Using Simulation to Teach Security and Encryption to Non-Technical Healthcare Professionals

Mark Gaynor, Saint Louis University, Saint Louis, MO, USA
Tracy Omer, Saint Louis University, Saint Louis, MO, USA
Jason S. Turner, Saint Louis University, Saint Louis, MO, USA

ABSTRACT

This paper intends to simplify challenging concepts through role-play demonstrations and serve as a foundation for understanding the basis of securing healthcare data. Disparity exists between the rising need for security of electronic healthcare information and the number of healthcare leaders who understand the concepts behind ensuring privacy and accuracy of such data. Healthcare managers with a basic understanding of data encryption and how it safeguards health information are vital to the success of Electronic Health Records. They often are responsible for proper oversight of such systems and should instill confidence in medical providers and patients that electronic medical data is safe and accurate. However, data security and privacy are complex concepts and remain foreign to many healthcare managers. This paper reviews the benefits of simulation learning and outlines a workshop and simulation game developed in response to difficulties teaching the technology of encryption. The results are validated with anecdotal and indirect statistical evidence.

KEYWORDS
Encryption, Security, Security for Healthcare, Simulations, Teaching Encryption

INTRODUCTION

Recent healthcare legislation brings increased attention to clinical data exchange. Current financial incentives and future financial penalties spur the widespread utilization of Electronic Health Records (EHRs). This fast-growing use of electronic health information technology requires the healthcare industry to consider carefully the protection of the privacy, security, and integrity of such data.

Existing publications on the topic of healthcare electronic data protection are primarily written for a technical audience with a deep knowledge and understanding of information technology (IT) concepts. Furthermore, many articles published today regarding the use of simulation as a teaching tool focus on its use in a clinical healthcare setting. As contemporary and future healthcare trends require placement of priority and focus on health information systems (HIS) and the security of those systems, this paper addresses the need for a simpler explanation of difficult concepts for a broad audience.
audience of non-technical healthcare professionals and demonstrates that simulation is an effective teaching tool, not only for clinical applications, but for most any complex topic.

This paper first addresses the need for protection of EHR information by considering specific legislation regarding “meaningful use” and financial incentives. Subsequent topics include a basic explanation of securing data through the use of encryption, consideration of using simulation as a valuable tool to teach difficult concepts, and related works using simulation-based techniques. Finally, a simulation-based role-playing game is presented, which allows participants to engage in the conceptual aspects of protecting EHRs. This includes symmetric encryption with one key and public-private encryption with a key pair (i.e., a public key and a private key). This simulation game has been vetted at meetings of the American Medical Informatics Association (AMIA) and the Association of University Programs in Health Administration (AUPHA). It has earned the Workshop Information Technologies and Systems (WITS) Award for Best Innovation in Technology Instruction in 2010. It has been proven successful in the classroom as a HIS teaching tool for health administration students with anecdotal and indirect statistical evidence.

The simulation’s hands-on approach to learning leaves students with confidence to manage security and privacy infrastructure in healthcare through an understanding of:

- Basic concepts of security;
- Basic concepts of privacy;
- Sender verification;
- Message integrity;
- Compliance with Health Insurance Portability and Accountability Act (HIPAA) security and privacy regulations.

PROTECTING ELECTRONIC INFORMATION IN HEALTHCARE

As part of the American Recovery and Reinvestment Act (ARRA) of 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act promotes accelerated adoption and meaningful use of certified EHR programs by providers. “Meaningful use” signifies that the end goal of the Act is not for providers simply to use EHRs, but for providers to use EHRs to improve the quality and safety of healthcare (HRSA, 2009). Currently, ARRA authorizes Centers for Medicare and Medicaid Services (CMS) to provide reimbursement incentives to providers who adopt EHR systems that comply with meaningful use guidelines. The incentive system has already paid out over $20.9 billion and payouts are projected to surpass $22.5 billion (Conn, 2014). Beginning in 2015, providers were expected to actively be using an EHR in compliance with the “meaningful use” definition, or they may be subject to financial penalties under Medicare (HRSA, 2009). To attest compliance with meaningful use, eligible providers must be able to generate and transmit prescriptions electronically and may be required to 1) contact patients for preventive and follow-up care, 2) submit electronic syndromic surveillance data, 3) submit electronic data to immunization registries, and 4) incorporate clinical lab-test results into the EHR (CMS, 2014). Protection and encryption of personal health information is critical to many of the elements associated with meaningful use. Penalties for those not compliant with meaningful use started with a 1% reduction to the Medicare Physician Fee Schedule (MPFS) in 2015, but will grow to 5% by 2018. More than half of eligible providers faced meaningful use penalties in 2015 (Marbury, 2014).

One of the key principles of meaningful use is to promote privacy and security of patient information in the electronic transmission of health information (ONCHIT, 2014). Regulations “require
Mining ICDDR, B Hospital Surveillance Data and Exhibiting Strategies for Balancing Large Unbalanced Datasets

The Mobile is Part of a Whole: Implementing and Evaluating mHealth from an Information Infrastructure Perspective
[www.igi-global.com/article/the-mobile-is-part-of-a-whole/113431?camid=4v1a](www.igi-global.com/article/the-mobile-is-part-of-a-whole/113431?camid=4v1a)