specific job functions. When setting these controls, healthcare organizations should consider:

- The minimum amount of PII required to execute typical HR transactions.
- How access privileges can fluctuate outside of typical work hours.
- How access privileges can fluctuate when access is coming from overseas.

Enable controls to be risk-aware

After setting initial controls, healthcare IT departments need to consider the change from an on-premises to a remote workforce. Many non-essential healthcare employees now work from home. Their home networks and devices may not incorporate the same levels of security as those on-premises. Incorporating risk-aware attributes to what resources these employees access, and how they access these resources can mitigate non-HIPAA associated privacy risks.

When considering risk-aware attributes, healthcare IT departments should consider:

- geolocation of users
- devices that access application data
- time of day users access resources, and
- how often a user is accessing a particular resource.

Each of these attributes enables healthcare organizations to better manage their risk. When thinking about ERP systems and the sensitive data they store, process and transmit, healthcare organizations must consider the expanded threat surface of remote access.

Remove the ambiguity of user identity

Doctors are some of the most highly paid employees in a healthcare organization. With that in mind, cybercriminals seeking to engage in financial fraud through payroll diversion or identity theft will attempt to leverage doctors' PII stored in ERP systems.

From a security standpoint, employees who manage payroll should have access only to the information necessary for processing payroll, as opposed to having the ability to make edits to account numbers or exporting data in bulk. The same should go for the doctors themselves, as some scenarios where a user would change their own sensitive records would immediately be considered suspicious, for example, in the middle of the night or from a foreign country.

By using risk-aware or attribute-based controls that triangulate privilege with context of access, healthcare organizations can ensure a higher degree of data security. This is largely because attribute-based controls remove the ambiguity of user identity and focus solely on protecting data. Healthcare organizations can spare themselves from experiencing a data privacy incident even if privileged credentials are stolen, as the cybercriminals won't be able to access PII due to the context of their access.

Consider the liability of shared workstations

Amidst the myriad of duties healthcare workers perform throughout their day, they must also budget time for HR-related tasks, ranging from checking work schedules and updating payroll information to adjusting benefits, etc. The problem is that workers perform these tasks in ERP applications at a shared workstation because access to these applications is typically available on-site due to security concerns.

Ironically, while limiting access to on-site workstations was designed to prevent security incidents, there is an increased liability with multiple users working from the same computer. Data exposure is inevitable if a user is quickly pulled away from a transaction and remains logged into their account.

Enable secure remote access to HR applications

For this reason, many organizations are moving toward enabling healthcare employees to have remote and mobile access to their HR systems, identifying that the liability of a user leaving their data exposed via a shared workstation is ultimately too great to ignore. Enabling remote access comes with its own security concerns, but these can largely be mitigated using established technology designed to strengthen and enforce data security policies in legacy HR applications.

When looking for the right data security technology, healthcare organizations should look for:

- adaptive multi-factor authentication (MFA)
- data masking, and
- user activity monitoring.

With adaptive MFA, healthcare organizations can leverage a user's contextual attributes as they move from one area of an application to another. For example, where are they coming from, what device are they using, and what time-of-day is it? This technology is excellent for users accessing self-service, but as most organizations shift to remote workforces – the ability to secure remote access for high privilege users (those in HR and finance departments) becomes mission-critical. The use of adaptive MFA has grown in popularity as security teams align data privacy policies to establish zero trust best practices. These principles discourage granting access to data using default privileges and recommend contextual attributes.

Physical and data health aren't mutually exclusive

Healthcare organizations are currently being tested, both from a physical and data health standpoint. As healthcare IT departments continue to respond to the increase in cyber-attacks, they need to find solutions that empower them to provide the best care for both patients and employees.

Data privacy is two parts people and one-part technology. However, the technology part needs to empower, not impede staff. IT departments need to find "quick wins" – technologies that can be rapidly deployed and provide near-immediate returns on investment by enabling an expansion of (secure) data access. Organizations can incorporate complementary technologies that natively integrate with their current identity and access management strategies. Moving towards an agile, data-centric and adaptive access model ensures that all users have the access they need – and only that access.

Greg Wendt, executive director of security at Appsian, is the Oracle® PeopleSoft security expert. He served as ERP Application Architect at TCU where he was responsible for TCU's PeopleSoft system and was Chairman of the Higher Education User Group's multinational Technical Advisory Group (HEUG TAG). He has led criminal justice and cyber security courses focusing on hacking techniques.

This article was originally published at Healthcare Business & Technology.

APPSIAN SECURITY

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

+1 (469) 906-2100

info@appsian.com

www.appsian.com