HIPAA Security and Privacy

May 2013

Our 2013 Strategy is Driven by Business Cybersecurity Needs

Vision

Advance Cybersecurity

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

Mission

Accelerate Adoption of Secure Technologies

Collaborate with innovators to provide real-world cybersecurity capabilities that address business needs

Goal 1

Provide Practical Cybersecurity

Help people secure their data and digital infrastructure by equipping them with practical ways to implement cost-effective, repeatable, and scalable cybersecurity solutions

Goal 2

Increase Rate of Adoption

Enable companies to rapidly adopt commercially available cybersecurity technologies by reducing their total cost of ownership

Goal 3

Accelerate Effective Innovation

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art collaborative environment

Foundations

NIST CSD

The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division. As a part of the NIST family, the center has access to a foundation of prodigious expertise, resources, relationships and experience.

Partnerships

The NCCoE is motivated by results. Established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County, the NCCoE is dedicated to furthering innovation through the rapid identification, integration and adoption of practical cybersecurity solutions.

CSD Thought Leadership

- Cryptography
- Identity Management
- Key Management
- Risk Management
- Secure Virtualization
- Software Assurance
- Security Automation
- Security for Cloud and Mobility
- Trusted Roots of Hardware
- Vulnerability Management
- Secure Networking
- Usability and Security

NCEP Companies

Core partners

- Intel
- HyTrust
- McAfee
- Splunk
- Cisco
- RSA
- Symantec
- Microsoft
- Vanguard
- HP
- Venafi

Contributions from our partners

NCEP Companies will have a persistent presence at the center that includes:

- **Technology –** the building blocks (software, hardware, tools, services) necessary to create example integrated "builds" to address industry's cybersecurity challenges;
- **Personnel –** engineers who will work in the NCCoE side-by-side with engineers from other companies, NIST, and other federal agencies to integrate their technologies into the composed solution

Engagement and Business Model

Define + Articulate
Describe the Business Problem

Well defined business problem and project description broadly and refine them through specific use cases

Organize + Engage
Partner with Innovators

Collaborate with partners from industry, government, academia, and the IT community

Implement + Test
Build a Usable Solution

Practical, usable, repeatable, and secure solution that addresses the business problem

Transfer + Learn
Help People Adopt a Solution

Set of all material necessary to implement and easily adopt the secure solution

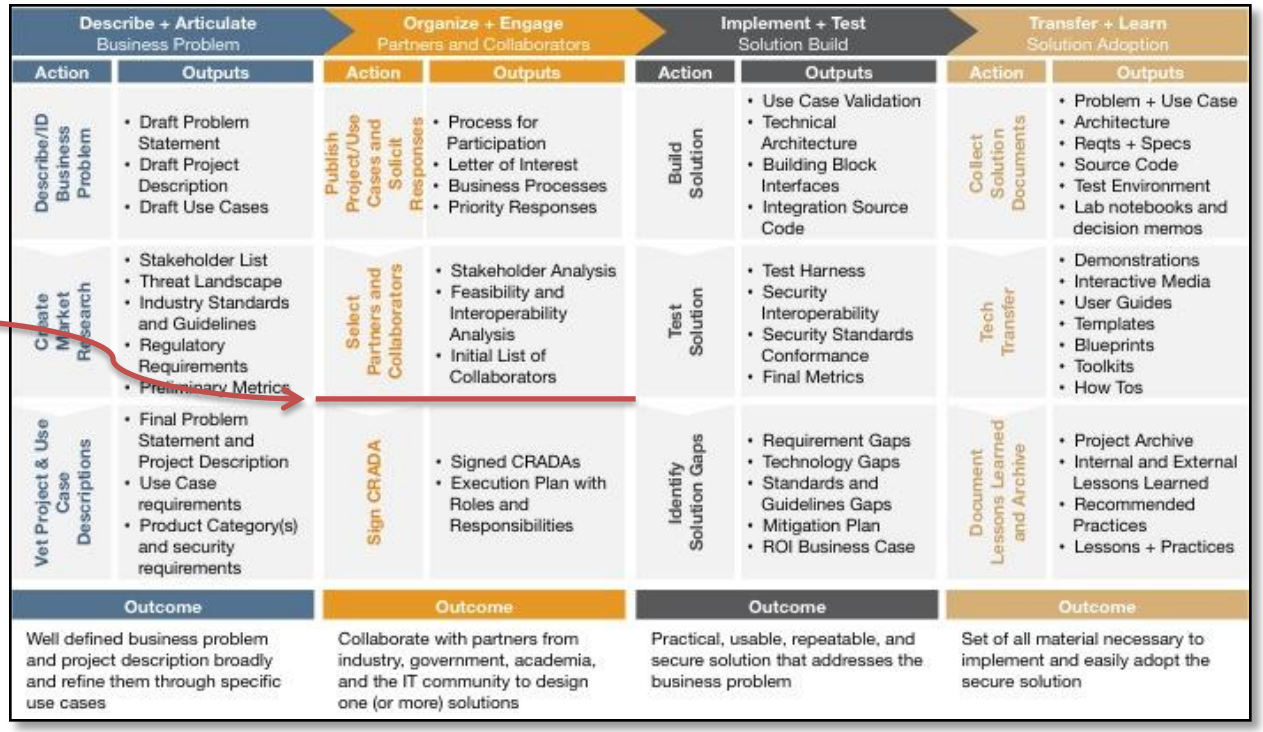
Engagement and Business Model

Describe + Articulate Business Problem		Organize + Engage Partners and Collaborators		Implement + Test Solution Build		Transfer + Learn Solution Adoption	
Action	**Outputs**	**Action**	**Outputs**	**Action**	**Outputs**	**Action**	**Outputs**
Describe/ID Business Problem	• Draft Problem Statement • Draft Project Description • Draft Use Cases	Publish Project/Use Cases and Solicit Responses	• Process for Participation • Letter of Interest • Business Processes • Priority Responses	Build Solution	• Use Case Validation • Technical Architecture • Building Block Interfaces • Integration Source Code	Collect Solution Documents	• Problem + Use Case • Architecture • Reqts + Specs • Source Code • Test Environment • Lab notebooks and decision memos
Create Market Research	• Stakeholder List • Threat Landscape • Industry Standards and Guidelines • Regulatory Requirements • Preliminary Metrics	Select Partners and Collaborators	• Stakeholder Analysis • Feasibility and Interoperability Analysis • Initial List of Collaborators	Test Solution	• Test Harness • Security Interoperability • Security Standards Conformance • Final Metrics	Tech Transfer	• Demonstrations • Interactive Media • User Guides • Templates • Blueprints • Toolkits • How Tos
Vet Project & Use Case Descriptions	• Final Problem Statement and Project Description • Use Case requirements • Product Category(s) and security requirements	Sign CRADA	• Signed CRADAs • Execution Plan with Roles and Responsibilities	Identify Solution Gaps	• Requirement Gaps • Technology Gaps • Standards and Guidelines Gaps • Mitigation Plan • ROI Business Case	Document Lessons Learned and Archive	• Project Archive • Internal and External Lessons Learned • Recommended Practices • Lessons + Practices
Outcome		**Outcome**		**Outcome**		**Outcome**	
Well defined business problem and project description broadly and refine them through specific use cases		Collaborate with partners from industry, government, academia, and the IT community to design one (or more) solutions		Practical, usable, repeatable, and secure solution that addresses the business problem		Set of all material necessary to implement and easily adopt the secure solution	

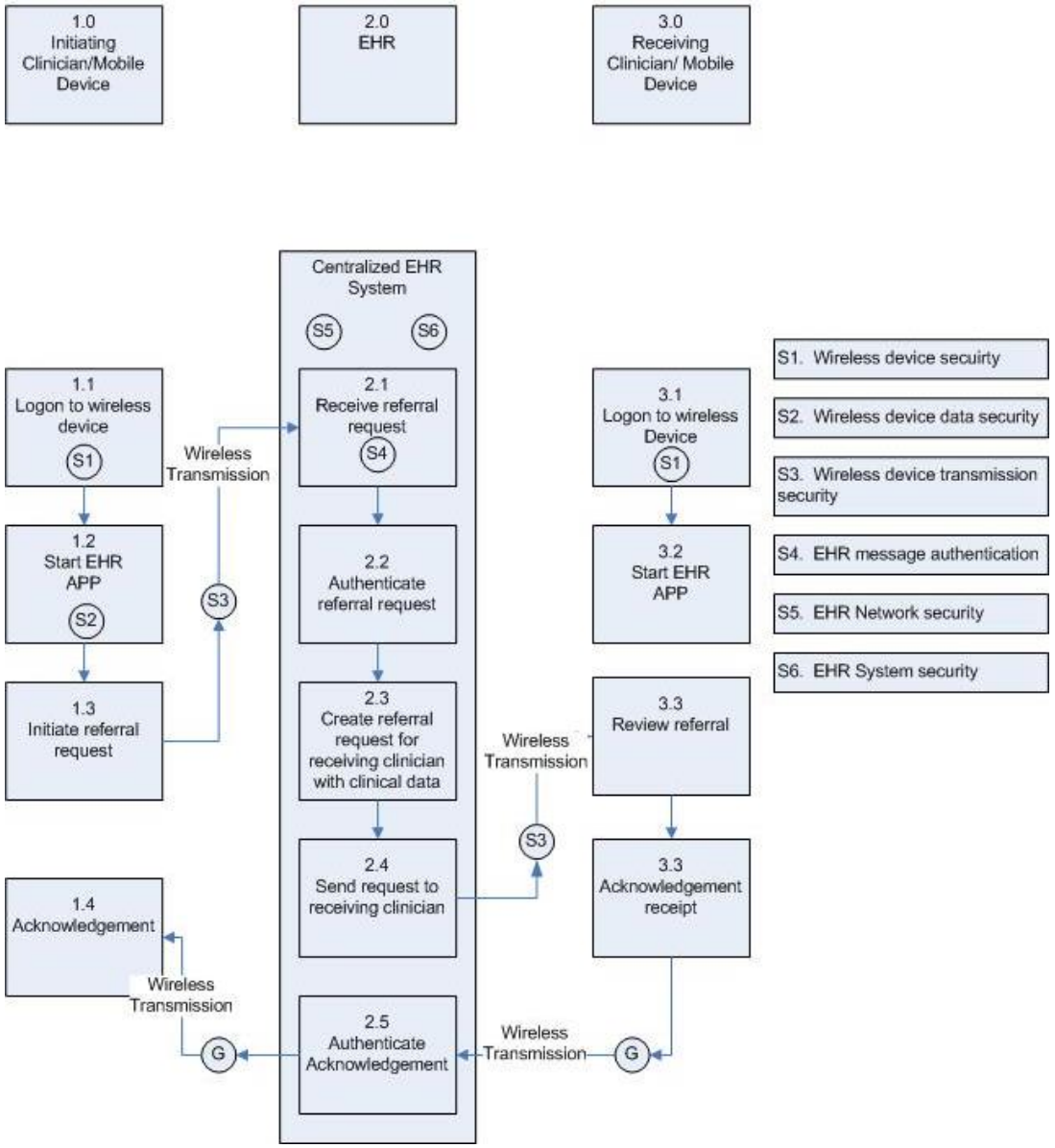
HIT Project – Mobile Device Use Case

- Physician uses a mobile device to collect patient data and send a referral to another physician
- Application sends patient data to a server running a certified EHR application
- Server routes the referral and patient data to the referred physician
- Referred physician uses mobile device to receive the referral

- Vendor conference held on 4/17
- CRADAs to be sent to vendors for legal review



HIT Project – Mobile Device Use Case



HIT Project – Mobile Device Use Case

CRADA Statement of Work

Objective	Collaborate on design and implementation of a build to secure a mobile device communicating to a back end electronic health record system
Need	Security platform to enable health care providers to exchange e-health information
Approach	Work as build teams to develop security
Build Teams	Build teams based on the solution architecture or the type of product
Contribution	Assistance in establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate the desired capabilities; and train NIST personnel as necessary, to operate its product in capability demonstrations to the healthcare community
NIST	Providing IT infrastructure, laboratory facilities, office facilities and staff support to component composition, security platform documentation, and demonstration activities.
Output	Publish a description of the security platform and its performance characteristics sufficient to permit organizations to duplicate the build -- develop and deploy identical security platforms (descriptions are public information)

HIT Project – Mobile Device Use Case

Technical Requirements

- Safeguards required by the HIPPA security rule and HITECH
- Mobile device security
- Supporting infrastructure security services

HIPPA Security Rule & HITECH Security Characteristics

- Access Control
  - Unique User Identification
  - Emergency Access Procedure
  - Automatic Logoff
  - Encryption and Decryption
- Audit Controls
- Integrity
  - Mechanism to Authenticate Electronic PHI
- Person or Entity Authentication
- Transmission Security
  - Integrity Controls
  - Encryption