WHITEPAPER

The importance of auditing insider access

imprivata®

Why it's vital for healthcare organizations to protect themselves from insider access risks

Healthcare organizations are increasingly relying on technology solutions that store and sometimes share patient information. While this has streamlined the care process, it has also become a major concern for healthcare organizations in relation to patient privacy. While the 2020 Insider Threat Report found that 61% of data breaches involving an insider are primarily unintentional[1], it's still critical to prevent breaches from occurring at all.

Whether insider threats come from malicious actors, or from an employee accidentally clicking on the wrong patient file, the consequences can be severe if these accesses are not found and investigated.

The healthcare organization environment

Healthcare organizations need to operate efficiently to ensure patient care is not affected by workflow delays, which also means that technology platforms used by healthcare staff members can't be heavily restricted. Why? Healthcare staff are all too familiar with the delay that can occur when needing to request access to a system. For example, the EHR can't be implemented with a Zero Trust mindset if the ER is short-staffed and needs help from other floors – after all, those care providers need to be able to quickly access the systems used on that floor. While expedience over security *does* help streamline patient care, it also can result in a high risk that clinicians will access patient information they shouldn't have access to. This type of unauthorized access can lead to data breaches, which have far-reaching consequences for both patients and healthcare organizations. A breach of patient privacy can put the organization at risk of regulatory fines, financial losses, and loss of trust from patients.

Whether the behavior is intentional or not, any negligence when handling highly sensitive patient information carries severe consequences for the healthcare organization. It's therefore essential to understand the risks that hospital employees present to their organization, and to take steps to protect against this risk by implementing policies and procedures aimed at preventing unauthorized access from insiders.

Risks presented by insider threats

Patient safety

Patient safety is the number one goal of any healthcare organization. But, in an increasingly digital world, it's no longer sufficient just to protect their physical safety – now, protecting and securing their digital safety is crucial, as well. Insider threats are a risk to a patient's physical and digital safety, as occurrences such as

[1] hhs.gov

data tampering can lead to incorrect diagnoses and improper treatments or privacy breaches, leaking confidential patient information outside of the organization systems. Unauthorized patient data access by internal employees can put a patient's personal safety and privacy at risk if their data falls into the wrong hands.

Regulatory penalties

Malicious or accidental, breaching a patient's privacy can lead to violations of HIPAA in the United States, GDPR regulations in Europe, and other regulatory safeguards. These can lead to significant financial losses for healthcare organizations that are held liable for any breach in security protocols that resulted in unauthorized access of patient records. Organizations may face hefty fines from regulatory bodies such as Health and Human Services (HHS) Office for Civil Rights (OCR), local data protection authorities, or even potential legal action from affected patients whose rights have been violated by the breach.

If an employee breaches HIPAA regulations, the organization can face fines of up to $50,000 per violation, with a maximum penalty of $1.5 million per year for multiple violations. Additionally, the organization may be subject to criminal penalties including imprisonment for up to 10 years.[2]

Furthermore, unauthorized access to patient data can put healthcare organizations under heavy scrutiny from regulatory agencies such as the OCR, which has become increasingly aggressive in its actions against healthcare organizations found guilty of violating HIPAA regulations. Hospitals that fail to follow these regulations could be hit with monetary settlements and corrective action plans, which require them to implement stricter security protocols and practices or risk further sanctions and fines.

Long-term reputational damage

A breach of patient privacy is a breach of patient trust, and healthcare organizations must consider the reputational damage that could arise if their employees are found responsible for inappropriately accessing patient data. Patients may lose trust in their healthcare provider and choose not to seek treatment there due to fears about their digital safety and privacy issues. This could lead hospitals to experience a decrease in patient visits and revenues as well as higher costs associated with hiring new personnel or providing additional training programs

[2] ama-assn.org

on topics around protecting patient data. The loss of patient trust can be one of the hardest outcomes to recover from, as it makes healthcare organizations a less attractive option for current and potential customers.

Staying protected

To ensure your organization is mitigating the potential of insider risks, staff should be continuously trained on how to handle patient data securely and safely while adhering to relevant laws and regulations governing privacy protection in healthcare settings. In addition, compliance and privacy teams should have procedures in place to monitor access to **patient data and investigate if necessary**. Utilizing an EHR auditing solution to help alert to, and investigate, potential risks can help save time during this process. These procedures should be documented and known throughout the organization to help foster an awareness of protecting patient privacy.

Healthcare organization have much at stake when it comes to protecting patient data – from insider threats due to potential fines from regulatory agencies, to costly reputational damage, or other penalties HIPAA or other regulatory policies haven't been followed. It's essential that healthcare organizations take proactive steps towards protecting against insider threats, by implementing robust security protocols such as user authentication, encryption technologies, employee training programs, regular system audits, and technology to assist in detecting insider threats. With these tools, healthcare organizations will be best able to preserve trust with patients while also safeguarding themselves against long-term risks.

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

Copyright © 2023 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.