PRACTICE GUIDE | Health IT
NIST SP 1800-1a

Securing Electronic Health Records on Mobile Devices

Executive Summary

- Patient information in electronic health records 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 using commercially available products.
- The example solution is packaged as a "How To" guide, providing organizations with the detailed instructions to recreate our example. 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 in the NIST Framework for Improving Critical Infrastructure Cybersecurity and Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

The National Cybersecurity Center of Excellence helps organizations adopt advanced technologies that improve the security of their digital assets such as electronic health record systems and the patient information they contain.

BUSINESS CHALLENGE

Health care providers increasingly use mobile devices to store, process, and transmit patient information. When health information is stolen, inappropriately made public, or altered, health care 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 electronic health record (EHR) system.

In our lab at the NCCoE at the National Institute of Standards and Technology (NIST), we built an environment that simulates interaction among mobile devices and an EHR system supported by the 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

electronic health record, the EHR system enables another physician to access the information through a mobile device, as well.

THE 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 health care 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 information technology 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 recreate our reference design

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization's security experts should identify the standards-based products that will best integrate with your existing tools and IT system infrastructure. Your 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 that best meets your mission needs.

ASSESS YOUR RISK

All health care organizations need to fully understand their potential cybersecurity vulnerabilities, the bottom-line implications of those vulnerabilities, and the lengths attackers will go to exploit them. According to our risk analysis (NIST SP 1800-1b, Section 4.3 and NIST SP 1800-1e), and in the experience of many health care organizations, mobile devices can present vulnerabilities in a health care organization's networks. At the 2012 Health and Human Services 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."[†]

Assessing risks and making decisions about how to mitigate them should be continuous to account for the dynamic nature of your businesses 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 to adopting this or other approaches that will increase the security of electronic health records.

SHARE YOUR FEEDBACK

You can improve our guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

- email HIT_NCCoE@nist.gov
- participate in our forums at http://nccoe.nist.gov/forums/health-it

Or learn more by arranging a demonstration of this example solution by contacting us at HIT_NCCoE@nist.gov.

TECHNOLOGY PARTNERS

The NCCoE issued a call in the Federal Register to invite technology providers with commercial products that matched our security characteristics to submit letters of interest describing their products' capabilities. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution.

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based example solutions using commercially available technologies. The NCCoE seeks problems that are applicable to whole sectors, or across sectors. This cybersecurity challenge was brought to us by members of the health IT community. The center's work results in publicly available NIST Cybersecurity Practice Guides that provide modular, open, end-to-end reference designs.

LEARN MORE

Visit http://nccoe.nist.gov

ARRANGE A DEMONSTRATION

nccoe@nist.gov
240-314-6800

[‡] Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 2015.

[†] HHS Mobile Devices Roundtable: Health Care Delivery Experts Discuss Clinicians' Use of and Privacy & Security Good Practices for mHealth, http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/mobile-devices-roundtable/, accessed June 1, 2015.