NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# HEALTH CARE

## Securing Electronic Health Records on Mobile Devices

The National Cybersecurity Center of Excellence (NCCoE), in collaboration with community members and cybersecurity vendors, has developed an example solution for securing electronic health records (EHR) on mobile devices. The example solution is detailed in NIST Cybersecurity Practice Guide, SP 1800-1, *Securing Electronic Records on Mobile Devices*. The solution we propose is not the only possible one; there may be other solutions in this fast-moving cybersecurity market. If you would like use the design or view a demonstration, please contact us at HIT_nccoe@nist.gov.

### CHALLENGE

Stolen medical information cuts to the very core of personal privacy. Medical identity theft already costs billions of dollars each year and altered medical information can put a person's health at risk through misdiagnosis, delayed treatment, or incorrect prescriptions. Yet, the use of mobile devices to store, access, and transmit electronic health records is outpacing the privacy and security protections on those devices.

In addition to the impact on patients, stolen health information also affects health care providers. 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.

### SOLUTION

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

With the help of the guide, your organization can choose to adopt the same approach. Commercial and open-source standards-based products are easily available and interoperable with commonly used information technology infrastructure and investments. The guide has a modular design, allowing organizations to adopt as much or as little of the reference design as suits their needs.

### BENEFITS

The NIST Cybersecurity Practice Guide, *Securing Electronic Records on Mobile Devices*, was developed by industry and academic cybersecurity experts, with the input of health care providers who first identified the challenge. This approach combines security best practices and industry guidance with a repeatable process for risk management and traceability for compliance with standards.

The NCCoE's solution provides the following benefits:

- defends protected health information (PHI) and the systems that facilitate its use – without getting in the way of delivering quality care
- uncomplicated yet in-depth approach to securing electronic health records on mobile devices
- takes into account the need for different types of implementation for different circumstances, whether cybersecurity is handled in-house or outsourced
- enables organizations to build on existing infrastructure and incorporate commercially available technologies



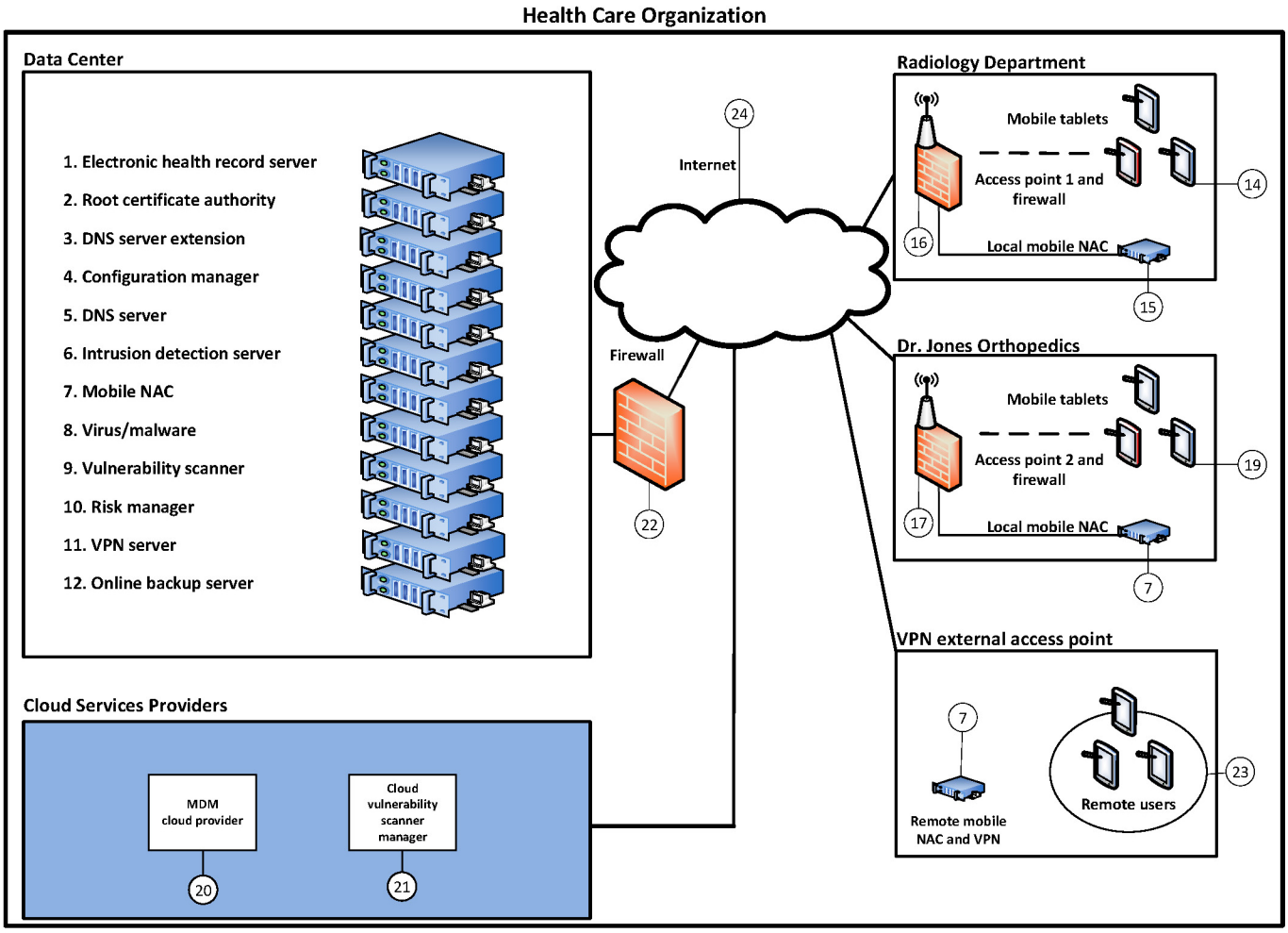
**LEARN MORE ABOUT NCCOE**
Visit http://nccoe.nist.gov

**CONTACT US**
nccoe@nist.gov
301-975-0200

## HIGH-LEVEL ARCHITECTURE

The high-level abstract architecture involves a four-step information transfer process:

1. a physician uses a mobile device application to send a referral to another physician
2. the application sends the referral to a server running a certified EHR application
3. the server routes the referral to the referred physician
4. the referred physician uses a mobile device to receive the referral




## 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. Technology collaborators on this project include:

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.

### DOWNLOAD THE PRACTICE GUIDE

For more information about this project, visit: https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices

### HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please email hit_nccoe@nist.gov.

June 2017