Managing Mobile Device Security

Kathy Downing, MA, RHIA, CHPS, PMP
AHIMA Director Practice Excellence

AHIMA
American Health Information Management Association®

Objectives

- Understand how HIPAA and HITECH apply to mobile devices.
- Understand the oversight needed for mobile devices either owned by the organization or the individual.
- Learn how to implement a successful security program for mobile devices.
- Understand the risks and how to manage a mobile device program.

HIPAA Requires:

- Protected health information (PHI) be safeguarded against threats to security, integrity, and unauthorized use.
- Implementation of physical safeguards for all workstations that access ePHI to restrict access to authorized users
- Policies and procedures that govern the receipt and removal of hardware and electronic media containing ePHI into and out of a facility as well as the movement of these items within the facility.
- Implementation of policies and procedures addressing the "final disposition of ePHI and/or the hardware or electronic media on which it is stored" and the "removal of ePHI from electronic media before the media are made available for re-use."
- Maintenance of a record of the movements of hardware and electronic media and any person responsible therefore.
- Creation of a retrievable, exact copy of ePHI, when needed, before movement of equipment.

AHIMA

Source: U.S. Department of Health and Human Services Office for Civil Rights: HIPAA Administrative Simplification

HIPAA Security Administrative Requirements:

- Unique user identification (required): the entity must "assign a unique name and/or number for identifying and tracking user identity"
- Emergency access procedure (required): an entity must "establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency"
- Automatic log-off (addressable): the entity must "implement electronic procedures that terminate an electronic session after a predetermined time of inactivity"
- Encryption and decryption (addressable): the entity must "implement a mechanism to encrypt and decrypt ePHI" as needed

AHIMA

Source: U.S. Department of Health and Human Services Office for Civil Rights: HIPAA Administrative Simplification

Today's Mobile Device Environment

- The next two slides present scenarios of some common issues in healthcare with today's mobile device environment
- For each scenario, think about these questions:
  1. What are the security and privacy issues?
  2. How should this be addressed?
  3. How is your organization handling this today?

AHIMA

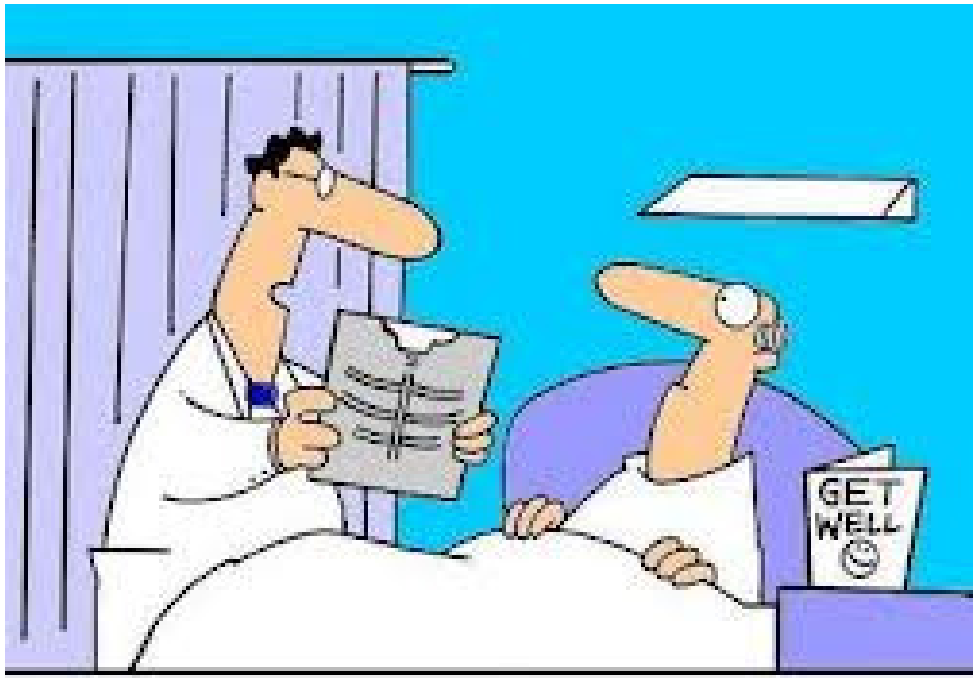
Scenario #1

A physician is seeking a consult from a specialist. The physician uses their personally-owned smartphone or iPad to photograph the patient, attach the photo to an email (the physician uses their personal Gmail account) and sends it off to the specialist.

"Nurse, get on the internet, go to SURGERY.COM, scroll down and click on the 'Are you totally lost?' icon."

Scenario #2

The telehealth system is not functioning properly. The caregiver and the patient decide to use Skype as their backup system.



"Your x-ray showed a broken rib, but we fixed it with Photoshop."

What Are Mobile Devices?

Smart Phones with personal computer-like functionality

Laptops, netbooks and ultrabooks

Tablet computers

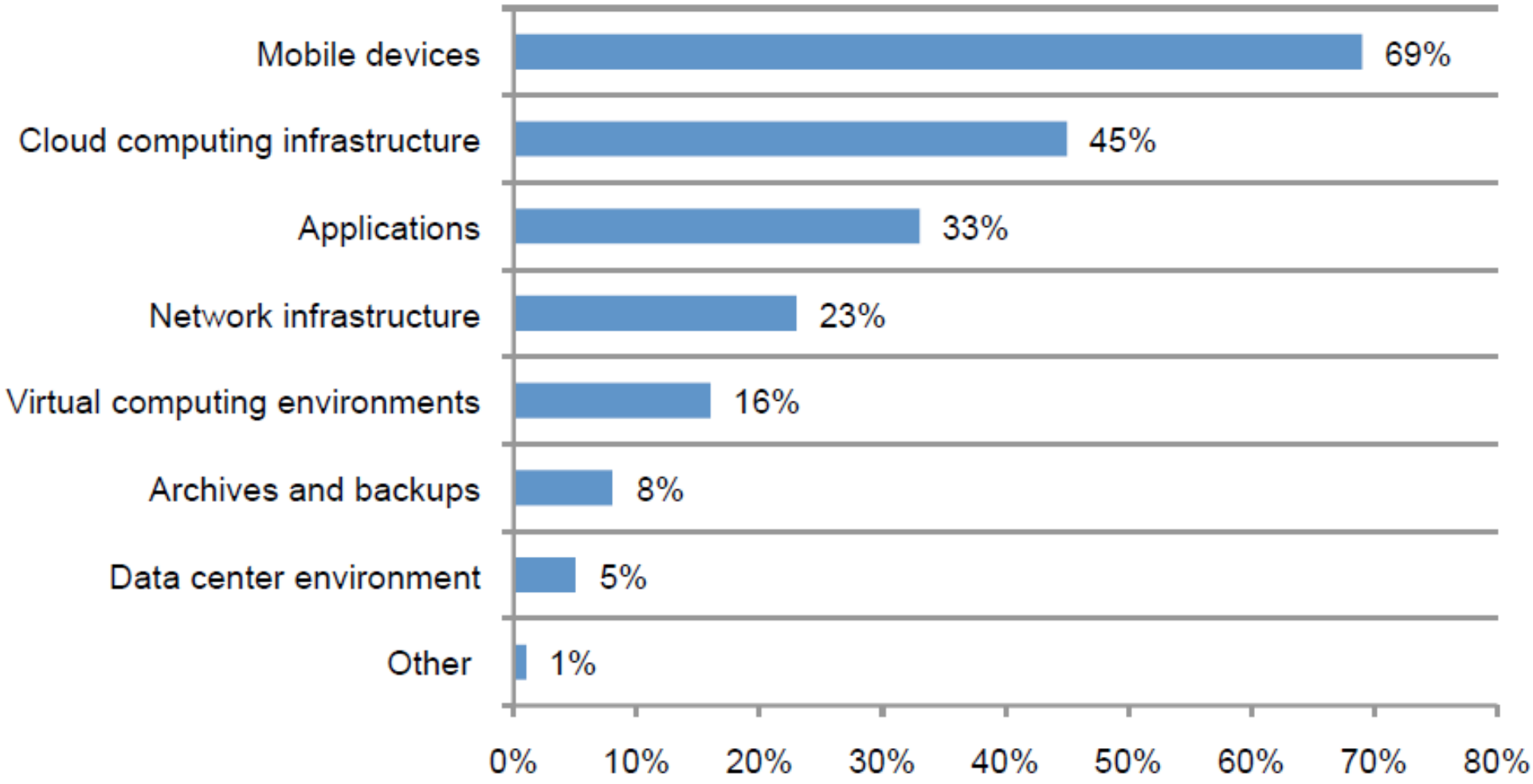
Universal Serial Bus (USB) devices (thumb drives)

Digital cameras

Radio frequency identification (RFID) devices

Source: Mobile Device Security, 2013 AHIMA Convention, Brian Evans , CISSP, CISM, CISA, CGEIT

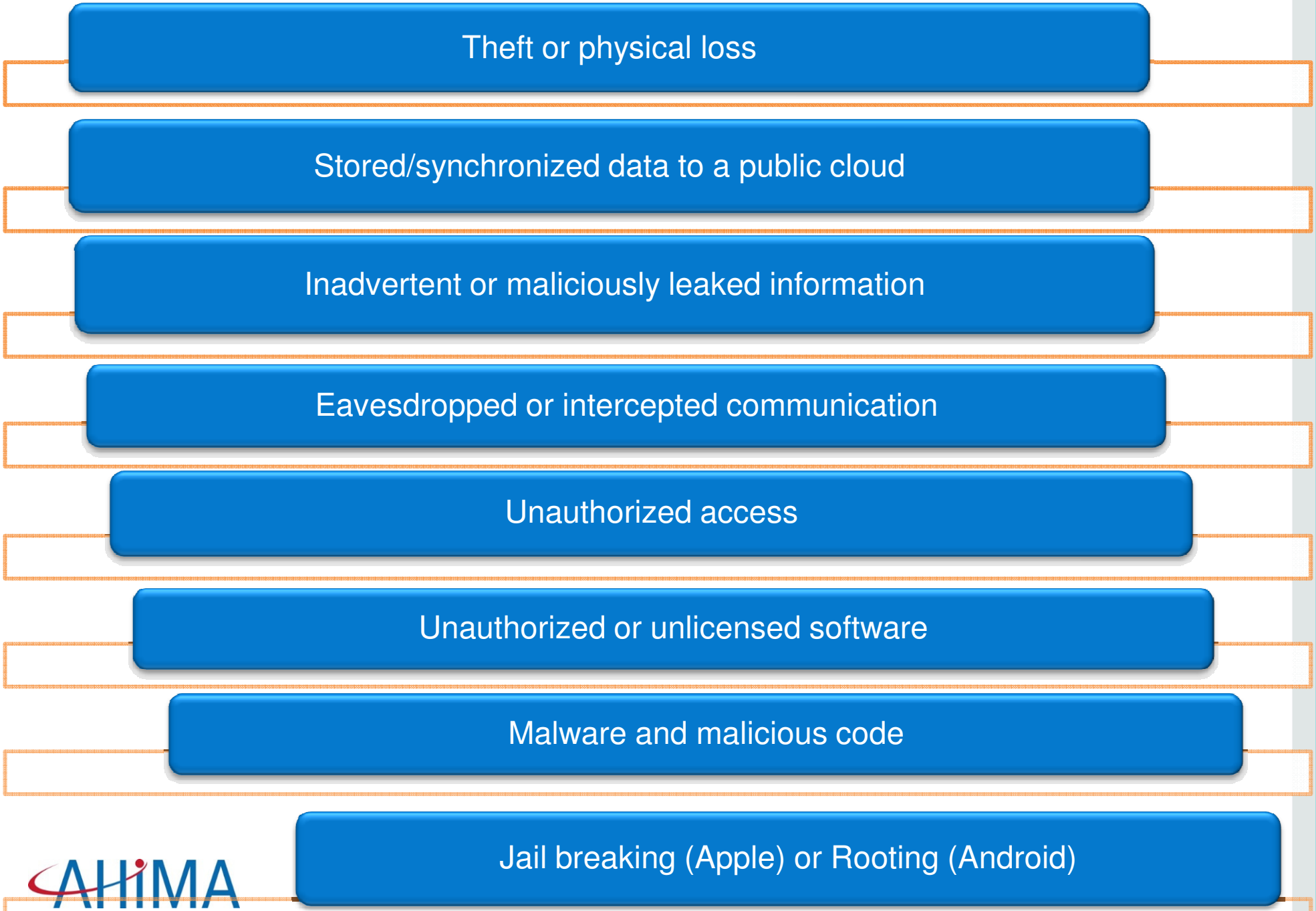
Greatest Data Protection Risks



Source: The Risk of Regulated Data on Mobile Devices & in the Cloud – Ponemon Institute June 2013

Only **19 percent** say their organizations actually **know how much regulated data** is on **mobile devices**

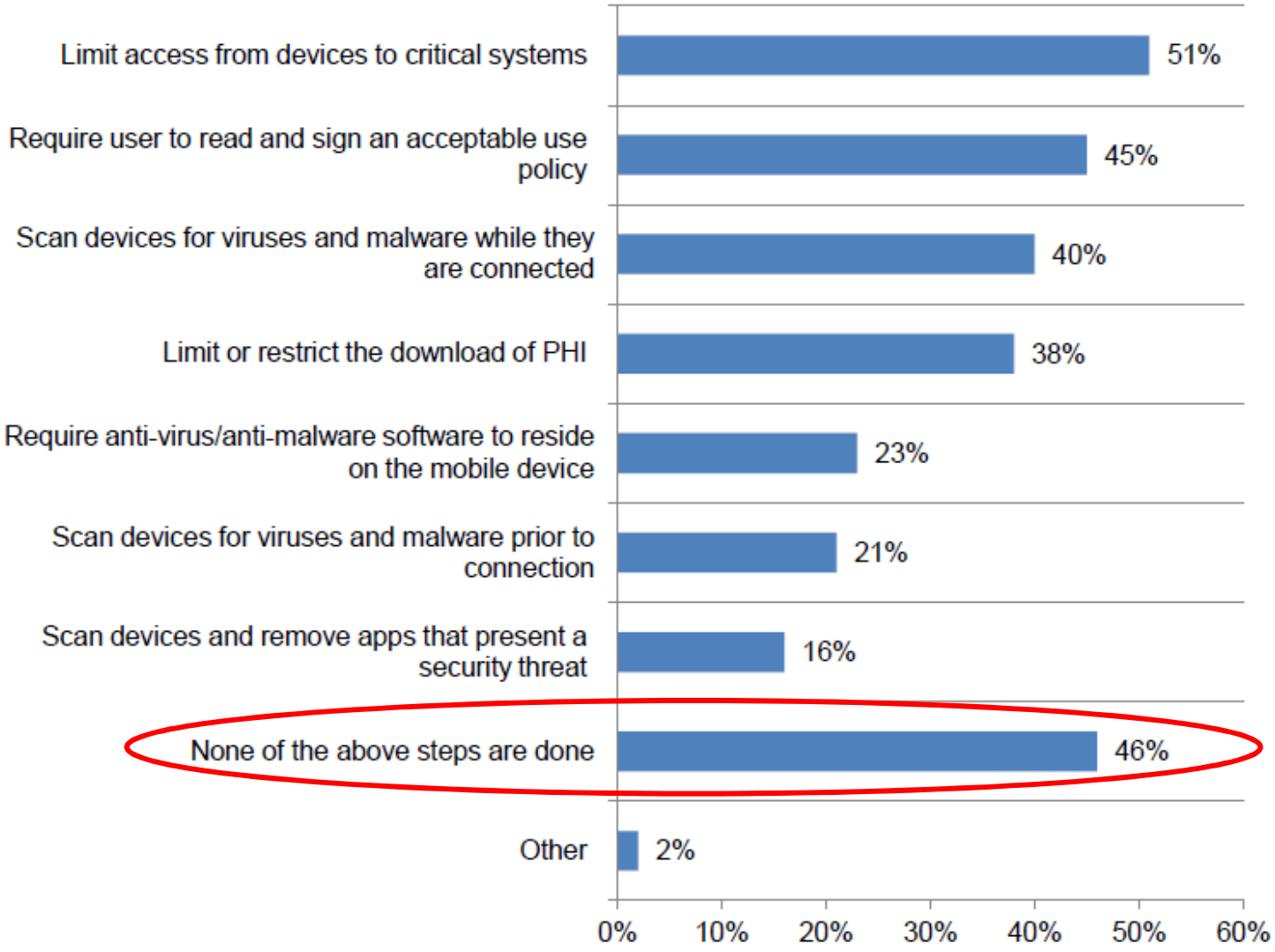
Mobile Device Threats



AHIMA

Source: Mobile Device Security, 2013 AHIMA Convention, Brian Evans , CISSP, CISM, CISA, CGEIT

Are Mobile Devices Secure Enough To Network Connect?



Source: Third Annual Benchmark Study on Patient Privacy & Data Security – Ponemon Institute Dec 2012

81% of healthcare organizations **permit employees/medical staff** to **use their own mobile devices** to **connect** to their networks and systems

HHS Breach Statistics

From September 2009 to June 30, 2013 - **627 breaches** >500 patients were reported to HHS - **22,199,754 patients** affected

Device Type	Number of Incidents	% of Total Incidents	Number of Patients	% of Patients
Laptop	152	24.2%	2,390,935	10.77%
Portable Devices	79	16.2%	1,601,642	7.21%
Hard Drives	1	0.2%	1,023,209	4.61%

Source: Credit Monitoring Service Review as of May 16, 2013

Identity Theft/Credit Protection averages **$136** per individual for 1 year

The Joint Commission on Texting

"It is **not acceptable** for physicians or licensed independent practitioners to **text orders** for patients to the hospital or other healthcare setting."

"This **method provides no ability to verify the identity of the person** sending the text and there is **no way to keep the original message as validation** of what is entered into the medical record."

Source: The Joint Commission

The Joint Commission did not ban all text messaging

AHIMA

The Joint Commission on Texting

Established **Administrative Simplification** (AS) Provisions that serve as **guidelines** for developing **secure communication systems** with four areas of compliance:

Secure Data Centers - Physical security as well as policies for reviewing controls and conducting risk assessments on an ongoing basis

Encryption - PHI must be encrypted both in transit and at rest

Recipient Authentication - Any communication containing PHI must be delivered only to its intended recipient and should allow the sender to know if, when and to whom a message has been delivered

Audit Controls - Any compliant messaging system must have the ability to create and record an audit trail of all activity that contains PHI

AHIMA

Risks and Trends

Trends

1. New mobile devices being released every month
2. Sales of Windows-based computers is down
   – Sales of Apple iPads and iPhones are up
   – Many technicians in healthcare are Microsoft certified, but are not Apple certified
3. iPads and iPhones went from "cute toys" to serious "business tools" used by executives and physicians
4. Mobile devices went from "company issued" to "personally-owned" – Bring Your Own Device (BYOD)

Trends

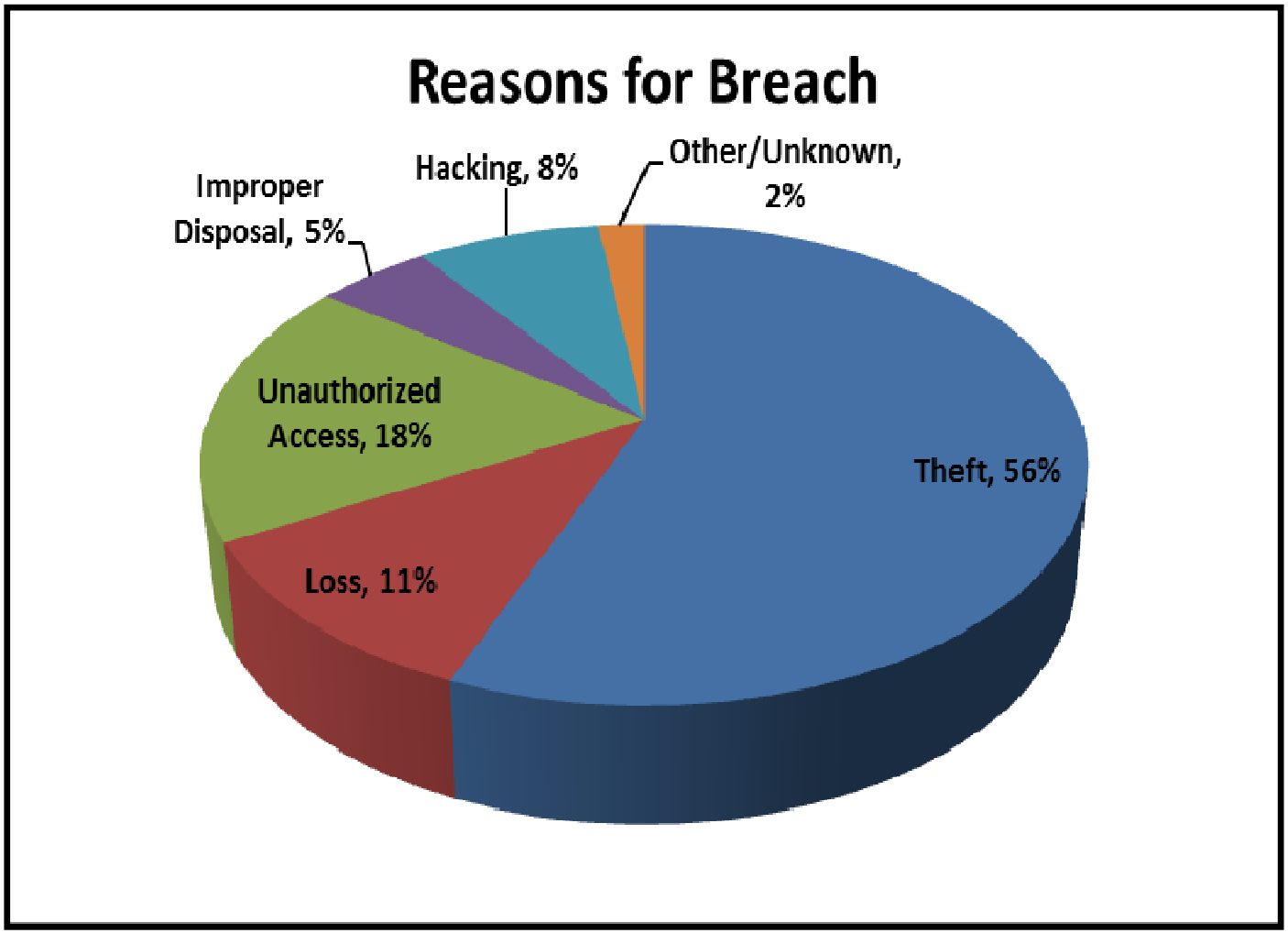
5. Proliferation of mobile apps including medical applications
6. Moving away from "remote access" to "secure access to data anywhere, anytime, on any mobile device"
   - From "data possession" to "data sharing"
7. Using mobile devices to communicate about patient care which may result in data leakage or loss
8. Because of their size and mobility, laptops, tablets, and smartphones are being stolen

Trend – Bring Your Own Device (BYOD)

- Most users don't want two mobile devices:
  - One for business communications
  - One for personal use
  - Users initially purchase a mobile device for their own reasons but later want to use their device for business purposes as well as personal use

- Many organizations reimburse employees for using their personal device to conduct business

Reported HIPAA Breaches



As of March 31, 2013 –

571 breaches were reported to HHS where each breach affected 500 or more patients

Total number of patients affected by these large breaches: **21,744,113**

Data Leakage – Defined

- Uncontrolled and unauthorized transmission of data or information from within an organization to an external location
- The majority of data loss is caused unintentionally by an individual's own actions *(carelessness or disregard to organizational policy)*

Data Leakage – Patient Care

- For efficiency and urgency, physicians, nurses and other clinical staff are increasingly using mobile devices to communicate:
  - Sharing lab or test results
  - Sending pictures of a wound or radiology images
  - Updating a physician on a patient's condition
  - Seeking direction on how to proceed with treatment
  - Finding an on-call consulting specialist
  - Transmitting photo/video from an accident scene to the team of trauma specialists in the ER

Recommendations

AHIMA

Ensure Minimum Security Requirements

Use a password or other user authentication

Install or enable encryption

Install or activate wiping and/or remote disabling

Disable and do not install file-sharing applications

Install or enable a firewall

Install or enable security software

Keep security software up-to-date

Research mobile applications (apps) before downloading

Maintain physical control of your mobile device

Use VPNs to send or receive health information over public Wi-Fi networks

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

AHIMA

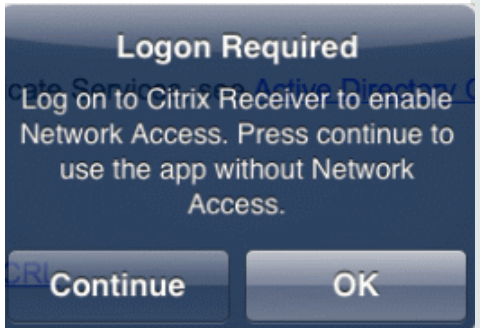
Source: Office of National Coordinator

Mobile Device Ownership

- **Device ownership. If personal devices are permitted** for business use, organizational policy must define the conditions that must be met and how compliance will be verified. For example**, policies and procedures** should consider the following in the event personal devices will be allowed:
  - Annual agreement and signing of the organization's "rules of behavior"
  - Requirements for password protection
  - Lock-out features and specifications
  - Appropriate use of texting
  - Appropriate use of camera and video
  - Appropriate use of sensitive information
  - Alteration of factory defaults and operating systems (i.e., jail-breaking)
  - Appropriate use of applications and conditions of downloading software
  - Reservation of rights by the healthcare facility to examine the system for compliance and investigation of incidents
  - Procedures during employee or contractor termination

Some BYOD Options

- Use a "guest" or "physician" network that is separate (VLAN) from the internal network
  - Otherwise, the device has to be certified to connect to the internal wireless network
- Manage any personally-owned devices used to access organizational information through a Mobile Device Management (MDM) tool
  - Forces users to install appropriate controls
- Access confidential information through virtualization as a secure remote access solution



Enhance Awareness and Training

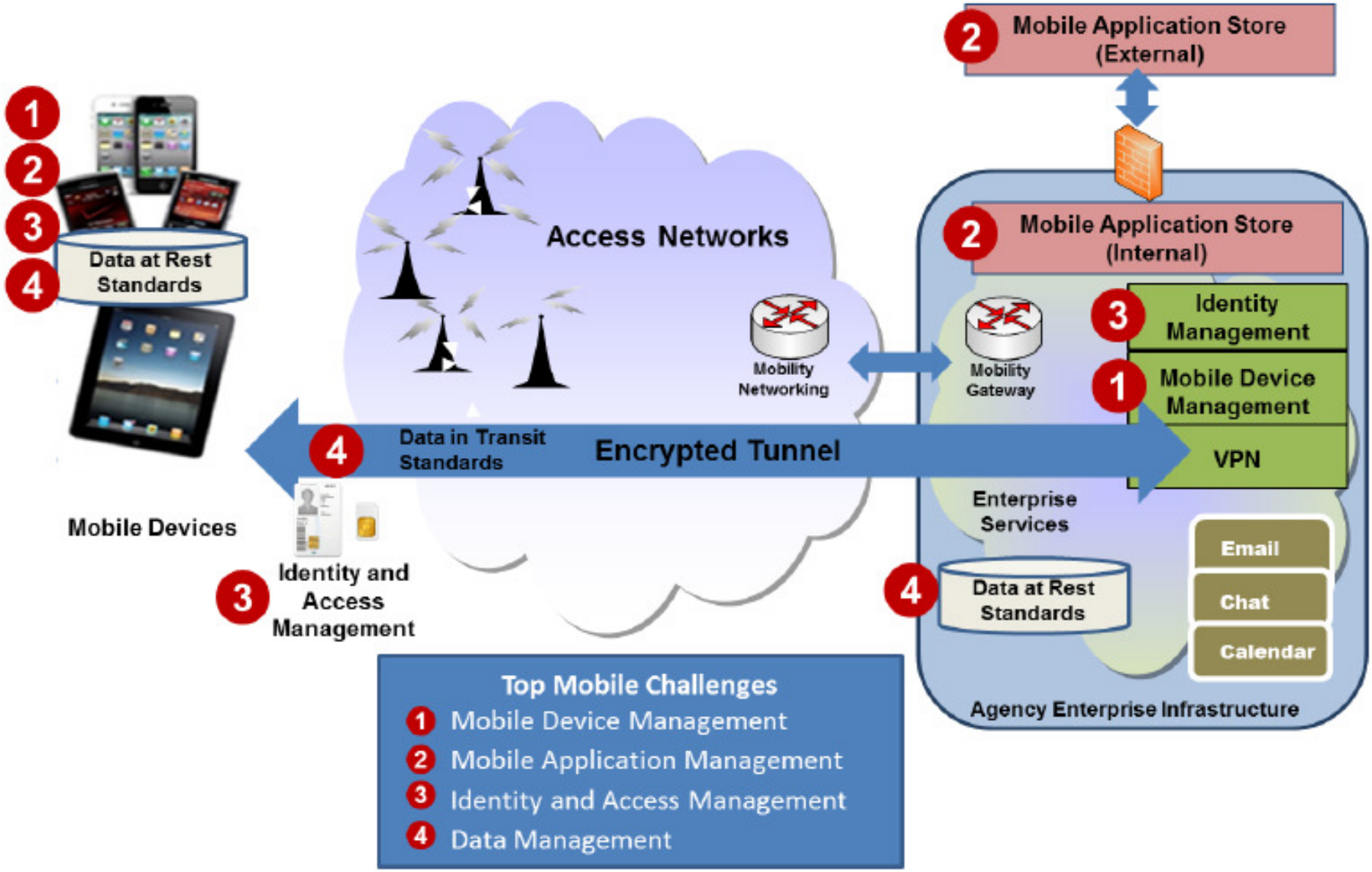
Ensure **users know what NOT to do:**

- **Share passwords** or **user credentials**
- **Allow** the use of mobile devices by unauthorized users
- **Store** or **send unencrypted** confidential **information**
- **Ignore** security software **updates**
- **Download applications** from **untrusted** sources
- **Leave** mobile devices **unattended**
- **Use unsecured** Wi-Fi **networks** for sharing confidential information
- **Discard** devices **without wiping** all confidential information
- **Ignore** organizational **policies** and **procedures**

AHIMA

Source: Office of National Coordinator

Build a Mobile Architecture (Sample)



Source: Government Mobile and Wireless Security Baseline

Depicts the devices, access networks and infrastructure

Immediate Next Steps

- **Define/refine scope and vision** of your mobility requirements

- **Establish/update strategy** and **implement/update** a mobile device **policy** addressing:
  - All mobile devices impacted
  - Acceptable-use guidelines
  - Responsibilities of users, managers and IT
  - Any consequences for non-compliance

- **Deploy** an **MDM** solution

AHIMA

Theft Precaution and Deterrent Information

- Avoid using mobile devices where they can be easily stolen.
- Transport mobile devices in a car's trunk rather than on a seat, thereby keeping it hidden (i.e., do not leave mobile devices in a visible location inside a vehicle).
- Place mobile devices on an airport conveyor after clearing the metal detector (when possible). Unless specifically requested to remove a mobile device other than a laptop from a carry-on bag during screening, leave the device in the bag. This will reduce the likelihood of the device being stolen or left behind in the screening area.
- Place unattended mobile devices in room safes when leaving a hotel room. (Some hotel room safes include an AC adapter so that the computer can be recharged while locked away.)
- Remove portable devices from their docking stations in offices and lock them in a desk drawer or cabinet.
- Lock the room or place the mobile device in a laptop depository when leaving a mobile device in an unattended meeting room. (A laptop depository is a portable safe in which computers can be placed. An alarm will sound if the depository is moved after it is closed.)

Mobile Device Management (MDM)

- An MDM solution would enforce certain security control settings on a personally-owned device to comply with organizational policy
  - Concern: Users may consider this unacceptable since it manages the entire device
  - "Once you become part of our network, we are going to apply our network policies to your device"
  - A wipe or kill command could erase personal data
- MDM can control what apps are allowed on a device
  - Some organizations have created their own "App store"

Implementing a Successful Program

- Conduct a risk analysis
- Present results to executive management
  - Verify that executives understand the possible impact and consequences if a breach occurs
- Create a balanced approach between meeting business objectives and security
- Create and implement a policy
  - Consider having users sign a use agreement
- Implement Mobile Device Management
- Develop an incident response plan

Mobile Device Strategy

- Develop a strategy, policy, and solution focused on:
  - Stronger device and user authentication
  - Data Loss/Leakage Prevention (DLP)
  - Encryption – or do not let the device store data (includes attachments from web mail)
  - Acceptable and supported mobile apps
  - Antivirus or malware protection

Develop a Policy Set

Policies for mobile devices should address:

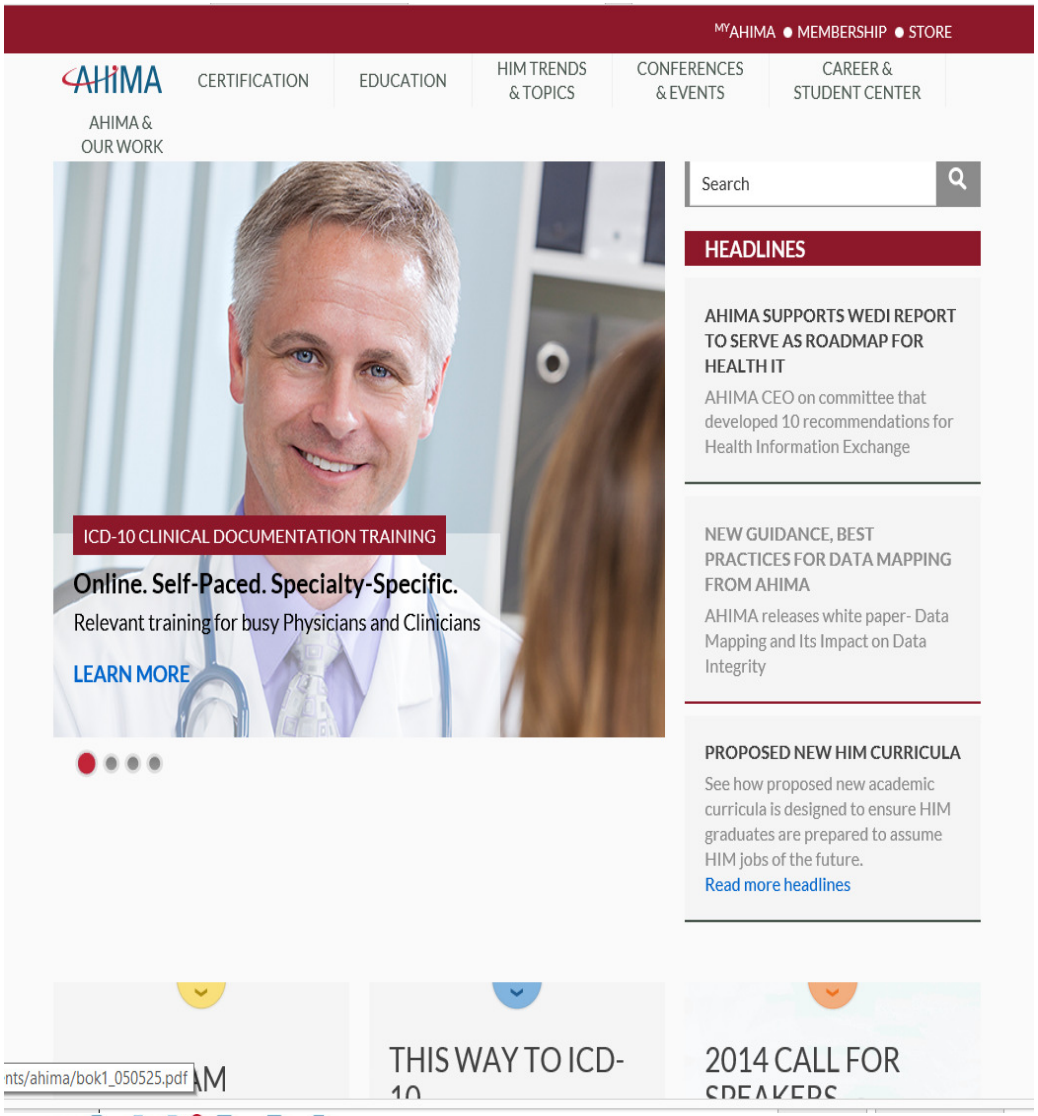
- Device ownership
- Data ownership
- Security safeguards and controls
- Appropriate use
- How to report a lost or stolen device
- Sanitization procedures prior to reuse or disposal

Summary

- You cannot stop mobile device proliferation
- You cannot stop data leakage
  - But you can certainly plug some holes
- You need to develop mobile device strategy
  - Create policies
  - Implement or require certain controls
- Educate users

Goal: Provide access while protecting the data!

AHIMA



AHIMA's Strategic Plan

- Take the lead in driving **information governance** and defining **standards for electronic health information.**
- Contribute to sound healthcare decision-making through analytics, informatics and decision support.
- Empower consumers to optimize their health through management of their personal health information

AHIMA Domains and Initiatives

Established in 1928

Over 71,000 Members

50 State Component Associations

National offices in Chicago and D.C.

Coding, Classification & Reimbursement

Confidentiality, Privacy & Security

Information Governance & Standards

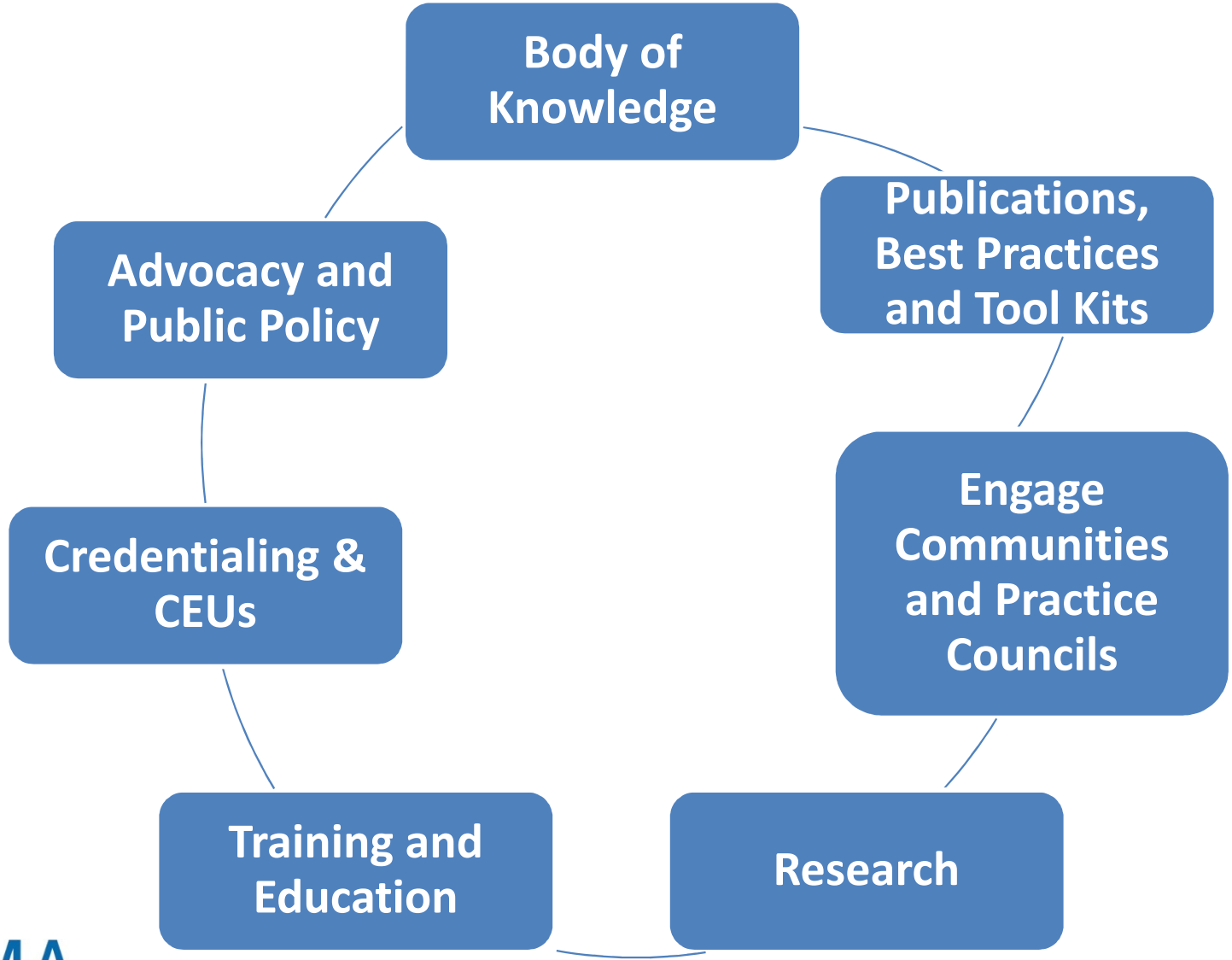
Health Information Management, Technologies & Processes

Health Informatics

Healthcare Leadership & Innovation

Consumer Engagement & Personal Health Information

AHIMA Resources



AHIMA
Certification and Credentials

Certified Healthcare Technology Specialist (CHTS)	Registered Health Information Technician (RHIT®)	Registered Health Information Administrator (RHIA®)
Certified in Healthcare Privacy and Security (CHPS®)	Certified Health Data Analyst (CHDA®)	Certified Documentation Improvement Practitioner (CDIP®)
Certified Coding Associate (CCA®)	Certified Coding Specialist (CCS®)	Certified Coding Specialist-Physician-based(CCS-P®)

AHIMA

Questions / Discussion

AHIMA

Driving the Power of Knowledge

Health Information Where and When It's Needed

AHIMA

Resources

- AHIMA 2013 Convention Presentation Mobile Device Security, Brian Evans, CISSP, CISM, CISA, CGEIT

- U.S. Department of Health and Human Services Office for Civil Rights: HIPAA Administrative Simplification - 45 CFR Parts 160, 162, and 164

- AHIMA HIM Products and Services Team. *HIPAA in Practice*. AHIMA 2004.

- AHIMA. "Regulations Governing Research (Updated)." (Updated January 2011). http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048639.hcsp?dDocName=bok1_048639

Resources

- Cartoon and Images from Google Images www.images.google.com
- AHIMA Analysis of the HITECH Omnibus Rule: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050067.pdf
- The Final HITECH Omnibus Rule (January 25, 2013) http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- U.S. Department of Health and Human Services Office for Civil Rights: HIPAA Administrative Simplification - 45 CFR Part 164

References

- NIST Computer Security Resource Center - SP 800-30 Rev. 1 Guide for Conducting Risk Assessments:
  - http://csrc.nist.gov/publications/PubsSPs.html
- Office of National Coordinator:
  - http://www.HealthIT.gov/mobiledevices
- Government Mobile and Wireless Security Baseline:
  - https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf
- Credit Monitoring Service Review:
  - http://www.fightidentitytheft.com/credit-monitoring.html
- Information Systems Audit and Control Association:
  - https://www.isaca.org/
- Gartner:
  - http://www.gartner.com/technology/home.jsp
- Ponemon Institute:
  - http://www.ponemon.org
- *Implementing Information Security in Healthcare: Building a Security Program*:
  - http://marketplace.himss.org/OnlineStore/ProductDetail.aspx?ProductId=376976692