Secure Logging and Auditing in Electronic Health Records Systems:

What Can We Learn from the Payment Card Industry

Jason King, Presenter
Laurie Williams
North Carolina State University
August 7, 2012

Motivation

- Both industries involve the management of sensitive, protected information
- If your cardholder data is breached…
  - Maybe issue a new payment card
  - Maybe remove fraudulent charges from accounts
- If your healthcare data is breached…
  - Issue a new health diagnosis to replace the old one?
  - Give you a completely new health history?

Motivation

- Protected Health Information *could/should* be considered *more sensitive* than cardholder data
- So let's compare Healthcare to the Payment Card Industry…

Payment Card Industry (PCI)

- Founded by five global brands in 2006
  - American Express
  - Discover Financial Services
  - JCB International
  - MasterCard Worldwide
  - Visa Inc.
- Promote mitigation of data breach and prevention of cardholder data fraud

PCI Data Security Standard Requirements

Requirement	Description
Requirement 1	Install and maintain a firewall configuration to protect cardholder data
Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters
Requirement 3	Protect stored cardholder data
Requirement 4	Encrypt transmission of cardholder data across open, public networks
Requirement 5	Use and regularly update anti-virus software or programs
Requirement 6	Develop and maintain secure systems and applications
Requirement 7	Restrict access to cardholder data by business need to know
Requirement 8	Assign a unique ID to each person with computer access
Requirement 9	Restrict physical access to cardholder data
Requirement 10	Track and monitor all access to network resources and cardholder data
Requirement 11	Regularly test security systems and processes
Requirement 12	Maintain a policy that addresses information security for all personnel

Requirement 10:

Track and monitor all access to network resources and cardholder data

10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

10.2 Implement automated audit trails for all system components to reconstruct the following events:

- **10.2.1** All individual accesses to cardholder data
- **10.2.2** All actions taken by any individual with root or administrative privileges
- **10.2.3** Access to all audit trails
- **10.2.4** Invalid logical access attempts
- **10.2 5** Use of identification and authentication mechanisms
- **10.2.6** Initialization of the audit logs
- **10.2.7** Creation and deletion of system-level objects

10.3 Record at least the following audit trail entries for all system components for each event:

- **10.3.1** User identification
- **10.3.2** Type of event
- **10.3.3** Date and time
- **10.3.4** Success or failure indication
- **10.3.5** Origination of event
- **10.3.6** Identity or name of affected data, system component, or resource.

10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

- **10.4.1** Critical systems have the correct and consistent time.
- **10.4.2** Time data is protected.
- **10.4.3** Time settings are received from industry-accepted time sources.

10.5 Secure audit trails so they cannot be altered.

- **10.5.1** Limit viewing of audit trails to those with a job-related need.
- **10.5.2** Protect audit trail files from unauthorized modifications.
- **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
- **10.5.4** Write logs for external-facing technologies onto a log server on the internal LAN.
- **10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

Requirement 10:

Track and monitor all access to network resources and cardholder data

10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

Non-repudiation

10.2 Implement automated audit trails for all system components to reconstruct the following events:

- **10.2.1** All individual accesses to cardholder data
- **10.2.2** All actions taken by any individual with root or administrative
- **10.2.3** Access to all audit trails
- **10.2.4** Invalid logical access attempts
- **10.2 5** Use of identification and authentication mechanisms
- **10.2.6** Initialization of the audit logs
- **10.2.7** Creation and deletion of system-level objects

Lists/Defines Auditable Events

10.3 Record at least the following audit trail entries for all system components for each event:

- **10.3.1** User identification
- **10.3.2** Type of event
- **10.3.3** Date and time
- **10.3.4** Success or failure indication
- **10.3.5** Origination of event
- **10.3.6** Identity or name of affected data, system component, or resource.

Log Entry Content

10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

- **10.4.1** Critical systems have the correct and consistent time.
- **10.4.2** Time data is protected.
- **10.4.3** Time settings are received from industry-accepted time sources.

Timestamp Reliability

10.5 Secure audit trails so they cannot be altered.

- **10.5.1** Limit viewing of audit trails to those with a job-related need.
- **10.5.2** Protect audit trail files from unauthorized modifications.
- **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
- **10.5.4** Write logs for external-facing technologies onto a log server on the internal LAN.
- **10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

Log Monitoring

Immutability

Log Backups

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

Log Retention

Related Requirements

3.1.1 Implement a data retention and disposal policy that includes:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements
- Processes for secure deletion of data when [illegible]led
- Specific retention requirements for cardholder data
- A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements

Log Disposal

12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:

- Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum
- Specific incident response procedures
- Business recovery and continuity procedures
- Data back-up processes
- Analysis of legal requirements for reporting compromises
- Coverage and responses of all critical system components
- Reference or inclusion of incident response procedures from the payment brands

Incident Response

Bringing it together…

- Ten requirement categories
  - Non-repudiation
  - Defining auditable events
  - Log entry content
  - Timestamp reliability
  - Immutability
  - Log monitoring
  - Log retention
  - Log disposal
  - Incident response

Healthcare

- HIPAA Security & Privacy Rules
  - Noncompliance may result in civil or criminal penalties, including fines up to $50,000 per violation
- HITECH Act of 2009
  - Notion of “meaningful use”
  - Professional and hospitals may qualify for incentive payments for adopting certified EHRs

Meaningful Use

- Stage 1 (2011)
  - Criteria for electronic data capture and exchange
- Stage 2 (FY/CY 2014)
  - Criteria for increasing patient safety and improving data portability
- Stage 3 (targeted for 2016)

Comparisons

Concept	PCI DSS	HIPAA	MU Stage 1	MU Stage 2
Non-repudiation	✓	✓	✓	✓
Auditable Events	✓	✗	✓	✓
Log Entry Content	✓	✗	✓	✓
Timestamp Reliability	✓	✗	✗	✓
Immutability	✓	✗	✗	✓
Log Backups	✓	✗	✗	✗
Log Monitoring	✓	✓	✓	✓
Log Retention	✓	✓	✗	✗
Log Disposal	✓	✓	✗	✗
Incident Response	✓	✓	✗	✗

Example – Auditable Events

PCI DSS

10.2 Implement automated audit trails for all system components to reconstruct the following events:

- **10.2.1** All individual accesses to cardholder data
- **10.2.2** All actions taken by any individual with root or administrative privileges
- **10.2.3** Access to all audit trails
- **10.2.4** Invalid logical access attempts
- **10.2 5** Use of identification and authentication mechanisms
- **10.2.6** Initialization of the audit logs
- **10.2.7** Creation and deletion of system-level objects

MU Stage 1

(b) Record actions related to electronic health information. The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded.

Example – Auditable Events

- PCI DSS incorporates security event logging
  - All actions performed by administrative or root users
  - Initialization & access to audit logs
  - Use of authentication mechanisms
- MU Stage 1
  - Only creation, modification, access, or deletion of PHI

Scenario

	Would this be logged… PCI DSS	MU Stage 1
Doctor creates a new prescription for a patient	✓	✓
Doctor conspires with Administrative user to grant an unauthorized privilege	✓	✗

Summary

- Secure logging & auditing involves *more* than just recording events

- What works in the PCI?
- What doesn't work in the PCI?
- What unique security vulnerabilities are not covered in the PCI DSS?