

Protect Your Patient Data: Learn How to Avoid Costly Privacy & Security Breaches within Your Organization

September 15, 2011

LOCKSTEP
TECHNOLOGY GROUP


LogRhythm[®]
COMPLY. SECURE. OPTIMIZE.

In this Knowledge-Sharing Webcast...

- Changing Health Care Landscape, Risks and Business drivers
- Data Breaches: frequency, impact, fines
- HIPAA updates and compliance timelines
- UNC Health Care Case Study
- How to Adopt Automated Log & Event Management Solutions

The changing landscape...

The healthcare industry is becoming more interconnected



What are some of the drivers? Why are risks on the rise?

- Regulatory Compliance
 - ▶ The Health Insurance Portability and Accountability Act (HIPAA) - regulations for protecting the privacy and security of health information
 - ▶ The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information.
 - ▶ Increase in vulnerability disclosure
- Cost cutting in current economic climate
 - ▶ Increased demands decreases efficiencies
- Enterprise Modernization
 - ▶ Traditional applications are being driven to the online world - increasing corporate risk
- User demand
 - ▶ The public is demanding rich applications requiring advanced coding techniques; which introduces more risk and threats



Regulatory Compliance – Recent Updates

— Regulatory Compliance

- HIPAA Data Breach disclosure and fines with tougher enforcement will be mandatory compliance by July 2012
- HITECH Act incentives for EHR (Electronic Health Record) system implementation may be impacted by Budget Control Act of 2011 (cuts will be finalized on November 23, 2011)
- Health Information Technology (HIT) standards the Office of National Coordinator (ONC) directed to manage by HITECH Act

— Security and protection of ePHI (Electronic Protected Health Information)

- User demand for online portals and access to patient data can improve care and efficiencies, drive up security risk and requirements for HIT security controls
- Increased risk of data breaches



Security and compliance risks in the healthcare industry

Healthcare Suffers More Data Breaches Than Financial Services - more than three times!

- Darkreading.com, August 2010

Data breach affects 1.9 million individuals - includes medical information, Social Security numbers and other sensitive information

- Health IT Law Blog, March 2011

Data Breach Affects 2,777 Patients

- eWeek.com, March 2011

Hackers Break Into Virginia Health Website - deleting records on more than 8 million patients

- Washington Post, May 2009

Survey shows that data breaches and unauthorized access to their clinical applications are Hospitals biggest worry.

- Darkreading.com, August 2010

Provider reports potential theft of data on 84,000 patients

- HealthImaging.com, February 2011



Data breaches of patient information cost healthcare organizations in the U.S. nearly \$6 billion annually, and many breaches go undetected!

- HealthImaging.com, November 2010

EHR Challenges

— Medical Identity Theft

- The total economic impact of medical identity theft is \$30.9 billion annually, up from \$28.6 billion in 2010 (Source: Ponemon Institute Study, March 1, 2011)

— Data Breach Disclosure and Penalties

- In first three years of HITECH act, about 260 data breached affected more than 10 Million patients (Source: HHS)
- Increased financial penalties up to \$1.5M/year
- Required to post data breach notices on HHS Site
- State Attorney's General enforcement powers

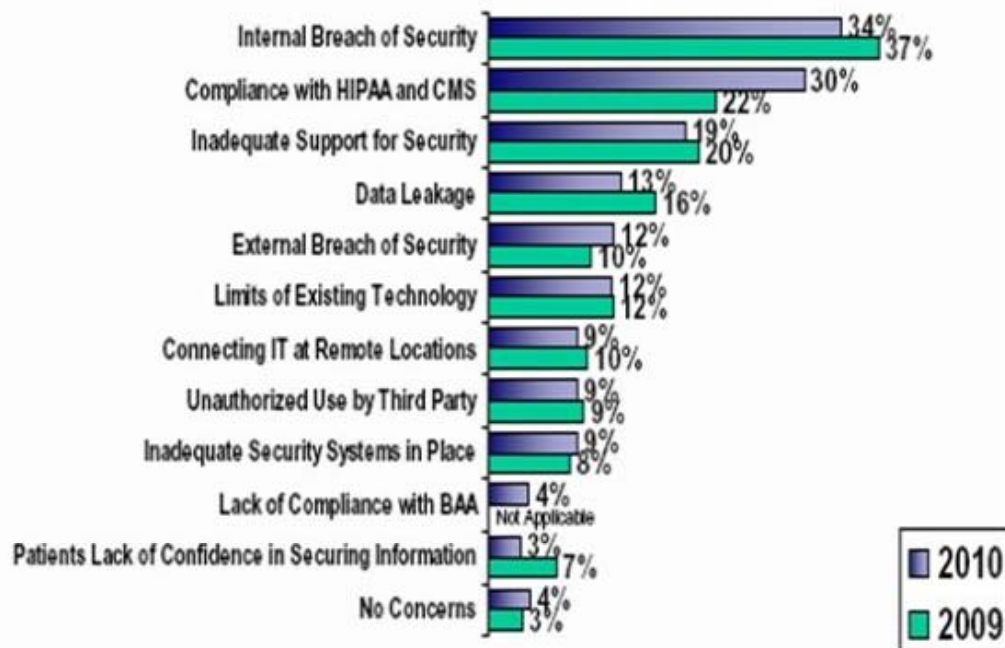
— HITECH Act financial incentives

- “Meaningful use” of EHRs



Top Concern — Security of computerized medical information

Security concerns are keeping CIOs in healthcare organizations awake at night



- Approximately 23% noted that their organization had a security breach in the past year
- 30% surveyed indicated compliance with HIPAA security regulations/CMS security audits was a concern
- Only 4% of respondents indicated that they don't have any concerns about their security

Source: 21st Annual HIMSS Leadership Survey, March 2010

The risk to sensitive information and compliance

Risks and Threats	Costs of Security Breaches	Compliance Demands
<p>Stealing Sensitive Information is the 2nd highest motivation for Web application attacks</p>	<ul style="list-style-type: none">▪ Average cost of a security breach is \$7.25 million▪ Client notification (\$214 per compromised record)▪ Fines (HIPAA annual maximum as high as \$1.5 million)▪ Brand loss and lawsuits▪ Disruption to business operations	<p>Failure to Comply - HIPAA allows both civil and criminal penalties, including fines and possible time in jail</p>

Failure is not an option!

Source: Ponemon Institute, Cost of Data Breach 2010

Case Study : UNC Health Care



- HIPAA compliance and HITECH Act Federal incentives
 - Address EHR “meaningful use” requirement
 - Online prescription compliance requirement for WebCIS (in-house, custom-built pharmaceutical application used by all the UNC Healthcare providers and facilities)
- Ability to run investigations and reports across 3 core applications
 - Replace Business Objects’ investigation functionality for records access and user activity across WebCIS, 2 Siemens off-the-shelf applications
- Improve application monitoring for patient data access
 - Enable IT Network, Security, Legal and Compliance teams to see any user accessing patient data across all applications and departments.
 - Ability to view ALL user activity to secure patient confidentially and for auditing against fraud/unauthorized record changes

The Solution



— Automate HIPAA compliance and Reporting

- Provided customizations for log collection/analysis/reporting from 3 core applications
- HIPAA Compliance package included out of the box for reporting
- Ensure compliance (avoid fines!) for on-line prescriptions (see HHS Certified Health IT Product list)

— Single Appliance solution within budget allocation

- Ability to collect and analyze logs across all applications, devices, servers, workstations, mobile devices, etc. in entire network
- Investigation and reporting capabilities to replace multiple products
- Easy to use, up and running quickly after purchase

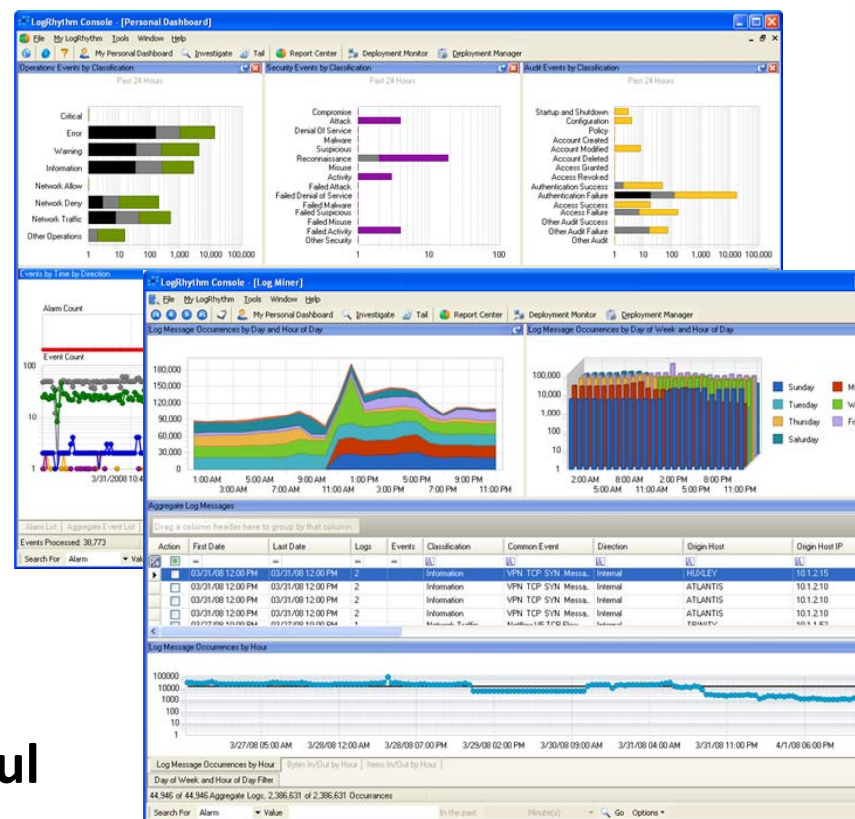
— Privileged User Monitoring for patient data access

- Real time alerts for business users and reports for auditors

Practical Implementation

— HITECH Act: Log & Security Event Management Enables Meaningful Use of EHRs

- Out-of-the box reporting packages that can “instantly” demonstrate compliance
- Automated alerting to immediately identify aberrant behavior related to access of patient data
- Automatic Remediation based on events or alerts
- Ability to easily & efficiently drill down into ALL log data, performing accurate & meaningful forensics investigations



Resources

- U.S. Department of Health and Human Services (HHS), Health Information Technology website, Office of National Coordinator home page:
 - http://www.healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_home/1204
- Budget Control Act of 2011 – HIMSS Fact sheet on Potential Impact on HITECH act and CMS EHR incentives (08/18/11)
 - http://www.himss.org/policy/d/20110818_FactSheetSuperCommittee.pdf
- Centers for Medicare and Medicaid (CMS) website
 - LogRhythm is a certified product module on the federal government's CHPL (Certified Health IT Products List under – UNC Health Care - WebCIS)
<http://onc-chpl.force.com/ehrcert/EHRProductSearch>
- UNC Health Care Meets the system capability requirements for Stage 1 of the Meaningful Use Eligible Hospital (EH) incentive program.
 - <http://news.unchealthcare.org/empnews/2011/june22/webcis>
- HHS – “Security Gaps may threaten Electronic Health Records”
 - <http://oig.hhs.gov/newsroom/news-releases/2011/security.asp>