HCCN
Health Center Controlled Network

MPCA

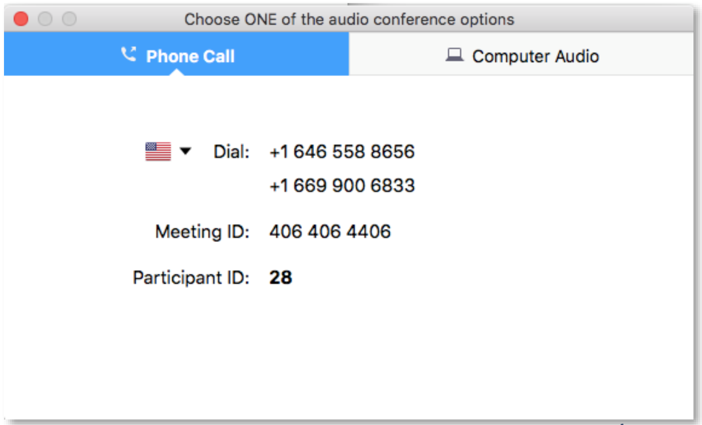
Montana Primary Care Association presents: "How to Use Mobile Technology While Keeping PHI Secure"

Wednesday, December 11 , 2019 | 11AM - 12PM

Presented by: Susan Clarke, BCS, HCISPP

PASS

Zoom tips and tricks!



Dial: +1 646 558 8656
+1 669 900 6833

Meeting ID: 406 406 4406

Participant ID: 28

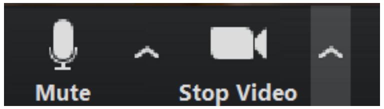
CHAT: Please jump in if you have something to share, but we also have this nifty chat function.

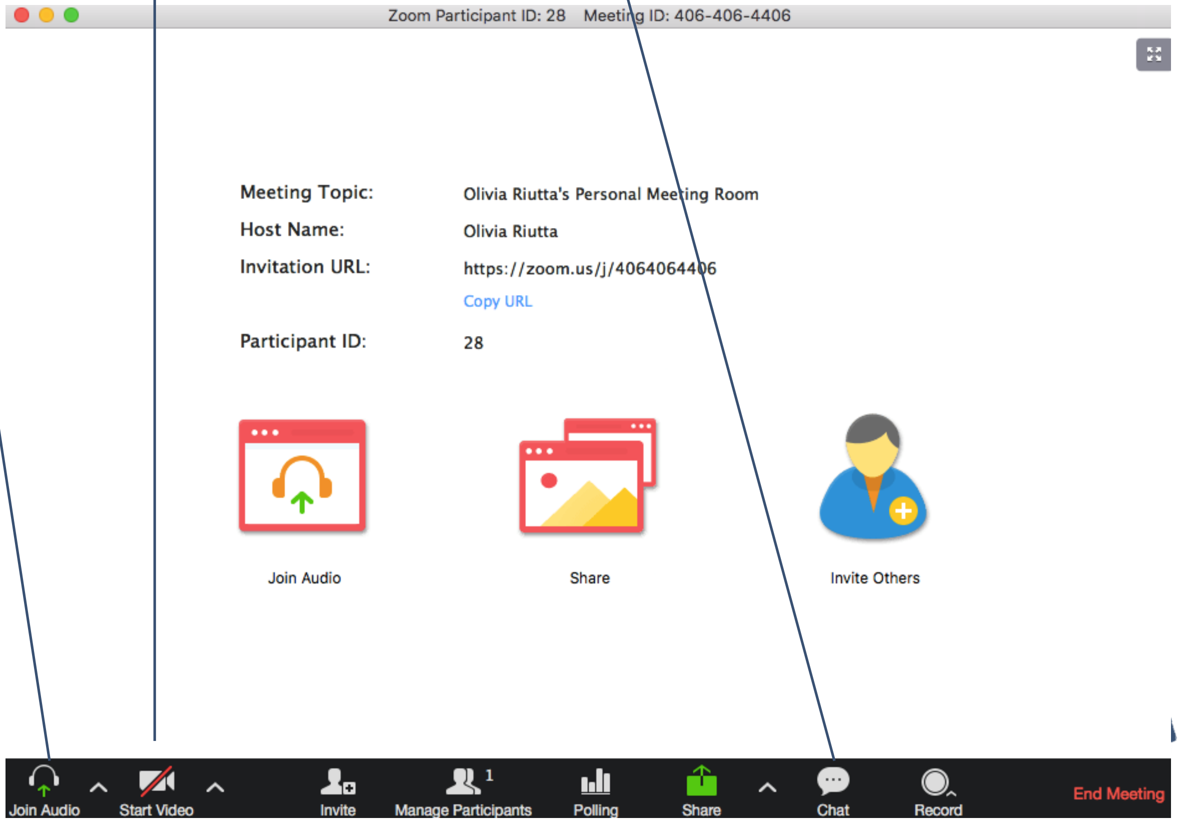
ATTENDANCE: If there are multiple attendees together on the call, please list the names and your location in the chat box

VIDEO: We want to see you! If your camera isn't on, start your video by clicking here.

AUDIO: You can use your computer speakers or your phone for audio. The phone is generally better quality. If you click "Join Audio," this "Choose one…" box will pop up. If you dial in, just make sure you include your audio code.

MUTE/UNMUTE: *6 or click the mic on the bottom left of your screen.





Meeting Topic: Olivia Riutta's Personal Meeting Room

Host Name: Olivia Riutta

Invitation URL: https://zoom.us/j/4064064406

Copy URL

Participant ID: 28

Susan Clarke, HCISPP

- (ISC)^2 certified Healthcare Information Security and Privacy Practitioner and Computer Scientist.
- 20 years of Healthcare Experience.
- 10 years design and coding EHR software including HL7 Healthcare application development.
- Served on IT Security, Disaster Recovery and Joint Commission steering committee at Mayo Clinic affiliated Healthcare system.
- Served as communications unit lead during Healthcare system's ready and complete alerts.

Mountain-Pacific

Mountain-Pacific Quality Health is a private, non-profit, community-based organization that has dedicated more than three decades to improving health and health care in: Alaska, Hawaii (including some U.S. Pacific Territories), Montana and Wyoming. Our goal is to increase access to high-quality health care that is affordable, safe and of value to the patients we serve.

Legal Disclaimer

The presenter is not an attorney and the information provided is the presenter(s)' opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar(s) and related materials (including, but not limited to, recordings, handouts, and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar(s) and webinar materials should not in any manner rely upon or construe the information as legal, or other professional advice. Users should seek the services of a competent legal or other professional before acting, or failing to act, based upon the information contained in the webinar(s) in order to ascertain what is may be best for the users patient needs.

Acronyms…

- BA: Business Associate
- CE: Covered Entity
- EHR: Electronic Health Record
- EMM/MDM: Enterprise Mobility Mgmt/Mobile Device Mgmt
- ePHI: Electronic Protected Health Information
- HHS: Department of Health and Human Services
- HIPAA: Health Insurance Portability and Accountability Act
- MTD: Mobile Threat Defense
- MTI: Mobile Threat Intelligence
- NIST: National Institute of Standards and Technology
- OCR: Office for Civil Rights
- PHI: Protected Health Information
- SRA: Security Risk Analysis
- VPN: Virtual Private Network

Learning Objectives

1. The Latest Trends in Mobility in Healthcare
2. NIST Guidance on Using Mobile Technology
3. The Vulnerabilities in Mobility Technology
4. How a EMM/MDM: Enterprise Mobility Mgmt/Mobile Device Mgmt Can Help
5. Using Behavior-Based Analytics to Detect Cyberattacks Before PHI is Breached
6. BYOD (Bring Your Own Device)

Background

As healthcare organizations continue to embrace mobile devices, mobile security challenges continue to escalate. If you communicate with patients using portable devices, it is critical to secure protected health information (PHI) using strong authentication, encryption and remote wiping of data if lost or stolen.

Mobile devices must be defended to keep the data on them from being accessed but security, alone, may not be enough.

Current Landscape

A growing and now key component for enterprise information sharing is mobile devices.

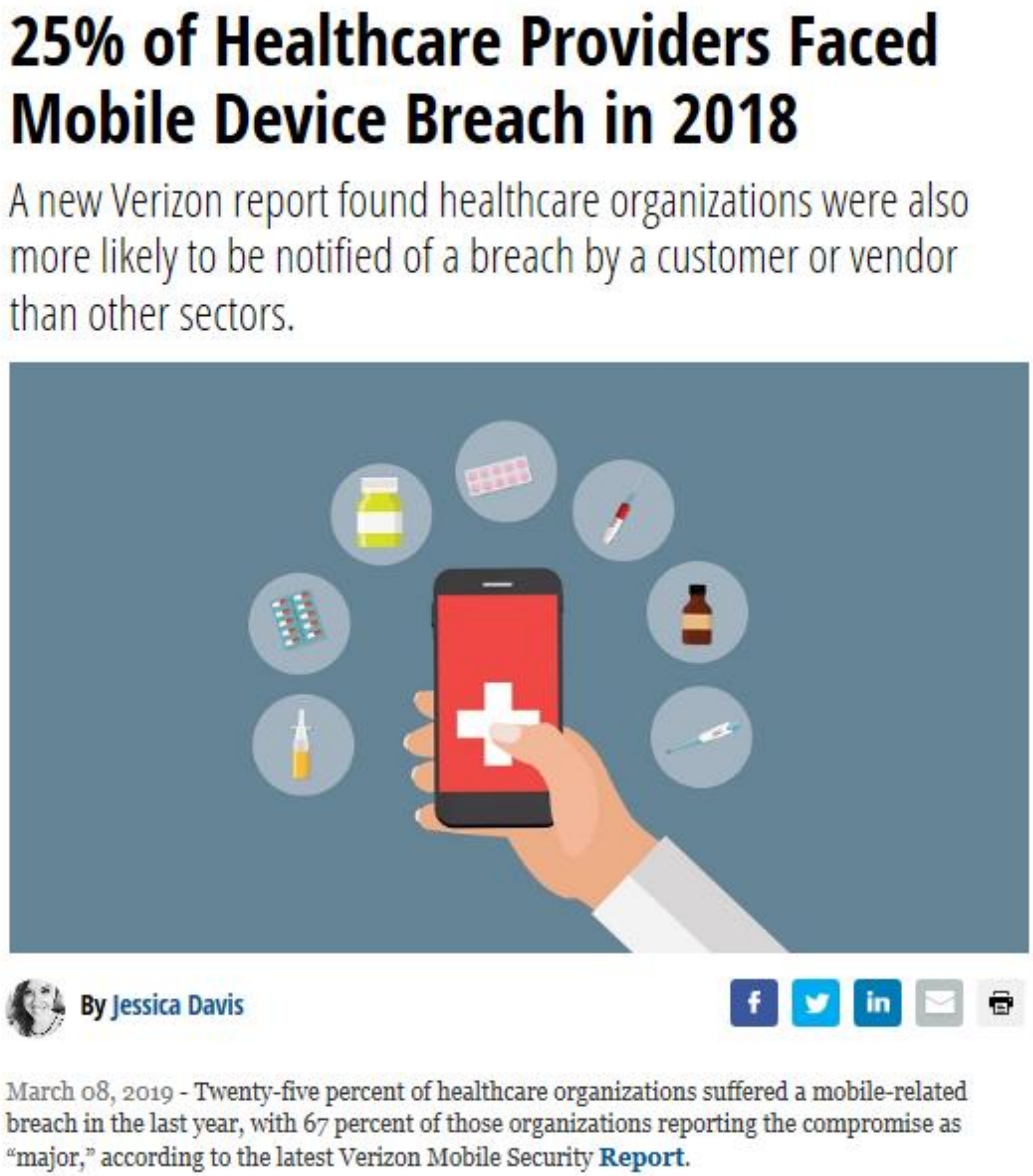
These devices provide access to data and resources vital for organizations to accomplish their mission while providing employees with the flexibility to perform their daily activities.

Preventing breaches before they happen is essential!

Mobile Brings Unique Threats

Mobile devices bring unique threats to the enterprise that need to be addressed in a manner distinct from traditional desktop platforms.

This includes securing against different types of network-based attacks on devices that generally have an always-on connection to the internet



25% of Healthcare Providers Faced Mobile Device Breach in 2018

A new Verizon report found healthcare organizations were also more likely to be notified of a breach by a customer or vendor than other sectors.

By Jessica Davis

March 08, 2019 - Twenty-five percent of healthcare organizations suffered a mobile-related breach in the last year, with 67 percent of those organizations reporting the compromise as "major," according to the latest Verizon Mobile Security **Report**.

Source= https://healthitsecurity.com/news/25-of-healthcare-providers-faced-mobile-device-breach-in-2018

Mobile Landscape and Challenges

- According to the Global System for Mobile Alliance (GSMA), over 70 percent of the world's population will have a mobile subscription by 2020.*
- Current gaps: Weak isolation between personal and work use-contexts, apps that exploit user trust or operating system (OS) vulnerabilities, and network-based attacks.
- Proper implementation is difficult to achieve for an end user because the method of implementation varies considerably from tool to tool.
- A lack of familiarity with the threats to mobile devices can further compound these implementation difficulties

*Source: DHS Study of Mobile Device Security

NIST

NIST (the National Institute of Standards and Technology) creates and releases guidance on best practices in numerous aspects of the hard sciences, including cybersecurity, mobile device security and risk assessments.

NIST and Federal Information Processing Standards (FIPS), can be used to support the requirements of both HIPAA and FISMA, may be used by organizations to help provide a structured, yet flexible framework for selecting, specifying, employing, and evaluating the security controls in information systems

NIST Current Status

Recently, the National Institute of Standards and Technology (NIST) issued mobile device security on the use of mobile technologies.

1) August, 2019, the NCCoE released the NIST Cybersecurity Practice Guide, SP 1800-1, Securing Electronic Health Records on Mobile Devices (260 pages)

- SP 1800-1A: Executive Summary
- SP 1800-1B: Approach, Architecture, and Security Characteristics
- SP 1800-1C: How-To Guide
- SP 1800-1D: Standards and Controls Mapping
- SP 1800-1E: Risk Assessment and Outcomes

https://www.nccoe.nist.gov/projects/use-cases/health-it/ehr-on-mobile-devices

NIST Current Status continued

2) The NCCoE recently released a draft of NIST Cybersecurity Special Publication 1800-21, Mobile Device Security: Corporate-Owned Personally-Enabled (COPE), 351 Pages:

- SP 1800-21A: Executive Summary (PDF)
- SP 1800-21B: Approach, Architecture, and Security Characteristics (PDF)
- SP 1800-21C: How-To Guides (PDF)

https://csrc.nist.gov/publications/detail/sp/1800-21/draft

3) Coming soon: NIST SP Mobile Device Security: Bring Your Own Device (BYOD)

NIST Corporate-Owned Guide

Provides an example solution demonstrating how organizations can use a standards-based approach and commercially available technologies to meet their security needs for using mobile devices to access enterprise resources:

- ✓ EMM/MDM capability located on-premises
- ✓ Mobile Threat Defense (MTD)
- ✓ Mobile Threat Intelligence (MTI)
- ✓ Application Vetting
- ✓ Secure Boot/Image Authentication
- ✓ Virtual Private Network (VPN)

https://www.nccoe.nist.gov/sites/default/files/library/fact-sheets/mds-cope-fact-sheet.pdf

Corporate-Owned Guide Participating Vendors

The technology participating vendors submitted their capabilities in response to a call in the Federal Register. Technology collaborators on this project include:

appthority

kryptowire

Lookout

MobileIron

paloalto NETWORKS

Qualcomm

Security EHR on Mobile Devices Guide Participating Vendors

The technology participating vendors submitted their capabilities in response to a call in the Federal Register. Technology collaborators on this project include:

CISCO.

intel

MaaS360 by Fiberlink

[illegible]

RAMPARTS

RSA

Symantec.

Building your Mobility Program

The rapid pace at which mobile technologies evolve requires regular re-evaluation of your program.

Built-in mobile protections may not be enough to fully mitigate the security challenges

Usability, privacy, and regulatory requirements each influence which mobile security technologies and security controls are going to be well-suited to meet the needs of an organization’s program.

https://www.nccoe.nist.gov/sites/default/files/library/fact-sheets/mds-cope-fact-sheet.pdf

NIST Practice Guide Benefits

- Reduce adverse effects on the organization if a device is compromised
- Reduce capital investment by embracing modern enterprise mobility models
- Apply robust, standards-based technologies using industry best practices
- Reduce privacy risks to users through privacy protections
- Provide users with enhanced protection against loss of personal and business data when a device is stolen or misplaced
- Deploy enterprise management technologies to improve the security of enterprise networks, devices, and applications
- Reduce risk so that employees can access the necessary data from nearly any location, using a wide selection of mobile devices and networks
- Enhance visibility for system administrators into mobile security events, quickly providing notification and identification of device and data compromise
- Implement government standards for mobile security

https://www.nccoe.nist.gov/sites/default/files/library/fact-sheets/mds-cope-fact-sheet.pdf

NIST Corporate-Owned Guide High-Level Architecture

The specific architecture varies based on the necessary enterprise services and management technology in use. Will use network-based confidentiality protection mechanisms, such as a Virtual Private Network. Additionally, device-side security mechanisms will be utilized to identify known vulnerabilities and mobile malware. Enterprise Mobility Management (EMM) policy sets will be created, and then tailored to an individual user’s risk profile in accordance with established best practices.

https://www.nccoe.nist.gov/sites/default/files/library/fact-sheets/mds-cope-fact-sheet.pdf

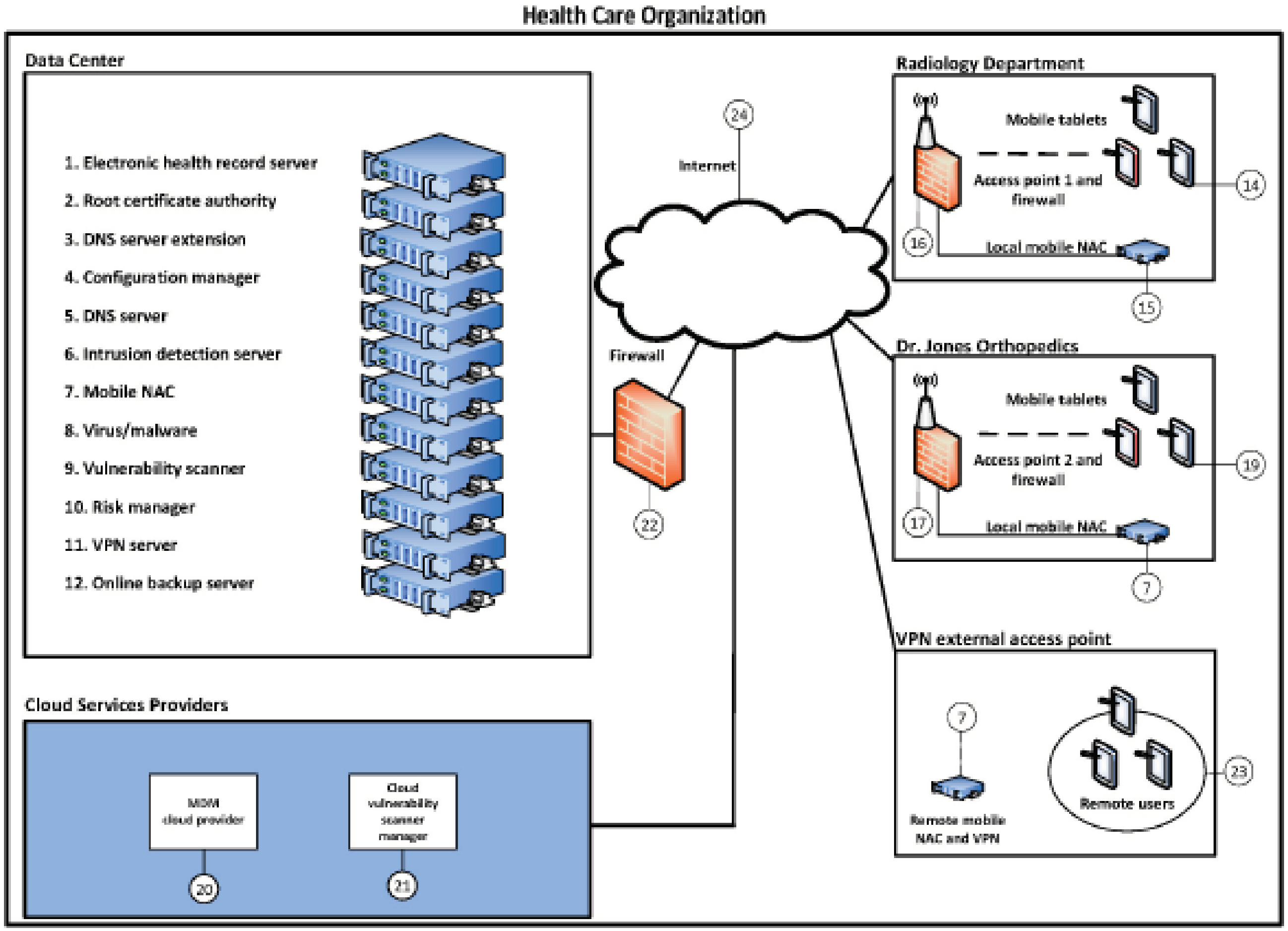
NIST Corporate-Owned Guide High-Level Architecture

Each implementation will include the following:

- a risk assessment using an established methodology (e.g., NIST SP 800-37, Cybersecurity Framework)
- installation and configuration instructions for a variety of mobile security technologies, such as an enterprise mobility management system, virtual mobile infrastructure, application vetting, or mobile threat defense
- a set of mobile security controls, mapped to a variety of industry and government standards i.e. NIST

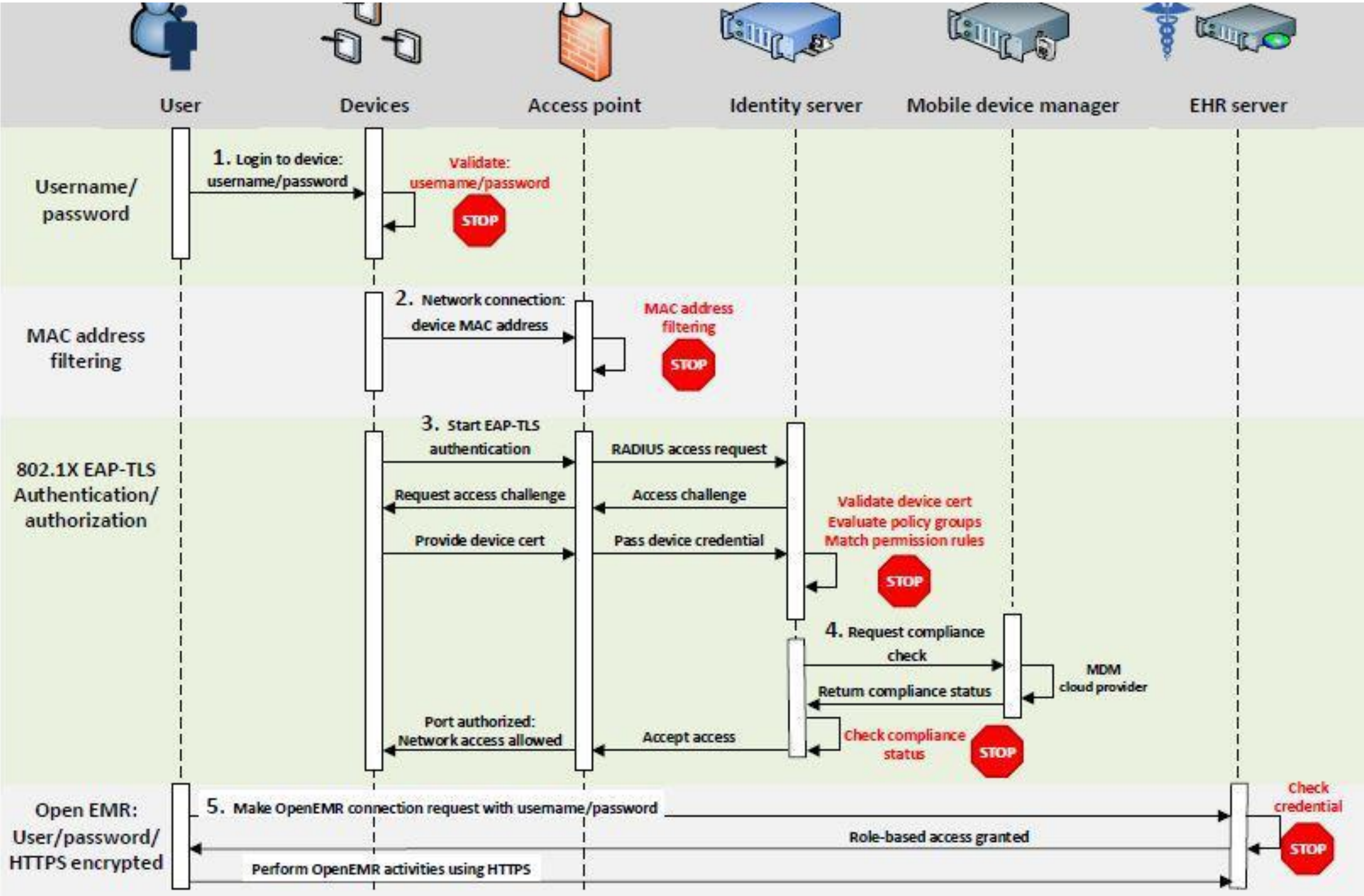
https://www.nccoe.nist.gov/sites/default/files/library/fact-sheets/mds-cope-fact-sheet.pdf

Security EHR on Mobile Devices Guide High Level Architecture



a physician uses a mobile device application to send a referral to another physician
the application sends the referral to a server running a certified EHR application
the server routes the referral to the referred physician
the referred physician uses a mobile device to receive the referral

Security EHR on Mobile Devices Guide



User

Devices

Access point

Identity server

Mobile device manager

EHR server

Username/ password

1. Login to device: username/password

Validate: username/password

STOP

MAC address filtering

2. Network connection: device MAC address

MAC address filtering

STOP

802.1X EAP-TLS Authentication/ authorization

3. Start EAP-TLS authentication

RADIUS access request

Request access challenge

Access challenge

Provide device cert

Pass device credential

Validate device cert

Evaluate policy groups

Match permission rules

STOP

4. Request compliance check

MDM cloud provider

Return compliance status

Port authorized: Network access allowed

Accept access

Check compliance status

STOP

Open EMR: User/password/ HTTPS encrypted

5. Make OpenEMR connection request with username/password

Check credential

Role-based access granted

STOP

Perform OpenEMR activities using HTTPS

The Steps Necessary for a User and Device to Gain Access to the EHR Server

Security EHR on Mobile Devices Guidance
Device Authentication and Authorization

1. Does the EHR system vendor restrict the type of mobile devices that can access the system?

2. Are mobile devices subject to some kind of mobile device management control for enforcing device security compliance?

3. Are there any security compliance policies for using a client's own device to access the cloud-based EHR system?

4. If a device is lost, stolen, or found to be hacked, are there any countermeasures in place to prevent protected data from becoming compromised?

5. Does the cloud-based EHR system require a user to be authenticated prior to obtaining access to patient health information?

    i. What are the authentication mechanisms used for accessing the system?

    ii. Are user IDs uniquely identifiable?

    iii. Is multifactor authentication used? Which factors?

    iv. If passwords are used, does the vendor enforce strong passwords and specify the life cycle of the password?

6. Does the system offer a role-based access control approach to restrict system access to authorized users to different data sources?

7. Is the least privilege policy used? (minimum necessary)

https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1.pdf

Security Questions Page 216 of 260

HIPAA Security Standards

ADMINISTRATIVE SAFEGUARDS

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

TECHNICAL SAFEGUARDS

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

PHYSICAL SAFEGUARDS

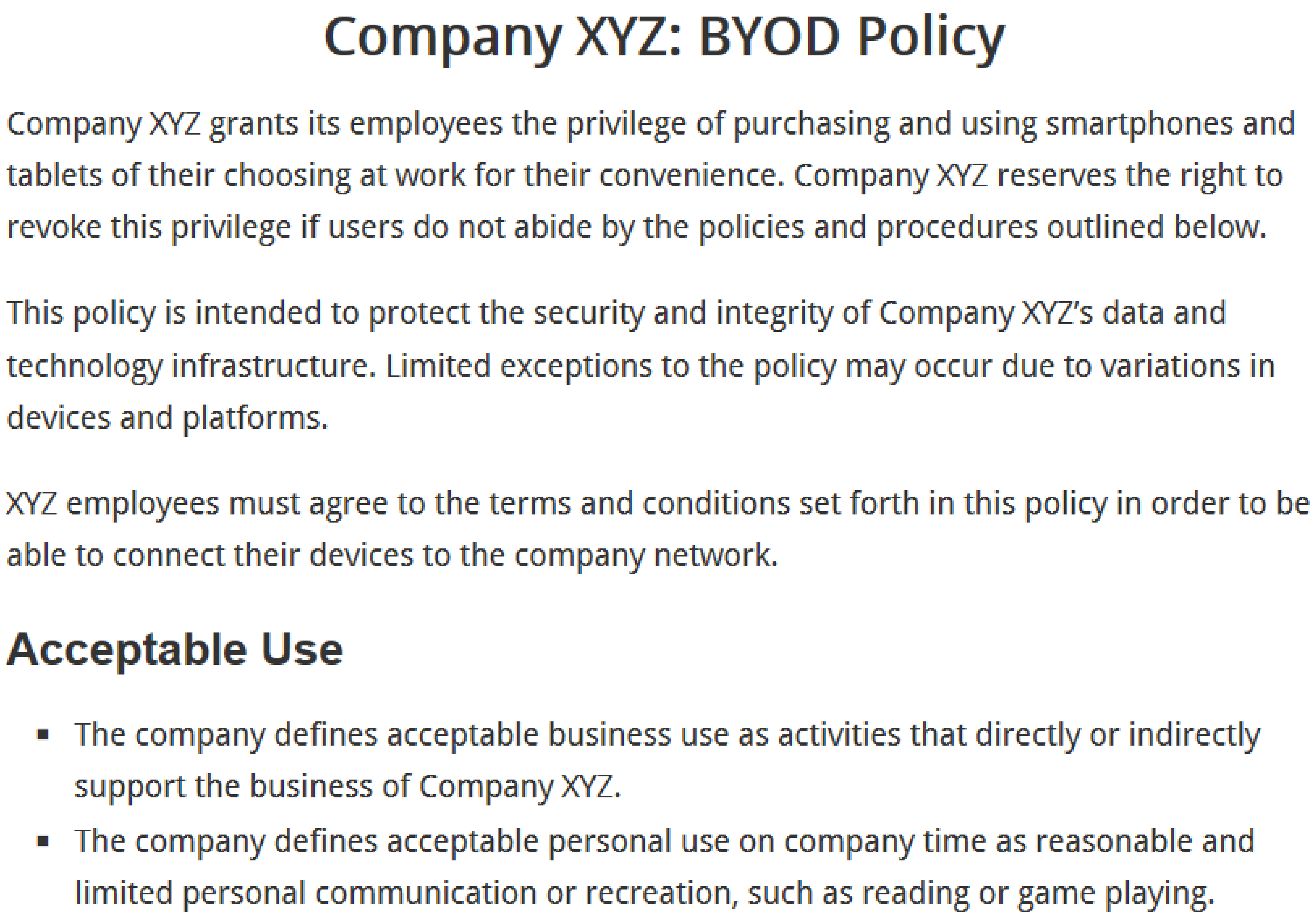
- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Bring Your Own Device Concerns

Administrative: data ownership (remote wiping), support ownership, privacy (ie geo-tagging), on-boarding/off-boarding, adherence to corporate policy, user acceptance, legal concerns, acceptable use policy (application control/whitelisting).

Technical: patch management, antivirus management, infrastructure considerations, forensics, onboard tools like: camera, video, microphone.

Physical: lost, stolen, unauthorized user access.



Company XYZ: BYOD Policy

Company XYZ grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. Company XYZ reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of Company XYZ's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

XYZ employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of Company XYZ.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.

Source= http://www.itmanagerdaily.com/byod-policy-template/

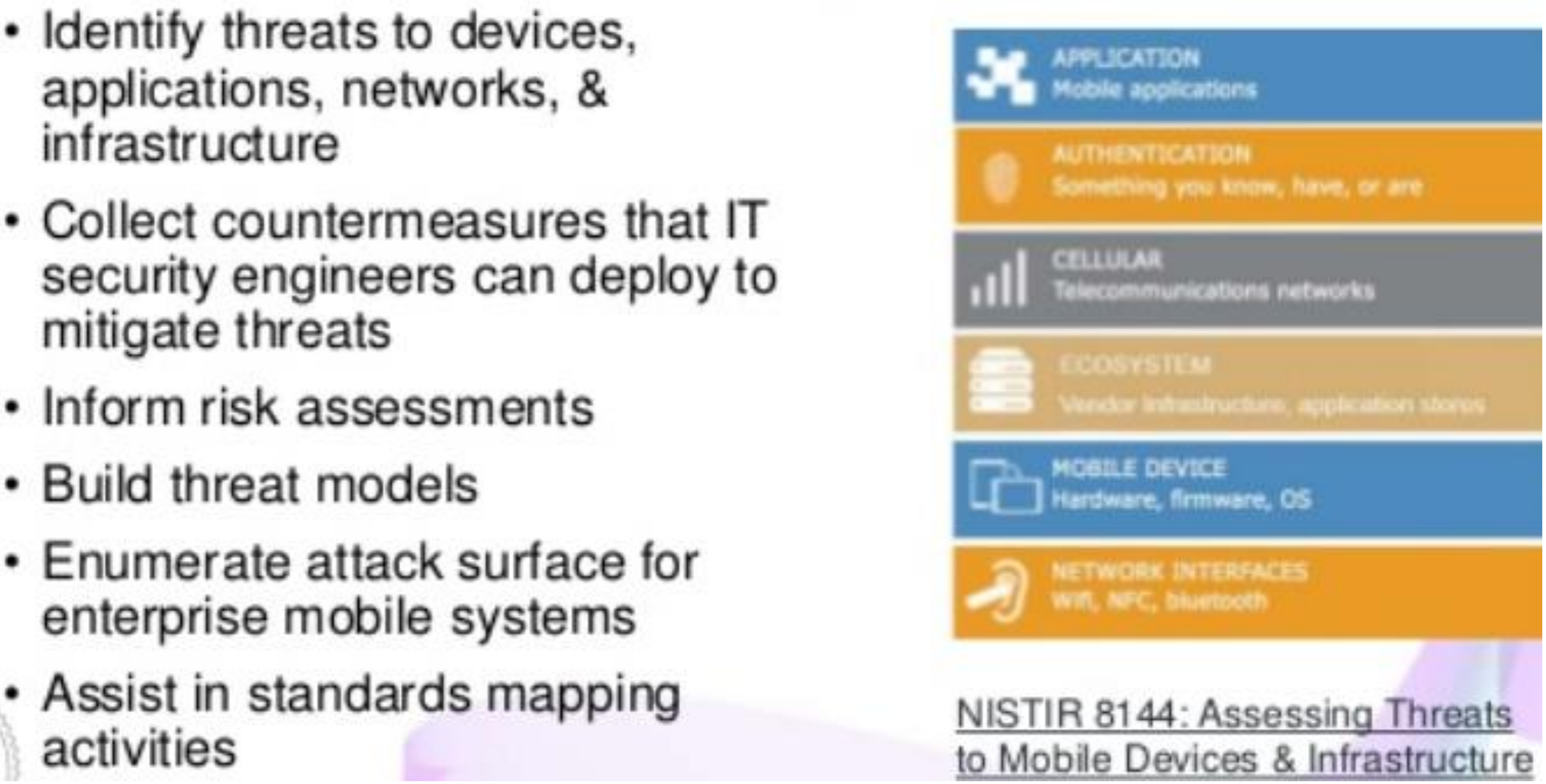
Behavior Based Threat Detection

EMM/MDMs are often embedded with a mobile threat defense tool that serves to perform on-device behavioral-based threat-detection and to trigger policy remediation without the need to communicate to any server or service outside the device.

This type of integration allows one application to manage, detect, and remediate device, network, application, malware, and spear phishing attacks.

Because the remediation is autonomous (does not require reaching a policy server), it has the advantage in addressing network-based threat vectors that can impersonate a valid Wi-Fi or cellular network.

Resource: Mobile Threat Catalogue



- Identify threats to devices, applications, networks, & infrastructure
- Collect countermeasures that IT security engineers can deploy to mitigate threats
- Inform risk assessments
- Build threat models
- Enumerate attack surface for enterprise mobile systems
- Assist in standards mapping activities

APPLICATION
Mobile applications

AUTHENTICATION
Something you know, have, or are

CELLULAR
Telecommunications networks

ECOSYSTEM
Vendor infrastructure, application stores

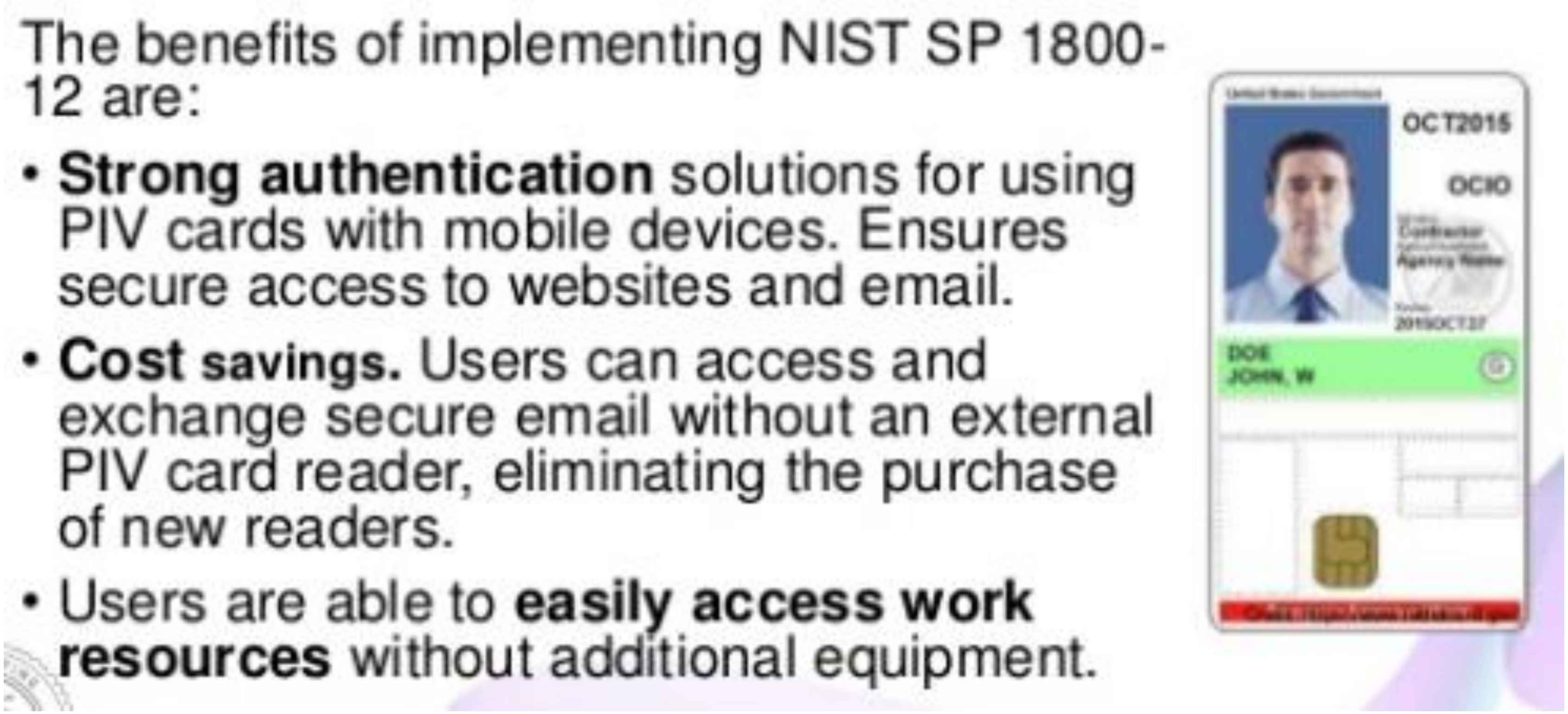
MOBILE DEVICE
Hardware, firmware, OS

NETWORK INTERFACES
Wifi, NFC, bluetooth

NISTIR 8144: Assessing Threats to Mobile Devices & Infrastructure

Source=2019 Mobile Security for the Enterprise, Identiverse

Resource: Derived PIV Credentials

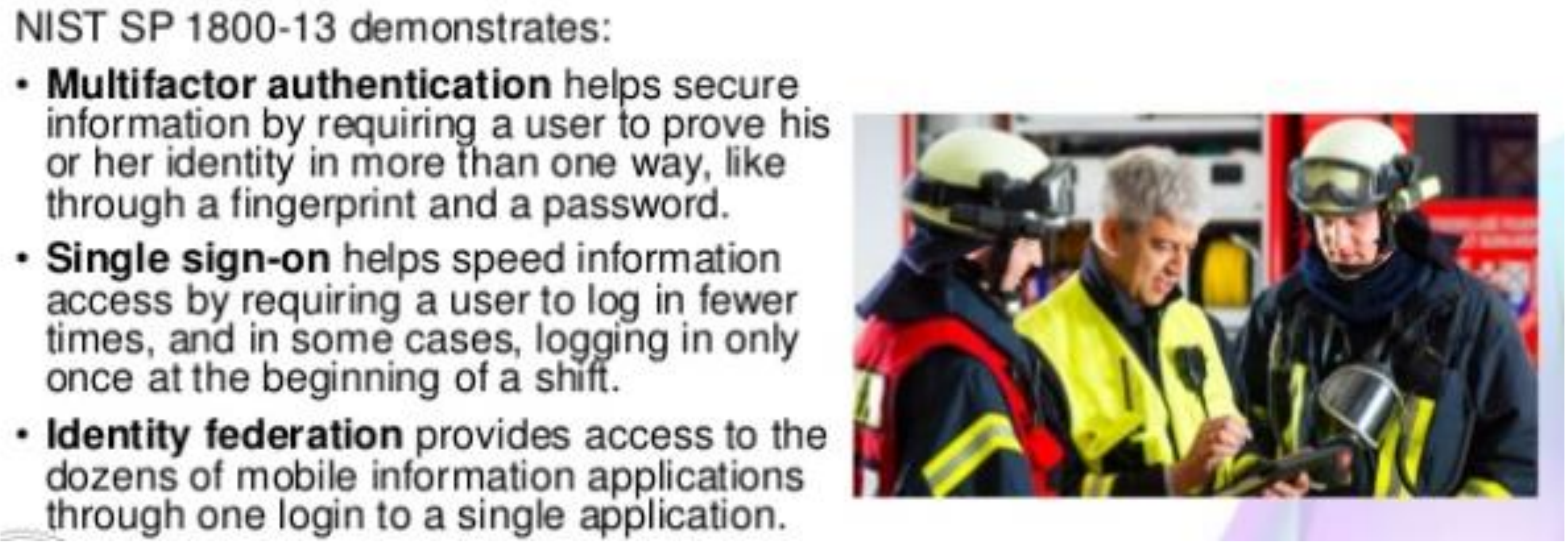


The benefits of implementing NIST SP 1800-12 are:

- **Strong authentication** solutions for using PIV cards with mobile devices. Ensures secure access to websites and email.
- **Cost savings.** Users can access and exchange secure email without an external PIV card reader, eliminating the purchase of new readers.
- Users are able to **easily access work resources** without additional equipment.

Source=2019 Mobile Security for the Enterprise, Identiverse

Resource: Mobile Single Sign-On



NIST SP 1800-13 demonstrates:

- **Multifactor authentication** helps secure information by requiring a user to prove his or her identity in more than one way, like through a fingerprint and a password.
- **Single sign-on** helps speed information access by requiring a user to log in fewer times, and in some cases, logging in only once at the beginning of a shift.
- **Identity federation** provides access to the dozens of mobile information applications through one login to a single application.

Source=2019 Mobile Security for the Enterprise, Identiverse

Thanks for your valuable time today

For assistance please contact:

Susan Clarke: sclarke@mpqhf.org, (307) 248-8179

HIPAA
PASS
PRIVACY AND SECURITY SOLUTIONS

Questions