Solving Healthcare’s Increasingly Complex Security, Compliance, and Workflow Challenges

Purpose-Built Identity and Access Management

October 24, 2019

Dan Borgasano
Vice President of Product Marketing
Imprivata
Agenda

• Why digital identity matters in healthcare?
• Digital IAM framework
• Unique healthcare considerations
• Imprivata digital IAM solutions for healthcare
• Q&A
Healthcare’s initial phases of digital transition
Time consuming and cumbersome to access patient information

45 MINUTES per shift
Increasing pressures on healthcare IT

- Fluid and Dynamic Workforce
- Clinical Operational Efficiency
- Cyberthreats
- Privacy & Compliance Regulations
- Mergers & Acquisitions
- Value Based Care
The care delivery ecosystem is growing in complexity

- Users
  - Admin
  - External users
- Location
  - Home
  - Road
  - Clinic
- Devices
  - Hospital
  - Workstations
  - Medical devices
  - Thin & zero clients
  - Personal devices
  - Virtual apps
  - Mobile apps
  - Web apps
  - SaaS & Cloud apps
- Applications
  - Clinicians
  - Thick-client EHR
  - Personal devices
  - Mobile apps
  - Web apps
  - SaaS & Cloud apps
- The care delivery ecosystem is growing in complexity
Identity is the new perimeter

- Users
  - Admin
  - External users
  - Clinicians
  - Hospital
  - Home
  - Telemedicine
  - Clinic
- Applications
  - SaaS & Cloud apps
  - Virtual apps
  - Thick client apps
  - Workstations
  - Medical devices
  - Thin & zero clients
- Devices
  - Mobile apps
  - Web apps
  - Mobile devices
  - Personal devices

Mobile & Medical devices

Personal & Workstation devices

Mobile & Cloud apps

Thin & SaaS apps

External & Clinicians  

Location

Imprivata
Digital identity and access management (IAM)

Identity Management
- Protect at the front door with day-one readiness

Access & Authentication
- Secure and simplify access to devices, apps, information

Governance & Compliance
- Robust modern solutions with a rich audit trail

- WHO is the user – really?
- WHAT systems does user have access to?
- What are the user’s privileges – to do WHAT, from WHERE?
- Can you PROVE it?
Healthcare has unique IAM needs

Challenges

- Physician burnout
- Fluid workforce
  - New affiliations, M&A
- Increased cyberattacks and regulations

Digital Transformation

- EHR implementation
- Virtualization, mobility, & cloud
- Digital security

Healthcare Digital Identities
Imprivata: Purpose-built IAM solutions for healthcare
Imprivata digital IAM for healthcare

Users
- Clinicians
- Non-clinical
- External users

Devices
- Shared workstation
- Dedicated workstation
- Medical
- Mobile

Apps
- On prem
- Cloud
- Private Cloud
- Mobile

Locations
- Home
- Road
- Hospital
- Clinic

Provisioning
Access
Single Sign-on
Multifactor Authentication

Governance and Compliance
Why it matters…

- IT teams need to provision users for access into appropriate applications
- Manually setting user accounts can be complex and error-prone
- Security team wants users to have right level of access – no more, no less
Provisioning

Why it matters…

• IT teams need to provision users for access into appropriate applications
• Manually setting user accounts can be complex and error-prone
• Security team wants users to have right level of access – no more, no less

Unique healthcare consideration…

• Clinicians need day-one access to deliver patient care
• Users have multiple roles, requiring different types of access
• Healthcare organizations use hundreds of on-prem and cloud apps
Why it matters…

• IT teams need to provision users for access into appropriate applications
• Manually setting user accounts can be complex and error-prone
• Security team wants users to have right level of access – no more, no less

Unique healthcare consideration…

• Clinicians need day-one access to deliver patient care
• Users have multiple roles, requiring different types of access
• Healthcare organizations use hundreds of on-prem and cloud apps

Why Imprivata:

• Quickly provision, update, and deactivate user access
• API-level integrations with major EHRs
• Identity proofing for EPCS
• SSO & MFA / provisioning integration strengthens security, license management, and audit readiness
Access

Why it matters...

- Users need anytime, anywhere access on any device
- Overreliance on usernames and passwords
- Emerging devices require different workflows

Provisioning  Access  Single Sign-on  Multifactor Authentication

Governance and Compliance
Access

Why it matters…

• Users need anytime, anywhere access on any device
• Overreliance on usernames and passwords
• Emerging devices require different workflows

Unique healthcare consideration…

• 78% of doctors have at some point experienced burnout
• 49% of healthcare organizations provide enterprise-owned, shared mobile devices
• Medical devices becoming interconnected
Access

Why it matters:

• Users need anytime, anywhere access on any device
• Overreliance on usernames and passwords
• Emerging devices require different workflows

Unique healthcare consideration:

• 78% of doctors have at some point experienced burnout
• 49% of healthcare organizations provide enterprise-owned, shared mobile devices
• Medical devices becoming interconnected

Why Imprivata:

• Medical and shared mobile device access
• Fast-user switching on shared workstations and mobile devices
• Secure walkaway for continued, proximity-based authentication
• Re-authentication for additional workflows
Single Sign-On

Why it matters…

• Widespread adoption of virtual desktops and mobile devices
• IT has a growing set of applications to support
• Increased adoption of cloud and mobile applications
## Single Sign-On

### Why it matters…

- Widespread adoption of virtual desktops and mobile devices
- IT has a growing set of applications to support
- Increased adoption of cloud and mobile applications

### Unique healthcare consideration…

- SSO needs to be supported on shared workstations and mobile devices
- HIPAA and HITECH require strict security at the expense of efficiency
- Healthcare IT teams manage clinical and non-clinical users
Single Sign-On

Why it matters:
• Widespread adoption of virtual desktops and mobile devices
• IT has a growing set of applications to support
• Increased adoption of cloud and mobile applications

Unique healthcare consideration:
• SSO needs to be supported on shared workstations and mobile devices
• HIPAA and HITECH require strict security at the expense of efficiency
• Healthcare IT teams manage clinical and non-clinical users

Why Imprivata:
• Fast user switching enables SSO on shared workstations and mobile devices
• Ubiquitous access for clinical and non-clinical users to cloud apps
• Easy-to-use application profile generator
• Integrates with identity governance system

Patient room
Roaming desktops
ICU
Pharmacy
Nurses station
Radiology
Emergency room
Roaming desktops
Multifactor authentication

Why it matters…

• Securing PHI and other sensitive data is more critical than ever

• 81% of data breaches involve weak or stolen passwords

• Phishing, other social engineering attacks are highly successful in stealing credentials
Multifactor authentication

Why it matters…

- Securing PHI and other sensitive data is more critical than ever
- 81% of data breaches involve weak or stolen passwords
- Phishing, other social engineering attacks are highly successful in stealing credentials

Unique healthcare considerations…

- EPCS and other unique healthcare workflows require MFA
- Security must be transparent so it does not impact workflow
- MFA must be consistent across workflows to avoid user frustration and workarounds
Multifactor authentication

Why it matters:
• Securing PHI and other sensitive data is more critical than ever
• 81% of data breaches involve weak or stolen passwords
• Phishing, other social engineering attacks are highly successful in stealing credentials

Why Imprivata:
• Innovative, convenient, authentication options tailored to specific MFA requirements
• Complete, end-to-end EPCS compliance
• Extensibility across all clinical, business, and operational MFA workflows

Unique healthcare considerations:
• EPCS and other unique healthcare workflows require MFA
• Security must be transparent so it does not impact workflow
• MFA must be consistent across workflows to avoid user frustration and workarounds
Governance and Compliance

Why it matters…

- Frequent audit requests
- Increased regulatory requirements
- Greater risk of data breaches with higher fines
Governance and Compliance

Why it matters…

• Frequent audit requests
• Increased regulatory requirements
• Greater risk of data breaches with higher fines

Unique healthcare consideration…

• Strict reporting requirements from the DEA for EPCS
• Healthcare orgs more likely to be hacked due to value of PHI
• Healthcare data breaches more costly than other industries
Governance and Compliance

Why it matters:
• Frequent audit requests
• Increased regulatory requirements
• Greater risk of data breaches with higher fines

Unique healthcare consideration:
• Strict reporting requirements from the DEA for EPCS
• Healthcare orgs more likely to be hacked due to value of PHI
• Healthcare data breaches more costly than other industries

Why Imprivata:
• Real-time reporting and logical access control for EPCS
• Integrates identity data with access data for license management and audit response
• Out-of-box and customizable reports delivering real-time utilization data
Imprivata Digital IAM for healthcare

Users
- Clinicians
- Non-clinical
- External users

Devices
- Shared workstation
- Dedicated workstation
- Medical
- Mobile

Provisioning
Access
Single Sign-on
Multifactor authentication

Governance and Compliance

Apps
- On prem
- Cloud
- Private Cloud
- Mobile

Locations
- Home
- Road
- Hospital
- Clinic
Questions?