Mobile Technology meets HIPAA Compliance

Tuesday, March 28, 2017

mountain-pacific quality health
HEALTH TECHNOLOGY SERVICES
transforming health care through innovative technology

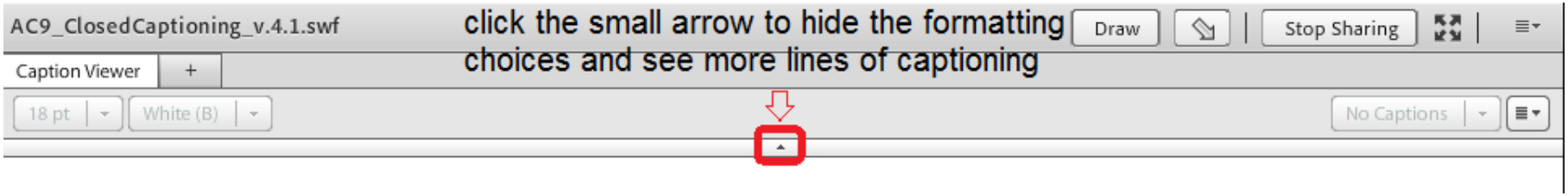
HealthInsight

Welcome

- Thank you for spending your valuable time with us today.
- This webinar will be recorded for your convenience.
- A copy of today's presentation and the webinar recording will be available on our website. A link to these resources will be emailed to you following the webinar.
- All phones will be muted during the presentation and unmuted during the Q&A session. Computer users can use the chat box to ask questions which will be answered at the end of the presentation.
- We would greatly appreciate your providing us feedback by completing the survey at the end of the webinar today.

Closed Captioning

- Closed captioning will appear under today's presentation. To see more lines of captioned text, click the small arrow below.



Susan Clarke, HCISPP

- $(ISC)^2$ certified Healthcare Information Security and Privacy Practitioner.
- 15+ years of Healthcare Experience.
- 10+ years design and development EHR software, BS with computer science major.
- National Incident Management Systems Certificate.
- Served on IT Security, Disaster Recovery and Joint Commission steering committee.
- Served as communications unit lead during Healthcare system's ready and complete alerts.

Mark Norby, CHP

- 15 Years of IT experience
- Eight Years as the CIO of the Community Health Center of Central Wyoming and University of Wyoming Family Medicine Residency Program
- Six Years as a HIPAA Compliance Officer
- Four Years as a HIPAA Compliance Consultant
- Provided help to more than 150 hospitals and clinics

HealthInsight & Mountain-Pacific

HealthInsight and Mountain-Pacific Quality Health are private, non-profit, community-based organizations that have dedicated more than three decades to improving health and health care in: Alaska, Hawaii, Montana, Nevada, New Mexico, Oregon, Utah and Wyoming. Our goal is to increase access to high-quality health care that is affordable, safe and of value to the patients we serve.

HealthInsight & Mountain-Pacific

HealthInsight and Mountain-Pacific Quality Health recognizes that HIPAA compliance can place an excessive burden on small and medium sized organizations so created HIPAA Privacy and Security Solutions (HIPAA PASS) to provide easy, affordable and comprehensive solutions for those who need us most.

Please check out our ***HIPAA PASS*** websites for Risk Analysis and Risk Management services.

Legal Disclaimer

The presenter is not an attorney and the information provided is the presenter(s)' opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar(s) and related materials (including, but not limited to, recordings, handouts, and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar(s) and webinar materials should not in any manner rely upon or construe the information as legal, or other professional advice. Users should seek the services of a competent legal or other professional before acting, or failing to act, based upon the information contained in the webinar(s) in order to ascertain what is may be best for the users individual needs.

Acronyms…

- BA: Business Associate
- CE: Covered Entity
- CEHRT: Certified Electronic Health Record Technology
- CEO: Chief Executive Officer
- CIO: Chief Information Officer
- CMS: Centers for Medicare and Medicaid Services
- EHR: Electronic Health Record
- ePHI: Electronic Protected Health Information
- HHS: Department of Health and Human Services
- HIPAA: Health Insurance Portability and Accountability Act
- HIT: Health Information Technology
- IT: Information Technology

…and more acronyms

- MDM: Mobile Device Management
- NIST: National Institute of Standards and Technology
- OCR: Office for Civil Rights
- ONC: Office of the National Coordinator
- PHI: Protected Health Information
- SP: Special Publication
- SRA: Security Risk Analysis

Session Overview

- What is regulated by HIPAA?
- News and statistics deliver the message.
- Mobile transforming health care delivery.
- Threats to mobile devices and types of threats.
- Considerations for laptops and tablets.
- Smartphone and Mobile Device Management musts do's
- Policies and other important take-away's
- Parting thought and Q&A

Mobile Medical Apps and HIPAA

- Mobile apps are software programs that run on smartphones and other mobile communication devices. They can also be accessories that attach to a smartphone or other mobile communication devices, or a combination of accessories and software--think fitbit
- What's not regulated by HIPAA, many domains such as FTC privacy and fair practices, State privacy laws, consumer reporting agency
- Mobile apps span a wide range of health functions, link to find out if regulated by FDA

http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm368743.htm

"Stolen personal information can have negative financial impacts, but stolen medical information cuts to the very core of personal privacy. Medical identity theft already costs billions of dollars each year, and altered medical information can put a person's health at risk through misdiagnosis, delayed treatment or incorrect prescriptions. Yet, the use of mobile devices to store, access, and transmit electronic health care records is outpacing the privacy and security protections on those devices."

https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices

In the news…

HOME / TOP NEWS / U.S. NEWS

Secret Service laptop stolen from agent's vehicle in New York

By Daniel Uria | March 18, 2017 at 8:54 AM Follow @upi

Comments Share Tweet Email Print

A laptop containing floor plans and evacuation protocol for Trump Tower was stolen from a Secret Service agent's vehicle. The agent's lapel assignment pins which granted her access to security details that protected Hillary Clinton, Donald Trump, the pope and the United Nations General Assembly were also stolen.Photo by Negative Space/Unsplash

March 18 (UPI) -- A bag containing a laptop and other items was stolen from a Secret Service agent's vehicle in New York, authorities said.

Why This Brilliant Tracking Device Is Selling Out Fast

Now you can track any vehicle using this tiny gadget and your smartphone.

READ MORE >>

smartfinancialtips.com

Mobile Device Statistics reported:

- Over 50% of users grab their smartphone immediately after waking up.
- 44% of all stolen smart phones were left in public places.
- A 2015 study published in the *Journal of Hospital Librarianship* estimated that 85 percent of healthcare professionals were bringing their own devices to work.
- Wearable usage has jumped 57% from 2014.
- 95% of business associate (HIPAA) security incidents attributed to lost or stolen devices.

Mobile is transforming Health Care

- Booming market, affordable, convenient and can handle it all (phone, camera, internet, etc).
- Portable, they fit anywhere, pocket, purse, lab coat.
- Larger displays, phone screens have increased in size and scalable.
- Location, directions to appointments, wearable devices provide real time analytics.
- Apps are plentiful and can be customized.

Mobile device benefits for Providers

- Information and time management
- Health record maintenance and access
- Communications and consulting
- Reference and information gathering
- Patient management and monitoring
- Clinical decision-making
- Medical education and training

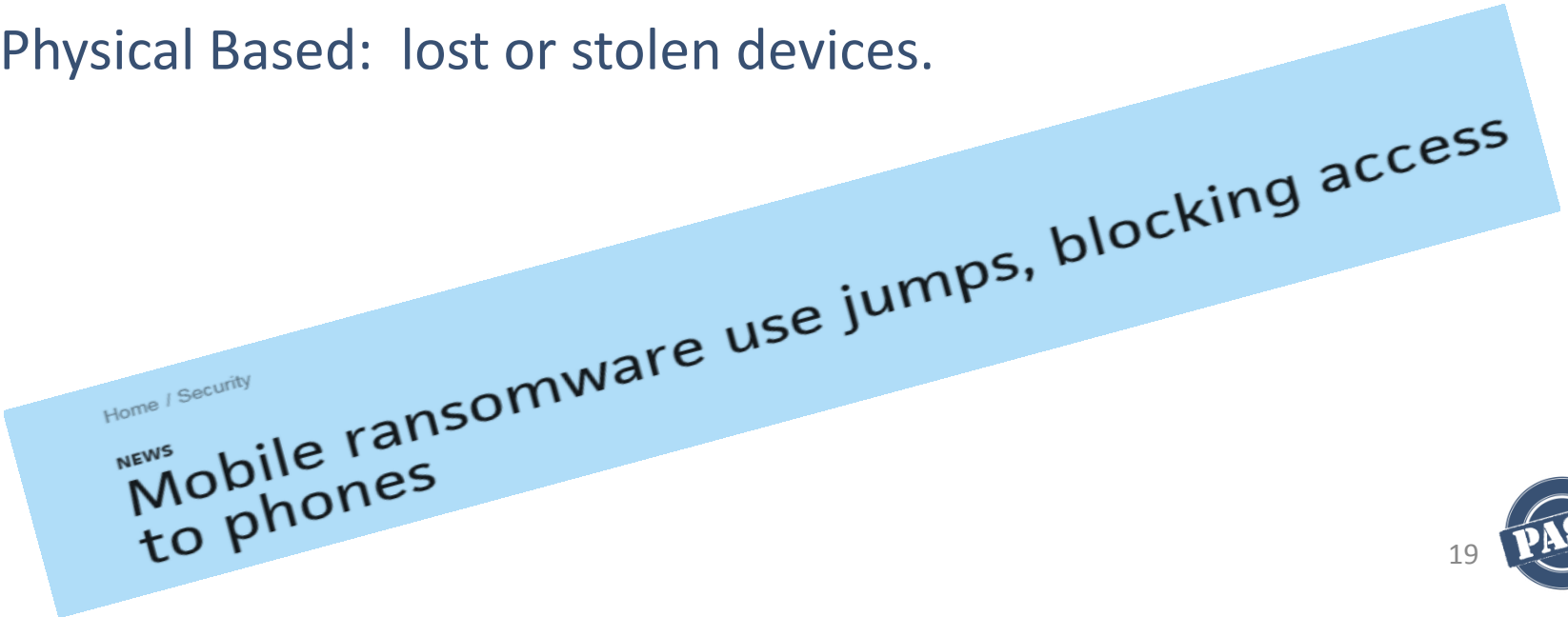
Source=http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4029126/

Mobile devices come with risks

- Easy to steal, misplace, damage.
- For 12 hour shift device may need recharging.
- Data security, authentication controls, able to remote and automatic lock and wipe, encryption, policy and procedure.
- Potential HIPAA violations.
- Patient's awareness of risks for their device.
- BYOD—consider full implications of allowing corporate data to be accessed on personal devices. Convenience clashes with security.

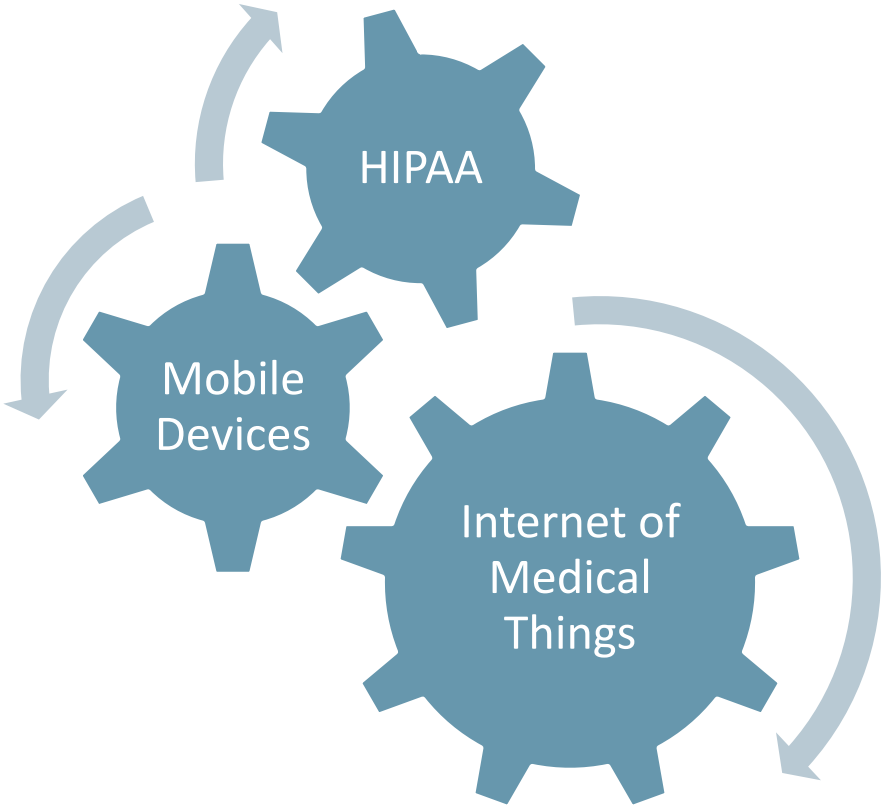
Small size same big threats

- Application Based: vulnerable apps, malware, spyware and privacy threats. mobile remote access Trojan, mRAT
- Web Based: phishing scams, drive by downloads, browser exploits.
- Network Based: man in the middle, sniffing traffic, eavesdropping.
- Physical Based: lost or stolen devices.



Drum roll for Mark Norby…

Heath care providers and professionals using mobile devices in their work must comply with HIPAA Privacy and Security Rules to protect and secure health information.



Things to Consider for Laptops and Tablets

- ✓ Typically owned by the organization and easier to control
- ✓ Encryption is your “get out of jail free card”
- ✓ Ensure that the anti-virus and firewall are enabled
- ✓ Be careful when connecting to public networks
- ✓ Use VPN’s when connecting to the organization remotely
- ✓ Develop Mobile Device policy

Smartphones

- ✓ Will you allow employee smartphones to access practice resources?
- ✓ Will you allow employee smartphones to access Protected Health Information (PHI)?
- ✓ Will smartphones be used for texting, email, and/or the EHR?
- ✓ Will users only be allowed to use practice-owned devices?
- ✓ Will you allow BYOD?
- ✓ Is there an app on Google Play Store or ITunes for your EHR?

Smartphones

Whether owned by the individual or the organization strongly consider the following:

- ✓ Encryption – it might be easier than you think
- ✓ Remote wipe/disable capabilities
- ✓ Ensure anti-virus is employed
- ✓ Use a secure messaging app for texting
- ✓ Have phone lock after period inactivity
- ✓ Use a VPN when using a public network
- ✓ Consider Mobile Device Management
- ✓ Do not expect privacy

Mobile Device Mgmt Solution

What MDM is:

- Software that secures, monitors, manages and supports mobile devices
- Can be deployed on a local server or on the cloud

Mobile Device Mgmt Solution

- **Why MDM?**
- Manage BYOD or practice owned devices
- Need for encryption of data in transit and at rest
- Multiple OS devices
- Configure MDM policies for device restrictions, layout, settings access, notifications
- Impact of a security breach
- http://www.pcmag.com/article/342695/the-best-mobile-device-management-mdm-software-of-2016

Smartphones – Policies and Procedures

- ✓ Consider prohibiting personally owned devices from accessing practice resources
- ✓ Establish an access approval process
- ✓ Establish protocols for practice access
- ✓ Institute standard configuration and technical controls on all mobile devices used to access internal networks or systems
- ✓ Employ a BYOD usage agreement
- ✓ Establish a process for lost or stolen devices
- ✓ Have termination procedures in place

Train your employees!

Insider threat is becoming one of the largest threats to organizations and some cyberattacks may be insider-driven. Although all insider threats are not malicious or intentional, the effect of these threats can be damaging to your organization. Safeguards are often more psychology than technology

According to a survey recently conducted by Accenture and HFS Research, 69% of organization representatives surveyed had experienced an insider attempt or success at data theft or corruption.

IMPORTANT: Conduct mobile device awareness and ongoing training.

Source=Privacy-List listserv, operated by the Office for Civil Rights (OCR)

Key Take-away's

- Create a formal device policy that educates staff of security risks and best practice to safeguard health information.
- Implement Mobile Device Management as part of device risk management strategy.
- Plan on hackers gaining access, lost or stolen devices, and know how to react quickly.
- Think security by design, know risks before deciding on use.
- Allowed in the cloud. Potential for data leakage, syncing data between devices.

More Key Take-away's

- No 1 rule is to have proper password protection, encryption and ENFORCEMENT!
- Keep software up to date.
- Don't use ePHI apps when on an unfamiliar network.
- Disable bluetooth when not in use.
- Have a BYOD policy in place, by ignoring the problem may lead to attack and as result regulatory or reputational threats.

https://healthinsight.org/hipaapass

http://mpqhf.com/corporate/health-and-technology-services/hts-services/hipaa-privacy-and-security/

Important Links on hhs.gov

Privacy rule:

http://www.hhs.gov/hipaa/for-professionals/privacy/

Security rule:

- http://www.hhs.gov/hipaa/for-professionals/security/

Business Associate:

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

Breach Notification Rule:

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html

A parting thought…

Please always remember that checking the box for compliance is important, and protecting patients and their health records is even more important.

Thanks for your valuable time today.

Please let us know if you have questions?

Also…please take just a few minutes to fill out a short survey at the end of our webinar today – we value your comments!

Presenters contact information:

Mark Norby, mnorby@healthinsight.org, (307) 258-5322

Susan Clarke, sclarke@mpqhf.org, (307) 248-8179