Security Challenges with Medical Devices and Apps in a BYOD World

Mitchell Parker, MBA, CISSP, Executive Director,
Information Security & Compliance

Indiana University Health

Why are we here?

- We have multiple factors driving the extensive use of consumer medical devices and apps as part of the patient care process
- The ubiquity, power, and low cost of smartphones, smart watches, and fitness devices means that they can often do the same work as more complex medical devices
  - Why spend $1000+ when a $50 FitBit is more effective?
  - Why buy a device when you can just put an app that does the work on it?

Why are we here?

- The drive by providers and payors to increase compliance with care regimens, combined with a need to drive down costs, leads to their use in the care process
  - Again, why spend when you don't need to?
- While this comes with significant benefits, there are also significant concerns with privacy and security
  - That's why we're here!

What is the situation providers face?

- We need to monitor patients for compliance
- We need to monitor and spot potential issues through monitoring
- We need to drive down costs – reimbursements are dropping
- Medical devices are expensive and require specialized maintenance
- We are using BYOD to monitor patients using devices they already have

What is the situation providers face?

- Structural differences in healthcare organizations are major contributors to confusion
  - Home Health is often its own organization separate from the rest of the team, even IS
    - Many times it is even outsourced
  - There are few interfaces between outpatient-facing organizations and the core IS and Security teams
  - Oftentimes you find out much later about these projects
  - These organizations also run very lean, meaning that they may not have the staffing needed to support these apps

What is the situation?

- We don’t have good unified processes (yet) to review usage of these apps and combine risks with need to “prescribe”
- We are using data from consumer devices to feed intelligent systems (AI/ML/Deep Learning) to help make decisions on patient care
- We have APIs, but don’t focus on the ultimate destination of data, how it gets there, or the entire process to verify the journey
- Structural challenges get in the way of addressing many of the issues we have

Brought Your Own Device aka BYOD

- EMR Apps on BYOD Devices (Haiku/Canto/Powerchart Touch)
  - The iPad was the first major use of BYOD in facilities
  - Providers don't want to carry two phones
- Secure messaging is split across multiple apps and people are moving toward the least common denominator despite the risks because they have to communicate
  - Providers want and need interoperability here
  - Pagers and text messaging still work across systems and secure messaging often does not
- Messaging Layer Security, presented at Black Hat by Raphael Robert of Wire, can address many of these challenges provided we use it

Black Hat Presentation

- Link: https://www.blackhat.com/us-19/briefings/schedule/index.html#messaging-layer-security-towards-a-new-era-of-secure-group-messaging-16230
- Slides: http://i.blackhat.com/USA-19/Wednesday/us-19-Robert-Messaging-Layer-Security-Towards-A-New-Era-Of-Secure-Group-Messaging.pdf
- Involved Companies: Google, WhatsApp, Cisco, Mozilla, MIT, ACLU, Twitter, Wickr, etc.

What do we have to deal with in Health Systems?

- We must evaluate these devices for risk
- Large varieties of encryption and protection on devices and with apps
- Large varieties on how device info makes its way to the Electronic Medical Record or for clinical decisioning
- Must evaluate each solution and device for how it handles identity
- We need to solve structural issues with good governance that is sensitive to the organization's needs

Data and Device Questions

- Question: How do we know this data is valid and belongs to the person?
  - We have a requirement under the HIPAA Security Rule for Confidentiality, Availability, and Integrity of data presented to an EMR for payment, treatment, or operations
- We have had to architect solutions to provide additional network security and wireless security
  - Security solutions often 1-2 years behind state of the art
- Only the higher end devices get full manufacturer support. Consumer devices have a much shorter lifecycle - a year if we are lucky

Identity Issues

- Numerous different ways to authenticate users, patients, providers
- While federation is prevalent in higher education, there are still a lot of islands in healthcare
- The VA has non-federated identities as part of their VistA EMR
- Many larger health systems don't federate their EMR systems
- This leads to an inability to review access at a global level
- Unique non-SSN patient identifier was part of the original Omnibus Rule, and was removed due to influence by former Rep. Ron Paul
  - True interoperability is not going to happen until we get this

Identity Issues

- Personal information gets duplicated all over the place and it becomes best guess - Every vendor has their own system, unlike higher ed!
- Best guesses for all three as vendors have to use either personal data such as SSN, reduplicate information on different web sites, or just leave out security altogether
- Password reuse leading to easily guessable passwords
- Password managers are another layer of complexity that only your most educated people are going to us - have to address the 99%
- Personal information all over the place and unmanaged
- Separate identity stores for each system

The Lack of Security is Measurable

- # of data breaches from IOT devices
- # of unprotected devices
- # of manuals of devices available on Google with instructions on how to override physician defaults (CPAP machines in particular)
- Ease of breaking or falsifying data on a device
- Ease of breaking into cloud providers to get the data
- # of health apps reselling information as a revenue stream (https://gizmodo.com/researchers-create-fake-profiles-on-24-health-apps-and-1833474535)

FDA Premarket Guidance

- What does this mean for engineering?
  - It hints at DevSecOps, but doesn’t go there
- Doesn't encompass cloud guidance and best practices for servers
  - We need to really address this as well – everyone is moving to the cloud
  - 5G = first true cloud-based telecom platform
  - Our devices will use the cloud to communicate whether we want to or not
- In its initial form, didn't account for log analysis

What is DevSecOps?

- This is the portmanteau of three areas:
  - Software Development (Dev)
  - Information Security (Sec)
  - Operations (Ops)
- It is both a management philosophy and process by which a unified team continually develops and addresses issues
  - This speeds up development significantly
  - It also allows for security issues to be more quickly addressed

What this adds up to…

- We have a best guess on identity
- We have a best guess on the data itself
- High variety on how it gets protected on the device
- High variety on how it gets protected in the cloud or to its ultimate EMR destination
- We have to evolve to a DevSecOps mindset

How can device and app engineers make it better for our patients?

- Identity - work together on federated identity systems for devices and applications that feed data to the cloud
  - Make it easy for the patients, who have to remember passwords - Google etc.
  - Federate with providers to use their identity systems whenever possible
  - This gets you the ability to use the latest and greatest security protection for accounts
  - Get out of the ID management business
- Protect data on the devices using encryption tied to the federated identities
- Adopt a DevSecOps mindset to continually develop and evolve secure code
- Don’t resell customer data
- If you want to sell it for AI/Machine Learning data sets, get affirmative consent from users!

Prescribing Apps

- Applications and smart devices are now part of the care process
- If our providers aren't recommending or prescribing their use, our patients are Googling and figuring it out themselves already
- The payors are also looking at these as more effective and cost-saving solutions
  - We also need to be thinking about apps and devices in this way!

Prescribing Apps and Devices

- Where do we start?
- Recommendations don't represent an acceptance of liability
  - Liability should be between the developing company and patients
  - Based on the opinions of your legal teams, this may change
- We have issues now with device security and liability
- Many med device and app vendors not willing to discuss this area yet
  - Many of the consumer providers don't want to deal with HIPAA
- This needs to be contractually addressed
  - Esp. with use of PHI and HIPAA!

Prescribing Apps and Devices

- Applications must go through a risk assessment process
  - Like an internal application would
  - Should meet same standards as internal apps
  - Cannot rely upon just the Cloud Provider security standards or SOC2
    - Too many application providers think they are secure because the site meets minimum security controls
    - Just because Amazon or Microsoft has good security controls doesn't mean a bad app can't cause havoc

– What's in your wallet?

Prescribing Apps and Devices

- Apps and applications need to have enhanced data security behind them in the wake of Capital One – especially for cloud-based storage
  - Protect Against Cross-Site Request Forgery Attacks
  - Protect Against Server-Side Request Forgery Attacks
  - Auditing of web application firewall rules
    - Complex rules lead to data breaches
  - Security scanning of web sites with a real security scanner
    - No “Hacker Proof and scanned daily” scans that mean nothing

Prescribing Apps and Devices

- Adoption of DevSecOps to demonstrate security at all levels of process
- Adoption of DevSecOps to have demonstrable processes that address security
- Usage of Secure APIs to transfer data
  - FHIR is now a must, not a nice to have
  - HL7 is slowly turning into legacy
  - We need to focus on APIs for better interoperability

User/Patient Obligations

- Users must read and understand terms of use
  - Understand what data the applications or devices store
  - Understand how they are protected
    - Required under the European Union General Data Protection Regulation (GDPR) and numerous others worldwide
    - Recommendation does not represent an acceptance of liability on the part of the health system
      - **This will be an ongoing issue!**
      - **My personal biggest concern is that we have to be very careful of app/device vendors that resell data**

Applicability

- Clinical applicability must be decided by the clinicians
  - Governance for these should be handled by the clinicians
  - IS and Information Security are there to ensure that technology does not introduce undue risk
    - Or gets resold, even in aggregate
  - IS is also there to ensure interoperability and that the data goes to the right place in the Electronic Medical Record
  - This is a place where IS needs to acquiesce and empower the organization

Who is Responsible?

- The CMIO or equivalent needs to facilitate these discussions and bridge the gaps between IS, Security, and Clinicians
  - Ability to integrate data with existing EMR must be a key decision point
  - Governance should be to the same scrutiny as clinical systems and EMR if data is to be used in the treatment process
- This is a new area for many organizations, and a strong CMIO helps guide along wary and skeptical team members

Governance – Thanks Dr. Freeman (former TUHS CMO)

- Validation of applications needs to be considered as part of the governance process
  - Who developed this app?
  - Did it have clinician oversight or is this something developed by someone without domain specific knowledge?
    - We have apps and web sites used for calculation that were not vetted
    - Never underestimate the power of medical staff to find something on the Internet that may be of use
      - **And that can give erroneous output and cause patient safety issues**

Governance

- Was there input from clinicians in its development?
- We ended up picking a patient privacy solution because we could demonstrate to the Senior Leadership Team that the CMIO who co-founded the company that had practical experience in addressing data breaches.
  - Senior leadership and C-suite want working solutions, not theoretical ones
  - Can a clinical chair understand its value and sign off on the risks and benefits?
    - Can you make them feel confident that we don't introduce new risks?

Governance

- Authenticity matters
  - We believe that a team that develops applications to meet their needs is more motivated to address issues and is committed to keeping it maintained
  - Many of the old specialist applications, and modern ones like OsiriX, have significant clinician input
  - Those apps stick around a long time, as opposed to ones that don't

Management

- Security is only one concern – it's about the overall management picture
  - Health systems are not normally structured or designed to deal with supporting apps or devices they do not control.
    - There are enough with devices moving in and out of the org
    - See: Every risk assessment of a healthcare organization
  - They are designed for telemedicine and devices that they do control
  - While there have been many successful pilots, this hasn't become pervasive yet
- We need to be consistent across organizational structures, which is the hidden organizational change that we need to address as part of this

Device and App Support

- What devices or apps can be used long term?
- Do they just patch or put a new OS with new features on?
  - Are there other apps on the devices that can cause long term problems?
  - What is the communication plan to communicate updates and fixes to customers?
  - How will we support them?
    - Who manages and monitors for compliance?
    - Who will provide device support?
    - Who will train users and provide their support?

Device and App Support

- Do we have vendor contacts?
- How do we support them remotely?
- How do we protect them from data breaches?
- How do we prevent leakage of information?
  - How do we minimize reselling of it?
- How do we get insurance to cover the costs?
  - How do we prove this is an effective solution that should be reimbursed because it costs less money than the alternative?

You need a plan

- Intake and Governance – Clinical review by a clinician and security
  - Treat like an internal app and assess for risk
  - Enforce across entire structure and provide resources to do so
- Management – Design workflow around a management plan to practically address security and management
  - Treat them like your own medical devices
  - Plan for Ongoing Usage
  - Develop a robust operating model across organization
- What happens when we stop using the data or app?
  - Do we delete or just stop recording?

We need to make a Business Case

- In the operating model:
  - Have security and support costs been figured in?
    - Are we not dumping on already overburdened home health staff?
    - Have we accounted for support that addresses customer needs and provides consistent, accountable service?
  - Is there a clear, measurable benefit?
    - Can we convince the payors there is?
  - Do we mitigate risks other than security?
  - Can we extend lessons learned to other areas?

What have we learned and still have yet to do?

- Security is an integral part of this process, however this is owned by the CMIO and business
  - We have a lot of challenges ahead, especially structurally, to address deployment
  - We have challenges communicating liability and usage for each organization and use case
  - We need to address security and privacy as part of the process whether or not we own the device or app
  - We need to address clinical effectiveness and have the clinicians evaluate and make the final call
  - Governance is essential for coordinating everything

Thank you!

- Please reach out with further questions at:
  - Twitter: @Mitchparkerciso
  - LinkedIn: https://www.linkedin.com/in/mitchparkerciso/
  - Email: mparker17@iuhealth.org