Secure Logging and Auditing in Electronic Health Records Systems: What Can We Learn from the Payment Card Industry

Position Paper

Jason King, Laurie Williams
Department of Computer Science
North Carolina State University
jtking@ncsu.edu, williams@csc.ncsu.edu

Introduction

Both health information technology (HIT) and the payment card industry (PCI) involve the exchange and management of sensitive, protected information. Compared to the PCI, HIT could consider protected health information (PHI) more sensitive than PCI cardholder data. If cardholder data is breached in the PCI, payment card companies may then remove fraudulent charges from the customer's account and/or issue the customer a new payment card. However, once a person's PHI has been breached, the PHI has been breached forever. Healthcare organizations cannot issue new health histories or new identities to affected individuals. Secure logging and auditing may deter users from performing unauthorized transactions with PHI since an irrefutable trace of the user's activity is recorded. Logging and auditing also provides an accounting of PHI disclosures for assisting data breach investigations.

Secure logging and auditing is one mechanism EHR systems should implement to promote security, user accountability, and trust. *The objective of this paper is to raise awareness of issues around electronic health record logging and auditing mechanisms through a comparison with the Payment Card Industry Data Security Standards.* With the recent push to move all health records to electronic format, the healthcare industry needs to define better standards for secure logging and auditing in EHR systems.

Background. The Health Insurance Portability and Accountability Act (HIPAA) Security and Privacy Rules from 2003 outline administrative and technical safeguards to promote the security, integrity, and availability of electronic PHI[1]. Noncompliance with HIPAA may result in civil or criminal penalties, including fines up to $50,000 per violation[2].

Under the Health Information Technology for Economic and Clinical Health (HITECH) Act [1] of 2009, eligible healthcare professionals and hospitals may qualify for incentive payments if they adopt certified EHR technologies that satisfy "meaningful use" objectives [1]. A portion of "meaningful use" intends to address privacy and security of PHI. Meaningful use is evolving in three separate stages. Stage 1 (2011) includes criteria for electronic data capture and exchange. Stage 2 (FY/CY 2014) includes proposed criteria for increasing patient safety and improving data portability. Stage 3 criteria are targeted for release in 2016[3].

In the PCI, five global brands, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., founded the PCI Security Standards Council[4] in 2006 to promote the mitigation of data breach and the prevention of cardholder data fraud. This council publishes detailed security standards for organizations that manage sensitive cardholder information. Individual payment brands enforce compliance, where penalties for noncompliance may reach up to $100,000 per month[5].

Observations

Since security and protection of PHI should be just as strong, if not stronger, than PCI data security, we extract ten secure logging and auditing concepts addressed by the PCI Data Security Standard (DSS). Table 1 summarizes our comparison of PCI DSS versus HIPAA, Meaningful Use Stage 1, and Meaningful Use Stage 2.

Overall, the PCI DSS provide more detailed requirements for secure auditing and logging than the HIT criteria and standards. For example, PCI DSS Requirement 10.2 lists seven specific user events that should be logged [2], including:

- All individual accesses to cardholder data;
- All actions taken by any individual with root or administrative privileges;
- Access to all audit trails; and
- Initialization of the audit logs

In comparison, Meaningful Use Stage 1 requires log entries when "electronic health information is created, modified, accessed, or deleted" [3]. Likewise, Meaningful Use Stage 2 requires log entries "when EHR

[1] http://www.hhs.gov/ocr/privacy/hipaa/understanding/
[2] http://www.justice.gov/olc/hipaa_final.htm
[3] http://www.hhs.gov/news/press/2012pres/02/20120224a.html
[4] https://www.pcisecuritystandards.org/
[5] http://www.pcicomplianceguide.org/pcifaqs.php

Table 1. Comparison of Secure Logging and Auditing Criteria and Standards in Health Information Technology versus the Payment Card Industry.

Concept	PCI DSS	HIPAA	Meaningful Use Stage 1	Meaningful Use Stage 2
Non-repudiation	R 10.1	164.312(b)	170.302(r)	170.314(d)(2), (3)
Auditable events	R 10.2	–	170.210(b)	170.314(d)(2)(ii)
Log entry content	R 10.3	–	170.210(b)	170.210(e)
Timestamp reliability	R 10.4	–	–	170.210(g)
Immutability	R 10.5.2, 10.5.5	–	–	170.314(d)(2)(iii)
Log Backups	R 10.5.3	–	–	–
Log Monitoring	R 10.5.1, 10.6	164.308(a)(1)(ii)(D)	170.210(b)(2)	170.314(e)(1)(ii) [Patient Accessible Log] 170.314(d)(3) [Audit Reports]
Log Retention	R 10.7	164.316(b)(2)*	–	–
Log Disposal	R 3.1*	164.310(d)(2)(i)*	–	–
Incident response	R 12.9.3*	164.308(a)(6)*	–	–

**Indicates the text does not specifically address logging and auditing, but instead addresses system-wide data management guidelines*

technology is used to record, create, change, access, or delete electronic health information” [4].

The PCI DSS defines auditable events more specifically than current HIT criteria and standards, especially since it considers security event logging (such as logging access to all audit trails, or logging the granting, modification, and revocation of user privileges). HIT could greatly improve guidelines for auditable events by incorporating security event logging into the criteria and standards. Suppose a doctor accesses a patient record and creates a new prescription for the patient. Under Meaningful Use, these two events would be logged appropriately. However, suppose the doctor conspires with an administrator of the EHR. The administrator provides the doctor with the new privilege to create prescriptions for himself or a neighbor. In this case, the PHI access and prescription creation would be logged, but the unauthorized addition of privileges for the doctor would not be logged. Security event logging is necessary to capture trails of unauthorized activity behind-the-scenes, in addition to user transactions with PHI. Even though an EHR may have access control mechanisms in-place, users may still abuse or manipulate these controls to perform unauthorized actions. Adequate secure logging would record these unauthorized actions.

Other key observations of the comparison between HIPAA, Meaningful Use (MU), and PCI DSS include:

- A gradual increase in acknowledgement of the scope of secure logging and auditing requirements from MU Stage 1 to Stage 2,
- The proposed addition of a standard for timestamp synchronization and reliability in MU Stage 2, since the key purpose of audit trails is to record user activity over time,
- Omission of log backup requirements in HIPAA and MU to ensure protection of audit logs in the event of hardware failure,
- Omission of log retention requirements in MU,
- Omission of incident response requirements in MU for documenting and reacting to noncompliance issues found through auditing log entries, and
- Omission of log disposal policies in MU to securely destroy log entries no longer needed for business or regulatory purposes.

Conclusion

Secure logging and auditing standards in HIT currently lag behind standards in the PCI. Even though secure logging and auditing practices in HIT are currently evolving, additional research into the PCI may provide insight into secure logging and auditing standards that work well, standards that do not adequately address intended security objectives, and standards that may need further clarification to conform to HIT practices. HIT needs to catch up with the PCI and surpass the PCI in terms of securing and protecting PHI.

References

[1] *Electronic Health Records and Meaningful Use*. Available: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__meaningful_use_announcement/2996

[2] Payment Card Industry Security Standards Council, "Payment Card Industry Data Security Standard," in *Requirements and Security Assessment Procedure, v2.0*, 2010.

[3] United States Department of Health and Human Services, "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology," Office of the National Coordinator for Health Information Technology, 2010.

[4] United States Department of Health and Human Services, "Health Information Technology: Standards, Implemenation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology," Office of the National Coordinator for Health Information Technology, 2012. Available: http://www.healthit.gov/sites/default/files/pdf/PublicCommentTemplate_3-13-12.pdf