Strafford

Presenting a live 90-minute webinar with interactive Q&A

Mobile Medical Devices and BYOD: Latest Legal Threat for Providers

Developing a Comprehensive Usage Strategy to Safeguard Health Information and Ensure Patient Privacy

WEDNESDAY, DECEMBER 18, 2013

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

C. Elizabeth O'Keeffe, Counsel, **Wyatt Tarrant and Combs**, Jackson, Miss.

Sarah E. Swank, Principal, **Ober | Kaler**, Washington, D.C.

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-888-601-3873** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

- In the chat box, type (1) your **company name** and (2) the **number of attendees at your location**
- Click the word balloon button to send

Mobile Medical Devices and BYOD: Latest Legal Threat for Providers

Developing a Comprehensive Usage Strategy to Safeguard Health Information and Ensure Patient Privacy

Agenda

- Going mobile
- Impact of HIPAA / HITECH on mobility
- Solutions for Mobile Security
- Practical Responses to New Technology

Going mobile

Challenges of Mobility in Healthcare

What Are the Issues that Affect Mobility in Healthcare?

- People
- Data
- Apps
- Access
- Compliance (HIPAA / HITECH)

People

- Benefits
  - Mobility enables people to work better
  - People are comfortable with tablets, smartphones, laptops
  - Users demand it
- Challenges
  - Do you trust your users?
  - Do they have the ability to make sound decisions about threats and risk?
  - What policies and procedures are necessary to make mobility work?
  - How can you handle personal devices?

Data

- Benefits
  - Allows staff to access information anywhere
  - Rapid access to data to serve clients better

- Challenges
  - What are the threats to the data?
  - How do you protect the data?
  - How do you control access to data?
  - What happens if data is lost or stolen?

Applications

- Benefits
  - Mobile apps can completely redefine workflow
  - Easy to use and learn
- Challenges
  - How do you controls what apps do what?
  - How do you prevent malware apps?
  - How do you balance personal apps vs. company apps

Compliance

- Benefits
  - You have a lot of control over your compliance efforts
  - There are no specific requirements for mobility in the relevant regulations
- Challenges
  - How do you craft a BYOD strategy to align with HIPAA / HITECH & Meaningful Use?
  - How can mobile security help with preventing breaches?
  - How do you prove compliance?

Why is Mobility So Hard for Healthcare?

- Caregivers demand access and do not want roadblocks
- Data is extremely sensitive
- HIPAA / HITECH
- A single breach can be disastrous
- Healthcare networks are large, complex and diverse
- Mobile devices and apps are maturing rapidly
- There is no one product or solution that protects mobile platforms

New Technologies, New Focus

- Recent OCR enforcement trends have focused heavily on mobile technology
- Entities have been faulted for a lack of policies and procedures directly addressing mobile tech tracking, authentication, and security (including, especially, encryption)
- Existing audit results – compliance in technology areas already a problem area for many smaller entities

Mobile Devices

- Who owns the devices
- Are personal devices used at work registered?
- Virtual Privacy Network (VPN) to exchange information
- Back up PHI on servers
- Remote wipe of devices
- Policy and procedures
- Training

Mobile Devices: **Know the RISKS. Take the STEPS.**
PROTECT & SECURE Health Information
Find out more at HealthIT.gov/mobiledevices

OBER | KALER
Attorneys at Law

WYATT TARRANT & COMBS LLP

Office for Civil Rights Overview

- Ensuring Federal financial assistance recipients comply with the national civil rights laws, such as those relating to discrimination based on race, color, national origin, disability and age
- Enforcing requirements and investigating complaints under the Health Insurance Portability and Accountability Act of 1996 (PL 104-191) (HIPAA) and its accompanying regulations
- Enforcing Federal Health Care Provider Conscience Rights
- Certifying Medicare applications for compliance with the national civil rights laws

Culture of Compliance

- Compliance involves active engagement of leadership within an organization

- A successful compliance program includes:
  - Employee training
  - Vigilant implementation of policies and procedures
  - Regular internal audits
  - Prompt action plan to respond to incidents.
  - Analyze, evaluate, and correct potential risk areas

Impact of HIPAA / HITECH

Challenges of Mobility in Healthcare

What Are the Threats

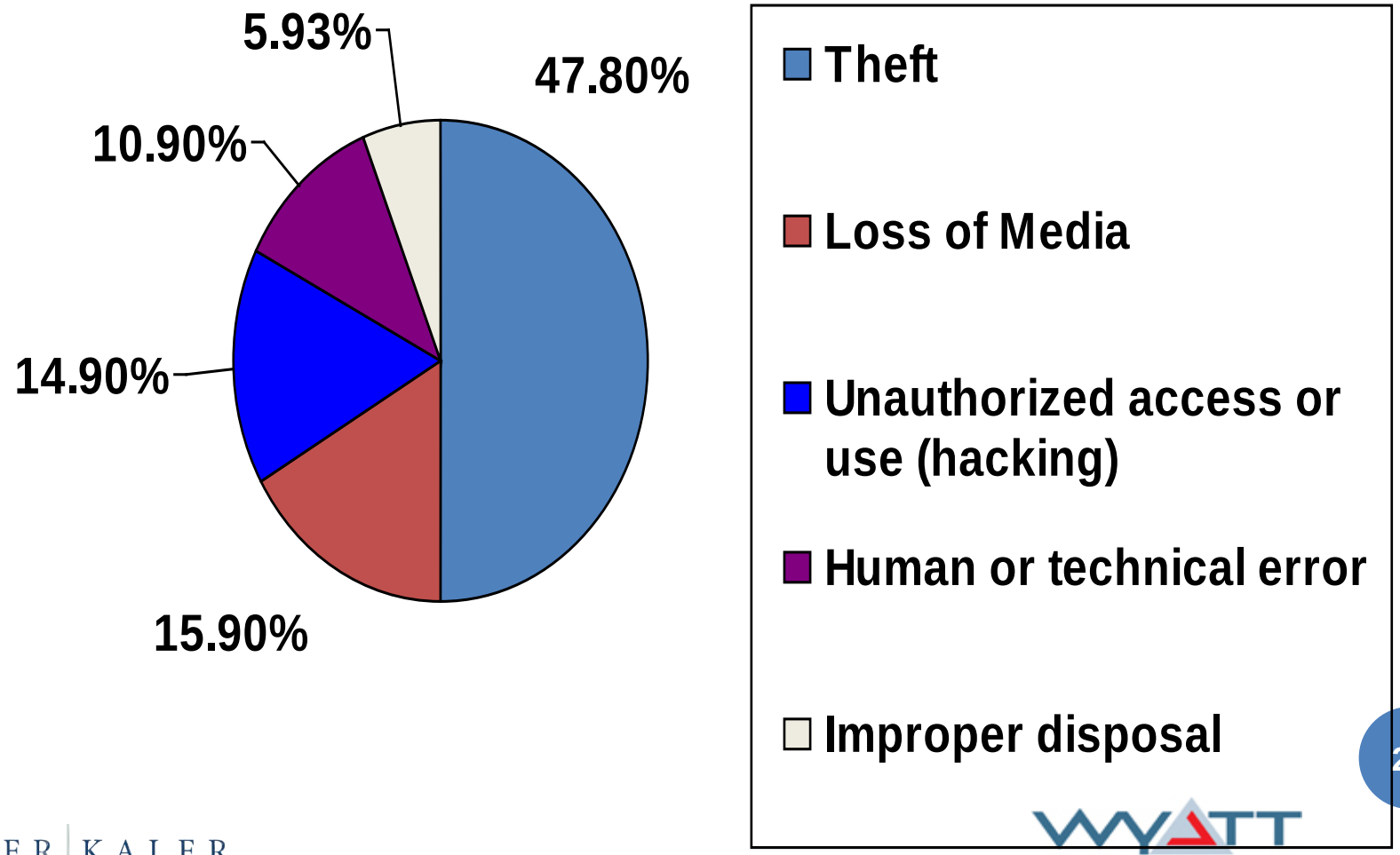
- Lost / theft
- Personal entanglement
- Malware
- Content sharing
- Phishing
- Toll fraud
- Productivity loss
- Breach

- **Reputational damage**
- **Legal liability**
- **HHS Fines**
- **Breach notification costs**
- **Estimated cost: $197 per record lost**

Costs Are Considerable

- Regulatory fines, penalties
- Lawsuits and civil action have larger cost than fines
- Response costs
  1. Forensic analysis
  2. Notification and communication costs
  3. Credit, identity monitoring
- Audits are required – to ensure you meet:
  1. Privacy rule
  2. Security rule
  3. Breach notification rule

Leading Causes of Breaches



OBER | KALER
Attorneys at Law

WYATT TARRANT & COMBS LLP

What Has Changed?

- HIPAA Omnibus announced in January 2013, in effect September 2013 now includes:
  - Covered entities
  - Business Associates
  - Contractors
  - Subcontractors
- Business Associates also encouraged to encrypt PHI
- HITECH also requires PHI breach notification, which was not part of the original HIPAA rules
- Must conduct a "good faith effort" risk assessment for any suspected breach

New HIPAA Rule

- New Omnibus Privacy Rule published January 25, 2013

- Compliance Date is September 23, 2013
  - Breach standard
  - Business associates
  - Notice of Privacy Practice
  - Access
  - Decedents
  - Research

- New audit protocol

HIPAA Security Rule Safeguards

- Access controls to restrict access to PHI to authorized personnel only
- Audit controls to monitor activity on systems containing e-PHI, such as an electronic health record system
- Integrity controls to prevent improper e-PHI alteration or destruction
- Transmission security measures to protect e-PHI when transmitted over an electronic network

How Do You Stay Compliant?

- Conduct an organizational risk assessment (this is required!)
- Develop a HIPAA/HITECH compliance program
- Classify data
- Encrypt anything that you can easily pick up and walk out the door with (laptops, tablets, mobile devices)
- Control access (UTM, ACLs, etc.), core firewalls
- Unify authentication & authorization to a common platform (which is monitored and audited)
- Monitor & audit all access (SIEM)
- Implement IDS/IPS organizational wide
- Implement DLP, control content
- Develop sound IR practices

Solutions for mobile security

Challenges of Mobility in Healthcare

What Policies / Procedures Are Necessary?

- Develop Mobile Security Strategy
  - Authority – Who is responsible for mobile security?
  - Define Resources – Money and people to implement the strategy.
  - Establish Need – Business justification for mobile security.
  - Requirements – What your mobile security solutions must do.
  - BYOD – How will you handle personally owned devices?
  - Awareness – A program to educate and inform users.
  - Policy – Organizational policy and standards for mobile security and operational authority.

More…

What Policies / Procedures Are Necessary?

- Update Incident Response Practices
  - IR Procedures should specifically address mobile security incidents
  - Train staff on procedures to report loss, theft or suspected breach
  - Update procedures to include risk assessment for suspected breach

What Policies / Procedures Are Necessary?

- Have a Mobile Security Policy
  - Sophos has a great template in their Mobile Security Toolkit: http://bit.ly/10zDpHP
  - Acceptable use
  - Rules for personal devices
  - Explain how devices will be reset / wiped
  - Define classes of employees and the access they have
- Have a Mobile Security Standard
  - Define the technical requirements for mobility in your environment
  - Supported platforms
  - MDM Rules

How Do You Control Access?

- Segment the network, implement a core firewall
- Separate mobile devices to protected (wireless) networks
- Implement standard UTM functionality (IPS, web filtering, AV, application control, DLP, etc.)
- Implement MDM
- Require passcodes or smart cards on mobile devices
- Use VPN clients for remote access
- Prevent use of unauthorized USB drives
- Use application delivery framework, such as Citrix or Remotium

How Do You Protect Data?

- If it moves, encrypt it: USB drives, laptops, systems, smartphones, tablets, backup tapes, etc.
- Use strict access controls on applications
- Control, filter, encrypt and monitor email
- Use application delivery framework
- Forbid storing data on mobile devices
- Wipe devices immediately if lost or stolen
- Implement DLP: network, email, web, systems, mobile
- Implement database monitoring (DAM)

How Do You Control Apps?

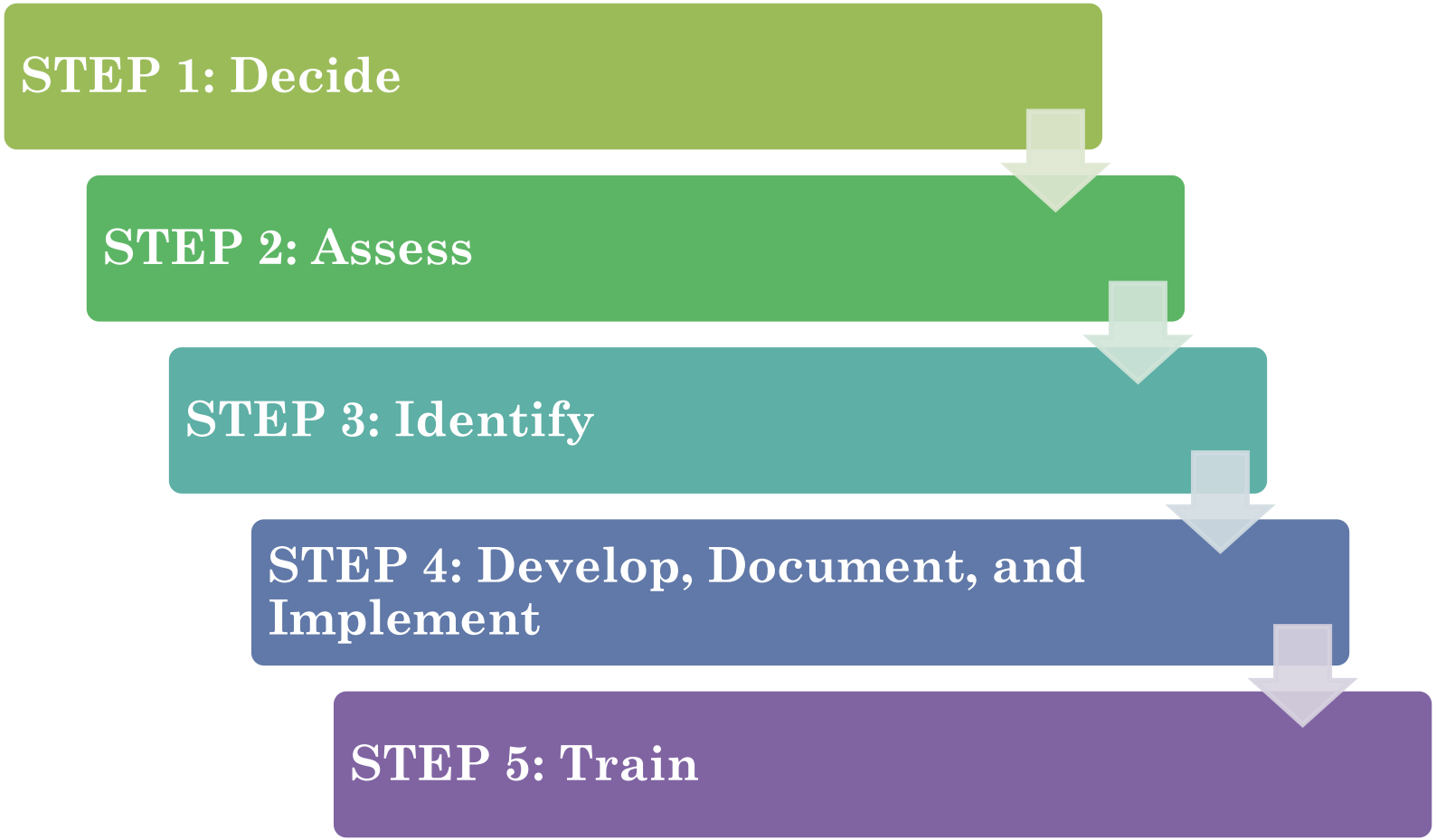
- Create your own App store
- Prohibit jail-breaking with MDM rules
- Deploy endpoint malware monitoring on Android
- Use network controls on UTM devices to block bothersome or dangerous apps
- Implement application compliance on MDM
- Use application delivery framework

How Do I Make this Work?

- HIPAA does not say "protect smartphones"; it says "protect data, and disclose if you fail"
- Find your data, know where it is and who needs to use it
- Automate enforcement – take users out of the protection loop where possible
- Look to the entire infrastructure, not just phones
- Own the devices, avoid sharing personal devices where possible
- Create classes of user, with stronger restrictions on users that access PHI
- Train users about the threats and good practices

Policies and Practical Solutions

Five steps organizations can take to manage mobile devices used by health care providers and professionals



BYOD Policies

- Necessary evil
- Medical record integration
- Device ownership
- Disposal
- Password
- Remote wipe
- Security incidents
- Investigations
- Ownership of data
- What data?
- Other items to include in the policy
- “Contracts” for mobile device use at work

Look at vulnerabilities in your organization – Risk Assessment

Risks vary based on the mobile device and its use. Some risks include:

- A lost mobile device
- A stolen mobile device
- Inadvertently downloading viruses or other malware
- Unintentional disclosure to unauthorized users
- Using unsecure WiFi

OBER | KALER
Attorneys at Law

WYATT TARRANT & COMBS LLP

THE STEPS TO PROTECT AND SECURE HEALTH INFORMATION WHEN USING A MOBILE DEVICE

Locations both "at work" and outside of work

Protect and secure health information when using mobile devices

- In a public space
- On site
- At a remote location

Regardless of whether the mobile device is

- Personally owned, bring their own device (BYOD)
- Provided by an organization

Mobile Devices: Tips to Protect and Secure Health Information

Use a password or other user authentication.

Install and enable encryption.

Install and activate wiping and/or remote disabling.

Disable and do not install file- sharing applications.

Install and enable a firewall.

Install and enable security software.

Keep security software up to date.

Research mobile applications (apps) before downloading.

Maintain physical control of your mobile device.

Use adequate security to send or receive health information over public Wi-Fi networks.

Delete all stored health information before discarding or reusing the mobile device.

You found a problem – Now what?

OBER | KALER Attorneys at Law

WYATT TARRANT & COMBS LLP

Role of Compliance

- Circle back to a culture of compliance
- Include privacy and security officer(s) in decision and training
- Proactive position rather than reactive

QUESTIONS

Sarah E. Swank
OBER | KALER
Washington, DC
(202) 326-5003
seswank@ober.com

C. Elizabeth O'Keeffe
Wyatt Tarrant and Combs LLP
Jackson, MS
(601) 987-5353
ceokeeffe@wyattfirm.com