OPTUM®

Microsoft CERTIFIED Partner

Security Manager

Broader access to greater amounts of patient health information improves operations and patient safety, but the increased availability of this data also invites risk.

Manage users and monitor suspect behavior

Optum® Security Manager is a component of Optum Data Exchange Manager and leverages its existing ETL framework to consolidate data from the practice management system and other enterprise applications into a single data model for reporting. Optum Security Manager offers a single application for IT to manage users and for the security office to monitor suspect behavior. Security Manager can help organizations:

- Manage workforce security for HIPAA compliance
- Analyze roles and rights to optimize staff productivity
- Respond quickly to access anomalies

HIPAA compliance

To comply with HIPAA regulations, medical organizations must effectively manage and monitor access to patient information across multiple applications and departments. The three key concerns for each system are identifying what protected health information (PHI) is being accessed, which users are accessing it, and the roles and privileges of these users.

The strength of Optum Security Manager lies in its data model. The base data from each system is unified into two simplified data structures representing user access of PHI and user rights in the enterprise: user events and user configuration.

Optum Security Manager enables effective analysis of user access rights and use of patient data.

The challenge lies in the intersection of patients and users across the enterprise. While all platforms allow for management of user access and provide a degree of date/time stamping for access to information, these disparate systems do not offer a standard method by which to view permissions and user exercise of those permissions. Optum Security Manager facilitates extraction and load of data from leading practice management and EMR systems and transforms data into a standard dataset for proactive analysis of user privileges.

User events

User events are records of user activity and access to patient information across systems, capturing what patient information has been viewed or modified as well as log-in and log-out activity. From this data, security managers can produce reports detailing what individual users saw or did and filter by patient to show who accessed individual information. This analysis is essential for HIPAA privacy compliance.

User configuration

User configuration includes records of user access rights and permissions across various systems. Reports and views of this data let IT manage user roles and rights as a part of their HIPAA security compliance plan.

For clients using Optum Data Exchange Manager, the components of the Optum Security Manager module deliver a dataset based on their existing practice management system data that is designed for HIPAA compliance. Adapters allow data from other enterprise systems to be included in the Security Manager database.

Major components of Optum Security Manager software

- **Data Exchange Manager data extractor:** collects security plus patient confidentiality and other related data permission and access event data from the system
- **Adapter:** collects or receives user event and configuration data from other applications (e.g., web framework, LDAP and Epic) and prepares them for load into the database
- **Data Exchange Manager auto loader:** executes load and transformation scripts and parses log files, sending email notifications when loads complete or errors occur

Control access and protect patient rights

For more information:
Email: gwsupport@optum.com
Visit: optum360.com/optimize

OPTUM®
optum360.com

11000 Optum Circle, Eden Prairie, MN 55344