National Cybersecurity Center of Excellence

Increasing the adoption of standards-based cybersecurity technologies

Safeguarding Health Information: Building Assurance through HIPAA Security

9/5/2017

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

Foundations

Collaborative Hub

The NCCoE assembles experts from businesses, academia, and other government agencies to work on critical national problems in cybersecurity. This collaboration is essential to exploring the widest range of concepts.

As a part of the NIST cybersecurity portfolio, the NCCoE has access to a wealth of prodigious expertise, resources, relationships, and experience.

Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

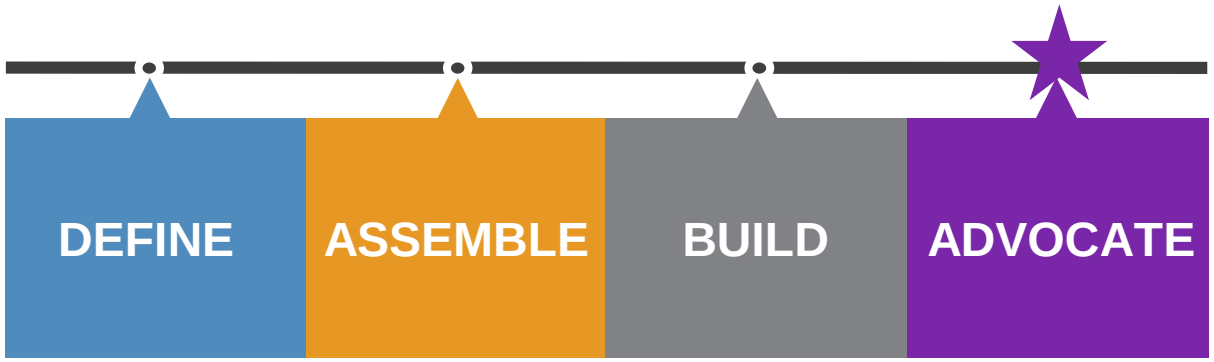
OUTCOME:
Advocate adoption of the example implementation using the practice guide

EHR on Mobile Devices: SP 1800-1

Secure exchange of electronic health information

Overview

- Medical identity theft costs billions each year, and altered medical information can put a patient's health at risk
- The use of mobile devices to store, access, and transmit electronic health records is outpacing the privacy and security protections on those devices
- This practice guide demonstrates how healthcare organizations can secure electronic health records on mobile devices using commercially available and open source products



Project Status

Revising practice guide to publish final SP 1800-1

Collaborate with Us

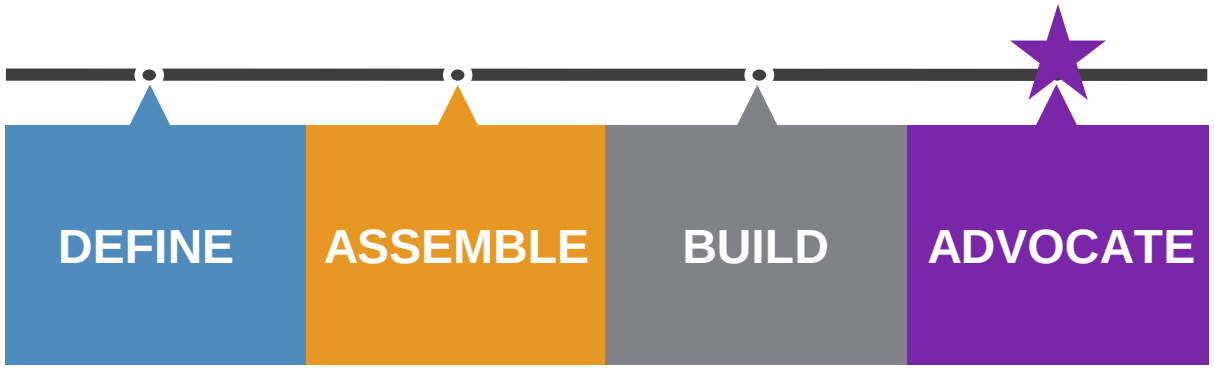
- Read Securing Electronic Health Records on Mobile Devices Practice Guide
- Email hit_nccoe@nist.gov to join the Community of Interest for this project

Wireless Medical Infusion Pumps: SP 1800-8

Medical device security

Overview

- Now that infusion pumps are network-enabled, they can be hacked and infected by malware
- A compromised infusion pump can harm a patient through incorrect drug dosing or expose protected health information
- This project identifies the actors interacting with infusion pumps, defines interactions between the actors and the system, performs a risk assessment, and provides an example solution for healthcare organizations



Project Status

Draft Practice Guide, SP 1800-8 is open for public comment through July 7.

Collaborate with Us

- Read SP 1800-8: Securing Wireless Infusion Pumps and submit feedback by July 7.
- Email hit_nccoe@nist.gov to join the Community of Interest for this project

Ways to Collaborate

Sign-up for email updates:
https://public.govdelivery.com/accounts/USNIST/subscriber/new

Submit a project idea: https://nccoe.nist.gov/projects

Attend an event: https://nccoe.nist.gov/events

Submit comments on drafts:
https://nccoe.nist.gov/projects

Join a Community of Interest:
https://nccoe.nist.gov/about_the_center/coi

Respond to an FRN: https://nccoe.nist.gov/projects

Share adoption stories: nccoe@nist.gov

National Cybersecurity Excellence Partnership