Executive Overview

Patient confidentiality is a growing 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. 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.

Until now most healthcare providers have treated application security and infrastructure security independently. Privacy and compliance teams 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.

NitroSecurity and FairWarning have teamed to deliver the industry’s most comprehensive EHR privacy monitoring and security solution. The integrated platform combines FairWarning’s market-leading clinical application privacy monitoring capabilities with NitroSecurity’s award-winning network and system infrastructure SIEM solution.

The unified solution helps healthcare providers eliminate operational inefficiencies, and detect and contain privacy issues before they impact compliance, trigger lawsuits or be the first clues of undiscovered cyber-attacks.
Introduction – Healthcare Privacy and Security

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.

Healthcare providers face a number of challenges:

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 health care 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 1st 2010 to comply with this law.

- **State Laws** – U.S. 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.

- **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.

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 - registration, accounting, nursing, physicians, technicians, and associates - 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 on-line 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.
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 On-line Personal Health Record Services

• New on-line services like Google Health and Microsoft Health Vault offer a convenient way for individuals to manage their healthcare records on-line, but they raise privacy concerns and expose users to identity theft.

Explosion of Global Healthcare Privacy Regulation

- HIPAA Audits – OIG January 2008
- HITECH/HIPAA February 2009
- FTC Red Flags Rule August 1st, 2009
- Massachusetts & Other State Laws

- Data Protection Act
- NHS IGT 206 & 302
- FOI Act

- Data Privacy Directive Refinements in Progress

Country by Country
- Privacy laws in Asia-Pacific & Middle-East that match Electronic Health Record adaptation
Healthcare Privacy Breach Examples

Patient privacy is a serious matter for healthcare providers and patients alike. Patients can suffer financial damage if their billing data (credit card number, social security number) is stolen or emotional harm if PHI is disclosed. Healthcare providers can face stiff fines and suffer damage to their reputation if their records or systems are compromised. Examples of privacy breaches include:

- **VIP record snooping** – disclosing a celebrity’s medical records. One notable case involved a UCLA Medical Center employee leaking Farah Fawcett’s cancer treatment records to the tabloids.

- **Financial identity theft** – stealing patient data for financial gain. An admissions clerk at the Baptist Health Medical Center in Little Rock, AR was recently accused of using stolen patient information to buy Wal-Mart gift cards. Approximately 1,800 patient records were exposed.

- **Medical identity theft** – using patient data to initiate bogus or inflated treatment claims, purchase prescription drugs, or obtain free medical treatment. Not long ago a front desk clerk at a Florida medical clinic downloaded information on more than 1,100 Medicare patients and gave it to a cousin who made $2.8 million in false Medicare claims.

- **Coworker, family member and neighbor snooping** – disclosing a patient’s medical records to an unauthorized person. In a recent investigative report CNN reporter Elizabeth Cohen was able to retrieve 18 months worth of medical records for colleague Gary Tuchman and his entire family in minutes – on live television – using only his date of birth and social security number.

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 end-points 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.
Conventional Approach to Protecting Patient Confidentiality – Separate Privacy Monitoring and SIEM Platforms

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 so treating privacy monitoring and security information management separately is inefficient and exploitable by insiders and outside threats. Privacy officers and security officers are both mandated by the same regulations and have a stake in ensuring patient privacy and integrity of systems. Yet they lack a common set of tools to identify and isolate threats and have no way to correlate clinical application events with IT infrastructure events. Their teams aren’t able to share information or collaborate effectively and they often waste time and resources working on the same problems in parallel.

By integrating privacy monitoring and SIEM systems healthcare providers can address application security and IT infrastructure security in a unified fashion. With an integrated solution privacy officers and security officers can:

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

<table>
<thead>
<tr>
<th>Privacy Monitoring</th>
<th>Security Information and Event Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>• Patient privacy</td>
</tr>
<tr>
<td><strong>Focus</strong></td>
<td>• Internal threats</td>
</tr>
<tr>
<td>• Clinical applications</td>
<td>• IT infrastructure</td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td>• Medical record snooping</td>
</tr>
<tr>
<td>• Internal identity theft</td>
<td>• External identity theft</td>
</tr>
<tr>
<td><strong>Audience</strong></td>
<td>• Privacy and compliance personnel</td>
</tr>
<tr>
<td>• Business-oriented</td>
<td>• Technology-oriented</td>
</tr>
<tr>
<td><strong>Audit Sources</strong></td>
<td>• Clinical applications</td>
</tr>
<tr>
<td><strong>Managed Attributes</strong></td>
<td>• Patients, users, departments,</td>
</tr>
<tr>
<td></td>
<td>function codes, etc.</td>
</tr>
</tbody>
</table>
NitroSecurity and FairWarning – Best of Both Worlds

NitroSecurity® – the leader in high-performance security information and compliance management solutions – 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 NitroSecurity’s award-winning SIEM platform with FairWarning’s market-leading privacy monitoring capabilities by adding support for FairWarning in NitroSecurity’s NitroView Enterprise Security Manager (ESM) platform.

FairWarning brings full visibility of patient information, policies and privacy violations into NitroView ESM, where this information is 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. NitroSecurity monitors network devices and applications to protect against data loss and risk. Integrated together into a common real-time interface, NitroView 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 non-compliance, or worse, lawsuits.

FairWarning privacy monitoring solutions are out-of-the-box compatible with over 100 healthcare applications and bundled with over 100 healthcare privacy analytic scenarios. NitroSecurity SIEM solutions are compatible with over 300 third-party sources (IDS/IPS, firewalls, switches, routers, etc.) and include over 200 pre-defined correlation rules for detecting infrastructure incidents and threats.
NitroView ESM 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, NitroView ESM 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.

NitroView ESM 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 (e.g. application access exceeded threshold) with network or system events (a suspicious email message or instant messaging session for example) for faster, more-efficient threat resolution.

Say FairWarning flags an application user 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 NitroView the IT security team would have to pore through discrete system and event logs from various sources – operating systems, intrusion detection systems, firewalls, etc – 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 NitroView network and system events for the suspected access point to identify the root offender.

### NitroSecurity/FairWarning 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
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, NitroView ESM is the ideal platform for integrating privacy monitoring and security information management functions. The unified NitroView/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 be the first clues of undiscovered cyber-attacks.

About NitroSecurity

NitroSecurity develops award-winning security information and compliance management solutions that protect business information and infrastructure. NitroSecurity solutions reduce business risk exposure and increase network and information availability by removing the scalability and performance limitations of security information management.

Utilizing the industry’s fastest analytical tools, NitroSecurity identifies, correlates and remedies threats in minutes instead of hours, allowing organizations to quickly mitigate risks to their information and infrastructure. NitroSecurity serves more than 500 enterprises across many vertical markets, including healthcare, education, financial services, government, retail, hospitality and managed services.

About FairWarning

FairWarning® is a leading supplier of privacy surveillance solutions for Electronic Health Records. FairWarning® patient privacy auditing and monitoring is essential for complying with recent privacy regulations such as ARRA HITECH / accounting of disclosures, FTC Red Flags Rule, HIPAA, California SB 541 & AB 211 and other State Laws, as well as UK & EU Data Protection Acts, NHS IGT guidelines and Canadian Provincial laws.

Healthcare’s leading organizations have deployed FairWarning® privacy surveillance solutions. FairWarning®’s production customers range in size from 1,000 to 70,000 users. FairWarning® customers represent nearly 300 hospitals and over 1,000 clinics in the United States, Canada and United Kingdom.