Bring Your Own Device: Calling for a Strategy

CHIME College Live

23 April 2014
Bring Your Own Device (BYOD)

Topics

» Introductions
» Learning Objectives
» Business Drivers
» Key Strategies
» Policy Issues
» Technical Infrastructure
» Wrap-Up
Introduction
Introductions

Kurt Salmon welcomes you to this CHIME College Live

Gerard Nussbaum
Director, Technology Services

Brian Lin
Partner
About Kurt Salmon

Extensive, relevant EXPERIENCE
  » Academic, children’s, community & national health systems
Change LEADERS
  » Highly pragmatic and focused
PROVEN team
  » Careers spent supporting leading health systems and complex environments
Track record of SUCCESS
  » Rich history dating to 1947
  » Over 75% of ongoing work with repeat clients
About Kurt Salmon: Information Technology

**STRATEGY and PLANNING**
- Strategic and Tactical Planning
- Physician-Hospital Alignment
- Connecting Communities
- Population Health and Care Coordination
- Technology Planning for New Facilities
- Business Intelligence and Analytics

**VENDOR SELECTION and SUPPORT**
- Vendor Selection and Contract Negotiation
- Pre-implementation Planning
- Implementation Oversight

**REGULATORY COMPLIANCE**
- Meaningful Use Achievement
- ICD-10 Preparation
- Security and Privacy Compliance

**INFRASTRUCTURE and OPERATIONS**
- IT Transformation
- Infrastructure Planning
- Right Sourcing
- Interim Leadership
Learning Objectives

» Understand the major business drivers for BYOD
» Articulate the key aspects of a successful BYOD strategy
» Identify key BYOD policies that should be adopted
» Articulate the key features and functions of the BYOD technical infrastructure
Business Drivers
Business Drivers

Rapid Growth in Mobile Devices

• By 2018 there will be almost five billion mobile devices
  
• Connected devices per knowledge worker
  • 2012: 2.8
  • 2014: 3.3

• Mobility/IT spending
  • 2014: 20%
  • 2010: 12%

Sources:
Business Drivers

The capabilities of mobile devices are increasing rapidly

» Data speeds
» Volume of data
» Memory
» Processing power
» Flexibility

Source:
Business Drivers

Beyond smartphones and tablets

» Wearable devices growth will be 57% through 2018 (projected)\(^1\)

» Wearable computing will introduce new issues

» Wearable computing linked to cloud computing

Source:
Business Drivers

Smartphones and Tablets

» Faster growth than other computing devices
» iOS and Android are the majority share
» Dedicated apps versus off-the-shelf apps

Sources: 1. Gartner Group; 2. BI Intelligence
Business Drivers

BYOD provides a number of advantages

» Productivity
» Accessibility
» Collaboration
» Staff and employee satisfier
» Evolving work models
» Just-in-time information
» Broadens cohort with mobile access
» Lowers asset investment
Business Drivers

BYOD raises challenges

» Security
» Information control
» Data
  – Protection
  – Loss
  – Secondary uses
» Support model
» Rapid life cycles
» Training
» Policies
» Enforcement
» Privacy
» Human resources and compensation
» Biomedical device
» Separating personal and work—blurring

Business Drivers

Mobile devices pose risk for loss of data

- One lost laptop = $1,725,220 + 2-year corrective action plan
  - Concentra Health Services (Missouri)
  - Unencrypted laptop stolen from a facility
  - Risk analyses identified unencrypted mobile devices deficiency
  - Settlement 22 April 2014

Covered entities and business associates must understand that mobile device security is their obligation … encryption is your best defense against these incidents

Susan McAndrew
Deputy Director, Health Information Privacy
Office of Civil Rights
U.S. Department of Health & Human Services

Key Strategies
BYOD: A Few More Statistics

» 90% of companies will offer BYOD options to employees by 2014, according to Gartner.

» According to a recent survey by Citrix, the percentage of BYO laptops will increase from 18% to 25% of an organization’s total desktop environment.

» Although 68% of organizations across industries have some form of a “bring your own device” policy, just 39% have a mobile data management system in place, according to a 2013 survey from InformationWeek.
BYOD Strategy

“Begin at the beginning”

» First determine if BYOD is appropriate for your organization

» Some organizations may not have the resources necessary to support all of the requirements—may pursue a “closed” policy for its mobile environment

» Many organizations will determine that BYOD is appropriate—and are in fact in the midst of supporting a “de facto” BYOD environment without a formal strategy
BYOD Strategy

The strategy needs to consider and define:

» Business Goals
  – “Ubiquitous access to information”
  – “Increase efficiency of workflows”
  – “Workforce satisfaction”

» Use Cases
  – Functional need
  – End-user experience
  – Information requirements
  – Security implications

» Architecture
  – Data storage
  – Device types
  – Operating systems
  – Network requirements

» Management
  – Mobile device management (MDM) system
  – Integration with enterprise workstation management tools
## BYOD Strategy—Infrastructure Architecture

<table>
<thead>
<tr>
<th>Key Architecture Areas</th>
<th>Options</th>
<th>Example Determining Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient and Confidential Data Storage</td>
<td>Virtual, locally encrypted, “containerized,” or hybrid</td>
<td>Level of security required, adaptability of application to endpoint</td>
</tr>
<tr>
<td>Types of Devices Supported</td>
<td>Phones, tablets, laptops, ultrabooks, PCs</td>
<td>Business goals, use cases, IT enterprise standards</td>
</tr>
<tr>
<td>Vendors’ Operating Systems Supported</td>
<td>iOS, Android (version/manufacturer), Windows, others</td>
<td>Business goals, use cases, IT support bandwidth/capabilities</td>
</tr>
</tbody>
</table>
Policy Issues
Policy Design

BYOD policies should take into account

» Business reasons for adopting BYOD
» Overall BYOD strategy
» Balancing risks and benefits
» Relationship to other policies, including
  – Information security
  – Remote access
  – Privacy
  – Employment
» Level of control over users
» Resources
Policy Areas of Coverage

» Legal regulatory requirements
  – HIPAA
  – Privacy
  – Labor

» Privacy and data security
  – Malware risk
  – Device loss
  – Cybercrime
  – Data theft
  – Password/PIN requirements
  – Encryption

» Ownership of data
  – Return of data
  – Personal data

» User monitoring
  – Location-aware apps
  – Access to data
  – Employee monitoring

» Mobile Device Management Requirements
» Intellectual property
» Cyber liability insurance
» Liability waivers
» Software licensing
» E-Discovery
» Investigation and incident response
» Backup responsibilities
» Privileges and revocations
» Remote wipe
» Limits on use of corporate provided/paid apps
» Sanctions

A policy is not a technical document. Delegate appropriately to information technology, security and privacy officers, and others for technical requirements.
Policy Development

Developing a robust BYOD policy requires a collaborative effort, including representatives from:

» Information Technology
» Legal
» Compliance/Internal Audit
» Risk Management
» Security
» Human Resources
» Medical Staff
» Finance
» Faculty
» Residents
Policy Considerations

» Classes/groups eligible for BYOD program
» Limits on eligible devices/operating systems
» Access to company network only through restricted channels
» No locally stored enterprise information
» Reporting lost/stolen devices
» Return of data/apps on end of relationship
» Exposure/loss of employee personal information
» Security requirements
  – Strong passwords, no password sharing
  – Mobile device management software; may not interfere
  – No device sharing
  – Containerization versus native experience
» Backup/data synchronization
» Differentiate use of Internet access from access to systems
Policy Care and Feeding

Your BYOD policy requires regular attention

» Review quarterly

» Adjust for changes
  – Device capabilities
  – Central management technology
  – Legal/regulatory changes

» Learn from your experiences
Policy Companions

The policy alone does not suffice

» Training
» Monitoring and auditing
» Enforcement
» Technical infrastructure
» Security risk analysis + risk management
» Incident response plans and simulations
» Regular inventories
  - Devices that have not connected in a while
  - Newly connected devices
» Service level agreements
Technical Infrastructure
Technical Infrastructure and Service

Prepare the technical environment and service capacity

*Implications for Enterprise Infrastructure Environment*

» Wireless capacity—multiple devices from a single employee
» Network access controls—need robust tools to limit access to internal networks
» VDI capacity and management
» Prepare existing infrastructure management tools for integration with MDM

*Implications for the Infrastructure Service Environment*

» Need to clearly define parameters and extent of services
» Estimate additional service desk volumes
Technical Infrastructure—Examples of Basic MDM Features

**Security**

- Enforcing device PIN/password usage
- Remote device lock/wipe
- Data encryption
- Jailbreak/root detection
- Data loss prevention

**Device Management**

- Remote configuration
- Remote operating system and application updating
- Remote inventorying
- Remote control

**Application Management**

- Applications whitelists and blacklists
- Enterprise app stores
- Data wipe by application
## Technical Infrastructure—Examples of MDM Differentiators

<table>
<thead>
<tr>
<th>Key Differentiators</th>
<th>Business Need/Function Addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Containerization capabilities</td>
<td>Separating personal from business</td>
</tr>
<tr>
<td>• Data</td>
<td></td>
</tr>
<tr>
<td>• Native OS/applications (dual personas)</td>
<td></td>
</tr>
<tr>
<td>• Enterprise applications</td>
<td></td>
</tr>
<tr>
<td>Ability to manage ultrabooks/laptops/integrate with third-party desktop management</td>
<td>Providing a single source for BYOD management—not just “mobility devices”</td>
</tr>
<tr>
<td>Breadth of hardware and operating systems supported</td>
<td>Required for organizations that have made the strategic decision to support multiple platforms</td>
</tr>
<tr>
<td>Geofencing/timefencing rules</td>
<td>Provides granular control of BYOD functions to enhance security</td>
</tr>
</tbody>
</table>
Wrap-Up
Key Takeaways

1. Understand why you are embarking on supporting BYOD
2. Identify key constituencies
3. BYOD is one element of the overall management of access
4. Create clear policies
5. Perform a security risk analysis and address deficiencies
6. Ongoing funding is needed to keep pace
7. BYOD is rapidly evolving, leading to short life cycles
8. Focus on a few device platforms to develop expertise
9. Consider leveraging service providers for user support
10. Define service level agreements with clear responsibilities

Source: Kurt Salmon Health Care Group
THANK YOU!

Gerard Nussbaum  
Director, Technology Services  
gerard.nussbaum@kurtsalmon.com  
212.508.8371

Brian Lin  
Partner  
brian.lin@kurtsalmon.com  
212.508.8301
Appendix
Sample Policy
Appendix: Sample Mobile Devices Policy

This appendix contains a sample policy

» For informational and educational purposes only
» In no way intended as legal advice
» Each organization will need to develop its policies in
  – Accordance with its own needs
  – Consonance with the organization’s overall policy framework
  – Compliance with all applicable laws and regulations
» Rely upon this sample at your own risk
» Credit is due to John Christiansen/Christiansen IT Law
  • Provided under a Creative Commons Attribution-ShareAlike license
  • No changes were made, except formatting to fit this document
Appendix: Sample Mobile Devices Policy

A. **Purpose.** The purpose of this Mobile Devices Policy is to allow for the authorized use of smartphones and other portable computing and communications devices (“Mobile Devices”) at COVERED ENTITY Facilities by authorized members of the COVERED ENTITY Workforce (“Users”).

B. **General Introduction.** Mobile Devices can support better health care and more efficient administration in health care organizations. At the same time the use of such devices creates new risks to patient privacy, Protected Health Information (“PHI”) and employee and organizational confidentiality, and intellectual property. This Policy is therefore intended to permit the use of such devices while managing the risks they present.

The use of Mobile Devices under this Policy is a privilege which may be terminated at any time for violation of this Policy, or as a sanction for violation of other COVERED ENTITY policies. Violation of this Policy may be grounds for other sanctions as well.

C. **Individuals Subject to this Policy.** This Policy applies to all members of the COVERED ENTITY Workforce, including all employees, volunteers, trainees and any other person whose conduct is under the direct control of COVERED ENTITY in the performance of work for or on behalf of COVERED ENTITY.

D. **Information Subject to this Policy.** This Policy applies to all information owned by COVERED ENTITY, as well as all private, sensitive or confidential information which COVERED ENTITY is obliged by law or contract to protect against unauthorized use, disclosure, copying or alteration. This includes, without limitation:

- Protected Health Information, as defined under HIPAA.
- Intellectual property such as copyrighted text or graphics.
- Confidential personal or organizational information, such as employee records and financial information.
- Sensitive visual information, such as patient faces or physical security safeguards, which may be subject to photographing or video capture.
- Metadata pertaining to events and activities occurring in or by use of a Mobile Device, or any other electronic computing or communication device.
Appendix: Sample Mobile Devices Policy

E. Devices Subject to this Policy. This Policy applies to all electronic computing and communications devices which may be readily carried by an individual and is capable of receiving, processing, or transmitting digital information, whether directly through download or upload, text entry, photograph or video, from any data source, whether through wireless, network or direct connection to a computer, other Portable Device, or any equipment capable of recording, storing or transmitting digital information (such as copiers or medical devices). Mobile Devices therefore include but are not limited to smartphones, digital music players, hand-held computers, laptop computers, tablet computers, and personal digital assistants (PDAs).

Digital storage devices such as portable hard drives and USB (thumb) drives, as well as office and medical equipment capable of recording, storing or transmitting digital information, such as imaging equipment or copiers, are not Mobile Devices subject to this Policy. Please see <applicable COVERED ENTITY policies> for information on such devices.

This Policy applies to personally-owned Mobile Devices as well as Mobile Devices owned or leased and provided by COVERED ENTITY.

F. Prohibited Mobile Devices. Mobile Devices which may produce electromagnetic interference with medical devices or equipment, or which cannot be or have not been configured to comply with this Policy, are prohibited.
G. Authorization to Use Mobile Devices. No Mobile Device may be used for any purpose or activity involving information subject to this Policy without prior registration of the device and written authorization by <the IT Department/Security Office/etc.>. Authorization will be given only for use of Mobile Devices which <the IT Department/Security Office/etc.> has confirmed have been configured so that it complies with this Policy. Authorization must be requested in writing by the <supervisor or head of the department in which the User works>. Access to, obtaining, use and disclosure of information subject to this Policy by a Mobile Device, and any use of a Mobile Device in any COVERED ENTITY facility or office, including an authorized home office or remote site, must be in compliance with all COVERED ENTITY policies at all times.

Authorization to use a Mobile Device may be suspended at any time:
» If the User fails or refuses to comply with this Policy;
» In order to avoid, prevent or mitigate the consequences of a violation of this Policy;
» In connection with the investigation of a possible or proven security breach, security incident, or violation of COVERED ENTITY’ policies;
» In order to protect individual life, health, privacy, reputational or financial interests; to protect any assets, information, reputational or financial interests of COVERED ENTITY;
» Upon request of the <supervisor or head of the department in which the User works>; or
» Upon the direction of <the CISO, CIO, General Counsel, CFO, COO, CEO, CRO?>.

Authorization to use a Mobile Device terminates:
» Automatically upon the termination of a User’s status as a member of the COVERED ENTITY Workforce;
» Upon a change in the User’s role as a member of the COVERED ENTITY Workforce, unless continued authorization is requested by the <supervisor or head of the department in which the User works>.
» If it is determined that the User violated this or any other COVERED ENTITY policy, in accordance with COVERED ENTITY’ policies.

The use of a Mobile Device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy.
Appendix: Sample Mobile Devices Policy

H. Audit of Mobile Devices. Upon request by the <the IT Department/Security Office/etc.>, at its sole discretion at any time, any Mobile Device may be subject to audit to ensure compliance with this and other COVERED ENTITY policies. Any User receiving such a request shall transfer possession of the Mobile Device to <the IT Department/Security Office/etc.> at once, unless a later transfer date and time is indicated in the request, and shall not delete or modify any information subject to this Policy which is stored on the Mobile Device after receiving the request.

I. Evidentiary Access to Mobile Devices. Upon notice of a litigation hold by the <the IT Department/Security Office/etc.> or <Legal Department>, at their sole discretion at any time, any Mobile Device may be subject to transfer to the possession of the <the IT Department/Security Office/etc.> to ensure compliance with the litigation hold. Any User receiving such a notification shall transfer possession of the Mobile Device to <the IT Department/Security Office/etc.> at once, unless a later transfer date and time is indicated in the notification, and shall not delete or modify any information subject to this Policy which is stored on the Mobile Device after receiving the request.
Appendix: Sample Mobile Devices Policy

J. Mobile Device User Responsibilities. In addition to other requirements and prohibitions of this and other COVERED ENTITY policies, Mobile Device Users have the following responsibilities:

» Information subject to this Policy which is stored on the Mobile Device must be encrypted as provided in COVERED ENTITY policy. Information subject to this Policy should not be stored on the Mobile Device for any period longer than necessary for the purpose for which it is stored.

» A Mobile Device may not be shared at any time when unencrypted information subject to this Policy is stored on the device.

» A Mobile Device which does not have unencrypted information subject to this Policy stored on it may be shared temporarily, provided that:

» The User may not share the password or PIN number used to access the Mobile Device, but must open access for shared use him- or herself.

» The configuration of the device to comply with this Policy must not be changed.

» The individual using the device must not further share it; must protect it against being misplaced, lost or stolen, and must immediately report to the User if it is; and must return it promptly to the authorized user when finished with the temporary use.

» The individual using the device must not use it to obtain, process, use or disclose information subject to this Policy.

» Access to each Mobile Device must be controlled by a password or PIN number consistent with COVERED ENTITY policy. Password or PINs must be changed periodically as provided in COVERED ENTITY policy. The Mobile Device must provide for a maximum of __ attempts to enter the password or PIN correctly.

» The timeout for access to the Mobile Devices must be a maximum of __ minutes.

» Information subject to this Policy which is transmitted wirelessly by the Mobile Device must be encrypted unless an exception is authorized. Exceptions must be authorized by <the IT Department/Security Office/etc.>.
Appendix: Sample Mobile Devices Policy

J. Mobile Device User Responsibilities. continued

» If possible, Mobile Devices must have antivirus software. Mobile Devices which cannot support antivirus software may be subject to limitations on use at the discretion of <the IT Department/Security Office/etc.>, as specified in writing by the <the IT Department/Security Office/etc.>.

» Physical protection for Mobile Devices must be provided as required by COVERED ENTITY policy.

» If the Mobile Device is misplaced, stolen or believed to be compromised this must be immediately reported to <the IT Department/Security Office/etc.>.

» Applications and services installed on the Mobile Device must be approved by <the IT Department/Security Office/etc.>.

» Bluetooth and infrared (IR) services must be configured as approved by <the IT Department/Security Office/etc.> or turned off.

» Mobile Devices must be disposed of according to COVERED ENTITY policy.
Appendix: Sample Mobile Devices Policy

K. Personal Use of Mobile Devices. Personal Use of Mobile Devices owned or leased and provided by COVERED ENTITY is subject to the COVERED ENTITY Acceptable Use Policy.

Personal use of personally-owned Mobile Devices is not subject to the Acceptable Use Policy, but must at all times be consistent with this Policy.

All information on a Mobile Device, including personal information about or entered by the User, may be subject to audit or evidentiary review as provided in this Policy. Any such personal information may be used or disclosed by COVERED ENTITY to the extent it deems reasonably necessary:

» In order to avoid, prevent or mitigate the consequences of a violation of this Policy;
» In connection with the investigation of a possible or proven security breach, security incident, or violation of COVERED ENTITY policies;
» In order to protect the life, health, privacy, reputational or financial interests of any individual;
» To protect any assets, information, reputational or financial interests of COVERED ENTITY;
» For purposes of determining sanctions against the User or any other member of the COVERED ENTITY Workforce;
» For purposes of litigation involving the User;
» If Required by Law.
Appendix: Sample Mobile Devices Policy

L. Prohibited Uses of Mobile Devices.

The following uses of Mobile Devices are prohibited:

» The storage of information subject to this Policy, including voice messages, voice notes, email, instant messages, web pages and electronic documents, photographs, images and videos, unless they are encrypted.

» The Internet or wireless transmission or upload of information subject to this Policy, including voice messages, voice notes, email, instant messages, web pages and electronic documents, photographs, images and videos, without encryption, unless previously authorized in writing by <the IT Department/Security Office/etc.>.

» The creation of any photograph, image, video, voice or other recording of any individual who is a patient or member of the Workforce of COVERED ENTITY, except in compliance with COVERED ENTITY policy.

» The creation of any photograph, image, video, voice or other recording of any document, record, computer or device screen which includes information subject to this Policy, except in compliance with COVERED ENTITY policy.