

# Sun and FairWarning

## Healthcare privacy surveillance solutions



### Highlights

- Automate many Health Insurance Portability and Accountability Act (HIPAA), FTC “Red Flags” Rule, and state-level privacy and security requirements to reduce patient and compliance risks
- Streamline incident investigations involving patients and users across all applications
- Eliminate laborious, expensive, and error-prone manual audit reviews
- Reduce privacy incident rates and respond rapidly and thoroughly to patient privacy inquiries
- Realize a strong ROI in resources (dollars and personnel) and risk mitigation
- Take advantage of the affordability, scalability, and performance of FairWarning on Sun to meet privacy surveillance needs regardless of healthcare organization size



Increased regulatory enforcement and a number of high profile snooping and identity theft incidents are driving healthcare providers to increase their efforts to protect the confidentiality and security of patient information in Electronic Health Records (EHR). Manual compliance can be costly and laborious, but violations create significant risk for healthcare organizations. FairWarning on Sun provides a turnkey appliance for patient privacy and security auditing that enables healthcare providers to automate compliance policies, reducing institutional risk and the cost and time required for compliance and incident investigations.

FairWarning is one of the world’s leading suppliers of privacy surveillance solutions for Electronic Health Records, focusing on proactive privacy and security auditing across multiple healthcare applications. FairWarning provides all-inclusive, appliance-based solutions, using Sun hardware and MySQL™ database, for detecting behavior-based privacy and security violations.

### Patient privacy incidents are a growing risk

The healthcare industry is experiencing an epidemic of high profile privacy incidents involving employees and affiliates using EHRs to conduct unlawful activities such as VIP record snooping, identity theft, and medical identity theft. These incidents have serious consequences for both the patients and institutions involved — government penalties, breach of patient trust, and organizational and executive liability.

Healthcare providers are recognizing that establishing and sustaining procedures for detecting and deterring anticipated risks are responsibilities mandated by HIPAA, the Federal Trade Commission’s (FTC) “Red Flags” Rule, and state level legislation (currently over 40 states have data privacy laws).

### Meeting regulatory requirements is costly

The primary drivers for increased privacy and security auditing are the enforcement of provisions of HIPAA, the FTC “Red Flags” Rule, and the increasing amount of state level legislation. The FTC’s Red Flags Rule took effect on January 1, 2008, and requires healthcare providers to develop a program to prevent, detect, and minimize the damage from identity theft. Compliance with any of these requirements, if performed manually, can require thousands of hours per year, resulting in significant overhead expenses. However, non-compliance can be much more expensive, due to penalties and legal costs.

Manual investigations and audit reviews can be laborious and error prone as well as expensive, especially when multiple audit log sources are involved. FairWarning streamlines incident investigations involving patients and users across all applications that have access to Patient Health Information. FairWarning supports and centralizes audit logs from a myriad of healthcare applications from every major EHR vendor, including Allscripts, Cerner, Eclipsys, Epic, GE, McKesson, MEDITECH, Misys, Siemens, and many others. The collection of audit log information and correlation with security events is automated, and ad hoc queries can be created, saved, and shared.

### FairWarning privacy surveillance

FairWarning automates common HIPAA best practices involving 164.306, 164.308, and 164.312. It has also developed specific Red Flag best practices to help customers complete aspects of an identity theft program. FairWarning systematically identifies users who are engaging in patient access patterns that are indicative of snooping, identity theft, or other risky behaviors. Privacy surveillance is performed for all crucial EHRs and applications that provide access to protected information. Privacy surveillance filters out known false positives, and brings any remaining potential incidents to the attention of appropriate privacy personnel.

FairWarning supports and centralizes audit logs from healthcare applications from every major EHR vendor, as well as logs from Windows and UNIX® servers, VPNs, and content filtering systems. It incorporates individual audit logs into a centralized user interface, providing the mechanism to create a proactive solution, not just a reactive one. Ad hoc queries can be created based on unlimited fields and criteria. New audit sources can be added in a matter of hours.

Manual processes are slow, expensive, and highly complex, and are usually conducted only when there is an incident or pending event, interrupting the normal work of security and compliance administrators. FairWarning provides a significant (10X) reduction in privacy audit review time and labor costs, and increases the visibility of internal privacy incidents by 5 times.

### FairWarning on Sun provides turnkey performance

FairWarning provides a turnkey appliance running FairWarning software on Sun Fire™ servers, using MySQL database as the onboard data store. Sun Fire servers provide enterprise-class performance and reliability in an affordable, energy-efficient design, with comprehensive, easy-to-use system management and monitoring built in. FairWarning also relies on MySQL database as a high-performance and scalable database — they found no other database offering that could compete with MySQL database's price, performance, and functionality.

Designed for growth and scalability, Sun Fire servers take advantage of open source technologies and open standards, and enable FairWarning to offer its comprehensive privacy surveillance solution to the full spectrum of healthcare providers — from smaller community hospitals to the largest multifacility institutions.

### Proactive privacy protection at MemorialCare

MemorialCare, a major Southern California healthcare provider, has implemented a proactive privacy solution by deploying FairWarning privacy surveillance software, enabling them to pursue an aggressive electronic health record initiative.

FairWarning's focus on the healthcare industry and its support for all leading electronic health record applications led to a successful proof-of-concept utilizing all of MemorialCare's mission-critical audit sources.

### Learn More

To learn more, visit [sun.com](http://sun.com), [www.fairwarningaudit.com](http://www.fairwarningaudit.com), or contact your Sun sales representative.

FairWarning then automated existing deployment processes that leverage remote technologies, helping to ensure consistent, cost efficient deployments. FairWarning filters millions of auditable transactions daily at MemorialCare, and has met or exceeded every performance and scalability expectation.

### Sun and FairWarning

FairWarning provides an affordable, all-inclusive, out-of-the box solution that automates privacy auditing, streamlines incident investigations, and centralizes a healthcare organization's mission-critical healthcare audit logs.

FairWarning solutions, running on Sun Fire servers with MySQL database as the data store, offer the scalability, high performance, and affordability required by healthcare providers of all sizes, enabling these organizations to proactively prevent, detect, and correct security violations, and to cost-effectively meet the regulatory compliance demands related to the privacy and security of patient data. FairWarning can handle millions of auditable transactions per day from multiple healthcare applications, aggregating, searching, and reporting on terabytes of patient data, and can scale to meet the needs of the largest healthcare providers.

**FAIRWARNING**

**Sun Microsystems, Inc.** 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** [sun.com](http://sun.com)

Copyright © 2008 Sun Microsystems, Inc. All right reserved. Sun, Sun Microsystems, the Sun logo, MySQL, Solaris, and Sun Fire are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the United States and other countries. Information subject to change. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd. All other product names mentioned herein are the trademarks of their respective owners. Printed in USA

