NIST SPECIAL PUBLICATION 1800-1A

Securing Electronic Health Records on Mobile Devices

Volume A:
Executive Summary

Gavin O'Brien
Nate Lesser
National Cybersecurity Center of Excellence
Information Technology Laboratory

Brett Pleasant
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

Colin Bowers
Kyle Kamke
Ramparts, LLC
Clarksville, MD

July 2018

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-1

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.pdf

Executive Summary

- Patient information in electronic health records (EHRs) needs to be protected so it is not exploited to endanger patient health or compromise identity and privacy.
- If not protected, patient information collected, stored, processed, and transmitted on mobile devices is especially vulnerable to attack.
- The National Cybersecurity Center of Excellence (NCCoE) developed an example solution to this problem by using commercially available products.
- The example solution is described in the "How-To" guide, which provides organizations with detailed instructions to re-create it. The NCCoE's approach secures patient information when practitioners access it with mobile devices.
- Organizations can use some or all of the guide to help them implement relevant standards and best practices contained in the National Institute of Standards and Technology (NIST) Cybersecurity Framework and in the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. In areas where there are no standards, such as malware prevention and detection or antivirus, our solution uses best practices.

CHALLENGE

Healthcare providers increasingly use mobile devices to store, process, and transmit patient information. When health information is stolen, inappropriately made public, or altered, healthcare organizations can face penalties and lose consumer trust, and patient care and safety may be compromised. The NCCoE helps organizations implement safeguards to ensure the security of patient information when doctors, nurses, and other caregivers use mobile devices in conjunction with an EHR system.

In our lab at the NCCoE at NIST, we built an environment that simulates interaction among mobile devices and an EHR system that is supported by the information technology (IT) infrastructure of a medical organization.

We considered a scenario in which a hypothetical primary care physician uses her mobile device to perform recurring activities such as sending a referral containing a patient's clinical information to another physician, or sending an electronic prescription to a pharmacy. At least one mobile device is used in every transaction, each of which interacts with an EHR system. When a physician uses a mobile device to add patient information into an EHR, the EHR system enables another physician to access the information through a mobile device as well. This guide does not address patients accessing their own data. In general, EHR systems are accessed by healthcare professionals only. Patients typically access their data via a patient portal, in which data is derived from the EHR system.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-1

SOLUTION

The NIST Cybersecurity Practice Guide *Securing Electronic Records on Mobile Devices* demonstrates how existing technologies can meet your organization's need to better protect the information in EHR systems. Specifically, we show how security engineers and IT professionals, using commercially available and open-source tools and technologies that are consistent with cybersecurity standards, can help healthcare organizations that use mobile devices share patients' health records more securely. We use a layered security strategy to achieve these results.

Using the guide, your organization may choose to adopt the same approach. Commercial and open-source standards-based products, like the ones we used, are easily available and interoperable with commonly used IT infrastructure and investments.

The guide:

- maps security characteristics to standards and best practices from NIST and other standards organizations, and to the HIPAA Security Rule
- provides a detailed architecture and capabilities that address security controls
- facilitates ease of use through automated configuration of security controls
- addresses the need for different types of implementation, whether in-house or outsourced
- provides a how-to for implementers and security engineers seeking to re-create our reference design in whole or in part

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization's information security experts should identify the products that will best integrate with its existing tools and IT system infrastructure. The organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

ASSESS YOUR RISK

All healthcare organizations need to fully understand the potential risk posed to their information systems, the bottom-line implications of those risks, and the lengths that attackers will go to exploit them. According to our analysis (NIST SP 1800-1B, Section 4.3, and NIST SP 1800-1E), and in the experience of many healthcare organizations, the combination of mobile devices and Protected Health Information can present unique risks in a healthcare organization's networks. At the 2012 Health and Human Services (HHS) Mobile Devices Roundtable, participants stressed that many health care providers are using mobile devices in health care delivery before they have appropriate privacy and security protections in place (http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/mobile-devices-roundtable/).

Assessing risks and making decisions about how to mitigate them should be continuous to account for the dynamic nature of business processes and technologies, the threat landscape, and the data itself. The guide describes our approach to risk assessment. We recommend that organizations implement a continuous risk management process as a starting point for adopting this or other approaches that will

increase the security of EHRs. It is important for management to perform regular periodic risk review, as determined by the needs of the business.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/health-it/ehr-on-mobile-devices. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the business processes associated with implementing it.

To learn more by arranging a demonstration of this reference solution, contact us at hit_nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200