TO BE BYOD OR NOT TO BE BYOD

_{Is a “Bring your own device” policy right for your organization?}_

HITECH Status in Michigan

_Navigating the Future of Electronic Health Records_

_September 25, 2012_

Brian Balow
Member with Dickinson Wright
bbalow@dickinsonwright.com

Tatiana Melnik
Associate with Dickinson Wright
tmelnik@dickinsonwright.com

DISCLAIMER: The views and opinions expressed in this presentation are those of the authors and do not necessarily represent official policy or position of Dickinson Wright or of its clients.
1. **What is BYOD?**
   - Overview
   - Why move to BYOD?

2. **Legal Issues**

3. **Drafting Your BYOD Policy**
   - Considerations
   - Example
   - Resources
Outline

1. What is BYOD?
   - Overview
   - Why move to BYOD?

2. Legal Issues

3. Drafting Your BYOD Policy
   - Considerations
   - Example
   - Resources
What is BYOD?

BYOD = Bring Your Own Device
What is BYOD?

- Mobile device shift
  - From single use – one for work, one for personal
  - To dual use – one device for both work and personal
88% of US adults are cell phone owners (Pew Internet, March 2012)

- 46% of those are smartphone owners
  - In May 2011 number was at 35% → ↑ of 11% in less than one year

17% of cell phone owners do most of their online browsing on their phone (Pew Internet, June 2012)

- Why?
  - Cell phone is more convenient – 38%
  - Cell phone is always with me – 23%
But don’t forget about tablets!

- iPad, Samsung Galaxy, Asus, Google Nexus, Microsoft Surface, Amazon Kindle Fire *(Apple has 60-70% of the market – NY Times)*

- 31% of the U.S. Internet users owns a tablet *(Online Publishers Association, June 2012)*
  - Expect that by Q2 2013, 47% will own a tablet

- 74% of tablet owners use their device daily and 60% use it several times a day *(OPA)*

- Tablet app market - ~ $2.6B spent in 2012 (up from $1.4B in 2011)
Why are companies moving to BYOD?

- Employee satisfaction
  - Too many devices
  - Employees want to upgrade
- Efficiency and productivity increases
  - Increased mobility
  - Better integration of work and personal lives
  - Flexibility – employees work in a way that maximizes their productivity
Overview: Why Move to BYOD?

- Why are companies moving to BYOD?
  - Cost/Benefit analysis
    - Decrease in costs because
      - Reduce device costs (life cycle assess management) → EEOC
      - Within first 3 months of 2012, no. of BlackBerry devices cut from 550 to 462 and monthly recurring costs lowered by 20-30% by optimizing rate plans
      - Reduce data costs
      - But, don’t forget that need to reimburse employees for use of their own devices for work!
    - Efficiency increase
Overview: Why Move to BYOD?

Why are companies moving to BYOD?

“75% of our users never made phone calls from their BlackBerrys … Email is the killer app. They either used the phone on their desk or they used their personal cell phone to make calls because it’s just easier. We also found there were a number of zero-use devices. People have them parked in their desk drawer, and the only time they use it is when they travel.” – Kimberly Hatcher, CIO, U.S. Equal Employment Opportunity Commission (EEOC) BYOD Pilot

More efficient use of resources!
OUTLINE

1. **What is BYOD?**
   - Overview
   - Why move to BYOD?

2. **Legal Issues**

3. **Drafting Your BYOD Policy**
   - Considerations
   - Example
   - Resources
Legal Issues

- HHS has strongly advocated for using mobile devices
  - Improving public health outcomes → drive down healthcare costs
    - Helping with chronic disease management
      - Reminding people to take medications
    - Reaching rural areas
    - Empowering expectant mothers
LEGAL ISSUES
**Legal Issues**

- **Text4Baby**
  - Community partnership (community and government health orgs., wireless carriers, businesses)
  - Free text messages to women (i) who are pregnant or (ii) whose babies are < 1 yr old
  - Provides them with reminders and other information aimed at improving their health and the health of their babies
LEGAL ISSUES

➢ Text4Baby
  • Why?
    – In 2011, the US ranked 30th in the world on infant mortality rates
    – Many face disabilities and lifelong health problems because they were born prematurely or had low birth weights
      ○ Encouraging pregnant women to pay attention to their nutrition, avoid alcohol, etc.
      ○ Helping pregnant women find resources to meet their budget
Text4Baby

- Send a text message to the number with the word BABY or BEBE (•)
- Prompted for due date or child’s birth zip code
- Receive 3 messages a week with information relevant to the pregnancy stage or child’s development
LEGAL ISSUES

- Are mobile devices different than other technology?
  - Yes! Special security challenges!
    - They’re mobile and so are more likely to be lost compared to other devices
    - BYOD = ↑ Risk
      - Share device with others
      - User not technically sophisticated
      - More likely to pick up a virus (download problematic apps. - IBM!)
LEGAL ISSUES

- Are mobile devices different than other technology?
  - Yes! Special security challenges!
    - Multiple devices – lots for your IT team to manage
    - Consider ways employees use devices and the kinds of issues that could arise
      - Social media
      - Random websites
      - Texting patient specific information
    - Jailbroken devices?
LEGAL ISSUES

- Legislators raised concerns with using mobile devices for healthcare
  - Safety
  - Security
  - Reliability of the network infrastructure
- Numerous agencies evaluating issues
  - FDA, FCC, NIST (Dept. of Commerce), FTC, Office of Civil Rights (HHS)
LEGAL ISSUES

- State regulators are also paying attention
  - California particularly active
    - Feb. – Launched Mobile App Privacy Program (Amazon, Apple, Google, HP, Microsoft, Research In Motion and Facebook all signatories)
    - July - Created a Privacy Enforcement and Protection Unit
LEGAL ISSUES

Why the Concerns?

- Compliance concerns → Healthcare highly regulated
- Privacy and Security issues (PHI, SSN)
- Breach Notification laws
- Data Destruction laws
- Litigation Holds – Where is your data?
- Wage and Hour laws
- Malpractice issues
LEGAL ISSUES

- Privacy & Security Issues seem to be most prominent at the moment
  - **Numerous** data breaches resulting from lost/stolen laptops
  - OCR has discovered organizations have not undertaken a Risk Assessment to evaluate issues with mobile devices
Legal Issues

Phoenix Cardiac Surgery, P.C.

- Resolution Agreement:
  A risk management plan that implements security measures sufficient to reduce risks and vulnerabilities to ePHI . . . , when ePHI is
    a) posted to an Internet-based e-calendaring system,
    b) transmitted over e-mail,
    c) accessed remotely, or
    d) transmitted to or from or stored on a portable device
      (including “ePHI in text messages that are transmitted to or from or stored on a portable device.”)
LEGAL ISSUES

Massachusetts Eye and Ear Infirmary

- Data breach: Feb. 19, 2010 – doctor’s laptop stolen during a lecture tour in South Korea
  - Impacted data of about 3,500 research participants
- Report to OCR (HITECH): April 21, 2010
- OCR Investigation Initiated: October 5, 2010, (all self reported breaches are investigated)
LEGAL ISSUES

- Massachusetts Eye and Ear Infirmary
  - Press Release announcing resolution: September 17, 2012 → Almost 2 years!
  - Financial penalty: $1.5 million
  - Corrective Action Plan: 3 years of monitoring
Massachusetts Eye and Ear Infirmary

- What did OCR find to be problematic?
  - MEEI did not demonstrate that it conducted a thorough analysis of the risk to the confidentiality of ePHI on an on-going basis as part of its security management process from the compliance date of the Security Rule to October 29, 2009 → did not fully evaluate the likelihood and impact of potential risks to the confidentiality of ePHI maintained in and transmitted using portable devices
Massachusetts Eye and Ear Infirmary

- What did OCR find to be problematic?
  - MEEI’s security measures were not sufficient to ensure the confidentiality of ePHI that it created, maintained, and transmitted using portable devices to a reasonable and appropriate level from the compliance date of the Security Rule to May 17, 2010
LEGAL ISSUES

Massachusetts Eye and Ear Infirmary

- What did OCR find to be problematic?
  - MEEI did not adequately adopt or implement policies and procedures to address security incident identification, reporting, and response from the compliance date of the Security Rule to March 8, 2010
Legal Issues

- Massachusetts Eye and Ear Infirmary
  - What did OCR find to be problematic?
    - MEEI did not adequately adopt or implement policies and procedures to restrict access to authorized users for portable devices that access ePHI or to provide it with a reasonable means of knowing whether or what type of portable devices were being used to access its network from the compliance date of the Security Rule to March 8, 2010
LEGAL ISSUES

- Massachusetts Eye and Ear Infirmary
  - What did OCR find to be problematic?
    - MEEI did not adequately adopt or implement policies and procedures governing the receipt and removal of portable devices into, out of, and within the facility from the compliance date of the Security Rule to May 17, 2010. MEEI had no reasonable means of tracking non-MEEI owned portable media devices containing its ePHI into and out of its facility, or the movement of these devices within the facility.
Massachusetts Eye and Ear Infirmary

- What did OCR find to be problematic?
  - MEEI did not adequately adopt or implement technical policies and procedures to allow access to ePHI using portable devices only to authorized persons or software programs . . . MEEI did not implement an equivalent, reasonable, and appropriate alternative measure to encryption that would have ensured confidentiality of its ePHI or document the rationale supporting the decision not to encrypt.
**Legal Issues**

- **Meaningful Use Stage 2 Requirements**
  - *Proposed Measure*: Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including **addressing the encryption/security of data at rest** in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider’s risk management process.
Legal Issues

Meaningful Use Stage 2 Requirements

- Same as Stage 1, except explicitly addresses encryption and security – WHY?
  - “Due to the number of breaches reported to HHS involving **lost or stolen devices**, the HIT Policy Committee recommended specifically highlighting the importance of an entity’s reviewing its encryption practices as part of its risk analysis.”
  - “Recent HHS analysis of reported breaches indicates that almost **40 percent of large breaches involve lost or stolen devices**. **Had these devices been encrypted, their data would have been secured.**”
Another benefit of encryption?

- Get out of the HITECH breach notification requirements!
  - “A CE that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHI . . . shall, in the case of a breach of such information. . . notify each individual whose unsecured PHI has been, or is reasonably believed by the CE to have been, accessed, acquired, or disclosed as a result of such breach.”
LEGAL ISSUES

- What does unsecured PHI mean?
  - “[T]he term ‘unsecured PHI’ means protected health information that is not secured through the use of a technology or methodology specified by the Secretary”

- Remember
  - BAs to notify CEs
  - If over 500 individuals, notify Secretary right away
Outline

1. What is BYOD?
   - Overview
   - Why move to BYOD?

2. Legal Issues

3. Drafting Your BYOD Policy
   - Considerations
   - Examples
   - Resources
Considerations

- Why have a policy?
  - To protect your patients' rights
  - To instill professionalism throughout your enterprise
  - To protect your organization from liability
  - To protect your employees from liability
**Considerations**

- Regulators are focusing on mobile devices!
  - Meaningful Use Stage 2
  - OCR Actions
  - Unlicensed practice of medicine
  - FDA mobile medical devices/apps
  - California encryption mandates
CONSIDERATIONS

- Understand your IT enterprise
- Understand the economic pros and cons of BYOD to your enterprise
- Understand the risks to your enterprise related to BYOD (formal risk assessment)
- Determine, based on these considerations, whether to adopt BYOD
Considerations

- Stakeholders
  - Senior management (resources; institutional support)
  - Chief IT officer (sets the strategic direction, including policy)
  - IT staff (implements strategy/policy)
  - Legal/Regulatory (subject matter expertise/enforcement)
  - Human resources (enforcement)
Many Policies Affect BYOD

- Acceptable Use Policies
- Security Policies (e.g., password, encryption)
- Social Media Policy
- Remote Access Policy
- Remote Working Policy (over 40 hours/wk?)
- Incident Response Policy
- Breach Notification Policy
- Privacy Policies
- Litigation Hold Policy
What Kind of Issues Should a *Discrete* BYOD Policy Address?


- Incorporate other related policies by reference (e.g., privacy, acceptable use, social media, etc.)
Policy Content

- Why (Purpose)
  - Protect patients’ privacy
  - Protect organization’s assets
  - Rules of access to/use of organization’s networks
  - Prevention of privileging/licensing violations
  - Delineation of work v. personal use
What (Scope)
- Supported devices
- State of supported devices (e.g., not jailbroken)
- Reimbursement of costs
- Approved applications
- Other limitations (camera?)
Who (Scope, Part 2)

- Employees
- Interns
- Students
- Contractors/consultants
How

- Roles and responsibilities
  - Senior management
  - Chief IT officer
  - IT staff
  - Legal and HR
- Enforcement
Resources

- **Federal Gov’t** – Bring Your Own Device Toolkit
  - [http://www.whitehouse.gov/digitalgov/bring-your-own-device](http://www.whitehouse.gov/digitalgov/bring-your-own-device)

- **HIMSS** – Bring Your Own Device & Consumerization
Disclaimer

This presentation is informational only. It does not constitute legal or professional advice.

You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation.
Please feel free to contact us with any questions:

- **Brian Balow**
  E-mail: BBalow@dickinsonwright.com
  Phone: (248) 433-7536

- **Tatiana Melnik**
  E-mail: TMelnik@dickinsonwright.com
  Phone: (734) 623-1713