imprivata

EPR access monitoring checklist

Access monitoring supports data governance compliance

An effective data compliance program must ensure that EPR records are maintained and protected according with data protection legislation. This is a continuous task undertaken by compliance and privacy teams to ensure that any inappropriate accesses are detected and resolved in a timely manner.

This 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 help you. It is important to remember to design a process in line with your team and healthcare organisation's priorities.

Protect patients and maintain compliance

- Better manage day-to-day tasks and ensure the proper data is being monitored
- Maintain data governance compliance
- Identify inappropriate accesses to patient records by internal users that need to be investigated
- Imprivata Digital Identity Intelligence (formerly Imprivata FairWarning) helps with EPR access auditing, reviewing up to 99% of accesses and presenting the remaining suspicious accesses for review

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:
London +44 (0)208 744 6500
Australia +61 3 8844 5533
or visit us online at www.imprivata.com/uk

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 patient information and provide an audit trail?)
- ☐ Map out what your team is looking for - what is a policy violation?

METHOD LAYOUT

- ☐ Ensure data governance requirements are being followed including any hardware, software, and/or processes that must be implemented for systems that hold sensitive patient data
- ☐ Layout method/identify resources for monitoring processes
- ☐ Layout tools to be used for monitoring EPR accesses
- ☐ Document practices for future onboarding
- ☐ Leverage software systems to help audit log report pull from EPRs
- ☐ Leverage software systems to help automate the monitoring processes

MONITORING FREQUENCY PLAN

- ☐ Determine frequency and high risk criteria to review within EPR 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