imprivata®

EHR access monitoring checklist

Access monitoring helps ensure compliance

An effective compliance program must include monitoring of EHR access records. This job is a continuous task that compliance and privacy teams must do to ensure any inappropriate accesses are detected and resolved in a timely manner.

This interactive checklist provides essential components necessary to build a successful access monitoring process. When discussing how your team should go about monitoring, this checklist can be a guide to aid you. It is important to remember to design a process in line with your team and healthcare facility's priorities.

Protect patients and maintain compliance

- Better manage day-to-day tasks and ensure the proper data are being monitored

- Maintain compliance with internal policies and external regulatory standards

- Identify inappropriate accesses to medical records by internal users to investigate

- Imprivata FairWarning Patient Privacy Intelligence helps with EHR access auditing, allowing teams to quickly discover risk and conduct investigations with the ability to fully understand why an access was alerted on, and how often a user is presenting risk to the organization across all platforms

About Imprivata

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

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

SUBJECT REVIEW

☐ Review who needs to be monitored (patients, VIPs, newborns, employees who have made previous inappropriate accesses)

☐ Review systems and determine if these need to be monitored (Do they hold large amounts of PHI/contain an audit trail?)

☐ Map out what your team is looking for - what is a policy violation?

METHOD LAYOUT

☐ Ensure external regulatory guidelines for monitoring and protecting patient data are being met

☐ Layout method/identify resources for monitoring processes

☐ Layout tools to be used for monitoring EHR accesses

☐ Document practices for future onboarding

☐ Leverage software systems to help audit log report pull from EHRs

☐ Leverage software systems to help automate the monitoring processes

MONITORING FREQUENCY PLAN

☐ Determine frequency and high risk criteria to review within EHR access logs

☐ Formalize an audit plan for compliance/HR regarding response to high risk events found

☐ Assign team members to specific tasks to meet report requirements

REPORTING

☐ Outline what information needs to be reported for compliance purposes or executive board reporting

☐ Determine how reports will be presented and who they will be presented to; different departments might need to consume data in different ways, so it's important to define specific metrics you present and how those are presented (raw data or aggregate results)

☐ Determine what metrics "matter" to the organization based on risk profile and previous events/audits