

# HEALTH IT: Legal Issues



April 14, 2016

Teresa D. Locke

**This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.**

# Overview

- **HITECH Act**
  - Electronic Health Records
  - Meaningful Use
  - Additional Provisions
- **Cybersecurity risks facing healthcare**
- **HIPAA privacy and security related to portable devices**
- **Using e-mail and texting to transmit ePHI**
- **HIPAA privacy and security related to medical scribes**
- **Additional resources**



# Written Materials

- .ppt slides
- NIST Cybersecurity Practice Guide  
([https://nccoe.nist.gov/projects/use\\_cases/health\\_it/ehr\\_on\\_mobile\\_devices](https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices))
- Publications on H&H website:
  - *HIPAA Omnibus Rule: Checklist for Compliance*
  - *Checklist for Security Rules*
  - *HIPAA, E-mails, and Texts to Patients or Others*

# HITECH Act , 42 USC § 17921 *et seq.*

An acronym searching for a name: **H**ealth **I**nformation  
**T**echnology for **E**conomics and **C**linical **H**ealth Act



# Where Does the HITECH Act Fit in to the Mix?

- **HIPAA Privacy Rule (2003).**
  - Requires healthcare providers and health plans (“covered entities”) to protect the privacy of protected health info (“PHI”).
  - Execute business associate agreements (“BAA”) with business associates.
- **HIPAA Security Rule (2005).**
  - Requires covered entities to protect electronic PHI.
- **Health Info Technology for Economic and Clinical Health (“HITECH”) Act (2009).**
  - Required business associates to comply with HIPAA.
  - Strengthened HIPAA and penalties for violations.
- **HIPAA Omnibus Rules (enforced 9/23/13).**
  - Finalized and implemented HITECH Act.

# Health Information Technology for Economics and Clinical Health Act

- Stimulus package legislation: Includes provisions and regulations to improve American health care delivery and patient care through an unprecedented investment in Health IT.
- \$25 billion is allocated specifically to achieving HITECH Act goals and objectives.
  - \$18 billion as incentives for hospitals and physicians who are “meaningful users” of EHR systems.
  - \$2 billion to the Office of the National Coordinator for infrastructure necessary to allow for, and promote, the electronic exchange and use of health information for each individual in the United States;
  - \$1 billion to be made available for renovation and repair of health centers and for the acquisition of health IT systems.

# Health Information Technology for Economics and Clinical Health Act

- Provides financial incentives to eligible professionals for the meaningful use of certified qualified EHRs
- Expands privacy and security requirements found in HIPAA
  - now includes Business Associates
- Public notification of security breaches when “unsecure PHI” is disclosed or used for unauthorized purpose
- Gives patients right to obtain their PHI in electronic format
- Enhances enforcement authority – civil penalties mandatory
- Both positive incentives (meaningful use payments) and negative incentives (civil penalties)



# Health Information Technology for Economics and Clinical Health Act

- Provides financial incentives to eligible professionals for the meaningful use of certified qualified EHRs

# What is a Electronic Health Record?

The term “electronic health record” means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

- *e.g.*, demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal statistics like age and weight, and billing information.

# What is a “Certified EHR”?

- **CMS and the Office of the National Coordinator for Health Information Technology (ONC) have established standards and other criteria for structured data that EHRs must use in order to qualify for EHR incentive program.**
- **To get an incentive payment, you must use an EHR that is certified specifically for the EHR Incentive Programs.**
- **EHRs certified or qualified for other Medicare incentive programs may not be certified for this program. Also, if you already own an EHR, it may not be certified for use in the EHR Incentive Programs.**

# What is Required?

- **The rule establishes payment penalties in future years for eligible providers who have not met the requirements for meaningful use of EHRs.**
- **Meaningful use means providers need to show they are using certified EHR technology in ways that can be measured significantly in quality and in quantity.**
- **Specific objectives must be achieved to qualify for incentives.**

# “Meaningful Use” Incentives

- Incentive payments made to eligible professionals, eligible hospitals, critical access hospitals, and Medicare Advantage Organizations to promote the adoption and meaningful use of interoperable health information technology and qualified electronic health records.
- As of October 2015, more than 479,000 health care providers received payment for participating in the EHR Incentive Programs.

# Three Stages of Compliance

<b>Stage 1:</b> <b>Meaningful use criteria</b> <b>focus on:</b>	<b>Stage 2:</b> <b>Meaningful use criteria</b> <b>focus on:</b>	<b>Stage 3:</b> <b>Meaningful use criteria</b> <b>focus on:</b>
Electronically capturing health information in a standardized format	More rigorous health information exchange (HIE)	Improving quality, safety, and efficiency, leading to improved health outcomes
Using that information to track key clinical conditions	Increased requirements for e-prescribing and incorporating lab results	Decision support for national high-priority conditions
Communicating that information for care coordination processes	Electronic transmission of patient care summaries across multiple settings	Patient access to self-management tools
Initiating the reporting of clinical quality measures and public health information	More patient-controlled data	Access to comprehensive patient data through patient-centered HIE
Using information to engage patients and their families in their care		Improving population health

# What You Need to Know for 2016

- **In October 2015, CMS released a final rule that specifies criteria that eligible professionals, eligible hospitals and CAHs must meet in order to participate in the EHR Incentive Programs in 2015 through 2017 (Modified Stage 2) and in Stage 3 in 2017 and beyond.**

# **What You Need to Know for 2016 (cont'd)**

- **All providers are required to attest to a single set of objectives and measures. This replaces the core and menu objectives structure of previous stages.**
- **For EPs, there are 10 objectives.**
- **For EH and CAHs, there are 9 objectives.**
- **In 2016, all providers must attest to objectives and measures using EHR technology certified to the 2014 Edition or the 2015 Edition, or a combination of the two.**



# **What You Need to Know for 2016 (cont'd)**

- Many of the alternate exclusions that were available in 2015 are not applicable in 2016.
- The EHR reporting period for all providers is based on the calendar year.
- In 2016, the EHR reporting period for all returning participants is a full calendar year (Jan. 1-Dec. 31).
- For first-time participants in 2016, the EHR reporting period is a minimum of a continuous 90-day period between Jan. 1-Dec. 31, 2016.

## **What if You Cannot Attest to MU in 2015 or 2016?**

- **CMS will impose a three percent penalty in 2017 to Medicare EPs who did not meet MU in 2015.**
- **EPs can avoid the penalty by submitting a hardship exception.**
- **The hardship exception deadline is July 1, 2016 for eligible professionals and eligible hospitals and CAHs.**
- **CMS will impose a four percent penalty in 2018 to Medicare EPs who did not meet MU in 2016.**

# **New Hardship Exception Process**

- **In the past, CMS reviewed each application on a case-by-case basis to determine if the penalty will be waived.**
- **Under the Patient Access and Medicare Protection Act (PAMPA), CMS may consider hardship exceptions for categories of providers.**
- **Practices can submit one application for multiple providers in one group.**

# Payment Adjustments 2016 forward

- EPs who are new participants in 2016 will avoid the 2017 penalty if they attest prior to October 1, 2016.
- EPs who attest prior to February 28, 2017 will avoid the 2018 penalty.
- By 2018, all providers will be required to move to Stage 3 Meaningful Use.
- The MU program will become one component of the Merit Based Incentive Program in 2019 based on 2017 reporting.

# EHR Incentive Program Educational Resources

https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/EducationalMaterials.html

Integrated Colorad Free Hotmail Integrated Colorad Lexis-Nexis MSN.com Suggested Sites Tarantella Westlaw Imported From IE

Home | About CMS | Newsroom | FAQs | Archive | Share Help Print

Learn about [your healthcare options](#)  Search

**CMS.gov**  
Centers for Medicare & Medicaid Services

Medicare Medicaid/CHIP Medicare-Medicaid Coordination Private Insurance Innovation Center **Regulations & Guidance** Research, Statistics, Data & Systems Outreach & Education

Home > Regulations and Guidance > EHR Incentive Programs > Educational Resources

## EHR Incentive Programs

- [2015 Program Requirements](#)
- [2016 Program Requirements](#)
- [2017 Program Requirements](#)

## Educational Resources

- [Payment Adjustments & Hardship Information](#)
- [Registration & Attestation](#)
- [Audits and Appeals Overview](#)
- [Data and Program Reports](#)
- [Medicare and Medicaid EHR Incentive Program Basics](#)
- [Clinical Quality Measures Basics](#)
- [eCQM Library](#)
- [2013 Clinical Quality Measures](#)
- [2014 Clinical Quality Measures](#)
- [2015 CQM Reporting Options](#)
- [Certified EHR Technology](#)
- [Eligible Hospital Information](#)
- [Medicaid State Information](#)
- [Medicare Advantage](#)
- [CMS EHR Incentive Programs Listserv](#)
- [Attestation Batch Upload Page](#)

## Educational Resources

Want to know more about the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs? CMS has a number of resources to help you participate in the programs. Select the links below to learn more.

### Registration Information

- [EHR Registration, Attestation, and PECOS Checklist](#)
- [Medicare Registration User Guide for Eligible Professionals](#)
- [Medicaid Registration User Guide for Eligible Professionals](#)
- [Medicare and Medicaid Registration User Guide for Hospitals](#)
- [Medicare EHR Provider Enrollment, Chain and Ownership System \(PECOS\) Notification](#)
- [Hospital EHR Provider Enrollment, Chain and Ownership System \(PECOS\) Notification](#)

### Payment Adjustment and Eligibility Information

- [CAH Method II Fact Sheet](#)
- [CAH Payment Adjustment and Hardship Exception Tipsheet](#)

### Meaningful Use

- [Instructions on how to use the National Broadband Map \(NBM\) tool](#)

### Audit Information and Guidance

- [Supporting Documentation for Audits](#)
- [Sample Audit Letter for EPs](#)
- [Sample Audit Letter for Eligible Hospitals & CAHs](#)
- [Audit Overview Fact Sheet](#)
- [Stage 2 Supporting Documentation for Audits](#)

### EHR Incentive Program Regulations and Notices

This section contains materials pertaining to the rulemaking for the Medicare and Medicaid EHR Incentive Programs. Click

# Health Information Technology for Economics and Clinical Health Act

- Provides financial incentives to eligible professionals for the meaningful use of certified qualified EHRs
- Expands privacy and security requirements found in HIPAA
  - now includes Business Associates

# **Imposes HIPAA Privacy and Security Regulations on BAs**

- **Under HITECH, HIPAA privacy and security regulations are codified to apply not only to covered entities, but also to business associates (BAs).**
- **Prior to HITECH, BAs were not subject to the HIPAA administrative, physical, and technical security rules.**
- **BAs must comply with the privacy requirements as well – typically handled through entering into a business associate contracts.**

# Business Associates

## (45 CFR 160.103)

- Entities that create, receive, maintain, or transmit PHI on behalf of a covered entity to perform:
  - A function or activity regulated by HIPAA (e.g., healthcare operations, payment, covered entity function), or
  - Certain identified services (e.g., billing or claims management, legal, accounting, or consulting services).
  - Health information organizations and e-prescribing gateways.
  - Data transmission companies if they routinely access PHI.
  - Data storage companies (e.g., cloud computing, off-site storage facilities) even if they do not access PHI.
  - Patient safety organizations.
- Covered entities acting as business associates.
- Subcontractors of business associates.



# Business Associate Obligations

- Execute and comply with the terms of the business associate agreement with covered entity.
  - Must contain certain terms required by HIPAA.
- Comply with the Security Rule.
  - Appoint security officer.
  - Perform and document a risk assessment.
  - Implement required safeguards.
  - Execute agreements with subcontractors.
  - Maintain written policies and procedures.
  - Train personnel.
- Comply with minimum necessary standard.
- Report breaches of unsecured PHI to covered entity.

May be difficult for some business associates and subcontractors to comply

# Business Associate Obligations

- **Business associates directly liable under HIPAA for:**
  - Use and disclosures in violation of the BAA or the Privacy Rule, including minimum necessary standard.
  - Failing to comply with the Security Rule.
  - Failing to notify covered entity of a reportable breach.
  - Failing to disclose PHI to HHS in response to investigation.
  - Failing to disclose PHI in response to an individual's request for e-PHI.
  - Failing to execute agreements with subcontractors.
  - Failing to address breach by subcontractor.

# Health Information Technology for Economics and Clinical Health Act

- Provides financial incentives to eligible professionals for the meaningful use of certified qualified EHRs
- Expands privacy and security requirements found in HIPAA
  - now includes Business Associates
- **Public notification of security breaches when “unsecure PHI” is disclosed or used for unauthorized purpose**

# Security Breach Notification Requirements

- HITECH also creates security breach notification requirements.
- A breach notification obligation occurs when there is a breach of unsecured PHI by a CE or a BA.
- Both the term “breach” and “unsecured PHI” have specific definitions that help CEs and BAs to understand when certain timing and notifications requirements under HITECH kick in.

# Security Breach Notification Requirements (cont'd)

- A “breach” is “the unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.” 42 U.S.C. § 17921(1).
- “Unsecured PHI” is PHI that is not secured “through the use of a technology or methodology, specified by the [HHS] Secretary in guidance that renders PHI ‘unusable, unreadable, or indecipherable to unauthorized individuals’” 45 C.F.R. § 164.402.

# “Unsecured” PHI

Currently, only two methods to secure PHI:

- **Encryption of electronic PHI.**
  - Transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
  - Notice provides processes tested and approved by National Institute of Standards and Technology (NIST).
- **Destruction of PHI.**
  - Paper, film, or hard copy media is shredded or destroyed such that info cannot be read or reconstructed.
  - Electronic media is cleared, purged or destroyed consistent with NIST standards.
- **Guidance updated annually.**

(74 FR 42742 or [www.hhs.gov/ocr/privacy](http://www.hhs.gov/ocr/privacy))

# **Security Breach Notification Requirements (cont'd)**

- Individual patients must be informed when a breach of the security rules relating to their private health information has occurred.
- HHS must be informed if 500 or more patients are affected, which will result in the business or organization causing the breach being published on the HHS website and the potential for local press to be informed if necessary.
- Notification is triggered whether the unsecured breach occurred externally or internally.

# Health Information Technology for Economics and Clinical Health Act

- Provides financial incentives to eligible professionals for the meaningful use of certified qualified EHRs
- Expands privacy and security requirements found in HIPAA
  - now includes Business Associates
- Public notification of security breaches when “unsecure PHI” is disclosed or used for unauthorized purpose
- Gives patients right to obtain their PHI in electronic format



# ePHI (Electronic Protected Health Information)

- Any health service provider that holds patient information in electronic form must provide the patient, or a third party named by the patient, with an electronic copy of these records on request.
- A patient has the “right to obtain from [his health care provider] a copy of [his medical records] in an electronic format.” 42 U.S.C. 17935(e)(1).
- A health care provider is allowed to bill “only the cost of ... [c]opying, including the cost of supplies for and labor of copying.” 45 C.F.R. 164.524(c)(4)(i).

## ePHI (cont'd)

- **Issues to consider:**
  - **What is the EHR? Data exist electronically in numerous locations. Need to understand which systems will be accessed to provide the information, such as the radiology system, the laboratory system, or the primary clinical system.**
  - **How will patients receive an electronic copy of the data? Will they use a Web portal, a CD, an e-mail, a thumb drive?**
  - **What will the format be for electronic access? Will the organization provide information in native format, or will it use PDF or proprietary data formats?**

## **ePHI Issues to Consider (cont'd)**

- What security protections will be employed to secure the electronic access (e.g., encryption, passwords)?**
- Will the data be marked to document they were issued to the patient and have not been modified?**
- Will the data be time stamped?**
- Will the organization instruct patients on protecting this electronic information?**
- Does the EHR system have the capacity to single out areas of a record and restrict access to specific individuals?**

# Health Information Technology for Economics and Clinical Health Act

- Provides financial incentives to eligible professionals for the meaningful use of certified qualified EHRs
- Expands privacy and security requirements found in HIPAA
  - now includes Business Associates
- Public notification of security breaches when “unsecure PHI” is disclosed or used for unauthorized purpose
- Gives patients right to obtain their PHI in electronic format
- **Enhances enforcement authority – civil penalties mandatory**

# Enforcement of the HITECH Act

- **The Office for Civil Rights (“OCR”) of the United States Department of Health and Human Services (“HHS”) is the primary enforcement authority for HITECH.**
- **As an alternative form of enforcement, state attorneys general also may bring suit in federal courts on behalf of their residents to enforce HITECH. 42 U.S.C. § 1320d-5(d).**
- **The HITECH Act also requires HHS to conduct periodic audits to ensure that healthcare organizations and their business associates are complying with HIPAA laws.**

# **Enforcement of the HITECH Act (cont'd)**

- **In its 2016 Phase 2 HIPAA Audit Program, OCR will review the policies and procedures adopted and employed by CEs and their BAs to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These audits will primarily be desk audits, although some on-site audits will be conducted.**

# **Enforcement of the HITECH Act (cont'd)**

- **The 2016 audit process begins with email verification of an entity's address and contact information. OCR will then transmit a pre-audit questionnaire to gather data about the size, type, and operations of potential auditees; this data will be used with other information to create potential audit subject pools.**
- **Communications from OCR will be sent via email and may be incorrectly classified as spam. If your entity's spam filtering and virus protection are automatically enabled, OCR expects entities to check their junk or spam email folder for emails from OCR.**

# Civil Penalties

## (45 CFR 160.404)


Conduct	Penalty
Did not know and should not have known of violation	<ul style="list-style-type: none"><li>• \$100 to \$50,000 per violation</li><li>• Up to \$1.5 million per type per year</li><li>• No penalty if correct w/in 30 days</li><li>• OCR may waive or reduce penalty</li></ul>
Violation due to reasonable cause	<ul style="list-style-type: none"><li>• \$1000 to \$50,000 per violation</li><li>• Up to \$1.5 million per type per year</li><li>• No penalty if correct w/in 30 days</li><li>• OCR may waive or reduce penalty</li></ul>
Willful neglect, but correct w/in 30 days	<ul style="list-style-type: none"><li>• \$10,000 to \$50,000 per violation</li><li>• Up to \$1.5 million per type per year</li><li>• <b>Penalty is mandatory</b></li></ul>
Willful neglect, but do not correct w/in 30 days	<ul style="list-style-type: none"><li>• At least \$50,000 per violation</li><li>• Up to \$1.5 million per type per year</li><li>• <b>Penalty is mandatory</b></li></ul>



# Civil Penalties

- **Counting penalties**
  - If violation results in disclosure of info for multiple individuals, each individual is a separate violation.
    - E.g., loss of laptop containing 2000 names = 2000 violations.
  - If violation results from failure to implement required safeguard or policy, each day the safeguard or policy was not implemented is a separate violation.
    - E.g., if you failed to put in place safeguards and policies after 9/23/13, you are at 871 violations for each requirement violated and counting...

# Civil Penalties

← →  http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

 Case Examples and Resolut... x

File Edit View Favorites Tools Help

    Page ▾ Safety ▾ Tools ▾   

- \$750,000
  - \$218,400
  - \$125,000
  - \$150,000
  - \$800,000
  - \$4,800,000
  - \$1,725,220
  - \$250,000
  - \$215,000
  - \$150,000
  - \$1,215,780
  - \$1,700,000
  - \$275,000
- [\\$750,000 HIPAA Settlement Emphasizes the Importance of Risk Analysis and Device and Media Control Policies](#) - August 31, 2015
  - [HIPAA Settlement Highlights Importance of Safeguards When Using Internet Applications](#) - June 10, 2015
  - [HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records](#) - April 22, 2015
  - [HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software](#) - December 2, 2014
  - [\\$800,000 HIPAA Settlement in Medical Records Dumping Case](#) - June 23, 2014
  - [Data Breach Results in \\$4.8 Million HIPAA Settlements](#) - May 7, 2014
  - [Concentra Settles HIPAA Case for \\$1,725,220](#) - April 22, 2014
  - [QCA Settles HIPAA Case for \\$250,000](#) - April 22, 2014
  - [County Government Settles Potential HIPAA Violations](#) - March 7, 2014
  - [Resolution Agreement with Adult & Pediatric Dermatology, P.C. of Massachusetts](#) - December 20, 2013
  - [HHS Settles with Health Plan in Photocopier Breach Case](#) - August 14, 2013
  - [WellPoint Settles HIPAA Security Case for \\$1,700,000](#) - July 11, 2013
  - [Shasta Regional Medical Center Settles HIPAA Privacy Case for \\$275,000](#) - June 13, 2013

# Criminal Penalties

(42 USC 1320d-6(a))

- Applies if employees or other individuals obtain or disclose protected health info from covered entity without authorization.

Conduct	Penalty
Knowingly obtain info in violation of the law	<ul style="list-style-type: none"><li>• \$50,000 fine</li><li>• 1 year in prison</li></ul>
Committed under false pretenses	<ul style="list-style-type: none"><li>• 100,000 fine</li><li>• 5 years in prison</li></ul>
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	<ul style="list-style-type: none"><li>• \$250,000 fine</li><li>• 10 years in prison</li></ul>

# Criminal Penalties

//cdn.ca9.uscourts.gov/datastore/opinions/2012/05/10/10-50231.pdf - Windows Internet Explorer provided by Holland and Hart

http://cdn.ca9.uscourts.gov/datastore/opinions/2012/05/10/10-50231.pdf

Edit Go To Favorites Help

Convert Select

HH Secure HIPAA (160) AHLA Lists AKS (2) AKS CMS home CMS Stark eCFR EMTALA guidelines Gmail HIPAA Hotmail Idaho Statutes IDAPA DH

//cdn.ca9.uscourts.gov/datastore/opinions/...

1 / 10 164% Collaborate Sign Find



FOR PUBLICATION

## UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,  
*Plaintiff-Appellee,*

v.

HUPING ZHOU,  
*Defendant-Appellant.*

No. 10-50231

D.C. No.  
2:08-cr-01356-  
AJW-1

OPINION

Appeal from the United States District Court  
for the Central District of California  
Andrew J. Wistrich, Magistrate Judge, Presiding

# State Attorney General Lawsuits

- May sue for \$25,000 per violation + costs

United States Department of Health & Human Services

HIPAA Enforcement Training for State Attorneys General

**Agenda**  
View Training Agenda

**Browse**  
View All Presentations

**Speakers**  
Browse Sessions by Presenters' Names

**Support**  
View Frequently Asked Support Question

Search...

United States Department of Health & Human Services

**HIPAA Enforcement Training for State Attorneys General**

[Click Here to Start Course](#)

# Healthcare Cybersecurity Risks



# 2015 Healthcare Data Breaches

- **Three out of the top seven cyberattacks in 2015 involved the healthcare industry.**
  - **Anthem – largest healthcare breach ever recorded – 78.8 million highly sensitive patient records breached**
  - **Premera Blue Cross – affected 11 million members**
  - **Excellus BlueCross BlueShield – affected 10 million members**
- **Incidents relating to phishing, hacking and malware were the cause of 31 percent of data security incidents during 2015, revealing a shift from 2014 when human error was the leading cause.**

# 2015 AHA Most Wired Survey

## Most Wired Survey Tracks Hospital Use of Important Cybersecurity Measures

Measure	Share of hospitals implementing measure:		
	More than 90%	More than 80%	More than 70%
Unique identification of system users	✓		
Automatic logoff of system users	✓		
Required use of strong passwords	✓		
Passcodes for mobile devices	✓		
Use of intrusion detection systems		✓	
Encryption of wireless networks		✓	
Encryption of laptops and/or workstations	✓		
Encryption of removable storage media			✓
Encryption of mobile devices			✓
Mobile device data wiping	✓		
At least annual risk analysis to identify compliance gaps and security vulnerabilities	✓		
At least annual infrastructure security assessment	✓		
Security incident event management			✓



# Cybersecurity Issues

- A new study from Skycure found that 80 percent of doctors use mobile devices for work and 28 percent store patient data on these mobile devices, but at the same time they aren't doing much about securing that information.
- As Dark Reading reported, a surprising number (14%) aren't even taking the most simple (and obvious) security step of using a passcode to lock the device nor updating its software (11%).
- Also, the study estimated that 27.79 million devices with medical apps installed might also be infected with high-risk malware.

# The Danger of Ransomware

- In 2014, the FBI Cyber Division issued a “Private Industry Notification” to healthcare systems to an anticipated increase in cyberattacks.
- Cyberattacks are now reality.
- Ransomware encrypts files, databases or other caches of information.
- The hackers are not generally after the information – holding data for a ransom.
- Most common source of ransomware are malicious email attachments that pretend to be some sort of invoice, bill or image. *Symantec 2015 Internet Security Threat Report.*

# OCR Cyber-Awareness Initiative

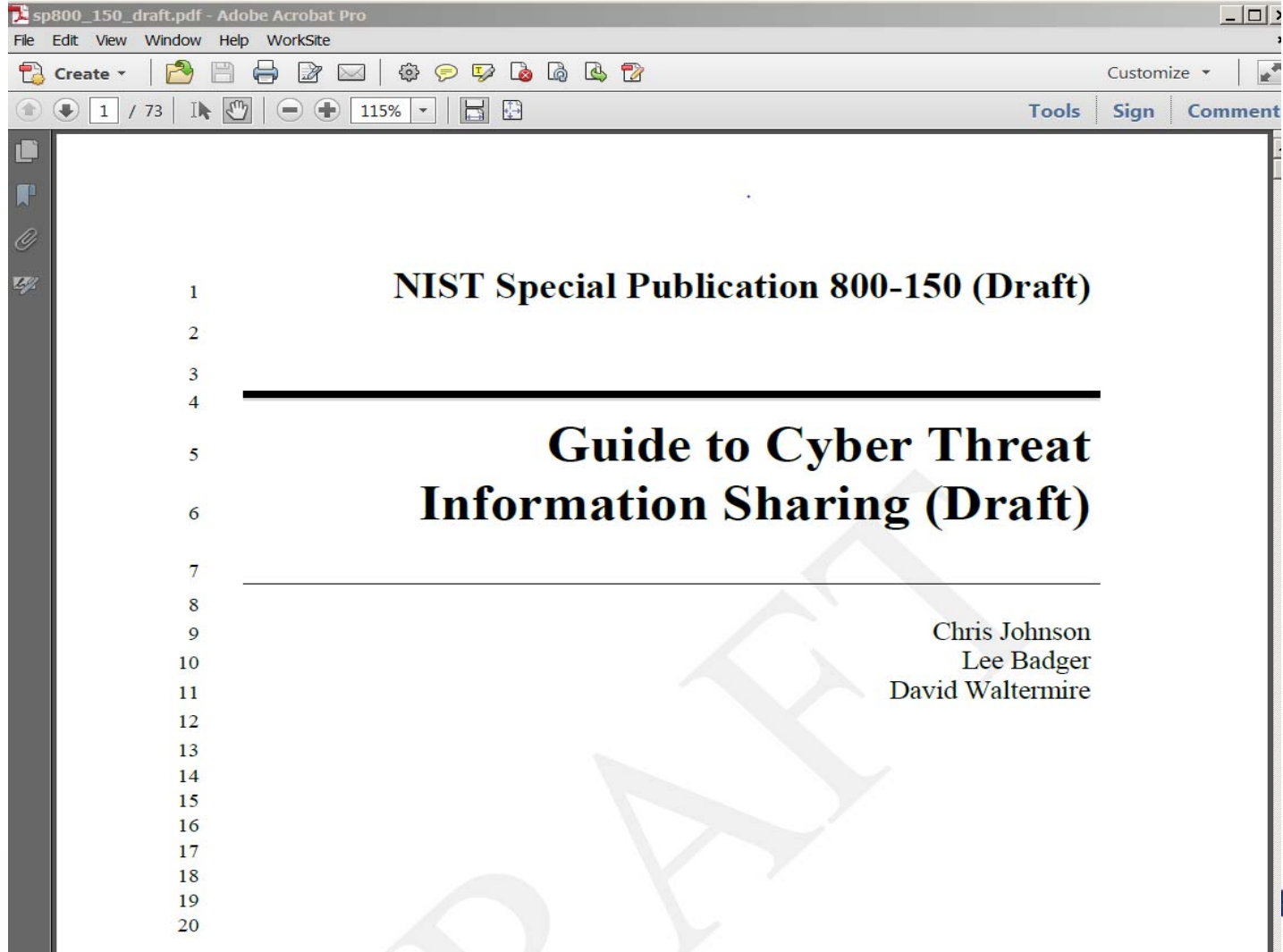
- Make ransomware and other malware attacks part of your risk analysis.
- Regularly back up data – laptops, desktops, servers, mobile devices.
- Ensure that anti-virus and anti-malware software is installed throughout the system.
- Ensure that all devices, systems and software are up to date with patches and security updates.
- Install pop-up blockers and ad-blocking software.
- Implement browser filters and smart email practices.

# OCR Cyber-Awareness Initiative

- The weakest link in any computer systems is the user – educate staff:
  - do not open attachments in emails or messages
  - never open attachments that come from non-client
  - do not provide login credentials to any individual
  - do not install any software program unless requested to do so by an internal IT department
- Procure cyber insurance with cyber extortion coverage.
- Utilize a new tool supplied by the Better Business Bureau which will help to keep them aware of the latest social engineering and phishing scams:  
<https://www.bbb.org/scamtracker/us>.

# Cybersecurity (cont'd)

<http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-150>



The screenshot shows the Adobe Acrobat Pro interface. The title bar reads "sp800\_150\_draft.pdf - Adobe Acrobat Pro". The menu bar includes "File", "Edit", "View", "Window", "Help", and "WorkSite". The toolbar contains various icons for file operations and navigation. The status bar at the bottom of the toolbar shows "1 / 73" pages, a hand cursor, and a zoom level of "115%". The document content is displayed in a large white area. On the left side of the document, there is a vertical list of page numbers from 1 to 20. The main text of the document is centered and reads:

**NIST Special Publication 800-150 (Draft)**

---

**Guide to Cyber Threat Information Sharing (Draft)**

---

Chris Johnson  
Lee Badger  
David Waltermire

A large, light gray "DRAFT" watermark is visible diagonally across the center of the page. In the bottom right corner of the document area, there is a logo for "HART" with a blue square icon.

# OCR Crosswalk

www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/

Integrated Colorado Free Hotmail Integrated Colorado Lexis-Nexis MSN.com Suggested Sites Tarantella Westlaw Imported From

HHS.gov

Health Information Privacy

U.S. Department of Health & Human Services



HIPAA for Individuals

Filing a Complaint

HIPAA for Professionals

Newsroom

HIPAA for Professionals

Text Resize A A A Print Share

Privacy

Security

Summary of the Security Rule

Guidance

Combined Text of All Rules

Breach Notification

Compliance & Enforcement

Special Topics

Patient Safety

Covered Entities & Business Associates

Training & Resources

FAQs for Professionals

Other Administrative Simplification Rules

## Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework

The sensitive health information maintained by health care providers and health plans has become an increasingly attractive target for cyberattacks. The need for health care organizations to up their game on health data security has never been greater.

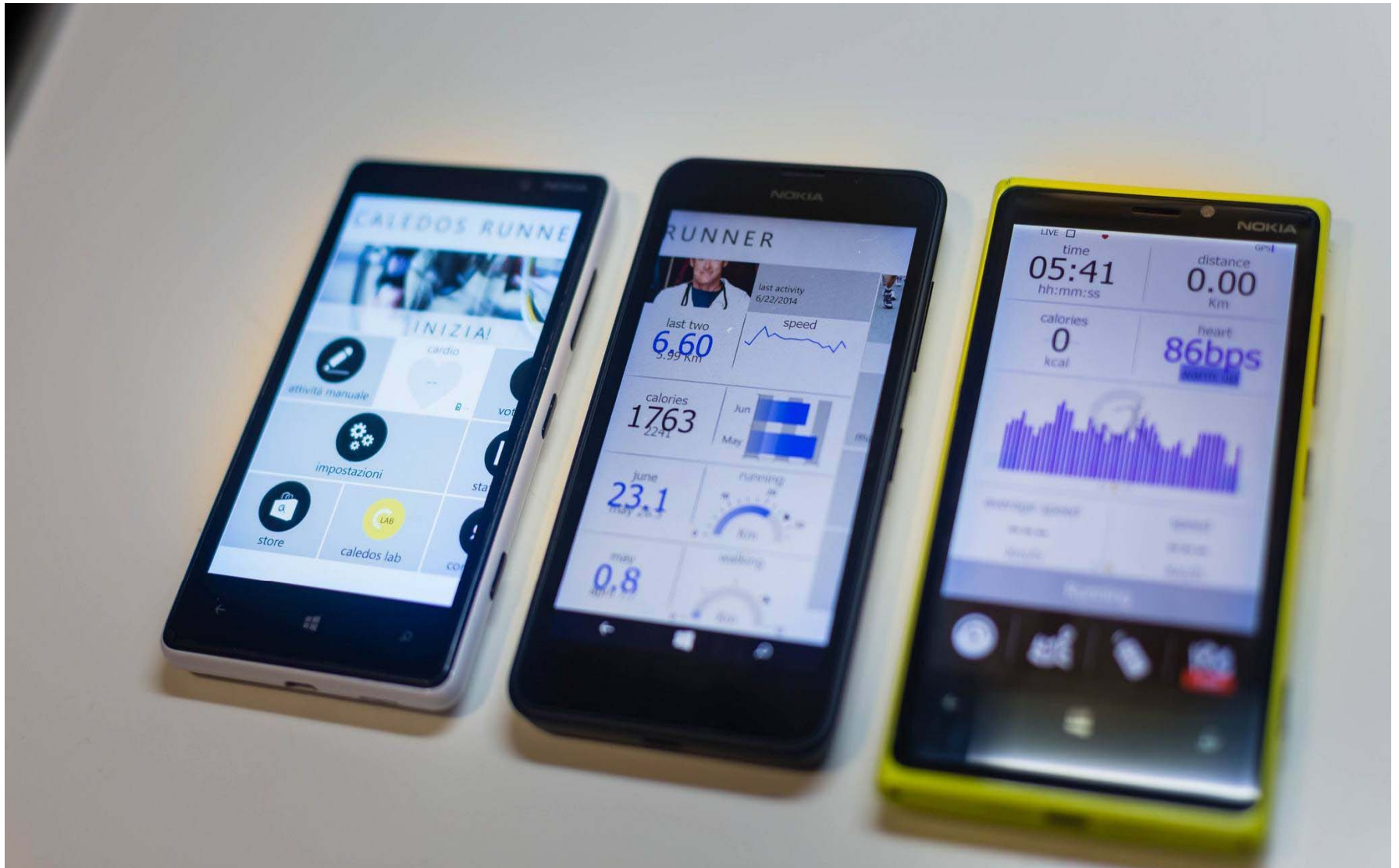
To help health care organizations covered by the Health Insurance Portability and Accountability Act (HIPAA) to bolster their security posture, the Office for Civil Rights (OCR) today has released a [crosswalk](#) developed with the National Institute of Standards and Technology (NIST) and the Office of the National Coordinator for Health IT (ONC), that identifies "mappings" between the NIST Framework for Improving Critical Infrastructure Cybersecurity (the Cybersecurity Framework) and the HIPAA Security Rule. The crosswalk also includes mappings to other commonly used security frameworks.

In addressing security, many entities both within and outside of the healthcare sector have voluntarily relied on detailed security guidance and specific standards issued by NIST. In February 2014, NIST released the Cybersecurity Framework to help organizations in any industry to understand, communicate and manage cybersecurity risks.

Entities covered by HIPAA must implement strong data security safeguards in their environments, and in particular, comply with the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of all of the electronic protected health information (ePHI) they create, receive, maintain or transmit. We hear frequently from covered entities and business associates who say they are working hard in an increasingly challenging atmosphere to assure their PHI is adequately protected. We also know from our HIPAA enforcement work that far too frequently entities are leaving PHI vulnerable to breach and access by unauthorized persons. [According to a report in USA Today](#), the healthcare industry has accounted for over 40 percent of data breaches over the last three years, and 91 percent of all health organizations have reported a breach over the last two years.

Organizations that have already aligned their security programs to either the NIST Cybersecurity Framework or the HIPAA Security Rule may find this crosswalk helpful in identifying potential gaps in

# HIPAA Privacy and Security Issues Related to Mobile Devices



# **HIPAA Privacy and Security Issues Related to Mobile Devices**

- **Providers are using devices for everything from communicating with patients via email or text message to viewing test results or medical images to make a diagnosis.**
- **Patients are using devices to make and confirm appointments via text, and using apps to access their medical records and patient accounts.**
- **Many places where things can go wrong – challenging for even the most technologically advanced organization to implement the proper controls and safety protocols to protect patient data and adhere to federal privacy and security guidelines.**



# **HIPAA Privacy and Security Issues Related to Mobile Devices (cont'd)**

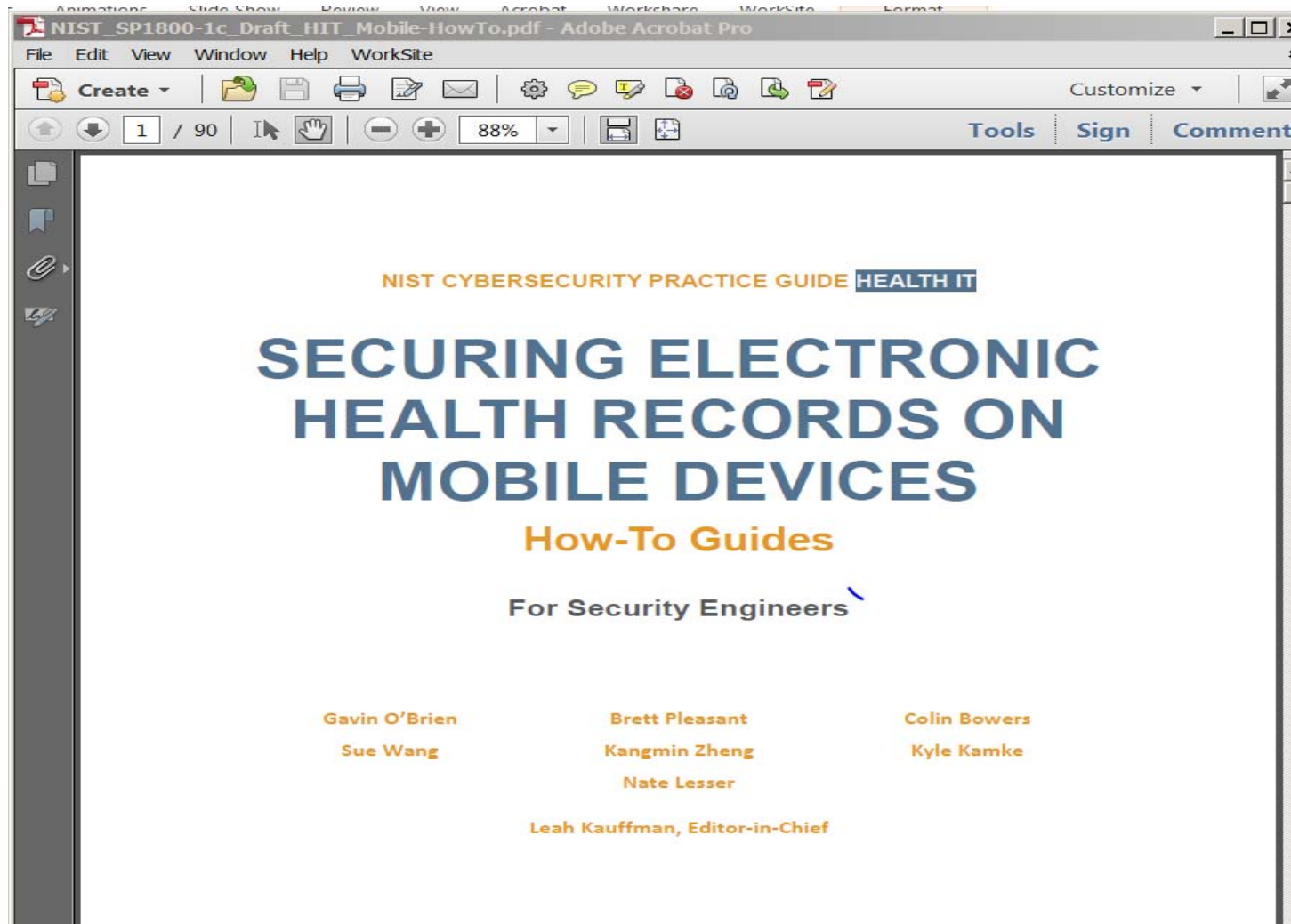
- **Risks unique to mobile devices**
  - **easy to lose, vulnerable to theft**
  - **exposure to electromagnetic interference – corrupts data**
  - **easier to be seen by others**
  - **not equipped with strong authentication and access controls**
  - **transmit and receive data wirelessly – susceptible to eavesdropping and interception**

# **Protect and Secure Health Information When Using a Mobile Device**

- **Use a password or other user authentication**
- **Install and enable encryption**
- **Install and activate remote wiping/remote disabling**
- **Develop an application policy – disable and do not install or use file sharing applications**
- **Install and enable a firewall**
- **Install and enable security software**
- **Keep your security software up to date**
- **Maintain physical control**
- **Use adequate security with Wi-Fi networks**
- **Delete all stored health info before discarding**

# NIST Cybersecurity Practice Guide

[https://nccoe.nist.gov/projects/use\\_cases/health\\_it/ehr\\_on\\_mobile\\_devices](https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices)



# Using Email and Texts to Transmit ePHI



# Using Email and Texts to Transmit ePHI

- Privacy Rule allows covered health care providers to communicate electronically, provided they apply reasonable safeguards when doing so. *See* 45 C.F.R. 164.530(c).
- Privacy Rule does not prohibit the use of unencrypted email for treatment-related communications.
- Precautions to avoid unintentional disclosures:
  - check email address for accuracy before sending
  - send an email alert to the patient for address confirmation prior to sending the message

# Using Email and Texts to Transmit ePHI (cont'd)

- The Security Rule does not prohibit communication via email or other electronic means, but it must be adequately protected.
- For information that contains ePHI, covered entities must do a risk analysis to determine the appropriate way to protect this information. Encryption is not required, but must be considered in the risk analysis.

# Using Email and Texts to Transmit ePHI (cont'd)

- Encryption is an addressable implementation standard. Thus, the covered entity or business associate must encrypt the ePHI if it determines that doing so is “reasonable and appropriate” and, if not, the covered entity or business associate must “(1) Document why it would not be reasonable and appropriate to [encrypt the data]; and (2) Implement an equivalent alternative measure if reasonable and appropriate.”
- Two options:
  - secure the transmission
  - warn the patient

# Using Email and Texts to Transmit ePHI (cont'd)

- **Best practice**
  - limit type of information disclosed through unencrypted email – don't include any highly sensitive information
  - do not use direct patient identifiers in the subject line or message content
  - ensure patient agrees in advance to being contacted by email or SMS, inform them of privacy issues, keep record of acceptance
  - educate patients and encourage them to protect their devices
  - include a disclaimer in patient privacy at the bottom of all communications



# Using Email and Texts to Transmit ePHI (cont'd)

- The HIPAA Privacy and Security Rules also apply to e-mails and texts to persons or entities other than patients.
- Unlike communications with patients, simply warning the third party that the communication may not be secure is not enough.
- Thus, although many providers do not think about it, they should generally *not* communicate ePHI with their staff or other providers via unencrypted email or text unless they have implemented appropriate safeguards consistent with Security Rule requirements.

# HealthIT.gov

Mobile Health Security: Mobile Health Device Privacy and Security | Providers & Professionals | - Windows Internet Explorer pro

http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

File Edit View Favorites Tools Help

Convert Select

Favorites HH Secure HIPAA (160) AHILA Lists AKS (2) AKS CMS home CMS Stark eCFR EMTALA guidelines Gmail HIPAA Hotmail Idaho Statutes IDAPA DHW IDSOS Search

Mobile Health Security: Mobile Health Device Pri...

Blog | Federal Advisory Committees (FACAs) | Contact | Get Email Updates

HealthIT.gov in Partnership with the National Learning Consortium

Newsroom | FAQs | Multimedia

Providers & Professionals | Patients & Families | Policy Researchers & Implementers

Benefits of EHRs | How to Implement EHRs | Privacy & Security | EHR Incentives & Certification | Success Stories & Case Studies | Resource Center

HealthIT.gov > For Providers & Professionals > Privacy & Security > Your Mobile Device and Health Information Privacy and Security

## Privacy & Security

Print | Share

## Your Mobile Device and Health Information Privacy and Security



Physicians, health care providers and other health care professionals are using smartphones, laptops and tablets in their work. The U.S. Department of Health and Human Services has gathered these tips and information to help you protect and secure health information patients entrust to you when

Worried About Using a Mobile Health Device for ...

### MOBILE DEVICE RISKS

- 1) Lost mobile device
- 2) Stolen mobile device
- 3) Downloaded virus

Done

Internet | Protected Mode: Off

# HIPAA Privacy and Security Issues Related to Medical Scribes



# What are Medical Scribes?

- **The Joint Commission defines a medical scribe as an unlicensed individual hired to enter information into the EHR or chart at the direction of a physician or licensed independent practitioner.**
- **The scribe industry has grown quickly since the HITECH Act.**
- **The American College of Medical Scribe Specialists predicts the number of scribes working in US will go from about 20,000 in 2015 to 100,000 by 2020.**
- **Ultimately, the chart is the responsibility of the provider, not the scribe – the provider must review the information entered by their scribes appropriately before signing off on patient documentation.**

# Joint Commission Guidelines

- In 2012, the Joint Commission released guidelines to help regulate the use of scribes. If an organization uses scribes, the Joint Commission expects to see:
  - A job description that recognizes the unlicensed status and clearly defines the qualifications and extent of the responsibilities (HR.01.02.01, HR.01.02.05).
  - Orientation and training specific to the organization and role (HR.01.04.01, HR.01.05.03).
  - Competency assessment and performance evaluations (HR.01.06.01, HR.01.07.01).
  - If the scribe is employed by the physician all non-employee HR standards also apply (HR.01.02.05 EP 7, HR.01.07.01 EP 5).

# Joint Commission Guidelines (cont'd)

- If the scribe is provided through a contract then the contract standard also applies (LD.04.03.09).
- Scribes must meet all information management, HIPAA, HITECH, confidentiality and patient rights standards as do other hospital personnel (IM.02.01.01, IM.02.01.03, IM.02.02.01, RI.01.01.01).
- Signing (including name and title), dating of all entries into the medical record-electronic or manual (RC.01.01.01 and RC.01.02.01). For those organizations that use Joint Commission accreditation for deemed status purposes, the timing of entries is also required. The role and signature of the scribe must be clearly identifiable and distinguishable from that of the physician or licensed independent practitioner or other staff.

# Joint Commission Guidelines (cont'd)

- The physician or practitioner must then authenticate the entry by signing, dating and timing (for deemed status purposes) it. The scribe cannot enter the date and time for the physician or practitioner. (RC.01.01.01 and RC.01.02.01).
- Although allowed in other situations, a physician or practitioner signature stamp is not permitted for use in the authentication of "scribed" entries-- the physician or practitioner must actually sign or authenticate through the clinical information system. (RC.01.02.01).
- The authentication must take place before the physician or practitioner and scribe leave the patient care area since other practitioners may be using the documentation to inform their decisions regarding care, treatment and services. (RC.01.02.01 and RC.01.03.01).

# Joint Commission Guidelines (cont'd)

- Authentication cannot be delegated to another physician or practitioner. The organization implements a performance improvement process to ensure that the scribe is not acting outside of his/her job description, that authentication is occurring as required and that no orders are being entered into the medical record by scribes. (RC.01.04.01).



# Other Payment Considerations Involving Scribes

- Third party payers may have specific guidelines for how a scribe documents and how the electronic signature must be applied. Each facility must contact their third party payers for any further requirements.
- When adding scribes to your practice, it is important to consult the MAC guidelines for your jurisdiction in order to develop CMS compliant scribe workflows and policies
- The use of a scribe may jeopardize ability to achieve meaningful use under the EHR incentive programs. To maintain eligibility for the EHR incentive payments, unlicensed scribes should not be permitted to enter orders into the EHR.

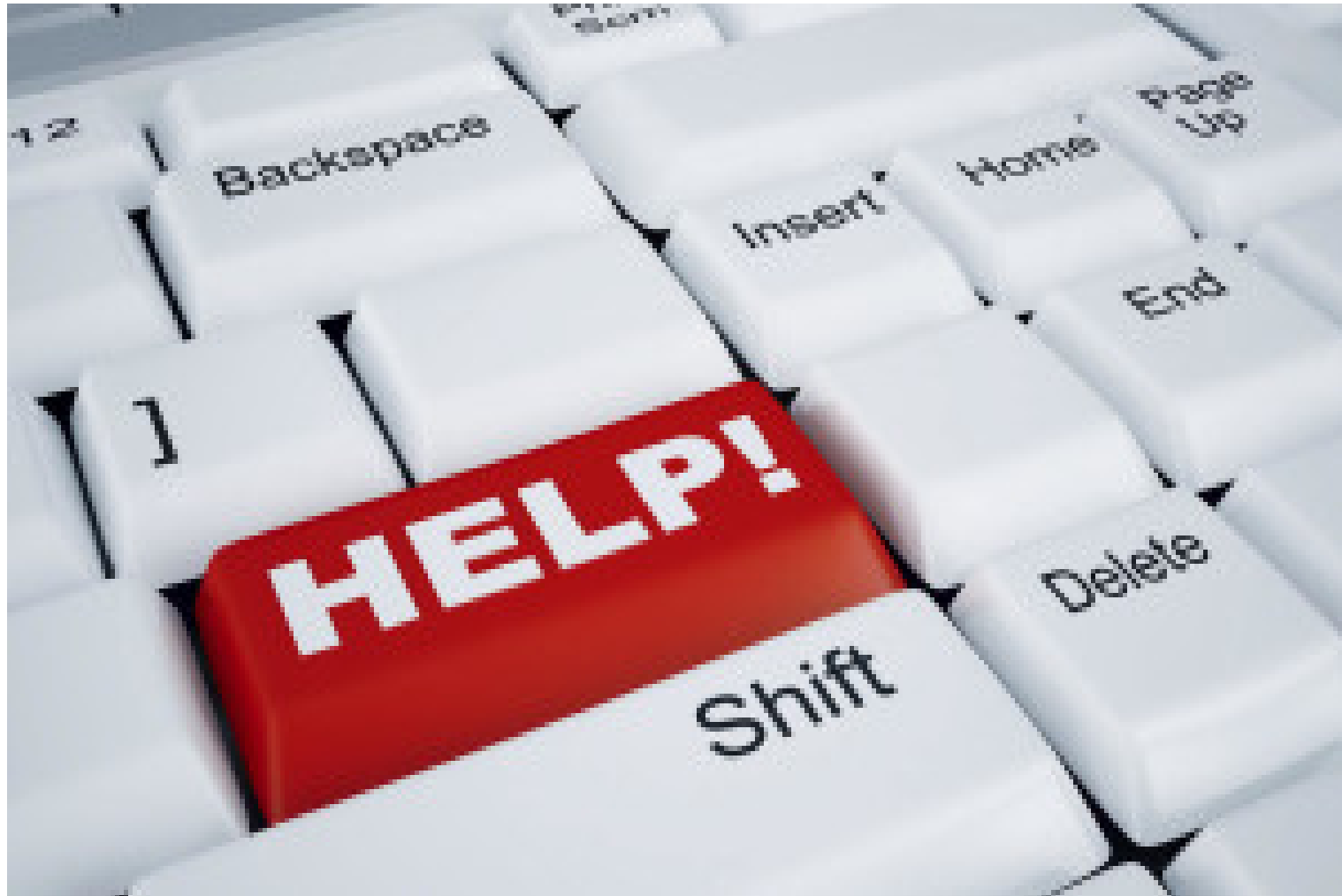
# **HIPAA Privacy and Security Issues Involving Scribes**

- **As with any employee or contractor who has access to patient records, a scribe must abide by HIPAA and HITECH regulations.**
- **The very nature of the scribe job description requires access to Protected Health Information (PHI) – scribes enter information into the patient’s record at the direction of a provider and retrieve patient information from various sources on behalf of the provider.**
- **It is imperative that HIPAA compliance is made a top priority during scribe training and continually monitored from a management perspective.**

# **HIPAA Privacy and Security Issues Involving Scribes (cont'd)**

- Each scribe must be issued a unique login or user identification with a secure password in order to gain access to any electronic system housing electronic PHI.
- Generic scribe logins or shared logins are not permissible, as unique identifiers are required in order to track each user's activity and system access in accordance with the HIPAA Security Rule.
- If an outside service is being used to supply the medical scribe, a business associate agreement must be signed prior to the use of the medical scribe.

# Additional Resources



# HealthIT.gov

Providers & Professional

healthit.gov/providers-professionals

Blog Federal Advisory Committees (FACAs) Contact Get Email Updates



in Partnership with the  
National Learning Consortium

Newsroom FAQs Multimedia Implementation Resources



Providers & Professionals

Patients & Families

Policy Researchers & Implementers

Benefits of EHRs

How to Implement EHRs

Privacy & Security

EHR Incentives & Certification

Success Stories & Case Studies

Resource Center

## What's in IT for you?

Learn about incentives for certification and find out how you can get paid for going paperless.

[Learn More >](#)



1 2 3 4 II

Print | Share

### Take the First Step Toward EHR Implementation

Whether you're just starting to think about adopting an electronic health record (EHR) system or are ready to make the change from paper records to EHRs, find out how to get started.

[Take the First Step >](#)

### Achieve Meaningful Use

Already have an EHR System? Learn about the meaningful use objectives that eligible professionals and hospitals must achieve to qualify for Centers for Medicare & Medicaid Services (CMS) Incentive Programs.

[Achieve Meaningful Use >](#)

### Get Local Technical Help

The EHR adoption process can be overwhelming. But you don't have to do it alone. The nationwide network of Regional Extension Centers (RECs) offers local, low-cost, on-the-ground support.

[Get Local Technical Help >](#)

# Holland & Hart Website

healthcare | Holland x  
https://www.hollandhart.com/healthcare

HOLLAND&HART

search this site

people

practices

firm

locations

news & resources

careers

diversity & inclusion

community

Contact  
Disclaimer  
Site Map

## Healthcare

### Overview

Holland & Hart provides a comprehensive health law practice to assist clients in navigating the dynamic healthcare industry. In recent years, healthcare has experienced dramatic change, extraordinary competition, and increasingly complex regulation. Our experienced attorneys and staff skillfully respond to these challenges. By remaining on the forefront of healthcare law, we are able to provide coordinated services to meet the business, transactional, litigation, and regulatory needs of our clients.

Our healthcare clients include hospitals, individual medical providers, medical groups, managed care organizations (MCOs), third-party administrators (TPAs), health information exchanges (HIEs), practice managers and administrators, independent practice associations (IPAs), owners of healthcare assets, imaging centers, ambulatory surgery centers, medical device and life science companies, rehabilitation centers, and extended and eldercare facilities. We have also assisted clients with the significant changes enacted by the Affordable Care Act, including advice regarding employer and health plan compliance, health insurance exchanges, accountable care organizations, and nonprofit cooperative health plans.

[+ Read More](#)

[+ Expand All](#)

### – Publications

#### HHS Issues New Rule Prohibiting Discrimination Based on Sex and Requiring Interpreters

*Holland & Hart News Update*  
Author(s): **Patricia Dean**

#### US District Court Decision Provides Cautionary Tale on False Claim Act Requirement to Return Identified Overpayments from Medicare or Medicaid

*Holland & Hart News Update*  
Author(s): **Patricia Dean**

#### Recruiting Physicians: Beware Stark, Anti-Kickback Statutes, and IRS Rules

View our [blog](#) and [webinar recordings](#) that cover HIPAA, antitrust, compliance, and more!



Contact



Kim C. Stanger

[View Profess](#)

- Related P
- [Business/ Litigation](#)
- [Compliance](#)
- [Audits, an](#)

HIPAA Resources

# Questions?

**Teresa D. Locke**

**Holland & Hart LLP**

**[tlocke@hollandhart.com](mailto:tlocke@hollandhart.com)**

**(303) 295-8480**

