CUSTOMER SUCCESS STORY

The Detroit Medical Center's Deployment of Privacy Breach Detection

Overview

The hospitals of the Detroit Medical Center (DMC) in Detroit, Michigan have been providing medical services to the Detroit metropolitan area since the 1860s. Now the largest healthcare provider in southeast Michigan, DMC has more than 2,000 licensed beds and close to 4,000 affiliated physicians.

DMC believes that access to quality health care is the right of every human being and has a long history of using advanced technology to provide the best clinical care. As an award-winning hospital in the areas of electronic health records (EHRs) and healthcare technology, they have an ongoing commitment to the privacy and security of electronic patient records.

In addition, DMC serves as a teaching hospital for Wayne State University, the United States' fourth-largest medical school, and is the official healthcare provider for the Detroit Tigers, Detroit Red Wings and Detroit Pistons. These prestigious areas of service, with a strong reputation to uphold, have prompted DMC to place a premium on protecting patients' privacy.

Challenges

DMC undertook the implementation of a broad-scale EHR in 1998, a project that would last twelve years and culminate in the 2010 achievement of Stage 6 in the HIMSS EMR Adoption Model. The new EHR rollout across hospitals and clinic locations brought new challenges in auditing the accesses of over 15,000 employees, and DMC increasingly recognized the need for privacy controls beyond existing capabilities. As the official healthcare provider for so many local sports teams, concerns over VIP snooping vulnerabilities prompted DMC to seek a privacy monitoring solution for Cerner Millennium. When ARRA HITECH of 2009 added privacy and security requirements for the achievement of "meaningful use" and financial incentives, finding a privacy auditing and monitoring solution became a top priority.

Organization

- Eight hospitals
- More than 100 clinics
- Teaching hospital for Wayne State University the country's fourth largest medical school
- More than 2,000 beds
- Official Healthcare Provider for the Detroit Tigers, Detroit Red Wings and Detroit Pistons

Awards

- U.S. News & World Report America's Best Hospitals, 2010-2011
- 2011 Most Wired Hospital (5th consecutive year)
- Acheived HIMSS EMR Adoption Model Stage 6 in 2010
- Healthcare Informatics 2009 Innovator Award

Health Information Systems

- Cerner Millennium
- Lawson HR
- Siemens Invision
- Sunquest Laboratory

Interviewees

- **Brenda Chambers**, HIPAA Security Officer
- **Karen Shastachuk**, Regulatory Data Analyst
  FairWarning® Ready Certified Master Professional

Solution

Once the need for a privacy auditing solution was identified, the team at DMC pulled together requirements, which included:

- Capable of fulfilling meaningful use requirements in combination with Cerner Millennium
- Providing compliance automation through automated alerting of potential privacy incidents via email
- Completing implementation of privacy auditing and monitoring within four months
- Allowing Compliance staff to create and save reports themselves, without involving IT
- Proven privacy auditing capabilities for:
  - Cerner Millennium
  - Siemens Invision
  - Sunquest (Misys) Laboratory

DMC also identified that the selected privacy breach detection solution must be able to provide an automated alert when specific behaviors occurred, such as employees accessing:

- Their own records (self-examination)
- A patient record with the same last name (family member snooping)
- A VIP patient record, such as a sports figure
- Any patient records after termination (former employees)

Finally, DMC wanted the ability to run stand-alone reports, including specific user audits showing all activity by a user within a certain date rang.

Ultimately, Detroit Medical Center chose FairWarning® privacy breach detection based on the strength of its 200+ privacy breach detection analytics, production customer references, and compatibility with over 180 healthcare applications.

Implementation Experience

Led by their assigned FairWarning® implementation manager, Detroit Medical Center moved through the FairWarning® implementation process quickly. Beginning with Sunquest Laboratory, DMC then began feeding Cerner Millennium and Siemens Invision audit logs into FairWarning.® The whole process from initial data extraction using scripts provided by FairWarning® to online training and report configuration was completed in less than 90 days.

Results

Prior to the implementation of FairWarning,® the Regulatory staff at Detroit Medical center was conducting all of their required HIPAA auditing activities manually. Each month, a pre-determined number of patients was selected for audit, and all accesses to those records were checked to ensure that there was a legitimate need for access. With over a million records in the system, this method was hit-or-miss, and very few privacy breaches were being identified. Most potential breaches were identified as a result of a patient complaint, and the resulting investigations were time-consuming and tedious.

"Before FairWarning,® employees did not believe their accesses were being monitored. Now they do."

-Brenda Chambers, HIPAA Security Officer

Detroit Medical Center

CUSTOMER SUCCESS STORY

Today, FairWarning®'s automated alerting capabilities have replaced random auditing, fulfilled key requirements for the achievement of meaningful use, and the staff is confident that they are proactively identifying potential privacy breaches. DMC has reduced the number of potential privacy breaches through a combination of continuous improvement of FairWarning® monitoring and employee education and training.

The Regulatory team has continued to refine the reports provided by FairWarning® and has expanded their initial list of reports to include employees viewing their supervisors' and co-workers' records. Using employee data from their Lawson HR system, DMC customized their family member snooping reports to identify employees accessing patients with the same address as their own. The additional user data also allows for advanced filtering and analytics, minimizing the number of false positives received.

Initially, FairWarning® was alerting on a higher number of potential privacy breaches; however, as education, training and sanctioning processes have been refined, fewer and fewer violations are being identified. During the FairWarning® rollout, information about the new monitoring system was included in each hospital's individual newsletter and the electronic DMC newsletter. In addition, managers were trained about the system's capabilities, and a screensaver notified employees that they were being monitored.

Additionally, through word-of-mouth, employees are aware that their access is being monitored, and that any violators will be disciplined. The Regulatory team is even taking advantage of the hospitals' competitive nature, providing privacy reports for each so they can see how they are performing in comparison to other hospitals in the system. Since the FairWarning® implementation, most investigations occur as a result of an automated alert, and so any violations are identified quickly before they escalate to a patient complaint.

As originally planned, FairWarning has been an integral piece of Detroit Medical Center's successful Stage 1 meaningful use attestation. Going forward, Detroit Medical Center will continue to refine and improve the automated monitoring provided by FairWarning,® fulfilling their commitment to protecting patient privacy.

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.

FAIRWARNING.

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