



PROACTIVE PRIVACY BREACH MONITORING & COMPLIANCE AUTOMATION



IMPRIVATA PRIVACYALERT™ FOR HEALTHCARE

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.

ENFORCE PATIENT PRIVACY

The Imprivata 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 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 surveillance 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.

FEATURES OF IMPRIVATA PRIVACYALERT

- Out of the box support for all leading healthcare applications
- Easy-to-use Web-based interface appropriate for privacy, audit and information security personnel
- Compliance automation with support for filtering and alerting
- Policy engine which includes best practices from dozens of healthcare providers
- Streamline incident investigations involving patients and users across all of your applications
- Create, save and share ad hoc reports
- Create a forensically secure master audit log repository
- Massive scalability

BENEFITS OF IMPRIVATA PRIVACYALERT

- Automate [HIPAA](#) privacy and security auditing responsibilities
- Automate compliance activities for PCI, SOX and PIPEDA
- Mitigate legal risks relating to civil lawsuits resulting from unlawful exposure of protected health information
- Eliminate laborious manual audit log reviews
- Leverage privacy auditing best practices
- Mitigate the damage of suspected incidents by streamlining investigations
- Reinforce privacy and security awareness training

“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

OUT OF THE BOX DATA SUPPORT

- Cerner Millennium
- Eclipsys
- GE Centricity Enterprise
- GE Business Centricity
- GE PACS
- Keane
- Kronos
- Misys Laboratory
- Misys Radiology
- McKesson
- MEDITECH MAGIC
- MEDITECH Client/Server
- MedPlus ChartMaxx
- MercuryMD
- Siemens Invision
- T-Systems
- WellSoft Emergency DIS
- Many others including the ability to add in-house or boutique audit sources rapidly

TECHNICAL SPECIFICATIONS

Enterprise Server

- Sun Fire X4150 Server, Base System Equipped with 2 Quad-Core Intel Xeon E5450, 2 x 6 MB L2, 3.0 GHz, 1333 MHz FSB, 80W, Processor, 64 GB, PC2-5300 667 MHz ECC fully buffered DDR2 Memory, 4 x 146 GB 10000 rpm 2.5-Inch SAS Drives, SAS RAID HBA, DVD-RW, 2 PSU, ILOM, 4 x 10/100/1000 Ethernet Ports, 5 USB 2.0 Ports, 3 x 8-Lane PCIe Slots, Red Hat Enterprise LINUX 5.1 and Java Enterprise System Software Pre-installed, RoHS-5 Compliant.

Architecture

- Processor: Intel XEON Processor E5450
- Main Memory: 8GB (4 X 2 GB DIMMS) PC2-5300, 667 MHz EDD fully buffered DDR2
- Additional Memory: Additional 7 X 8 GB (2 x 4 GB DIMMs) Memory Kits added. PC2-5300 667 MHz ECC Fully Buffered DDR2 Memory, RoHS-6 Compliant. Total configured memory 32GB.

System Architecture

- Based on Intel Xeon architecture, two-socket (eight cores total)

Standard/Integrated Interfaces

- Network: Four on-board Intel GbE NICs
- Network management: One 10/100 MbE NIC
- Serial: RJ-45
- USB: Five USB 2.0 ports (two front, two rear, one internal)
- Expansion bus: Three PCI Express slots (x8 electrical/x16 mechanical)

Software

- Red Hat Enterprise LINUX 5.1, 1 – Year Standard Subscription for X86, AMD64 and Intel EM64T. Up to 2 sockets. Includes Media, documentation. RedHat provides support.

Networking

- Four 10/100/1000 Base-T Ethernet ports



Imprivata Healthcare Division: Simplifying and Securing
User Access to Patient Information

Belgium | Germany | Italy | Singapore | UK | USA

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

Copyright © 2010 Imprivata, Inc. All rights reserved. Imprivata and OneSign are registered trademarks of Imprivata, Inc. in the U.S. and other countries. The Application Profile Generator and OneSign Agent are trademarks of Imprivata, Inc. All other trademarks are the property of their respective owners.