



Privacy Monitoring for Healthcare

*How to End Patient Health Information
Snooping and Identity Theft*

TABLE OF CONTENTS

Protecting Healthcare Information from Privacy Breaches	2
Why Healthcare Organizations are Vulnerable to Insider Incidents	2
Limitations of the Security “Laundry List”	3
What is Privacy Monitoring?	4
Why is Privacy Monitoring so Powerful?	5
Take The Next Step To Enforce Patient Privacy	5

PROTECTING HEALTHCARE INFORMATION FROM PRIVACY BREACHES

With the proliferation of electronic patient information, hospital administrators, compliance officers, privacy officers and information security officers are required to enforce patient privacy. Motivated by patient-citizen damages from increased healthcare privacy breaches, law-makers across the United States, Canada, and Europe have enacted new regulation protecting patient privacy and penalizing those involved. Snooping, identity theft and general inappropriate access of medical records are now explicitly prohibited. Additionally, a patient's right to know who has accessed their records has been expanded, requiring hospitals and their business associates to account and disclose for personal health information breaches. Beyond putting patients at risk, personal health information breaches are increasingly putting healthcare organizations at a significant risk of financial, and reputational harm.

“Deployment of robust processes to ensure privacy and security of electronic medical records is critical to achieving their widespread deployment. The American public will not accept failure when it comes to protecting their healthcare information from privacy breaches.”

—Barry P. Chaiken, MD, MPH, CMO DocsNetwork and HIMSS Chair, 2009-2010

Additionally, a patient's right to know who has accessed their records has been expanded, requiring hospitals and their business associates to account and disclose for personal health information breaches. Beyond putting patients at risk, personal health information breaches are increasingly putting healthcare organizations at a significant risk of financial, and reputational harm.

This whitepaper explores why healthcare is so vulnerable to “insider” privacy incidents and outlines why privacy monitoring is a required component of every entity-wide privacy and security program.

WHY HEALTHCARE ORGANIZATIONS ARE VULNERABLE TO INSIDER INCIDENTS

A patient's personal health information (PHI) must be accessible by an increasingly wide range of specialized healthcare personnel, including: Registration, Accounting, Nursing, Pharmacy, Physicians, Technicians, Partner Clinics, Partner Physicians and others. Compounding this wide-scale access is the fact that healthcare organizations must operate with patient safety as the number one priority. This means that generally access to patient records is granted to all clinical personnel that may need access which presents even greater privacy challenges. In no case can a limitation of access jeopardize the rendering of care. Lastly, EHRs are built with patient safety in mind, meaning their wide-scale access controls lack granularity. For technical and patient safety considerations, healthcare organizations find themselves unable to reel in access to patient information.

DAMAGING HEALTHCARE PRIVACY INCIDENTS

According to the October 2009 Ponemon report, Electronic Health Information at Risk: A Study of IT Practitioners, 80 percent of healthcare organizations surveyed had experienced at least one incident of lost or stolen electronic health information in the past year—four percent had more than five patient data breaches. More than two-thirds of these healthcare organizations had already digitized at least a quarter of their patient records, and a third had digitized more than half.

Below are just a few of the publicized incidents that have been in the news recently—there are many others not covered in the media or disclosed in states where disclosure is not mandatory.

- UCSF Medical Center—Information on patients was accessible on the Internet—Patients informed 6 months later
- New York-Presbyterian Hospital/Weill Cornell Medical Center—2000 patient records sold; 50,000 improperly accessed

- University Medical Center in Clark County—Internal resources sold the hospital’s daily registration forms for accident patients which includes names, birth dates, Social Security numbers and injuries —personal identification that can also be used for identity theft.
- NHS Hull - Unauthorised NHS employee accessed confidential electronic records without authorization using a smartcard.

LIMITATIONS OF THE SECURITY “LAUNDRY LIST”

The above incidents, as well as a series of preceding incidents occurring in prior years, forced the U.S. Federal and State governments to enforce privacy and security legislation, including HIPAA, more aggressively than in the past. This is motivating healthcare organizations to re-evaluate their security plan and technologies. A laundry list of security technologies ,all promising to deliver the silver bullet to stop insider security incidents in healthcare,can be purchased:

- **Encryption:** An essential component of any security and privacy program. Many healthcare organizations are implementing encryption on laptops since they can be carried off-site along with PHI. Encryption is not a factor in stopping insiders with authorized access to EHRs and applications.
- **Single Sign On (SSO):** SSO is a good addition for organizations wishing to enforce password policies and provide convenient login to applications. While important, SSO technology does not stop authorized users from abusing their access privileges.
- **Identity Management and Provisioning:** This technology assists with credentials management and fills a gap related to denying access to former employees (their userids are removed automatically). Identity management / provisioning does not stop active, authorized users from abusing their access privileges. Secondly, identity management / provisioning deployments can be lengthy and expensive.
- **Security Information Management (SIM):** SIM or SIEM technology collects information security events from infrastructure systems such as firewalls, routers, IPS, IDS, servers and VPNs. SIM technology was not designed to support EHRs and, in turn, they have a significant HIPAA compliance gap. A core HIPAA requirement mandates that all systems accessing PHI must be systematically reviewed and audited. Clearly, EHRs and healthcare applications access PHI and by definition must be reviewed and audited. SIM products do not curtail insider incidents involving EHRs and applications because they do not access EHR audit logs and were not designed to deal with concepts such as patients, users and function codes.

COMPLIANCE CONSIDERATIONS

HIPAA & HITECH Act

When the U.S. Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996, among the law’s many provisions was the establishment of formal regulations designed to protect the confidentiality and security of patient information. In February of 2009, with the passage of the HITECH Act (Health Information Technology for Economic and Clinical Health Act)—part of the American Recovery and Reinvestment Act—the U.S. Congress gave teeth to the HIPAA law. Because the HITECH Act mandates a massive expansion in the exchange of electronic protected health information (ePHI), it also broadens the scope of privacy and security protections available under HIPAA. The HITECH Act strengthens these privacy and security standards, expands the scope of accountability, and increases the penalties of HIPAA. HIPAA and HITECH compliance and reporting are now mandatory.

- Increasing civil penalties for HIPAA violations, according to a tiered scale, to a maximum of \$1.5 million per entity in a calendar year
- Requiring HHS to formally investigate and impose penalties for HIPAA violations that are due to “willful neglect”

- Requiring HHS to conduct audits to determine whether covered entities are complying with the law and to report the results to U.S. Congress
- Clarifying that employees of covered entities may be prosecuted for criminal violations
- Allowing state attorney generals to file suit in federal courts seeking civil damages on behalf of residents injured by HIPAA violations
- If initial complaint is confirmed by review, a full investigation must be conducted
- If initial complaint finds “willful neglect”, a civil monetary penalty will be imposed
- Individuals—not only organizations—will be held accountable

Without privacy monitoring, hospitals are non-compliant with key portions of HIPAA specifically with the mandates to:

- Systematically review and audit systems that access Protected Health Information
- Mitigate damages when there is reason to believe a patient privacy incident has occurred
- Take preventive measures against reasonably anticipated patient privacy incidents

State Laws

- **Missouri:** HB 62 includes many provisions that are similar to other state laws requiring notice to individuals when the security of their personal information has been compromised. HB 62 applies to the “typical” categories of personal information, including Social Security numbers, driver’s license numbers and information that would permit access to an individual’s financial accounts. However, unlike most other state data breach notification laws, HB 62 also applies to medical and health insurance information, including an individual’s medical history, mental or physical condition, treatment or diagnosis, health insurance policy number and any other unique identifier used by a health insurer.
- **Texas:** On June 19, 2009, Texas Governor Rick Perry signed House Bill 2004 (“HB 2004”), which expanded the scope of Texas’ data breach notification law to include public sector entities and health information. Specifically, HB 2004 amends the definition of “sensitive personal information” to include health care information, such as information about an individual’s physical or mental health or payment for health care services.
- **California:** Expanded disclosure law CA SB 1386 to include healthcare institutions, Governor Schwarzenegger has endorsed state laws that fine employees and other authorized users within a healthcare organization. Under the legislation healthcare workers who unlawfully view patient records would be fined from \$1,000 to \$250,000, depending on the seriousness of the violation. Hospitals and other health facilities would face fines of \$25,000 to \$250,000 for similar violations.

ISO 27000 - An International Security Standard

The ISO 27001 standard was published in October 2005, essentially replacing the old BS7799-2 standard. It is the specification for an ISMS, an Information Security Management System. The objective of the standard itself is to “provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System”. Regarding its adoption, this should be a strategic decision. The standard is similar to Legislations such as HIPAA, GLBA and Sarbanes-Oxley identify security requirements that are consistent with the ISO 17799 standard in many areas. The ISO 17799 standard provides a common framework for implementing IT security controls that map to the requirements of several regulations.

More information on new healthcare privacy laws by following the links below:

- [U.S. ARRA HITECH privacy provisions](#)
- [U.S. state disclosure laws \(45 states\)](#)
- [FTC Red Flags Rule, effective to healthcare, November 1, 2009](#)

- U.S. Whistle-Blower Lawsuit
- California Senate Bill 541, Assembly Bill 211
- Massachusetts Data Privacy, 201 CMR 17.00, effective January 1, 2010
- Canadian Provincial Laws
- Ontario's Freedom of Information and Protection of Privacy Act
- UK Information Commissioner's Office
- Less recent, but pertinent privacy laws include: HIPAA, PIPEDA, UK Data Protection Act and European Union Data Protection Directive

WHAT IS PRIVACY MONITORING?

Privacy monitoring systematically identifies users who are engaging in patient access patterns that are indicative of snooping, identity theft or other risky behaviors. Privacy monitoring is performed for all crucial EHRs and applications which provide access to Protected Health Information (PHI). Privacy monitoring filters out known false positives and brings any remaining potential incidents to the attention of appropriate privacy personnel. For organizations conducting tedious manual audit log reviews, privacy monitoring automates the work-load and is dramatically more comprehensive.

WHY IS PRIVACY MONITORING SO POWERFUL?

Essential to deterring and eliminating insider privacy incidents, is creating the right culture through technology, training and an entity-wide security plan. Privacy monitoring ties these concepts together to deliver sustainable privacy and compliance. Privacy officers in today's healthcare environment are "driving blind" without privacy monitoring. For example, patient complaints and employee tips are the primary methods in identifying potentially damaging incidents. Manual random privacy audits may help, but they are unreliable, incomplete and unsustainable.

TAKE THE NEXT STEP TO ENFORCE PATIENT PRIVACY

Imprivata's healthcare division delivers solutions to help hospitals gain control over their patient's data privacy exposure as they align with state/provincial and country legislations. Privacy officers can now be proactive in investigating and auditing personal health information breaches. Snooping, identity theft and general inappropriate access of medical records are quickly detected through Imprivata PrivacyAlert's automated pattern recognition, delivering alerts on 100+ patient privacy scenarios. Imprivata PrivacyAlert enables privacy officers, along with information security officers, to deploy automated and scalable privacy monitoring solutions that assist them in investigating and reporting on patient data privacy breaches. They can be relieved from the manual complexity of accessing, sorting and reporting audit trails associated with privacy breaches. Privacy officers can manage with ease all of the increasing regulatory mandated functions and perform required audits in a timely and scalable manner. More importantly, through the use of Imprivata PrivacyAlert, healthcare organizations can deter snooping and medical identity theft and ultimately establish a culture of privacy and compliance.

For more information about Imprivata Patient PrivacyAlert visit: www.imprivata.com



Offices In:
Belgium • Germany
Italy • Singapore
UK • USA

1 877 ONESIGN
1 781 674 2700
www.imprivata.com

WP-PS-Ver1-02-2010