

FairWarning®

Healthcare Privacy Auditing in a Mixed Application Environment

February 18, 2009

Trust but Verify®

<http://www.FairWarningAudit.com>

info@FairWarningAudit.com

727 576 6700 x115 U.S.A.

Biography – Chuck Burbank

- 29 years experience in Healthcare
- Involved with various aspects of HIPAA since 2002
- Certified HIPAA Professional
- Certified HIPAA Security Specialist

Our Environment

Wide spectrum of applications from multiple vendors that create, store and allow access to Protected Health Information (PHI), such as:

- McKesson STAR
- McKesson Clinical Horizons (Care Manager)
- McKesson Physician Portal
- McKesson Meds Manager
- McKesson HMI PACS
- MedPlus - Chartmaxx
- PICIS
- SIS (Surgical Information System)
- GE Healthcare's Centricity Ultra Lab
- Heartlab

Challenges of Auditing in a Multi-System mixed environment

- Difficult to search across all the systems
- Significant time delay in obtaining audit logs
- Difficulty finding audit logs in some systems
- Vendors were not always willing to share how to locate audit information

Challenges of Auditing (cont.)

- Vendor fees to access the audit logs
- Logs from different applications often in different formats
- Logs provided not in user friendly format and often times not in a searchable format.
- Limited in how you could search

Random Audits in the Past

- Monthly obtained a list of patients by facility broken down into 3 categories, VIP, employees and others.
- Select patients from each facility and category randomly and requested audit logs.
- IT would provide audit logs
- Attempt to determine if any inappropriate access occurred.
- Contact the appropriate manager if there was suspicious activity to determine if there was a legitimate reason for the activity.
- H.R. was hesitant to act because of the time delay

Investigations in the Past

- Time delays in finding and obtaining logs
- Formatting and reading challenges
- Supervisors remembering events
- H.R. being hesitant to act.
- Manual and time consuming

The Frustration

- We lacked an effective audit program, and the attitude was that it was just too hard to create one so we simply performed a bare minimum number of random audits

Drive to Change

- Due to a changing environment there was increased pressure to expand our surveillance efforts.

Some of the drivers were:

- Increased public awareness due to media stories about breaches
- New risk imposed as states enact tougher privacy and security legislation

Criteria for Solution

- Ability to audit across multiple sources
- Ability to search by patient name, user name, and user ID. Additionally desired to be able to search by MRN and account #.
- Automated concerning the data sources (less labor intensive)
- Real time or close to real time
- Possibility of automating some audit functions such as VIP monitoring

Obtaining the Solution

- Identified possible solutions
- Arranged demonstrations
- Made a final selection
- Obtained approval for purchasing the tool
- Signed a BAA and purchase agreement
- Developed with the vendor an implementation plan

The Solution

FairWarning was chosen, and here are some of the reasons why:

- Allows as many audit sources as we desire
- Willingness to provided us with contacts for existing customers that we could contact.
- Allows automated monitoring of such things as VIP access, Family snooping, Questionable practices by billing and registration staff, possible attempts to gain access through obtaining employee's or physician's user id.

The Solution (cont.)

- Real time or almost real time auditing and investigation capability
- Ability to search across some or all audit sources by multiple fields
- A multitude of canned reports available for most audit sources
- Excellent customer service

Auditing Now

- Weekly Audits
- Random patient list and search across multiple audit sources
- Utilize user ID reports to look for suspicious activity
- Ability to search by terminal (ie. terminal on 12th floor is accessing patient on 20th floor)
- Ability to monitor what is being remote accessed

Auditing Now (cont.)

- Last name = last name searches
- On demand investigations based on complaint received or report by an employee.
- Approved templates to notify managers and H.R. of violations.
- Approved tiered sanction policy.
- Email notifications when an automated policy is triggered

Questions

- Submit questions electronically using the Q&A feature
- Email me directly at charles.burbank@yahoo.com



FairWarning® Privacy Surveillance

John Anderson
Director, Solutions Management

February 18, 2009

FairWarning® Privacy Surveillance

The Challenge

- Patient Health Information must be accessible by a wide range of specialized healthcare personnel
- The hospital must operate with patient safety as the number one priority
- The more people who have access to the information, the more risk the organization assumes
- Auditing access is an application-dependant, time-consuming process

FairWarning® Privacy Surveillance Privacy Incidents (1H2008)

- **New York-Presbyterian Medical Center* - New York City, New York**
 - ▶ Patients' names, phone numbers, and in some cases social security numbers were stolen by an admissions department employee and sold to organized crime groups focused on identity theft. *[Name redacted]* was arrested.
- **UCLA Medical Center* - Los Angeles, California**
 - ▶ An employee accessed actress Farah Fawcett's cancer treatment records. The employee was fired, because treatment details were leaked to the Enquirer and the Globe.
 - ▶ Another story reported that the employee snooped on 61 patients files, all told. (Note: all counted as 1 incident with multiple affected/victims). She was indicted and charged with obtaining and selling information to an unnamed media outlet. Three UCLA facilities were cited by the California Dept. of Public Health. 14 more employees were subsequently cited.

Healthcare privacy incidents damage patient lives and harm the trust they have in our healthcare institutions.

FairWarning® Privacy Surveillance Appliance-based Solution

- Turn-key privacy auditing solution which provides
 - ▶ Compliance automation
 - ▶ Policy-based filtering & alerting
 - ▶ Ad hoc reporting
 - ▶ Audit support for both patient & user investigations
 - ▶ Master audit repository
- The solution is non-invasive and is capable of scaling with the needs of the institution



Multi-U configurations available

FairWarning® Privacy Surveillance McKesson Applications Supported

- STAR
- Star Audit
- Pathways Healthcare Scheduling
- Horizon Clinical Infrastructure
- Horizon Patient Folder
- Horizon Meds Manager
- Horizon Expert Documentation
- Horizon Lab
- Horizon Care Record
- Horizon Emergency Care
- Horizon Surgical Manager
- Horizon Medical Imaging (PACS)
- Horizon Radiology Manager
- HealthQuest
- Series
- Horizon Physician Portal

BACKUPS

Questions?

Submit a question through the Q&A window on your screen or,
email johnv.anderson@mckesson.com

Entity-wide Plan

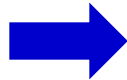
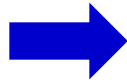
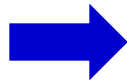
Drivers

HIPAA REQUIRED.
PHI Information system activity review. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports

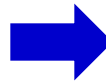
HIPAA REQUIRED.
Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

HIPAA REQUIRED.
Risk management. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level

Patient privacy risks
Return on investment



FAIRWARNING



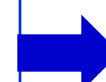
Functional Results

- Investigate & mitigate damages of suspected patient and user incidents

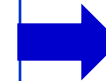
- Detect, track, deter and report vulnerabilities:
 - Medical identity theft
 - Co-worker snooping
 - VIP snooping
 - Neighbor snooping
 - Many other scenarios

- Breach notifications

- Accounting of disclosures



HIPAA REQUIRED.
Sanction policy. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.



HIPAA STANDARD.
Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

