Cerner High-Availability Privacy Auditing with FairWarning®

Overview

Memorial Hermann Healthcare System is the largest not-for-profit healthcare system in Texas with a vast network of affiliated physicians and numerous specialty programs and services. Memorial Hermann’s Texas Medical Center is the teaching hospital for The University of Texas Medical School at Houston. With close to 20,000 employees, more than 3,500 beds and the largest emergency department in the country, Memorial Hermann considers their reputation to be a key part of their success.

With a variety of hospitals and treatment centers, including a Level 1 Trauma Center, cancer centers, sports medicine and rehabilitation, and many others, Memorial Hermann’s electronic health records (EHRs) and clinical applications include 128 different systems with over 100 patient-related data systems. Their primary EHR is Cerner Millennium, but they also use McKesson for patient management, GE for labor and delivery, and CGI Sovera for imaging.

Challenges

With Cerner as their primary EHR, Memorial Hermann had selected to use Cerner’s P2 Sentinel product for proactive privacy monitoring. However, with hundreds of other systems, Memorial Hermann was concerned that they would not be in compliance with HIPAA and ARRA HITECH unless they expanded their monitoring capabilities to include the other systems.

At the same time, Information Security was getting feedback from the primary users, the Privacy department, that P2 Sentinel was unable to provide the desired reporting and perform the advanced analytics the Privacy department needed.

“We didn’t have the ability or the understanding to manage and slice the data to provide reporting,” says Randy Yates, Director of Information Security.

Organization

- 12 Hospitals
- 3,514 beds
- 19,500 Employees
- U.S. News Top Hospital 2009-2010

Health Information Systems

- ArcSight Enterprise Security Manager
- Cerner Millennium
- CGI Sovera
- GE Quantative Sentinel
- McKesson HealthQuest

Interviewee

- Randy Yates, Director of Information Security

Webinar Replay

For more details on Memorial Hermann’s implementation and use of FairWarning®, please view the webinar replay.

Date: January 20, 2011

Link:
**Solution**

With ARRA HITECH requirements and Meaningful Use deadlines fast approaching, Memorial Hermann made the decision to seek another solution that would fulfill all of their patient privacy auditing and monitoring requirements:

- Reporting across all clinical applications
- Proactive breach detection
- Advanced analytics with filtering using HR data, staff location, etc.
- Fulfillment of Meaningful Use Stage 1 core criteria

While in the market researching alternative solutions, Memorial Hermann consistently heard of FairWarning® privacy breach detection. In fact, other IT employees had already had experience implementing FairWarning® at other hospitals, as had Randy Yates' peers at other institutions. Memorial Hermann decided to evaluate FairWarning® compared to their current P2 Sentinel solution, with the evaluation including product demonstrations, vigorous testing, and ultimately proving FairWarning® was scalable and had the processing power to well-handle high volumes of audit log data.

At the same time, Memorial Hermann was evaluating Security Information and Event Management (SIEM) solutions for infrastructure logs. They considered whether they could use one solution to do both infrastructure and application layer audit log reporting; However quickly realized that these are two very distinct processes, with different data elements, different end users, and different purposes. Memorial Hermann chose to implement ArcSight as the best solution for infrastructure, FairWarning® as the best in privacy monitoring at the application layer, and were pleased the two solutions work together in cooperative correlation for incident investigation. Finally, FairWarning®’s relationship with Hewlett Packard, and the ability to deliver the solution on high powered HP appliance servers, gave Memorial Hermann confidence that they were making the right decision.

**Implementation Experience**

In creating the architecture to enable privacy breach detection as well as HIPAA compliance, Randy Yates considered the following:

- How long does audit log data need to remain available?
- How many years of past data should be loaded in initially?
- Where is data archived?
- How long must audit log data be kept to fulfill regulatory requirements?
- Is data redundancy required in case a server is unavailable for a period?

“FairWarning® was more than willing to engage with us in defining our data flows and creating the architecture,” says Yates. Memorial Hermann chose to create a high-availability environment to be confident that they would have uninterrupted privacy breach monitoring, running a primary appliance server for processing and a secondary FairWarning® appliance server for fully functional fail-over capabilities. Both servers have the same Cerner Millennium XML listener capabilities, as well as file-writing, file-cutting, and file management capabilities. Memorial Hermann keeps three years of audit log data available within the system, and six years available on their back-up SAN database.

“FairWarning® already knew how to retrieve the audit logs from our various systems, and what to do with the data, which was very attractive.”

- Randy Yates, Director of Information Security

“At the end of the day, the Privacy Officers were satisfied that FairWarning® had better reporting.”

- Randy Yates, Director of Information Security
We’ve been really happy with the interaction between Cerner and FairWarning, and the ability to switch back and forth between those two servers when necessary," says Yates who plans to leverage the fully functional fail-over capabilities in cases of interruption in service due to a network problem or routine maintenance.

Results
Today, FairWarning processes more than 200,000 events per hour, or nearly 6GB of data each day, providing Memorial Hermann Privacy and Security users proactive, automated alerting of potential privacy breaches.

Memorial Hermann is proactively monitoring activities within Cerner Millennium as well as GE PACS and CGI Sovera. They also plan to begin auditing GE Quantitative Sentinel and McKesson HealthQuest in the near future, using FairWarning’s advanced analytics and filtering capabilities.

“FairWarning already knew how to retrieve the audit logs from our various systems, and what to do with the data, which was very attractive,” says Yates.

About FairWarning
FairWarning invented and is the global leader in patient privacy monitoring solutions which guard against abuse of patient information in Electronic Health Records (EHRs) and Health Information Exchanges (HIEs), enabling care providers to confidently connect physicians, clinics, patients and affiliates.

FairWarning’s patient privacy monitoring solutions are compatible with healthcare applications from every major vendor, and available as either on-premise or software-as-a-service with managed services available to complement existing resources.

Customers consider FairWarning solutions essential for compliance with healthcare privacy regulations such as ARRA HITECH privacy and meaningful use criteria, HIPAA, EU Data Protection, UK Freedom of Information Act, California SB 541 and AB 211, Texas HB 300, Massachusetts 201 CMR 17.00 and Canadian provincial healthcare privacy law.

Solutions@FairWarning.com
www.FairWarning.com

North America Headquarters
13535 Feather Sound Drive, Suite 600
Clearwater, Florida 33762 USA
1-727-576-6700

United Kingdom & Europe
Oxford House, Campus Six
Caxton Way, Stevenage
Herts SG1 2XD
+44 0800 047 0933