Security and Privacy of Electronic Medical Records

McAfee® SIEM and FairWarning team up to deliver a unified solution
Table of Contents

Executive Overview 3
Healthcare Privacy and Security Drivers 3
Healthcare Privacy Responsiveness 4
Clinical Application Privacy and IT Infrastructure Security 4
The Conventional Approach—Separate Privacy Monitoring and SIEM 4
Unifying Privacy and Security Information Management Functions 5
McAfee SIEM and FairWarning—The Best of Both Worlds 5
Conclusion 7
Executive Overview
Until now, most healthcare providers have treated application security and infrastructure security independently. Patient confidentiality continues to grow as a leading concern for healthcare organizations. Government regulations, electronic health records, and new Internet health services create a myriad of security challenges for healthcare compliance and information security teams. Security management needs to change to provide value, visibility, and viable information to keep this information protected.

Privacy and compliance teams continue use special-purpose solutions to protect patient privacy and monitor compliance with government regulations. Information security personnel use SIEM solutions to monitor and secure the IT infrastructure. This disjointed approach is inefficient and exploitable by insiders and outside threats. To alleviate these concerns, healthcare providers must secure access to clinical applications and protect the underlying IT infrastructure from misuse by insiders, hackers, and identity thieves.

McAfee and FairWarning have teamed to deliver a comprehensive electronic health record (EHR)-privacy monitoring and security solution specialized for this industry. The integrated platform combines FairWarning’s market-leading clinical application privacy monitoring capabilities with award-winning McAfee® network and system infrastructure security information and event management (SIEM) solution.

The unified solution helps healthcare providers eliminate operational inefficiencies and detect and contain risk and privacy issues. Now clinical applications and underlying IT infrastructure can be monitoring jointly and trigger on issues that may negatively affect compliance and privacy mandates and provide first alerts to potential cyberattacks.

Healthcare Privacy and Security Drivers
Patient privacy is a major issue for today’s healthcare providers. Safeguarding the confidentiality, integrity, and availability of patient information is no longer a goal—it is a legal requirement. Keeping pace with ever-expanding government regulations is an expensive and resource-intensive proposition. The adoption of new technologies, such as electronic health records (EHRs) and on-line personal health services, makes the task even more difficult.

Challenges faced by healthcare providers
Proliferation of healthcare regulations
- HIPAA—The Health Insurance Portability and Accountability Act (HIPAA) protects the privacy of an individual’s health information and governs the way healthcare providers manage and disclose protected health information (PHI). Healthcare providers must introduce appropriate systems and practices to comply with HIPAA.
- ARRA-HITECH—The Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of the American Recovery and Reinvestment Act (ARRA) expand HIPAA privacy requirements and create new challenges for healthcare privacy and security teams. In particular, the act introduces new regulations governing the confidentiality of EHRs.
- FTC Red Flags Rule—The Federal Trade Commission (FTC) Red Flags Rule require healthcare providers to institute new systems and practices to combat identity theft. Providers have until June 1, 2010 to comply with this law.
- State laws—US healthcare providers must abide by both federal and state regulations. Forty-five states have enacted privacy breach notification laws, many of which are more stringent than federal laws.
Integrated Privacy Monitoring and SIEM Applications

- **Regulatory compliance**—Federal and state laws (HIPAA, FTC Identity Theft, California AB 211, and California SB 541) require healthcare providers to tightly monitor and control access to medical records, IT systems, and clinical applications.
- **Investigations and audits**—Healthcare providers must archive patient, user, physician, consultant, and contractor records for investigations and audits.
- **Privacy assurance monitoring**—Numerous healthcare personnel, including registration and accounting personnel, nurses, physicians, and technicians have access to a patient’s records. Providers must find innovative ways to protect patient privacy without blocking legitimate access to medical records or impairing patient safety.
- **Identity theft protection**—EHRs and online personal health services open new doors for hackers and identity thieves. Healthcare providers must detect and curtail identity theft plus introduce systems and practices to comply with the FTC Red Flags Rule.
- **Incident response and remediation**—Compliance and information security teams must identify and contain internal and external security threats as quickly as possible to minimize exposure and mitigate risk.
- **International regulations**—Healthcare privacy rules are not limited to the United States. The European Union and many individual countries and provinces in other parts of the world have implemented patient confidentiality laws.
- **Adoption of electronic health records**—Healthcare organizations are implementing EHRs to bolster patient safety and care, increase efficiencies, and improve the exchange of information. New systems and practices are needed to protect the privacy and security of EHRs and ensure compliance with ARRA-HITECH and other electronic record keeping regulations.
- **Advent of online personal health record portal and services**—New web-based services offer a convenient way for individuals to manage their healthcare records online, but they raise privacy concerns and expose users to identity theft.

Healthcare Privacy Responsiveness

Patient privacy is a serious matter for healthcare providers and patients alike. Patients can suffer financial damage if their billing data (credit card numbers and Social Security numbers, for example) is stolen or emotional harm if their PHI is disclosed. Healthcare providers can face stiff fines and suffer damage to their reputation if their records or systems are compromised. Regulatory requirements have specific timelines in reporting breaches of more than 500 records to customers, government, and the media. According to the Ponemon Institute, a single lost healthcare record can cost an organization $240.1

There is continued pressure towards “as soon as possible” notification that must be weighed in measuring and evaluating the extent of the breach in terms of what privacy data was disclosed across the records in question. Having an integrated event management platform that looks at the applications and the supporting IT infrastructure gives quicker alerts to issues and is key to ascertaining and minimizing the scope of damage in a timely manner.

Clinical Application Privacy and IT Infrastructure Security

Protecting the confidentiality, integrity, and availability of patient information is a complex task. A foolproof solution must secure both the clinical applications and the underlying IT infrastructure.

Dozens of healthcare personnel—registration, accounting, nursing, physicians, technicians, and associates—have access to clinical applications. To safeguard patient privacy, healthcare providers must monitor access to applications and protect against inappropriate data disclosure without impeding legitimate use or obstructing patient care.

Application-layer surveillance alone is not sufficient. Providers must also monitor underlying IT systems, employee communications, and endpoints for policy violations. A rogue administrator can circumvent an application-centric privacy monitoring solution by accessing raw patient records from databases or network storage devices. Sensitive data can also be leaked via email, chat, removable media, or something as simple as printing patient records in a public area.

The Conventional Approach—Separate Privacy Monitoring and SIEM

Many healthcare providers treat privacy monitoring and infrastructure security independently. The functions are performed by separate teams using separate tools. Privacy and compliance teams use special-purpose privacy monitoring solutions to protect patient privacy and monitor compliance with government regulations. Privacy monitoring solutions focus on privacy violation scenarios.

IT infrastructure integrity is the responsibility of the IT security team. Information security personnel leverage security information and event management (SIEM) solutions to monitor and protect the IT infrastructure. SIEM platforms focus on network and system vulnerabilities and protect against both internal and external threats.
Unifying Privacy and Security Information Management Functions
Privacy and security are tightly intertwined. Treating privacy monitoring and security information management separately is inefficient and exploitable by insiders and outside threats. Both privacy officers and security officers need to meet the same regulations and both have a stake in ensuring patient privacy and the integrity of the healthcare systems. Yet what has been lacking is a common set of tools to identify and isolate threats and a way to correlate clinical application events with IT infrastructure events.

Healthcare providers can address application security and IT infrastructure security in a unified fashion with McAfee SIEM and FairWarning. This solution enables you to:

- Improve communications and collaboration
- Identify and contain threats more quickly and efficiently
- Recognize and remedy security gaps and business process deficiencies
- Improve compliance with government regulations
- Eliminate duplication of efforts for auditing and compliance reporting

<table>
<thead>
<tr>
<th>Privacy Monitoring</th>
<th>Security Information and Event Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>• Patient privacy</td>
</tr>
<tr>
<td></td>
<td>• Network and system security</td>
</tr>
<tr>
<td>Focus</td>
<td>• Internal threats</td>
</tr>
<tr>
<td></td>
<td>• Internal and external threats</td>
</tr>
<tr>
<td></td>
<td>• Clinical applications</td>
</tr>
<tr>
<td></td>
<td>• IT infrastructure</td>
</tr>
<tr>
<td>Examples</td>
<td>• Medical record snooping</td>
</tr>
<tr>
<td></td>
<td>• Malicious attacks (viruses, worms, Trojan horses)</td>
</tr>
<tr>
<td></td>
<td>• Internal identity theft</td>
</tr>
<tr>
<td></td>
<td>• External identity theft</td>
</tr>
<tr>
<td></td>
<td>• Eavesdropping</td>
</tr>
<tr>
<td>Audience</td>
<td>• Privacy and compliance personnel</td>
</tr>
<tr>
<td></td>
<td>• Information security personnel</td>
</tr>
<tr>
<td></td>
<td>• Business-oriented</td>
</tr>
<tr>
<td></td>
<td>• Technology-oriented</td>
</tr>
<tr>
<td>Audit Sources</td>
<td>• Clinical applications</td>
</tr>
<tr>
<td></td>
<td>• IDS, IPS, firewalls, AAA, switches, routers</td>
</tr>
<tr>
<td>Managed Attributes</td>
<td>• Patient, user, and department function codes</td>
</tr>
<tr>
<td></td>
<td>• IP addresses, MAC addresses, TCP/UDP ports</td>
</tr>
</tbody>
</table>

McAfee SIEM and FairWarning—The Best of Both Worlds
McAfee SIEM, the leading high-performance security information and compliance management solution, and FairWarning, the leader in healthcare privacy auditing solutions, have teamed to bring healthcare providers the industry's most advanced EHR privacy monitoring and security solution. The integrated solution combines the award-winning McAfee SIEM platform with FairWarning's market-leading privacy monitoring capabilities by adding support for FairWarning in the McAfee Enterprise Security Manager platform.

FairWarning brings full visibility of patient information, policies, and privacy violations to McAfee Enterprise Security Manager, where this information is then correlated and analyzed in real time, along with network security events from firewalls, hosts, databases, and applications. The result is a common platform for the detection, investigation, and response of healthcare security and privacy concerns.

FairWarning monitors clinical applications and systems to ensure patient privacy. McAfee SIEM monitors network devices and applications to protect against data loss and risk. Integrated into a common real-time interface, McAfee ESM and FairWarning privacy solutions provide early-warning notification to both privacy officers and information security analysts, simplifying the mitigation of privacy issues before they lead to noncompliance, or worse, lawsuits.
Integrated Solution Benefits

- Improve visibility into healthcare and clinical systems—patient records and policies; network, database, and application events
- Reduce compliance and legal exposure and minimize loss with a faster and more comprehensive early warning system
- Track policy violations to their source by correlating security logs and events with privacy alerts
- Improve security officer/privacy officer coordination, and reduce operational inefficiencies with a unified privacy and security platform

FairWarning privacy monitoring solutions are out-of-the-box compatible with more than 100 healthcare applications and bundled with more than 100 healthcare privacy analytic scenarios. McAfee SIEM solutions are compatible with more than 300 third-party sources (IDS/IPS, firewalls, switches, routers, and more) and include more than 200 predefined correlation rules for detecting infrastructure incidents and threats.

McAfee Enterprise Security Manager is the ideal platform for consolidating privacy monitoring and security information management functions. Built on top of the industry’s fastest data collection, management, and analytics engine, McAfee Enterprise Security Manager is able to look deeper into network and application activity and detect a broader range of threats with fewer false positives compared to alternative solutions.

McAfee Enterprise Security Manager extensions for FairWarning include:

- **Event integration**—Support for FairWarning privacy monitoring events
- **Custom views**—Dashboards for privacy officers
- **Consolidated reporting**—Unified privacy monitoring and security information event reporting
- **Detailed analysis**—Drill-down from privacy monitoring events to perform deep analysis

The integrated solution improves collaboration and communication between the privacy and security teams so they can solve problems more quickly and effectively. With a unified platform, security officers can correlate clinical application events (when application access exceeds the threshold) with network or system events (a suspicious email message or instant messaging session) for faster, more efficient threat resolution.

Let’s say FairWarning flags a user of a particular application who is snooping VIP records or accessing the records of a family member or neighbor. This information may not be enough to implicate the staff member because another staff member may have successfully guessed the password, or the account may have been taken over by an external hacker.

A privacy officer can’t determine if the offender was an authorized user or an external hacker. Without McAfee Enterprise Security Manager, the IT security team would have to pore over discrete system and event logs from various sources—operating systems, intrusion detection systems, and firewalls—hoping to pinpoint the attack.

With the integrated solution, a security administrator can readily correlate the privacy event with the network access point, and quickly drill down on consolidated McAfee SIEM network and system events for the suspected access point to identify the root offender.
Conclusion

Patient privacy is a serious concern for healthcare organizations. Protecting the confidentiality, integrity, and availability of patient information is a major undertaking. Ever-expanding government regulations and the adoption of EHRs are taxing privacy and security officers alike. By consolidating privacy monitoring and SIEM solutions, compliance and security teams can share information and work together to address application privacy and infrastructure security issues.

With the industry’s fastest data collection, management and analytics engine, McAfee ESM is the ideal platform for integrating privacy monitoring and security information management functions. The unified McAfee and FairWarning solution helps security officers and privacy officers work together to eliminate operational inefficiencies and detect and contain privacy issues before they impact compliance, trigger lawsuits, or become the first clues of undiscovered cyberattacks.