CAPITA

Patient Privacy Monitoring

Challenges

The healthcare industry has experienced a number of high profile privacy incidents involving employees and affiliates using Electronic Health Records to conduct unlawful activities such as record snooping, unauthorised access to information and loss of sensitive data.

These electronic health record systems have a comprehensive audit trail, producing large amounts of data which often rely on a manual and costly process of review. It is also difficult to achieve a complete view of staff interactions with data across all systems. All this increases the risk of government penalties, breach of patient trust and personal or organisational liability.

Capita Managed IT Solutions has been supporting health organisations in their drive to be more proactive and improve data security and compliance.

Solution

The patient privacy monitoring software processes the massive amount of records from multiple healthcare applications by pulling audit files from each system that has been identified to be monitored. The solution is compatible with over 100 electronic health record systems out of the box.

The surveillance is non-evasive and systematically identifies users who are engaging in patient access patterns that are indicative of snooping, password sharing, identity theft and other suspicious behaviours. The solution also links to the staff ID system which helps to build an intelligent profile and identify patterns which may link patient records to the individual accessing the files.

Privacy & Compliance Auditing

Regulatory Investigations and Auditing

- Individual Patients
- Individual Users
- GP / Physician
- Consultant / Contractor
- Random Patients
- Random Users

Detecting "Snooping" Patterns

- VIP Scenarios: Prominent government officials, celebrities etc.
- Family Member Snooping
- Employee and Patient Snooping
- Executive Snooping
- Neighbour Snooping
- Self Examination

Detecting Identity Theft Patterns

- Sequential Patient Records
- Patient Access Thresholds
- Printed Record Thresholds
- Deceased Patient Records
- Discharge Patients Records
- Address Changes
- Expired Logins
- Simultaneous Logins

Published: 27/03/13

It doesn't just track the identity of users who log on to the systems but also what information or record the user has accessed. For example, family members, neighbour and workgroup members. Incidents are automatically reported in real time to managers, enabling health organisations to be proactive and timely in how they address the issue.

Information governance capabilities and privacy policies are also supported as the solution streamlines patient privacy investigations and provides:

- Centralised privacy investigations
- Proactive monitoring and alerts based on customised rules and filters
- Enforcement of compliance policies
- Identification of areas with the most potential for non-compliance
- Tracks issues to resolution
- Reporting and accounting of disclosures.

Key Benefits

- Improved data security
- Improved patient confidence
- Supports proactive approach to data security
- Reduce privacy incident rates
- Reduced costs and resources

"The introduction of FairWarning as an addition to our existing capabilities has allowed us to significantly move ahead as we strive to ensure compliance with the DPA and provide assurance to our patients that their data is in safe hands."

Martin Egan,
NHS Lothian, Director of eHealth

Capita Managed IT Solutions Hillview House, 61 Church Road, Newtownabbey, BT36 7LQ Tel: 0289085 9085 mits@capita.co.uk www.capita-mits.co.uk