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/reprogramming
- Device availability (DDoS attacks)
- Exfiltration of PHI
- Improper disposal of PHI
- Unauthorized access to network and other connected devices
- Uncontrolled distribution/disablement of passwords
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” and electronic media stored in its immediate environment.”
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
An integrated approach to device access control
Imprivata, streamlined IoMT access

Bringing Imprivata workflows and security enhancements to devices

Who

Access Control

What

Workflow Visibility

When
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
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

Imprivata Mobile Device Access
3 minutes/shift
logins per nurse per shift: 8
Time to login: 20 sec
ROI @100 nurses: $22,838/year

What would you do with an extra 20 minutes?

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

Tap-n-go access everywhere with Imprivata
Imprivata enables healthcare securely by establishing trust between people, technology, and information.
Imprivata – trusted market leader

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

6m care providers
1700 global healthcare customers
39 countries

Industry leadership

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
Questions?