Audit Mechanisms in Electronic Health Record Systems: Protected Health Information May Remain Vulnerable to Undetected Misuse

Jason King, North Carolina State University, USA
Ben Smith, North Carolina State University, USA
Laurie Williams, North Carolina State University, USA

ABSTRACT

Inadequate audit mechanisms may result in undetected misuse of data in software-intensive systems. In the healthcare domain, electronic health record (EHR) systems should log the creating, reading, updating, or deleting of privacy-critical protected health information. The objective of this paper is to assess electronic health record audit mechanisms to determine the current degree of auditing for non-repudiation and to assess whether general audit guidelines adequately address non-repudiation. The authors analyzed the audit mechanisms of two open source EHR systems, OpenEMR and Tolven eCHR, and one proprietary EHR system. The authors base the qualitative assessment on a set of 16 general auditable events and 58 black-box test cases for specific auditable events. The authors find that OpenEMR satisfies 62.3% of the general criteria and passes 63.8% of the black-box test cases. Tolven eCHR and the proprietary EHR system each satisfy less than 19% of the general criteria and pass less than 11% of the black-box test cases.

Keywords: Accountability, Audit, Electronic Health Record (EHR), Healthcare, Log, Non-Repudiation, Privacy, Security

INTRODUCTION

Without adequate audit systems to ensure accountability, users of electronic health record (EHR) systems could create, read, modify, or delete protected health information (PHI) without these actions being traceable. To this end, the United States Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule states that one must implement, “mechanisms that record and examine activity in information systems that contain or use electronic protected health information” (Health Insurance Portability and Accountability Act, 2007). Additionally, Meaningful Use Stage 2 objectives from the United States Department of Health and Human Services (EHR Incentives & Certifications, 2011) include criteria for providing patient accessible logs of protected health information (PHI) disclosure. Patients need to
trust the privacy practices and accountability of healthcare organizations. Administering software audit mechanisms forms a basis for privacy-driven and accountability-driven policy and regulations, including government regulations (Kent & Souppaya, 2006).

Ensuring accountability in an EHR system is essential, since a user should be unable to deny performing certain actions because these actions were recorded by the audit mechanism. The United States Department of Justice’s Global Justice Information Sharing Initiative defines:

Non-repudiation – a technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Non-repudiation provides undeniable proof that a user took a specific action. (Privacy Technology Focus Group, 2006)

Audit mechanisms should help ensure privacy of PHI by focusing on recording and detecting inappropriate accesses to PHI to promote non-repudiation. The healthcare field needs specific standards that address the implementation of software audit mechanisms to monitor access and information disclosure, including details of what should be logged, how it should be logged, and how logged information should be monitored.

In a previous study, we assessed the audit mechanisms of OpenEMR, OpenMRS, and Tolven eCHR to determine how well the three EHR audit mechanisms address non-repudiation (King, Smith, & Williams, 2012). We based our qualitative assessment on both (1) a set of 16 general auditable events derived from four professional sources of audit guidelines, and (2) set of 58 black-box test cases for specific auditable events derived from the Certification Commission for Health Information Technology (CCHIT) criteria (CCHIT Certified, 2011). We found a noteworthy lack of easily accessible and readable auditing for non-repudiation in each of the three EHR systems. Since our initial assessment, newer versions of OpenEMR and Tolven eCHR were released. We also obtained access to a proprietary EHR system for evaluation. With new versions of two open-source EHR systems and a proprietary EHR system now available, we revisit and expand our previous audit mechanisms assessment.

The objective of this paper is to assess electronic health record audit mechanisms to determine the current degree of auditing for non-repudiation and to assess whether general audit guidelines adequately address non-repudiation. In performing this study, we investigate the following questions:

Q1: What events should be included in an EHR log file for non-repudiation?
Q2: How well do EHR systems perform in logging and auditing for non-repudiation?

For this paper, we focus on human-readable, semantic user activity logs that contain data related to user interaction with PHI that should be monitored for the purpose of audit and user accountability. In this study, we first perform an analysis of EHR audit mechanisms by deriving a set of 16 general assessment criteria from four academic and professional sources of general auditable events (such as “view data” and “create data”). Next, we perform an analysis by deriving 58 audit-related black-box test cases to assess specific user actions (such as “view diagnosis data” and “view patient demographics”) in an EHR system. We analyze three EHR systems:

- Open Electronic Medical Records (OpenEMR) v4.1 (http://www.oemr.org),
- Tolven Healthcare Innovation’s Electronic Clinician Health Record (eCHR) v2.1 (http://www.tolven.org/echr.html),
- ProprietaryMed v1 (a proprietary EHR system, unidentified by request).

By evaluating each EHR’s audit mechanism with both our general and specific analyses, we compare and contrast the results and suggest techniques for healthcare software developers to strengthen EHR audit mechanisms.

The remainder of this paper is organized as follows. The “Background” section discusses additional definitions and concepts associated with ensuring non-repudiation in an EHR.
Related Content

Non Linear and Non Gaussian States and Parameters Estimation using Bayesian Methods-Comparatives Studies

New Evolutionary Algorithm Based on 2-Opt Local Search to Solve the Vehicle Routing Problem with Private Fleet and Common Carrier
www.irma-international.org/chapter/new-evolutionary-algorithm-based-opt/69722/

G-HABC Algorithm for Training Artificial Neural Networks
www.irma-international.org/article/habc-algorithm-training-artificial-neural/70235/

Regulatory Compliance and the Correlation to Privacy Protection in Healthcare
www.irma-international.org/chapter/regulatory-compliance-correlation-privacy-protection/65155/
Subspace Discovery for Disease Management: A Case Study in Metabolic Syndrome
www.irma-international.org/article/subspace-discovery-disease-management/53720/