BYOD, BYOC, BY Say What?

Bring Your Own Device Implementation, Legal Concerns, and Best Practices

PAHCOM – Spring Hill Chapter
May 13, 2014

Tatiana Melnik – Attorney, Melnik Legal PLLC

Outline

I. Overview of BYOD
II. Legal Concerns and Drafting Considerations
III. Technical Issues and Considerations
IV. Questions

Outline

I. Overview of BYOD
II. Legal Concerns and Drafting Considerations
III. Technical Issues and Considerations
IV. Questions

Terminology

- BYOD = Bring Your Own Device/Data
- BYOC = Bring Your Own Cloud/Computer
- BYOL = Bring Your Own Laptop/Lessons

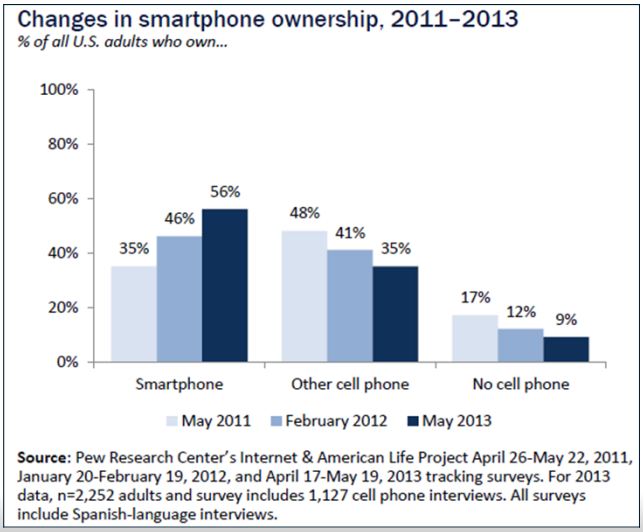
B.Y.O.D Movement – Natural Evolution

- Forbes:

  "The primary business driver is getting work done. Business users do not want to compromise. They want convenience. They want to be able to do the work without being tethered to their laptops. People deserve and demand a great user experience."

B.Y.O.D Movement – Natural Evolution

As of May 2013, 91% of U.S. adults own a cell phone



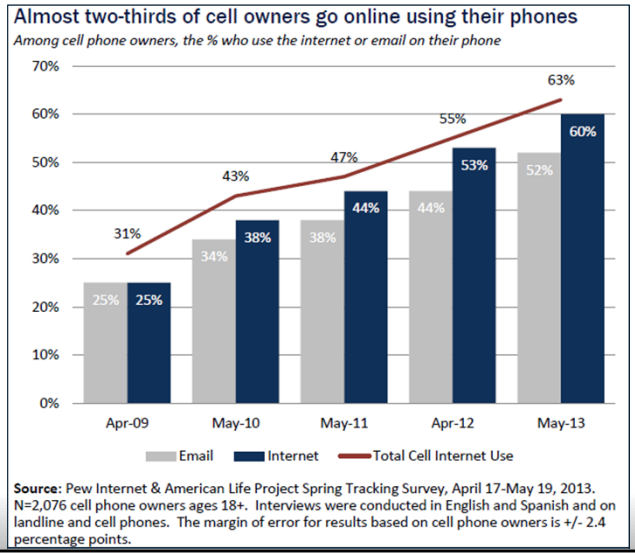
Source: Pew Research Center's Internet & American Life Project, Aaron Smith (June 5, 2013), http://www.pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx

B.Y.O.D Movement – Natural Evolution

91% of Americans owning cell phones

equals

57% of *all* Americans going online using a mobile phone



Source: Pew Research Center's Internet & American Life Project, Maeve Duggan & Aaron Smith (Sept. 16, 2013), http://www.pewinternet.org/Reports/2013/Cell-Internet.aspx

B.Y.O.D Movement – Natural Evolution

What else are people doing with their cell phones?

Downloading apps up from 22% in 2009

Cell phone activities

The % of cell phone owners who use their cell phone to...

81	send or receive text messages
60	access the internet
52	send or receive email
50	download apps
49	get directions, recommendations, or other location-based information
48	listen to music
21	participate in a video call or video chat
8	"check in" or share your location

Source: Pew Research Center's Internet & American Life Project Spring Tracking Survey, April 17 – May 19, 2013. N=2,076 cell phone owners. Interviews were conducted in English and Spanish and on landline and cell phones. The margin of error for results based on all cell phone owners is +/- 2.4 percentage points.

Source: Pew Research Center's Internet & American Life Project, Maeve Duggan (Sept. 19, 2013), http://www.pewinternet.org/Reports/2013/Cell-Activities.aspx

B.Y.O.D Movement – Single / Dual Use

- Mobile device shift
  - From single use – one for work, one for personal
  - To dual use – one device for both work and personal
- Why?
  - Convenience
  - Increased integration of work and personal lives
  - Less maintenance (one phone vs. two phones)
  - Cost savings

B.Y.O.D Movement – Cost Savings

- **Case Study**: **Equal Employment Opportunity Commission**
  - In 2011 – EEOC's budget for mobile devices (BlackBerry) = $800K
  - In 2012 – Budget reduced to $400K
  - Question?
    - **How do you reduce expenses?**

B.Y.O.D Movement – Cost Savings

- **Two-pronged approach to reduce expenses**
  - "Negotiate" with wireless carrier
    - Saved $240K
  - Implement a BYOD program
    - BYOD was a good option because there was a **more efficient use of resources**

B.Y.O.D Movement – Cost Savings

- **Two-pronged approach to reduce expenses**
  - "Negotiate" with wireless carrier

"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*

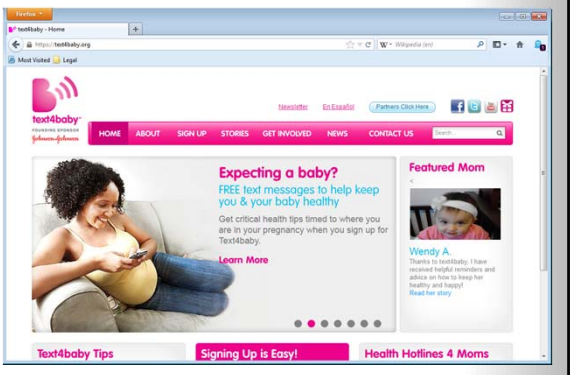
cient

Strong Support

- Recognizing the proliferation of mobile technology, 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 individuals through education

Strong Support

- **Community Partnerships – Text4Baby**
  - Many partners (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



Why are there Concerns?

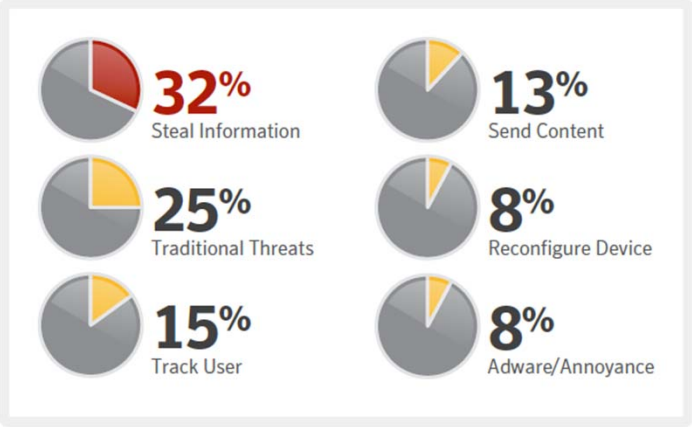
- Are mobile devices different than other technology?
  - YES! Special security challenges!
    - Mobile = More likely to be lost
    - BYOD/BYOC = ↑ Risk
      - Share devices with others
      - User not technologically sophisticated
      - More likely to pick up a virus, download problematic apps
      - Consider ways employees use devices and the kinds of issues that could arise (e.g., social media, texting patient information, theft)
      - Jailbroken devices

B.Y.O.D Issues – Security challenges

- Personal devices plugged into corporate computer network via USB
- Personal devices connecting to corporate Wi-Fi networks
- Data exfiltration and data theft from lost or stolen devices
  - Applications such as office readers on phones
  - Dropbox used to sync documents from a work laptop to a personal phone
  - Potentially sensitive corporate e-mail left on phones

B.Y.O.D Issues – Security challenges

Mobile Threats in 2012



Source: Source: Symantec, Internet Security Threat Report – 2012 Trends, vol 18, Pub. April 2013

s

Outline

I. Overview of BYOD
II. Legal Concerns and Drafting Considerations
III. Technical Issues and Considerations
IV. Questions

Legal Concerns

- Why the concerns?
  - Compliance
  - Privacy and Security Issues (*e.g.*, PHI, SSNs, trade secrets))
  - Breach Notification Laws (Fla. Stat. 817.5681)
  - Data Destruction Laws
  - Litigation Holds
  - Wage and Hour Laws
  - Malpractice Issues
  - Reliability of the Network Infrastructure

Privacy & Security

- Privacy and security issues are currently the most prominent concern
  - **Numerous** data breaches resulting from lost/stolen laptops and USB drives
  - Data breaches from devices sold on eBay, Craigslist, etc. because they were not properly wiped

HHS Office of Civil Rights

- Since the compliance date in April 2003
  - Received over 89,045 HIPAA complaints
  - Resolved complaints through -
    - investigation and enforcement (over 21,942)
    - investigation and finding no violation (9,869)
    - closure of cases that were not eligible for enforcement (51,910)

HHS Office of Civil Rights

- **Compliance issues investigated most:**
  - impermissible uses and disclosures of PHI
  - lack of safeguards of PHI
  - lack of patient access to their PHI
  - uses or disclosures of more than the minimum necessary
  - lack of administrative safeguards of ePHI

HHS Office of Civil Rights

OCR has taken action against:

Entity	Amount	Rules	Breach	Incident	Settlement
Cignet Health	**$4.3M**	Privacy Rule, $3M for willful neglect per HITECH	Denying patients access to medical records	Prior to 3/1/2009	2/4/2011 *(this was not a settlement)*
General Hospital Corp. & Physicians Org.	**$1M**	Privacy Rule	Left documents on subway	3/9/2009	2/14/2011
UCLA Health System	**$865,500**	Privacy & Security Rules	Workers snooping on celebrity patients	Prior to 6/5/2009	7/5/2011

HHS Office of Civil Rights

Entity	Amount	Rules	Breach	Incident	Settlement
Blue Cross Blue Shield of TN	**$1.5M**	Privacy & Security Rules	Unencrypted hard drives stolen from a leased facility	Prior to 11/3/2009 (self reported)	3/13/2012
Phoenix Cardiac Surgery	**$100K**	Privacy & Security Rules	Posting appt. on an online, publicly accessible calendar	Prior to 2/19/2009	4/11/2012
Alaska Dept. of Health & Human Services	$1.7M	Privacy & Security Rules	Unencrypted portable media device stolen from car of employee	10/12/09 (self reported)	6/25/2012

HHS Office of Civil Rights

Entity	Amount	Rules	Breach	Incident	Settlement
Massachusetts Eye and Ear Infirmary	**$1.5M**	Privacy & Security Rules	Theft of unencrypted personal laptop while at conference	Prior to 4/21/10 (self reported)	9/13/2012
Hospice of Northern Idaho	**$50K**	Security Rule	Theft of unencrypted laptop (less than 500 patients)	Prior to 2/16/11 (self reported)	12/17/2012
Idaho State University	**$400K**	Security Rule	Disabled server firewall for ~ 10 mo. resulting in a breach	Prior to 8/9/2011 (self reported)	5/10/2013

HHS Office of Civil Rights

Entity	Amount	Rules	Breach	Incident	Settlement
Shasta Regional Medical Center -	**$275K**	Privacy Rule	Senior leaders at co. met w/media to discuss medical services provided to a patient w/o a valid written authorization	1/4/2012 (read article in LA Times)	6/3/2013
WellPoint	**$1.7**	Privacy & Security Rules	Software update to web-based database left ePHI publicly accessible	Prior to 6/18/10 (self reported)	7/8/2013

HHS Office of Civil Rights

Entity	Amount	Rules	Breach	Incident	Settlement
Affinity Health Plan	**$1,215,780**	Privacy and Security Rules	Returned copiers to a leasing agent w/o erasing the copier hard drives	Prior to 4/15/10 (self reported)	8/7/2013
Adult & Pediatric Dermatology	**$150K**	Privacy, Security & Breach Notification	Theft of unencrypted personal thumb drive from employee vehicle	Prior to 10/7/11 (self reported)	12/24/2013
Skagit County, Washington	**$215K**	Privacy, Security, and Breach Notification	Moved ePHI of 7 individuals to a publicly accessible server	Prior to 12/9/11 (self reported)	3/7/2014

HHS Office of Civil Rights

Entity	Amount	Rules	Breach	Incident	Settlement
Concentra Health Services	**$1,975,220**	Privacy and Security Rules	Theft of an unencrypted laptop	11/30/2011 (self reported)	4/21/2014
QCA Health Plan, Inc. of Arkansas	**$250,000**	Privacy and Security Rules	Theft of an unencrypted laptop	Prior to 2/21/2012 (self reported)	4/14/2014
New York and Presbyterian Hospital Columbia University	**$3,000,000** **$1,500,000**	Privacy and Security Rules	Joint breach report; breach impacted 6,800 patients; removal of server by doctor employee permitted PHI to be visible on the internet	**FIRST** Joint breach report - Prior to 9/27/10 (self reported)	5/8/2014 (reported)

OCR – A Few Identified Problems

- **Risk Analysis issues**
  - Failure to conduct a Risk Analysis **in response to new environment**
    - BCBSTN – Changed offices
    - WellPoint – Installed software upgrade
    - Alaska DHHS – Never conducted an assessment
  - Failure to conduct **an accurate and thorough risk analysis** that incorporates all IT equipment, applications, and data systems utilizing ePHI
    - New York Presbyterian Hospital and Columbia University Medical Center

OCR – A Few Identified Problems

- **Workforce Members**
  - Failure to train and train on an on-going basis
  - Failure to "apply appropriate sanctions"
  - Failure to install security measures to monitor unauthorized access
    - UCLA case – workforce members repeatedly snooping on patients between 2005 – 08
  - Failure to implement appropriate policies and procedures for authorizing access to patient data bases

OCR – A Few Identified Problems

- **Technical/Security Failures**
  - Failure to take an inventory of equipment that access PHI
  - Failure to implement processes to assess and monitor the equipment that accesses PHI
  - Failure to implement appropriate security measures
  - Failure to follow existing policies and procedures on information access management
    - New York Presbyterian Hospital - **$3M settlement**

Policy Drafting Considerations

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

Policy Drafting Considerations

- **Regulators are focusing on mobile devices!**
  - OCR Actions
  - State data breach laws
  - GLBA/FTC Safeguards Rule
  - PCI DSS

Policy Drafting Considerations

- **Many Policies *Affect* BYOD**
  - Acceptable Use Policies
  - Security Policies (*e.g.*, password, encryption)
  - Social Media Policy
  - Remote Access Policy
  - Litigation Hold Policy
  - Remote Working Policy (over 40 hours/wk?)
  - Incident Response Policy
  - Breach Notification Policy
  - Privacy Policies

Policy Drafting Considerations

- **Include the right team**
  - 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)

Policy Drafting Considerations

- **What kind of issues should a discrete BYOD policy address?**
  - http://www.sans.org/reading_room/whitepapers/pda/security-policy-handheld-devices-corporate-environments_32823
  - Incorporate other related policies by reference (e.g., privacy, acceptable use, social media, etc.)
- **Require the use of specific apps?**

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
- History
  - Report to OCR (HITECH): April 21, 2010
  - OCR Investigation Initiated: October 5, 2010
  - Press Release announcing resolution: September 17, 2012

  → **Almost 2 years!**

Massachusetts Eye and Ear Infirmary

- Financial penalty: **$1.5 million**
- Corrective Action Plan: 3 years of monitoring

Massachusetts Eye and Ear Infirmary

- What did OCR find problematic?
  - MEEI did not demonstrate that it conducted **a thorough analysis of the risk** to the confidentiality of ePHI ***on an on-going basis*** [and] did not fully evaluate the likelihood and impact of potential risks to the confidentiality of ePHI **maintained in and transmitted using portable devices**
  - 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

Massachusetts Eye and Ear Infirmary

- What did OCR find problematic?
  - MEEI did not adequately adopt or **implement policies and procedures to**:
    - address security incident identification, reporting, and response
    - restrict access to authorized users for portable devices
    - provide it with a reasonable means of knowing whether or what type of portable devices were being used to access its network
    - receipt and removal of portable devices into, out of, and within the facility

Massachusetts Eye and Ear Infirmary

- What did OCR find 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 **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 problematic?
  - 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***

Policy Drafting Considerations

- **Must have a policy and a separately signed agreement**
  - What will a judge say in litigation when you try to rely on a policy?
  - Who will be responsible for spoliation sanctions when an employee tries to "help" you by erasing the data?

Outline

I. Overview of BYOD

II. Legal Concerns and Drafting Considerations

III. Technical Issues and Considerations

IV. Questions

Technical Issues

- Is your company technically mature enough to enforce the policies its writing?
- What is the security poverty line? https://451research.com/t1r-insight-living-below-the-security-poverty-line

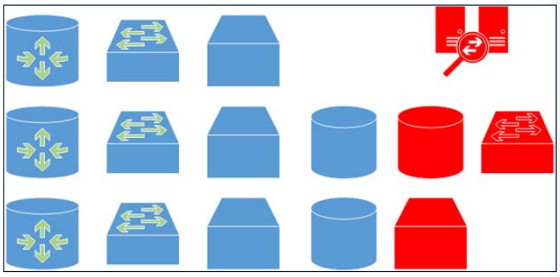
s

Technical Issues

- Mobile device encryption
- Pass code requirements
- Enforce screen lock timers
- Enforce no jail broken phones
- Enforce an enrollment system for remote wipe
- Enforce application and OS update policies

Technical Issues

- Data classification: not everything has the same value so separate it
- Data isolation: you can't protect everything so separate it



Technical Issues

- VPN
  - Try and keep services off the open Internet
- 2 Factor Authentication
  - Use it
- Strong encryption: Baked in with new operating systems
  - Windows XP end of life April 8, 2014 (extended support)

Other Things on the Horizon

- FTC becoming increasingly active
  - LabMD
    - Two cases: (1) Federal lawsuit; (2) Administrative action
    - The FTC filed a complaint against medical testing laboratory LabMD, Inc. alleging that the company failed to reasonably protect the security of consumers' personal data, including medical information. The complaint alleges that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers. The complaint alleges that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves.

Other Things on the Horizon

- FTC becoming increasingly active
  - LabMD – Failures identified
    - Respondent did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information
    - Respondent did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. For example, by not using measures such as **penetration tests**, Respondent could not adequately assess the extent of the risks and vulnerabilities of its networks.
    - Respondent did not use adequate measures to prevent employees from accessing personal information **not needed to perform their jobs** → referencing to Interrogatory that listed the LabMD employees with access to Personal Information and stating Respondent is "unable to answer" which types of Personal Information each employee had authority to access

Other Things on the Horizon

- FTC becoming increasingly active
  - LabMD – Failures identified
    - Respondent did not adequately train employees to safeguard personal information
      - records stored in clear text
      - no policy on who should have access to records,
      - access granted ad hoc, resulting in most employees receiving administrative access to servers
      - information transmitted from doctor's offices unencrypted
      - informal policy that doctors' offices would get unique access credentials, but credentials would then be shared amongst multiple users at a practice

Other Things on the Horizon

- FTC becoming increasingly active
  - LabMD – Failures identified
    - Respondent did not require employees, or other users with remote access to Respondent's networks, to use common authentication-related security measures, such as
      - periodically changing passwords
      - prohibiting the use of the same password across applications and programs
      - using two-factor authentication
      - Implementing credential requirements
      - mechanism to assess the strength of users' passwords
      - using the same username/password across multiple applications

Other Things on the Horizon

- FTC becoming increasingly active
  - LabMD – Failures identified
    - Respondent did not maintain and update operating systems of computers and other devices on its networks
      - Failed to patch system even though solutions readily available (some since 1999)
      - on some computers Respondent used operating systems that were unsupported by the vendor, making it unlikely that the systems would be updated to address newly discovered vulnerabilities
    - Respondent did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks
      - Respondent did not use appropriate measures to prevent employees from installing on computers applications or materials that were not needed to perform their jobs or adequately maintain or review records of activity on its networks.
    - **Respondent could have corrected its security failures at relatively low cost using readily available security measures**

Other Things on the Horizon

- Change to Florida Data Breach Statute
  - Current: Fla. Stat. 817.5681
  - New: Passed Legislature on April 30, 2014 and waiting to be sent to the Governor for signature
    - Status: http://www.flsenate.gov/Session/Bill/2014/1524/
    - Probably not getting to Governor until sometime in July 2014
    - . . . (2) REQUIREMENTS FOR DATA SECURITY. Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information.

Disclaimer

This slide presentation is informational only and was prepared to summarize relevant legal considerations when evaluating obligations under HIPAA/HITECH. 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, and Melnik Legal PLLC would be pleased to assist you on these matters.

Questions?

Tatiana Melnik
734.358.4201
tatiana@melniklegal.com