imprivata®

Enabling Healthcare. Securely.®

Ensuring Clinical Efficiency when Implementing Security Measures

The IoMT Security Conundrum

Dr. Sean Kelly
Chief Medical Officer

Imprivata

Rachel Pickering
IoMT Security Manager

Imprivata

Agenda

- Security vs efficiency
- Interoperability and point of care workflows
- Regulatory drivers for device security
- Security’s impact on clinical efficiency
- Clinical workflow variability

Balancing security and convenience

Common concerns with new technology:

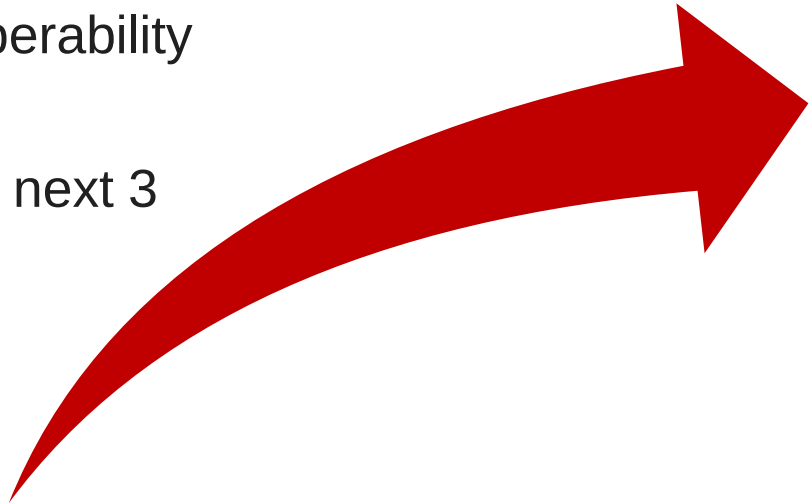
- Learning curves
- Security barriers
- Less time spent face-to-face with patients
- Compounded by IoMT

The reality:

It doesn't have to be this way!

IoMT’s rapid expansion

- Connectivity drives system interoperability and real-time visibility
- IoMT Market to grow by 26% over next 3 years



There is a need to **simplify and streamline** workflows at the bedside to ensure efficiency and mobility

Why IoMT Device Security Matters

- Altered PHI on a device
- Device management/reprograming
- Device availability (DDoS attacks)
- Exfiltration of PHI
- Improper disposal of PHI
- Unauthorized access to network and other connected devices
- Uncontrolled distribution/disablement of passwords

Confidentiality

Integrity

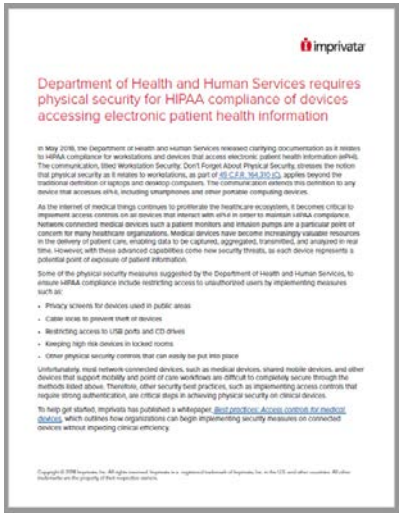
Availability

Safety

HIPAA Compliance for Devices

May 2018 – DHHS updates guidance on physical security

*"The term is defined in the HIPAA Rules as **"a computing device,** for example a laptop or desktop computer, or any **other device that performs similar functions** [emphasis added] and electronic media stored in its immediate environment."*



imprivata

Department of Health and Human Services requires physical security for HIPAA compliance of devices accessing electronic patient health information

In May 2018, the Department of Health and Human Services released clarifying documentation as it relates to HIPAA compliance for workstations and devices that access electronic patient health information (ePHI). The communication, titled Workstation Security Don't Forget About Physical Security, stresses the notion that physical security as it relates to workstations, as part of 45 C.F.R. 164.310 (C), applies beyond the traditional definition of laptops and desktop computers. The communication extends this definition to any device that accesses ePHI, including smartphones and other portable computing devices.

As the internet of medical things continues to proliferate the healthcare ecosystem, it becomes critical to implement access controls on all devices that interact with ePHI in order to maintain HIPAA compliance. Network-connected medical devices such a patient monitors and infusion pumps are a particular point of concern for many healthcare organizations. Medical devices have become increasingly valuable resources in the delivery of patient care, enabling data to be captured, aggregated, transmitted, and analyzed in real time. However, with these advanced capabilities come new security threats, as each device represents a potential point of exposure of patient information.

Some of the physical security measures suggested by the Department of Health and Human Services, to ensure HIPAA compliance include restricting access to unauthorized users by implementing measures such as:

- Privacy screens for devices used in public areas
- Cable locks to prevent theft of devices
- Restricting access to USB ports and CD drives
- Keeping high risk devices in locked rooms
- Other physical security controls that can easily be put into place

Unfortunately, most network-connected devices, such as medical devices, shared mobile devices, and other devices that support mobility and point of care workflows are difficult to completely secure through the methods listed above. Therefore, other security best practices, such as implementing access controls that require strong authentication, are critical steps in achieving physical security on clinical devices.

To help get started, imprivata has published a whitepaper, Best practices: Access control for medical devices, which outlines how organizations can begin implementing security measures on connected devices without impeding clinical efficiency.

The challenge of user authentication

- Enforcing authentication for devices improves security, but…
  - Usernames/passwords are inefficient
  - Providers authenticate to devices **20-25 times/shift**
- Alternative is to not require authentication for devices…
  - Introduces security risks and auditing challenges

Common security workarounds

Password/credential sharing

- Audit issues
- Data integrity

Circumnavigating Interoperability

- Security vulnerabilities
- Wasted investments
- Human error

Removing the need for credentials

- HIPAA Fines
- Unauthorized device access

Clinical Workflow Optimization

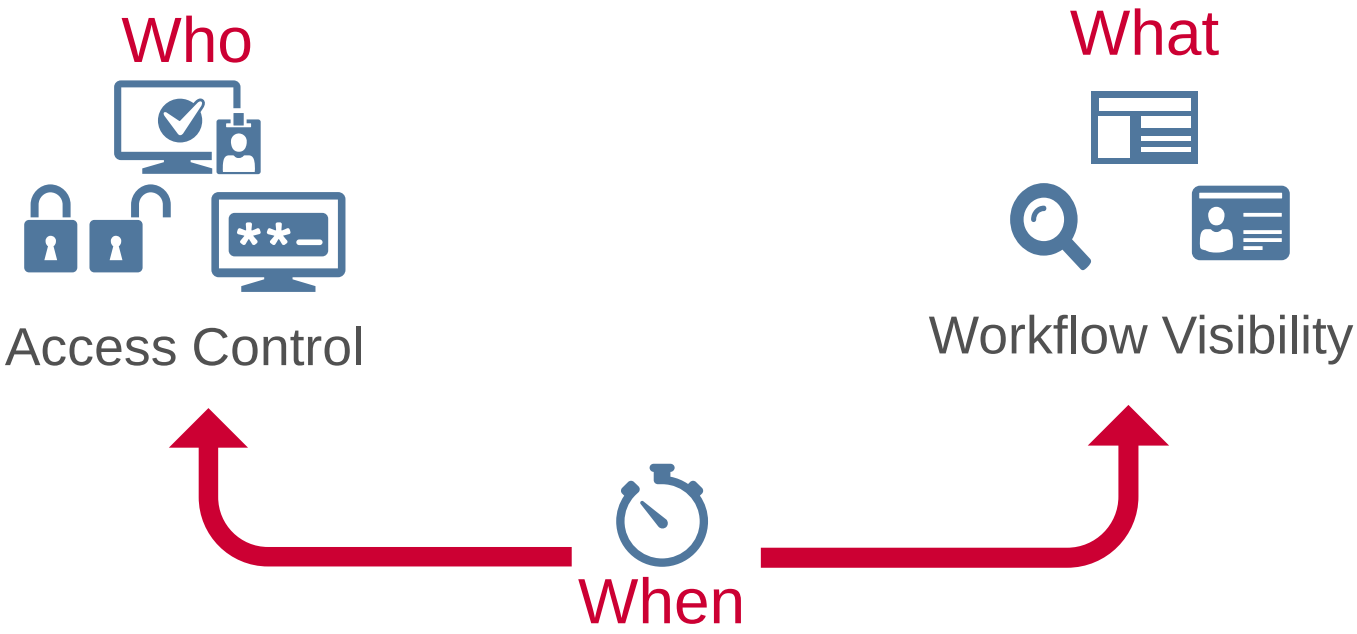
- Workflow variability
- Single-factor vs two-factor authentication
- Grace periods
- Break-glass considerations

imprivata®

An integrated approach to device access control

Imprivata, streamlined IoMT access

Bringing Imprivata workflows and security enhancements to devices



The quick wins of streamlined authentication

Reduce time to log-in by 90%

Allow for tighter auto-lock parameters

Eliminate the use of shared pins or factory-set pins

Achieve complete visibility for user interaction with devices

Improve compliance with security protocols

What would you do with an extra 20 minutes?

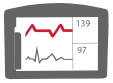
Nurses save time by tapping into workstations with Imprivata

Imprivata OneSign
10 minutes/shift

logins per shift: **30**
Time to login: **20 sec**
ROI @100 nurses: **$85,644/year**

Tap-n-go access everywhere with Imprivata

Extend these workflows to other areas and save even more time:



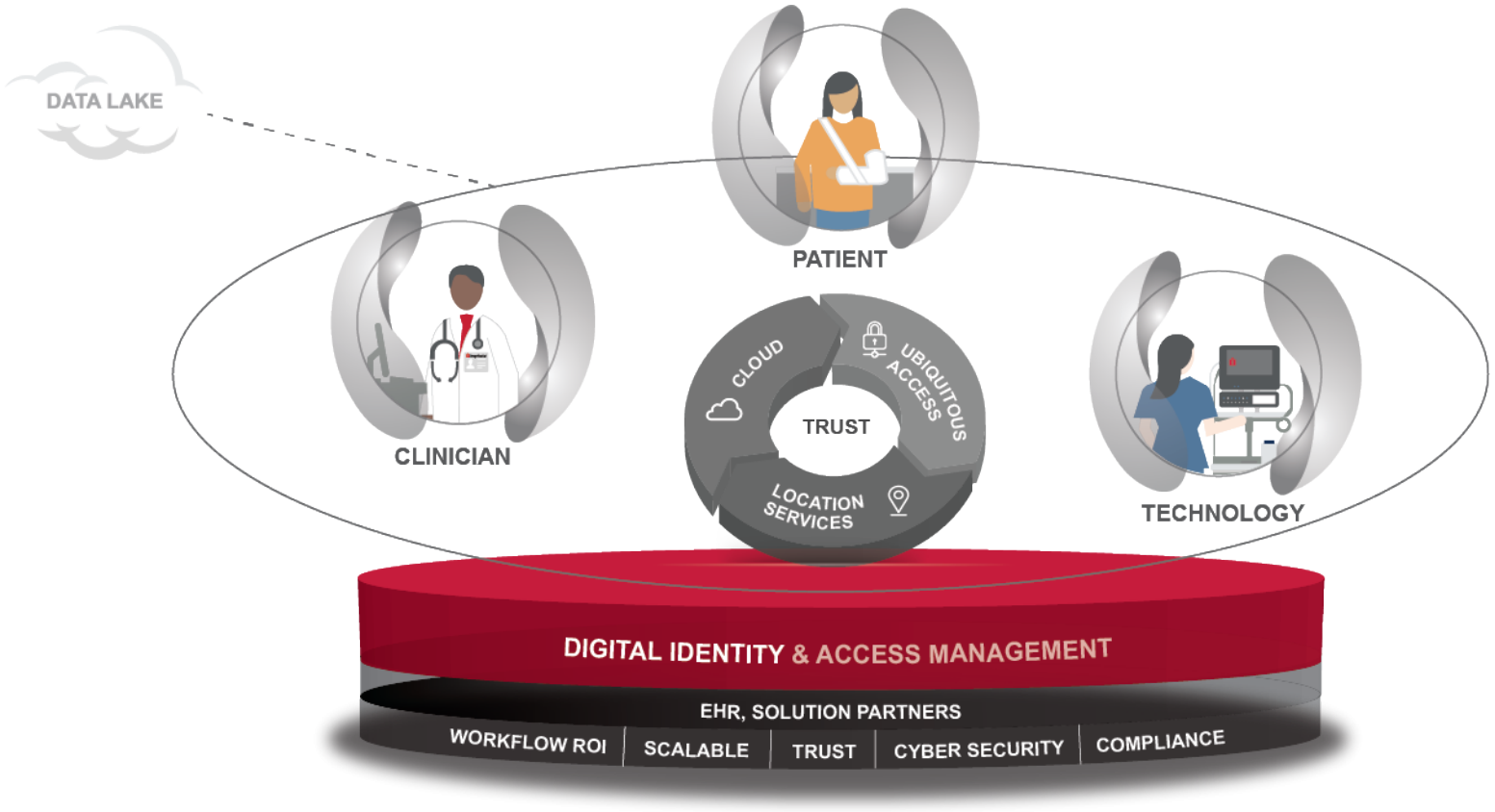
Imprivata Medical Device Access
7 minutes/shift

logins per nurse per shift: **20**
Time to login: **20 sec**
ROI @100 nurses: **$57,200/year**

Imprivata Mobile Device Access
3 minutes/shift

logins per nurse per shift: **8**
Time to login: **20 sec**
ROI @100 nurses: **$22,838/year**

Imprivata enables healthcare securely by establishing trust between people, technology, and information.



Imprivata – trusted market leader

6m
care providers

1700
global healthcare customers

39
countries

Industry leadership

- 30 patents issued to-date
- 2015 & 2016 Best in KLAS
- Elaborate partner eco-system

Company information

- Founded 2002
- Offices in US, UK and Australia
- 420+ employees worldwide

“Imprivata and their solutions are core and strategic to our business because they help access and exchange critical health information securely across the entire enterprise.”
- Baystate Health System, VP, CIO

imprivata®

Questions?


imprivata®
Enabling Healthcare. Securely.®