Mobile Device Security in Healthcare

June 2015

Ricky Bloomfield, MD
Director, Mobile Technology Strategy
Assistant Professor, Internal Medicine-Pediatrics
Duke Medicine
In 2013, there were:

- ~43,000 health-related apps
- 7,400 for health professionals
- >50% had been downloaded less than 500 times
- 5 apps accounted for 15% of sales
Apple HealthKit

Apple HealthKit

The Information Security Tug-of-War...

Laws & Regulations
Business & Legal Risks
Strict Policies & Procedures
Reduced Revenues & Reimbursements
Higher Costs

Quick & Easy Access to Clinical Records
Research & Innovation
Engagement & Collaboration
Agility & Time to Market
Flexibility & Adaptability

DATA CLASSIFICATION: PUBLIC
Mobility in Healthcare – It's here, and it's not going away
The Mobile Security Must-Dos

- Risk Management
  - Enterprise Risk Assessment
  - Application Risk Assessment
- Administrative Controls (Policy)
- Technical Controls
- Awareness
Enterprise Risk Management Process

• Identify and evaluate the organization's mobile device threats and vulnerabilities

• Use governance processes to determine tolerance levels for identified risks
  – Where possible, use established governance processes / groups

• Establish controls to address identified vulnerabilities
  – Administrative controls (policies and procedures)
  – Technical controls (MDM / MAM)
  – Mandatory training

• Review and update the risk assessment on a regular basis
  – e.g. every 1 to 3 years
Mobile Device Risk Assessment
Reference Resources

• NIST Special Publication 800-124 – “Guidelines for Managing the Security of Mobile Devices in the Enterprise” (June 2013)

• ENISA report – “Smartphones: Information security risks, opportunities, and recommendations for users” (Dec 2010)
Common Mobile Device Threats

- Data leakage from unsecured lost or stolen devices
- Improper disposal of retired devices
- Unintentional data disclosure through untrusted apps
  - Poor data handling and privacy controls in apps
  - Automated data syncing to cloud-based services
  - Spyware, malware, and other rogue applications
- Unintentional data disclosure through untrusted networks
  - Wi-Fi and Bluetooth network spoofing
  - Surveillance of network traffic
- Phishing attacks
Common Mobile Device Vulnerabilities

- App and OS patching weaknesses
- Intentionally compromised devices (jailbreaking/rooting)
- Inadequate app review processes
- Impersonation of apps
- Sandboxing failures
- User permissions fatigue
- Encryption weaknesses
- Lack of software development best practices for apps
- Lack of user awareness
Mobile Application Risk Assessment

• Understand and document the app's data flows and storage
  – Ensure encryption is used where appropriate
  – Identify third parties who are storing, processing, or transmitting data
    • For clinical applications, these are probably Business Associates, and a BAA may be required
    • Ensure that you’re using the latest BAA from your institution, as the HITECH Act may have necessitated changes
Application Risk Assessment: Understanding the Data Flows

1. **wearable**
   - Bluetooth
   - Data: Pedometer, Sleep

2. **pulse oximeter**
   - Bluetooth
   - Data: Oxygen, pulse

3. **scale**
   - WiFi
   - Data: Weight

4. **BP monitor**
   - Bluetooth
   - Data: Blood Pressure

5. **Participant phone**
   - Data tracking, analysis, and visualization

6. **Online Dashboard 1**
   - HTTPS
   - Data: Pedometer, Sleep, Dietary, Blood Pressure

7. **Online Dashboard 2**
   - HTTPS
   - Data: Pedometer, Sleep, Dietary

8. **Central Mobile Platform Manager**
   - HTTPS
   - Data: Pedometer, Sleep, Dietary, Blood Pressure, phone number, health messages, patient study number

9. **Commercial Texting Service**
   - SMS/Text
   - Data: Phone number, health messages
   - E-mail
   - Data: Phone number, health messages

**DATA CLASSIFICATION: PUBLIC**
Mobile Application Risk Assessment

- Review the app's privacy and security settings
- Determine possible interactions with other apps
  - Social media (Facebook, Twitter, etc...)
  - Camera roll
  - Contacts
  - Calendar
  - Location (GPS)
  - Microphone
- Review the app developer's software development practices
  - Are best practices like OWASP employed?
  - Are vulnerability assessments and penetration tests performed?
Mobile Device Policy Considerations

- Select an approach: corporate-owned devices vs. BYOD vs. hybrid
  - Industry trends point towards the inevitability of BYOD
  - In academic medical centers, BYOD is a fact of life
- Disallow or limit the storage of PHI and other company data on mobile devices
  - Use remote access vs. storing data locally on mobile devices
- Define policies for technical controls
  - Require passcodes / passphrases
  - Require auto-lock
  - Set to wipe after X failed logins
  - Require encryption features to be enabled
  - Disallow jailbroken / rooted devices from connecting to the network
  - Malware protection (more important for Android; not available for iOS)
  - App whitelisting or blacklisting
  - Data loss prevention (DLP)
- Define policies for device decommissioning
  - Wiping before disposing of the device or upon employ termination
Mobile Device Policy Considerations: User Education

1. Use password protected access and auto-lock
2. Control wireless network and service connections
3. Backup your data
4. Beware of free applications and feeds
5. Never store sensitive or confidential data on your device
6. Control application access and permissions
7. Keep your OS, firmware, and software up-to-date
8. Wear devices automatically if lost or stolen
9. Use it approved antivirus or scanning tools
10. Use it authorized device management software
Mobile Device Policy Considerations: User Acceptable Use Agreement

• Users should be required to sign an acceptable use agreement, including terms such as the following:
  – The user acknowledges that company has the right to install security agents and manage security settings on the user's mobile devices
  – The user acknowledges that the company has the right to disallow the use of certain apps or functionality on the device
  – The user agrees to not disable, modify, or otherwise bypass security agents and settings
  – The user agrees to not to store PHI on the device, except in cases that may be explicitly allowed (e.g. cached email)
  – The user agrees to immediately report any lost or stolen device
  – The user acknowledges that the company has the right to remotely wipe the device if lost or stolen
  – The user acknowledges that the company has the right to monitor usage of the device, and to inspect or make a copy of the device for investigations or legal hold
  – The user acknowledges that company data and apps must be removed from the device if the user's relationship with the company ceases; this may involve wiping the device
  – User acknowledges that they may be subject to sanctions if they fail to follow policies
Enforcing Technical Controls: MDM & MAM

• There are a variety of Mobile Device Management (MDM) solutions that can enforce device security settings and other configuration items:
  – Microsoft ActiveSync is the entry level MDM solution for most organizations, as it is built into Exchange
    • Does not include more advanced capabilities, such as app whitelisting and blacklisting
  – Others provide more sophisticated controls:
    • MobileIron, Airwatch, Citrix ZenMobile (was ZenPrise), Zscaler, IBM Endpoint Manager, Symantec, McAfee, Sanf, etc...

• Also consider Mobile Application Management (MAM) as an alternate approach
  – MDM provides the ability to control and monitor device settings, where MAM provides wrappers around applications to ensure that they behave within policy definitions
Mobile Device Security Awareness

- Important for creating a "culture of compliance"
- Incorporate into new hire and annual training modules
  - Where possible, integrate with existing Learning Management System to leverage centralized tracking of training completion
- Topics to consider:
  - Overview of security threats to mobile devices, such as:
    - Untrusted apps
    - Untrusted networks
    - Lost & stolen devices
    - Dangers of jailbreaking / rooting devices
  - Review of required mobile device security settings
  - Review of corporate acceptable use policies
iOS vs. Android

• Per the F-Secure Mobile Threat Report for Q1 2014, Android has consistently faced more threats than iOS
  – In the first three months of 2014 alone, 275 out of 277 new threats targeted the Android platform
  – 1 new threat for iOS
  – 1 new threat for Symbian

• More creative threats for Android:
  – Trojan:Android/Torsm.A – first threat to use Tor to hide communications with its command and control server
  – Trojan:Android/Oldboot.A – first bootkit
  – Dendroid toolkit – promises to make creating Android trojans as simple as clicking a few buttons (and comes with a lifetime warranty!)
Mobile Device Security Benefits (Yes, there are some!)

• Modern mobile device operating systems were generally designed to be more secure than desktop operating systems
  – Smaller memory footprint requires reduced functionality
  – Application sandboxing limits the ability of an app to gain unauthorized access to another app's data
  – In later releases of iOS and Android, device encryption has become a standard feature (your mileage may vary on Android)
  – Curated app stores can help reduce the chance of malware installation (particularly true for iOS)
  – Ability to remotely locate and wipe a lost or stolen device has become a standard feature
Duke: Maestro **Innovate**  
Interoperability Framework

- Set of **technologies** and **policies** to allow applications to easily and **securely** access patient data

- Two major app categories:
  - **Patient-centric**: intended to be used primarily by patients as informational references or to submit patient-generated data (e.g., smartphone-tethered medical devices, patient-reported outcomes, etc.)
  - **Provider-centric**: intended to be used primarily by providers in a clinical setting (e.g., references, calculators, decision-support tools, patient monitoring, telemedicine, etc.)
Duke: Maestro **Innovate**
SMART on FHIR

- Based on FHIR REST APIs sponsored by HL7
- Incorporates OAuth and OpenID Connect
- Allows for creation of app once, the deployment across all EHRs that support the standards
## Regulations that Impact Mobile Apps

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Health Insurance Portability and Accountability Act of 1996 (HIPAA):</strong></td>
<td>Title II requires national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers and addresses security and privacy of health data.</td>
<td><a href="http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html">http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html</a></td>
</tr>
<tr>
<td><strong>Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH):</strong></td>
<td>Provides incentives for demonstrating meaningful use of Certified Electronic Health Record Technology (CEHRT) through 2015 and penalties for non-use thereafter. Guidance on breach notification. Increases criminal and civil liability for non-compliance.</td>
<td></td>
</tr>
<tr>
<td><strong>Omnibus Rule (2013):</strong></td>
<td>Strengthens and clarifies prior protections. Expands requirements for business associates and contractors. Sets new limits on how information is used, disclosed or sold.</td>
<td></td>
</tr>
<tr>
<td><strong>Family Educational Rights and Privacy Act of 1974 (FERPA):</strong></td>
<td>Outlines access to educational records and provides for some control over disclosure of educational information.</td>
<td><a href="http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hipaferpajointguide.pdf">http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hipaferpajointguide.pdf</a></td>
</tr>
<tr>
<td><strong>Payment Card Industry Data Security Standard (PCI &amp; PA DSS):</strong></td>
<td>Guidelines to increased controls around cardholder data to reduce credit card fraud.</td>
<td><a href="https://www.pcisecuritystandards.org/security_standards/">https://www.pcisecuritystandards.org/security_standards/</a></td>
</tr>
<tr>
<td><strong>Food and Drug Administration (FDA):</strong></td>
<td>2013 guidance to inform manufacturers, distributors, and other entities about how the FDA intends to apply its regulatory authorities to select software applications intended for use on mobile platforms (mobile applications or &quot;mobile apps&quot;).</td>
<td><a href="http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf">http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf</a></td>
</tr>
</tbody>
</table>
• **Regulated apps** are those that are either intended:
  - to be used as an accessory to a regulated medical devices; or
  - to transform a mobile platform into a regulated medical device

• **App for which the FDA intends to exercise enforcement discretion:**
  - apps that may meet the definition of medical device but likely pose lower risk to the public
  - will not be regulated unless the FDA decides the app poses a significant patient safety risk
  - includes clinical decision support apps

• **Apps that are not medical devices** and will not be regulated, including apps:
  - that provide medical reference material
  - used as educational tools for medical training
  - used for patient education
  - that automate office operations in a health care setting
  - that are generic aids of general purpose products (e.g., apps that magnify images, record audio, facilitate communication, provide turn-by-turn directions)
Other Resources

- HealthIT.gov Mobile Device Privacy and Security
  - [http://www.healthit.gov/providers-professionals/you-your-organization-and-your-mobile-device](http://www.healthit.gov/providers-professionals/you-your-organization-and-your-mobile-device)
- HealthIT.gov training video - "Securing Your Mobile Devices is Important!"
  - [http://www.healthit.gov/providers-professionals/securing-your-mobile-device-important](http://www.healthit.gov/providers-professionals/securing-your-mobile-device-important)
- SANS Mobility/BYOD Security Survey
- SANS Mobile Security Policy Templates
  - [http://www.sans.org/security-resources/policies/mobile.php](http://www.sans.org/security-resources/policies/mobile.php)
- SANS Securing The Human Training Modules
- F-Secure Mobile Threat Report for Q1 2014
Thank You!

Ricky Bloomfield, MD
Director, Mobile Technology Strategy
Assistant Professor, Internal Medicine-Pediatrics
Duke Medicine
Email: ricky.bloomfield@duke.edu