The 411 on HIPAA and OCR Guidance

Wednesday, March 5th, 2014

The information provided in AHC Media Webinars does not, and is not intended to constitute medical or legal advice. Opinions, references and links provided by our speakers are provided for your convenience and do not represent our endorsement of such opinions, products or services.
Sue Dill Calloway RN, Esq. CPHRM, CCMSCCP

AD, BA, BSN, MSN, JD

President of Patient Safety and Education Consulting

Board Member
Emergency Medicine Patient Safety Foundation at www.empsf.org

614 791-1468

sdill1@columbus.rr.com
Learning Objectives

1. Explain the impact of new HIPPA regulations on hospital policies and procedures

2. Recall that all staff should be trained on new HIPAA requirements
You Don’t Want Headlines Like This

FOR IMMEDIATE RELEASE
July 11, 2013

WellPoint pays HHS $1.7 million for leaving information accessible over Internet

The managed care company WellPoint Inc. has agreed to pay the U.S. Department of Health and Human Services (HHS) $1.7 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

This case sends an important message to HIPAA-covered entities to take caution when implementing changes to their information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers’ health data using the Internet.

The HHS Office for Civil Rights (OCR) began its investigation following a breach report submitted by WellPoint as required by the Health Information Technology for Economic and Clinical Health, or HITECH Act. The HITECH Breach Notification Rule requires HIPAA-covered entities to notify HHS of a breach of unsecured protected health information.

The report indicated that security weaknesses in an online application database left the electronic protected health information (ePHI) of 612,402 individuals accessible to unauthorized individuals over the Internet.

OCR’s investigation indicated that WellPoint did not implement appropriate administrative and technical safeguards as required under the HIPAA Security Rule.

The investigation indicated WellPoint did not:

- adequately implement policies and procedures for authorizing access to the online application database
- perform an appropriate technical evaluation in response to a software upgrade to its information systems
- have technical safeguards in place to verify the person or entity seeking access to electronic protected health information maintained in its application database.

As a result, beginning on Oct. 23, 2009, until Mar. 7, 2010, the investigation indicated that WellPoint impermissibly disclosed the ePHI of 612,402 individuals by allowing access to the ePHI of such individuals maintained in the application database. This data included names, dates of birth, addresses, Social Security numbers, telephone numbers and health information.

Whether systems upgrades are conducted by covered entities or their business associates, HHS expects organizations to have in place reasonable and appropriate technical, administrative and physical safeguards to protect the confidentiality, integrity and availability of electronic protected health information – especially information that is accessible over the Internet.

Beginning Sept. 23, 2013, liability for many of HIPAA’s requirements will extend directly to business associates that receive or store protected health information, such as contractors and subcontractors.
ISU hands over $400K for HIPAA violation

Clinic disabled server firewall for nearly one year
POCATELLO, ID | May 23, 2013

Idaho State University will pay $400,000 to the U.S. Department of Health Human Services to settle alleged violations of the HIPAA Security Rule. The settlement comes after ISU’s Pocatello Family Medicine Clinic disabled server firewall protections for a period of at least 10 months, resulting in the breach of electronic protected health information for 17,500 patients.

Idaho State University, photo: Eric Kjaemperud, wikicommons

ISU operates 29 outpatient clinics and is required to provide health information technology systems security at those clinics. Between four and eight of the ISU clinics are subject to the HIPAA Privacy and Security Rules, including the clinic where the breach occurred, HHS officials say.

The HHS Office for Civil Rights opened an investigation in November 2011 after ISU’s August 2011 notification of the breach, which resulted from disabling of firewall protections at servers maintained by ISU. Over the course of the investigation, agency officials say it found that, for more than three years, ISU’s risk analyses and assessments of its clinics were incomplete and inadequately identified potential risks or vulnerabilities. ISU also failed to assess the likelihood of potential risks occurring.

[See also: Get set. New HIPAA has teeth.]

OCR concluded that ISU did not apply proper security measures and policies to address risks to ePHI and did not have procedures for routine review of its information system in place, which could have detected the firewall breach much sooner.

“Risk analysis, ongoing risk management, and routine information system reviews are the cornerstones of an effective HIPAA security compliance program,” said OCR Director Leon Rodriguez, in a May 21 press statement. “Proper security measures and policies help mitigate potential risk to patient information.”

ISU has agreed to a comprehensive corrective action plan to address the issues uncovered by the investigation and its failure to ensure uniform implementation of required HIPAA Security Rule protections at each of its covered clinics.

To date, OCR has collected $15.3 million relating to HIPAA violations and settlements.
2. Massive breach spawns class-action lawsuit against Advocate Medical Group

By Susan D. Hall

On top of federal and state investigations into its data breach, Advocate Medical Group in Downers Grove, Ill, faces a class-action lawsuit from affected patients.

The lawsuit claims the Chicago area’s largest physician group violated privacy regulations by failing to use encryption and other security practices, according to the Chicago Tribune.

Personal information for more than 4 million patients was compromised in the July theft of four computers. It’s the second-largest loss of unsecured health information reported to the Department of Health and Human Services since the agency made notification mandatory in 2009.

Though the computers were password protected, the information was not encrypted.

"Nothing leads us to believe the computers were taken for the information they contain, and there is no information to suggest any of that data has been used in an inappropriate way," Kelly Jo Golson, senior vice president and chief marketing officer for the nonprofit group, told the Tribune.

The records included names, addresses, dates of birth and Social Security numbers, but no full medical records. However, diagnoses, medical record numbers, medical service codes and health insurance information on patients seen between the early 1990s through July were among the data potentially exposed.

HHS and the Illinois attorney general are investigating the breach, one of at least 10 reported in the state this year, according to the Tribune.

Though most healthcare organizations understand the risks of a breach, including violating the Health Insurance Portability and Accountability Act, many nevertheless fail to take proper steps to prevent one, according to a Ponemon Institute report.

Many times organizations don’t fully grasp the need to do so until a breach occurs. And in the Ponemon survey, even among organizations that had been breached, 39 percent still had not put a data risk plan in place. It put healthcare organizations’ cost of responding to breaches at $6.78 billion annually.

Beth Israel Deaconess Medical Center CIO John Halamka recently described the risk audit process...
Introduction

- Referred to as the 563 Page Omnibus HIPAA Rule or the “Long Awaited Mega Rule”

- HHS’s Office of Civil Rights (OCR) published the final regulations on January 17, 2013

- The official notice was filed in the Federal Register (FR) on January 25, 2013
  

- Effective March 26, 2013 but compliance for covered entities (like a hospital) is Sept 23, 2013
  
  - Except grandfathered BAs which is Sept 23, 2014
FEDERAL REGISTER

Vol. 78                Friday,
No. 17                 January 25, 2013

Part II

Department of Health and Human Services

Office of the Secretary
45 CFR Parts 160 and 164
Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

Introduction

- Changes were made to the following four sections:
  - HIPAA Privacy rules
  - HIPAA Security rules
  - HITECH rule (Health Information Technology for Economic and Clinical Health)
  - GINA (Genetic Information Nondiscrimination Act of 2008)
Objectives

- Describe that hospitals will have to rewrite their Notice of Privacy Practices which is provided to patients.
- Recall that hospitals will have to rewrite their policies and procedures to comply with the HIPAA law.
- Discuss that hospitals will longer conduct a “harm analysis” to determine if the patient’s medical record information (PHI) has been breached and that a four part objective risk factor test must be used.
- Recall that staff should be trained on the new HIPAA requirements.
- Describe the four penalties that apply if one violates the new HIPAA law.
Agenda

- Overview of final rule
- Business Associations and BA Agreements
- Revised definition of breach
- Notification of breach
- Marketing
- Prohibitions on the Sale of PHI
- Enforcement
- Penalties
Agenda

- Immunization records
- Fundraising
- Revised Notice of Privacy Practices & samples
- Deceased Individual
- Request for restrictions
- Requests for access to PHI
- Genetic information
- Accounting of disclosures
Abbreviations Used in This Presentation

- CMS is the Center for Medicare and Medicaid Services
- HHS is Health and Human Services
- HIPAA is the Health Insurance Portability and Accountability Act
- HITECH is the Health Information Technology for Economic and Clinical Health
- HITECH was part of the stimulus bill initially called ARRA or the American Recovery and Reinvestment Act of 2009
Abbreviations Used in This Presentation

- PHI stands for protected health information
  - For example, a discharge summary, the face sheet, and history & physical, are medical records and are protected against unauthorized disclosure which are PHI

- GINA stands for the Genetic Information Nondiscrimination Act of 2008

- BA stands for Business Associates
  - The TJC surveyor is a BA or the hospital uses a company to do their transcription of H&Ps

- PSO is patient safety organizations

- HIO is a health information organization
Abbreviations Used in This Presentation

- **NPP** is the Notice of Privacy Practice
  - This is the document we give patients to explain to them how we use information about them

- **CE** stands for covered entity and a hospital and physician office is an example of a CE
  - Includes a health plan or healthcare provider that conducts certain transactions in electronic form

- **OCR** stands for the Office of Civil Rights

- **HP** is a health plan and includes insurance companies, HMOs, Medicare, and Medicaid
Omnibus HIPAA Rulemaking

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights announces a final rule that implements a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- Read the [HHS Press Release](https://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html)
- Read the Final Rule in the [Federal Register](https://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html)
OCR Lists Complaints Evaluated

Status of All Complaints
April 14, 2003 - February 28, 2013

Complaints Remaining Open (9%) 7,316
Complaints Resolved (91%) 71,555

Total Complaints Received 78,871

* Referrals to DOJ - 514

Status of All Complaints
Complaints Remaining Open 7316 9% of Total
Complaints Resolved 71555 91% of Total
Total Complaints Received 78871

* Referrals to DOJ - 514

Back to Top
Topics Discussed in the Final HIPAA Rule

- A major revision to the definition of breach which will result in notifying more patients
  - The new risk assessment standard replaces the harm standard and is a four part test
- Changes to the Notice of Privacy Practices document we give patients about how we use information about them
- New restrictions to the sale of PHI (protected health information) with a patient authorization
  - Adopted the changes in the proposed rule and further clarifies what is the sale of PHI and remuneration
Topics Discussed in the Final HIPAA Rule

- Changes a number of definitions including marketing, health care operations (HCO), breach, and business associates

- New rules for research authorization

- New rules for the protection of genetic information and its use by a health plan
  - Adopts almost all of the changes of the proposed rule and adds requirements for underwriting under GINA

- Adopts a number of the sections in the proposed rule on enforcement actions and penalties
Topics Discussed in the Final HIPAA Rule

- Changes to *fundraising* opt-out and disclosures for fundraising
- New provisions for *business associates* and subcontractors—now directly liable for compliance with certain privacy and security rules
- Allows disclosure of *immunization records* to a school when required by state law
- Changes to the rules on the *use and disclosure* of PHI and request for *restrictions*
- *Deceased patients* PHI is protected for 50 years and adopts proposed rule changes
What Was Not Addressed in the Final Rule

- Accounting of Disclosures
  - Patient has the right to ask for an accounting of all disclosure made on them
  - Example, reporting related to communicable disease, cancer registry, court order for medical records, records reviewed after subpoena from state medical board etc.
  - No accounting if released pursuant to HIPAA compliant authorization or for treatment, payment or healthcare operations
What Was Not Addressed in the Final Rule

- The Penalty Distribution Methodology
  - The final rules has four categories of penalties which will be discussed later
  - The final rule said that the penalty distribution methodology under the HITECH act will be the subject of future rulemaking
  - So watch for new changes in the future
Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement

What is the HIPAA Privacy Rule?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule provides Federal privacy protections for individually identifiable health information, called protected health information or PHI, held by most health care providers and health plans and their business associates. The HIPAA Privacy Rule sets out how and with whom PHI may be shared. The Privacy Rule also gives individuals certain rights regarding their health information, such as the rights to access or request corrections to their information.

Who must comply with the HIPAA Privacy Rule?

HIPAA applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically (e.g., billing a health plan), and others, hired by covered entities to perform services or functions that involve access to PHI.

Who is not required to comply with the HIPAA Privacy Rule?

Many entities that may have health information are not subject to the HIPAA Privacy Rule, including:

- employers,
- most state and local police or other law enforcement agencies,
- many state agencies like child protective services, and
- most schools and school districts.

While schools and school districts maintain student health records, these records are in most cases protected by the Family Educational Rights and Privacy Act (FERPA) and not HIPAA. HIPAA may apply however to patient records at a university hospital or to the health records of non-students.
First we had the HIPAA law (statute) called the Health Insurance Portability and Accountability Act of 1996 effective 8-21-1996

Final regulations on privacy were published December 2000 and modified August 14, 2002

- Privacy rules effective April 14, 2003
- Security rules were effective April 20, 2005
- HITECH interim final rules issued August 24, 2009 and effective September 23, 2009

www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf
HIPAA Privacy Rules

Thursday, December 28, 2000

www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf

Part II

Department of Health and Human Services
Office of the Secretary

45 CFR Parts 160 and 164
Standards for Privacy of Individually Identifiable Health Information; Final Rule
Privacy Rule History

The Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164.

Click here to view the combined regulation text of all HIPAA Administrative Simplification Regulations found at 160, 162, and 164.

Privacy Rule History

- August 14, 2002 - Modifications to the HIPAA Privacy Rule - Final Rule (PDF)
- March 27, 2002 - Modifications to the HIPAA Privacy Rule - Proposed Rule (PDF)
- February 28, 2001 - Request for Comments on December 28, 2000, Final HIPAA Privacy Rule (PDF)
- February 26, 2001 - Correction of Effective and Compliance Dates of the Final HIPAA Privacy Rule (PDF)
- December 29, 2000 - Technical Corrections to the Final HIPAA Privacy Rule (PDF)
- December 28, 2000 - HIPAA Privacy Rule - Final Rule (PDF)
- November 3, 1999 - HIPAA Privacy Rule - Proposed Rule (PDF)

Learn more about the Rulemaking History of the HIPAA Enforcement Rule at 45 CFR Part 160, Subparts C, D, and E.
Interim Breach Notification Rules

Monday,
August 24, 2009


Part II

Department of Health and Human Services

45 CFR Parts 160 and 164
Breach Notification for Unsecured Protected Health Information; Interim Final Rule
**Breach Notification History**

**Health Information Privacy**

**Office for Civil Rights** | **Civil Rights** | **Health Information Privacy**

---

**Breach Notification Rule**

Interim final breach notification regulations, issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act by requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

**Breach Notification Regulation History**


---

**Definition of Breach**

**Unsecured Protected Health Information and Guidance**

**Breach Notification Requirements**

**Burden of Proof**

**Instructions for Covered Entities to Submit Breach Notifications to the Secretary**

---

The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings. The HIPAA Enforcement Rule is codified at 45 CFR Part 160, Subparts C, D, and E.

Enforcement Rule History

- **October 29, 2009** - HITECH Act Enforcement Interim Final Rule
- **February 16, 2006** - HIPAA Enforcement Rule - Final Rule (PDF)
- **September 14, 2005** - Extension of Expiration Date of Interim Final Rule (PDF)
- **April 18, 2005** - HIPAA Enforcement Rule - Proposed Rule (PDF)
- **September 15, 2004** - Extension of Expiration Date of Interim Final Rule (PDF)
- **April 28, 2003** - Correction of Expiration Date of Interim Final Rule (PDF)
- **April 17, 2003** - Procedures for Investigations, Imposition of Penalties, and Hearings-Interim Final Rule (PDF)
History

- The Stimulus Bill Amended HIPAA and made substantial changes to the privacy and security laws
  - The American Recovery and Reinvestment Act of 2009 created interim final rules for HITECH (Health Information Technology for Economic and Clinical Health)
  - When do we need to notify the patient if there has been a breach of their PHI?
- Now we have major changes to HIPAA privacy, GINA, security enforcement and the breach notification rules
Department of Health and Human Services
Office of the Secretary
45 CFR Parts 160 and 164
Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule
CMS Privacy & Confidentiality Memo

- CMS issues memo to hospitals regarding HIPAA on March 2, 2012 which hospitals should be aware
- Discusses privacy & confidentiality consistent with HIPAA
- Discusses incidental uses and disclosures
- Combines tag 441, 442, and 442 and amends 143 and 147 in the hospital CoP manual
  - Allows name on spine of chart
  - Allows name on outside of patient room
  - Allows signs such as fall risk or diabetic diet
DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C2-21-16
Baltimore, Maryland 21244-1850

Office of Clinical Standards and Quality/Survey & Certification Group

DATE: March 2, 2012
TO: State Survey Agency Directors
FROM: Director Survey and Certification Group
SUBJECT: Hospital Patient Privacy and Medical Record Confidentiality

Memorandum Summary

- **Hospital Patient Privacy and Medical Record Confidentiality**: Guidance concerning the protection of patient privacy and medical record information is clarified. This guidance is consistent with the standards under the Federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.
- **Incidental Uses and Disclosures**: Guidance concerning permitted incidental uses and disclosures is clarified and includes reasonable safeguards that must be in place to ensure patient privacy.
- **Automated Survey Processing Environment (ASPEN) Changes**: Tags A-0441, A-0442, and A-0443 have been combined. It will take time for this guidance to be incorporated into a future ASPEN release. Prior to this conversion citations should be made only to Tag A-0441.

Patient Rights to Privacy and Medical Record Confidentiality

We are taking this opportunity to clarify our guidance for the hospital requirements governing patient privacy and medical record confidentiality at 42 CFR §482.13(c)(1), §482.13(d)(1) and §482.24(b)(3).
Person not involved with care may not be present while exam is being done unless consent required (medical students who are observing not those caring for patient)

Information in directory may not be disclosed without informing patient in advance
  - Visitor must ask for the patient by name

Can use information for payment and healthcare operation

Must have P&P that restrict access to MR to those who need to know such as nurse who takes care of patient
Personal Privacy & Confidentiality

- Discusses incidental uses and disclosures
  - Whiteboards that list patient present in OR or PACU
  - No medical diagnosis or other information should be on the whiteboard

- Take reasonable safeguards
  - Ask waiting patients to stand back a few feet from a counter used for patient registration
  - Speak quietly if patient in semi-private room
  - Passwords on computers
  - Consent if patient is in room with camera
Financial Penalties and Enforcement
Financial Penalties and Enforcement

- The final rule retains the four tiered levels of fines
- Enforcement of HIPAA was increased in the HITECH act
- Final rule made changes to the enforcement provisions
- Secretary HHS can impose a fine (civil money penalty) for a violation including a penalty against a BA
- Good news is that HHS does not have to impose the maximum penalty if she doesn’t want to
## Financial Penalties (Civil Monetary Penalties)

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Penalty Range for Each Violation</th>
<th>Maximum Penalty for all Violations of an Identical Provision in a Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity did not know (and, by exercising reasonable diligence, would not have known) that it violated the applicable provision.</td>
<td>$100 to $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Violation is due to reasonable cause and not to willful neglect.</td>
<td>$1,000 to $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Violation is due to willful neglect and was corrected during the 30-day period beginning on the first date the entity knew, or, by exercising reasonable diligence, would have known that the violation occurred.</td>
<td>$10,000 to $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Violation is due to willful neglect and was not corrected during the 30-day period beginning on the first date the entity knew, or, by exercising reasonable diligence, would have known that the violation occurred.</td>
<td>At least $50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Financial Penalties and Enforcement

- Determined on a case by case basis
- Will evaluate a number of factors
- Will look to see if any history of non compliance even if no formal finding of a violation
- What was the nature and extent of the resulting harm (diagnosis disclosed, SSN, patient name, address, H&P, EKG results, etc.)
- Will look at the financial situation of the entity
- Did not know, reasonable cause, corrected the willful neglect or didn’t correct the willful neglect
Financial Penalties and Enforcement

- An example of willful neglect is the case of a bank who called the local hospital on seven different occasions to let them know they had the wrong fax number and they kept getting discharge summaries and H&Ps of patients.
  - Hospital did not do anything until the bank notified the local newspaper who ran an article on the willful neglect of the hospital.

- Factors can be mitigating (the good) or aggravating (the bad and the ugly).
Financial Penalties and Enforcement

- OCR is required to investigate hospital (CE) or BA if the preliminary investigation indicates a possible violation due to willful neglect (no longer discretionary)

- OCR is allowed, but not required, to resolve investigations by informal means

- OCR can proceed directly to financial penalties without exhausting informal resolutions especially if it involves willful neglect

- Others factors as justice may require
Financial Penalties and Enforcement

- Was there a neglect on the part of the hospital, physician office, HHA, or CE to conduct a security risk assessment?

- Does the institution have a privacy and security officer and did they implement HIPAA compliant P&P?

- First settlement involving a security breach of less than 500 patients occurred in January of 2013 against the Hospice of North Idaho:
  - Settlement of 50,000 related to unencrypted laptop
  - They had never done a risk analysis to safeguard ePHI
  - No P&P to discuss mobile device security
Financial Penalties and Enforcement

- Affirmative defense (a set of facts which is presented to diminish the charge or claim)
  - The final rule made changes
  - OCR can not fine you if violation is corrected within 30 days of when the hospital knows about it or has constructive knowledge of the violation
    - Except for willful neglect
    - So correct the problem immediately
- A civil penalty will also not be applied if a criminal penalty has already been imposed
Financial Penalties and Enforcement

- Business Associate (BA) liability
  - BAs are directly subject to enforcement under interim final rules February 17, 2010
  - BAs are directly liable for compliance with certain of the HIPAA privacy and security regulations
  - OCR has direct enforcement authority with regard to BAs and subcontractors
    - Example is the hospital has a BA that transcribes their medical records and the BA is backed up and hires another transcription company (a subcontractor of the BA) to help catch them up
Financial Penalties and Enforcement

- CEs (hospitals, physicians) and BAs can be vicariously liable for their BAs who are their agents under federal agency law (downstream)
  - BA must be an agent of the hospital or CE and acting within the scope of agency
  - This is troublesome for hospitals and hospitals may need some oversight of BAs so consider this before entering into a relationship with a BA
  - Hospitals will want to consider an indemnification clause so the hospital or CE will be reimbursed
Financial Penalties and Enforcement

- Calling someone a “independent contractor” is not determinative of whether it is an agency relationship or not

- Whether the BA is an agent of the hospital or CE will be a fact specific determination

- Factors to determine if an agency relationship exists
  - Time, place and purpose of BAs conduct
  - Was the BAs conduct subject to the control of the hospital
  - Whether the BAs conduct is commonly done by a BA to accomplish the services performed on behalf of the CE or other BA
  - Would hospital or CE reasonable expect that BA would engage in the conduct question
Who are the HIPAA Police?

- The primary enforcer is the Office of Civil Rights
- The state attorney general can also enforce
- The prosecutor has filed criminal charges in the past for a HIPAA violation
- OIG, DOJ, or FTC
- A hospital that accepts Medicare or Medicaid reimbursement can be cited by CMS under the hospital conditions of participation (CoPs)
- An accreditation organization for violation of its privacy and confidentiality provisions: TJC, AOA Healthcare Facility Accreditation Program, DNV Healthcare or CIHQ
Notice of Privacy Practice
Hospitals and other CE will have to update their NPP

The NPP discusses how information about the patient may be used and disclosed

We have a good faith effort to obtain written acknowledgment that they have received it

Remember an inmate does not have a right to a NPP

New regulations require additions to the NPP
Sample Notice of Privacy Practice

JOINT NOTICE OF PRIVACY PRACTICES

Effective Date:   April 14, 2003
Last Revision Date: None

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice serves as a joint notice for Barnes-Jewish Hospital, St. Louis Children’s Hospital and Washington University School of Medicine (collectively referred to herein as “we” or “our”). We have designated ourselves as an organized health care arrangement under the Health Insurance Portability and Accountability Act of 1996. We will follow the terms of this Notice and may share health information with each other for purposes of treatment, payment and health care operations as described in this Notice. Since we maintain health information separately, we will respond separately to your questions, requests and complaints concerning your health information.

OUR DUTIES REGARDING YOUR HEALTH INFORMATION

We respect the confidentiality of your health information and recognize that information about your health is personal. We are committed to protecting your health information and to informing you of your rights regarding such information. We are also required by law to protect the privacy of your protected health information and to provide you with notice of these legal duties. This Notice explains how, when and why we typically use and disclose health information and your privacy rights regarding your health information. In our Notice, we refer to our uses and disclosures of health information as our “Privacy Practices.” Protected health information generally includes information that we create or receive that identifies you and your past, present or future health status or care or the provision of or payment for that health care. We are obligated to abide by these Privacy Practices as of the effective date listed above.
www.hhs.gov/ocr/privacy/hipaa/model_notices.html
| Help with public health and safety issues | We can share health information about you for certain situations such as:  
|  | • Preventing disease  
|  | • Helping with product recalls  
|  | • Reporting adverse reactions to medications  
|  | • Reporting suspected abuse, neglect, or domestic violence  
|  | • Preventing or reducing a serious threat to anyone’s health or safety |

| Do research | We can use or share your information for health research. |

| Comply with the law | We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we’re complying with federal privacy law. |

| Respond to organ and tissue donation requests | We can share health information about you with organ procurement organizations. |

| Work with a medical examiner or funeral director | We can share health information with a coroner, medical examiner, or funeral director when an individual dies. |

| Address workers’ compensation, law enforcement, and other government requests | We can use or share health information about you:  
|  | • For workers’ compensation claims  
|  | • For law enforcement purposes or with a law enforcement official  
|  | • With health oversight agencies for activities authorized by law  
|  | • For special government functions such as military, national security, and presidential protective services |

| Respond to lawsuits and legal actions | We can share health information about you in response to a court or administrative order, or in response to a subpoena |
Notice of Privacy Practices NPP

- To include a description of the types of uses and disclosures that require an authorization

- A statement that if the hospital or CE wants to engage in any of the following, there must be a separate authorization
  - Uses and disclosures for marketing
  - Uses and disclosures that constitute the sale of PHI
  - Uses and disclosure of psychotherapy notes unless you do not maintain these
  - Other uses and disclosures not described in the notice will be made only with an authorization from the patient
A statement regarding the patient’s right to notice in the event of a breach of their unsecured PHI

Hospitals and other healthcare providers need to include a statement so patients will be aware they can restrict PHI to their health plan if they pay for the service

- Patient has Chlamydia and gonorrhea and does not want the hospital to tell their insurance company so if they pay the bill themselves we must abide by their request
Notice of Privacy Practices NPP

- May not use or disclose PHI unless the NPP includes a statement that with each fundraising communication the patient can opt out and not receive any further fundraising communication.

- Health plan (insurance company) must include they can not use or disclose genetic information for underwriting except for LTC plan.

- Hospital and providers must:
  - Give a copy of the revised NPP to new patients.
  - Make the revised NPP available to patients on request.
  - Post the NPP on their website if they have one.
Changes to the Breach Notification Rule

HITECH
Breach Notification

- The interim final rules (IFR) were adopted under HITECH and became effective September 23, 2009.
- We have waited four years for the final rules which are effective September 23, 2013.
- The change from the “risk of harm” to a “presumption of a breach” will most likely have the result that in more communications to patients that their PHI has been breached.
- OCR felt risk of harm standard was not applied correctly.
  - 70 comments and only 10 wanted it changed.
Breach Notification Rule

Interim final breach notification regulations, issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act by requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

- Breach Notification Regulation History
- Definition of Breach
- Unsecured Protected Health Information and Guidance
- Breach Notification Requirements
- Burden of Proof
- Instructions for Covered Entities to Submit Breach Notifications to the Secretary
Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

**Full DataSet** [CSV format (18 KB)] [XML format (57 KB)]

Select a column head to sort by that column. Select again to reverse the sort order. Select an individual record to display it in full below the table.

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Individuals Affected</th>
<th>Date of Breach</th>
<th>Type of Breach</th>
<th>Location of Breached</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st response Medical Transp Corp.</td>
<td>MD</td>
<td>582</td>
<td>06/15/2012-10/01/2012</td>
<td>Unauthorized Access/Disclosure</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>ABQ HealthPartners</td>
<td>NM</td>
<td>778</td>
<td>2012-12-20</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Accenda</td>
<td>AZ</td>
<td>175,350</td>
<td>2011-01-01</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper</td>
</tr>
</tbody>
</table>

OCR Home > Health Information Privacy > HIPAA Administrative Simplification Statute and Rules > Breach Notification Rule
Breach Notification

- Hospitals and other CEs will need to update their policies and procedures to reflect these new changes.
- Hospital and other CEs will need to educate their staff and physicians and LIPs on this.
- Hospitals are well advised to make sure all laptops are encrypted.
  - If one stolen still need to do a risk assessment to be sure the PHI was not breached.
- Don’t forget about any state breach notification rules.
Definition of Breach

- It is now a four part objective risk factor test – low probability analysis

- The old definition of breach (risk of harm) in the IFR was defined as follows

  - Breach means the acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Privacy Standards which compromises the security or privacy of PHI...that poses a significant risk of financial, reputational, or other harm to the individual

- OCR removed the risk of harm
Definition of Breach

- We have the **burden** to prove the unauthorized disclosure is not a breach.

- If OCR investigates we have to prove conclusive documentation of the risk assessment and analysis as to why the incident did not result in a compromise of PHI.

- If we don’t meet that burden then the hospital may been found negligent in not notifying the patient and could be subject to fines, penalties and corrective actions.
Breach Notification

- The old definition required a significant risk of financial, reputational, or other harm to the individual.

- The new rule has a much lower standard of PHI disclosure or use that does not have a low probability that the PHI has been compromised.

- We need to evaluate the potential breach of PHI and document our good faith evaluation and reasonable conclusion using the 4 part test:
  - If you determine that the probability of compromised PHI is low you do not have a problem, if yes then patient must be notified.

- Will most likely result in notifying more patients that the PHI has been breached.
Low Probability Objective Risk Factors

- A breach is presumed unless the hospital or CE can show that there is a “low probability” that the PHI has been compromised based on the risk assessment considering the following four;

1. The nature and extent of the PHI involved including the types of identifiers and likelihood of reidentification
   - Was it sensitive information such as a STD such as gonorrhea or HIV status or treatment for substance abuse or mental health treatment
   - Was it just the name of the patient, or did it include their diagnosis, SSN or credit card information or just how much information was disclosed
Low Probability Objective Risk Factors

- 1. The nature and extent of the PHI involved including the types of identifiers and likelihood of reidentification (continued)
  - Was it a list of deidentified list of cancer diagnosis of patients seen in an outpatient department disclosed with a separate list of patient appointments for the day the patient was treated would present a higher probability of impermissible use or disclosure
  - PHI that had scanned images may include patient identifiers that would present a higher probability of disclosure.
Low Probability Objective Risk Factors

2. Whether the PHI was actually acquired or viewed
   - Was there an opportunity to view or access the PHI
   - PHI information sent to the wrong patient but the letter was returned unopened by the post office so good chance it was never viewed
   - Patient is handed the wrong discharge instructions but nurse notices it before going over them with patient and retrieves them
   - The laptop was stolen and a forensic analysis shows that none of the PHI was accesses
Low Probability Objective Risk Factors

3. The unauthorized person who used the PHI or to whom the disclosure was made

- You have to evaluate the recipient of the impermissible disclosure
  - Was the person who received the unauthorized information a physician or another hospital who generally has a duty to protect PHI?
  - A impermissible disclosure to a party who has been trained in HIPAA and who works for the hospital or a BA may present a lower probability than disclosing it someone who has not been trained
4. The extent to which the risk to the PHI has been mitigated

- Were there any mitigating issues that lead you in good faith and reasonable conclusion that the information was not disclosed?

- Get assurance and confidential agreement from the person that the PHI has been shredded and assurances no copies have been made.

- Is the person who received the PHI a physician or healthcare professional?

- Can we rely on the promise of the party to whom the information was improperly disclosed?
Document the Risk Assessment

- It is important to thoroughly document the risk assessment.
- This is especially important if there is a finding that there was a low probability that the PHI was compromised.
- Hospitals can just skip the assessment and notify the patient that their PHI was breached.
- Be sure to notify timely:
  - Breaches over 500 are made immediately to OCR.
  - Send written notice to media and keep a copy-no requirement they must publish it and do not have pay to publish.
Three Exceptions to the Definition of Breach

There are three exceptions to the definition of breach that Congress intended not to be breaches and these were retained:

1. Unintentional access or use by employee or individual acting under authority of CE or BA (includes similarly situated individuals) and in good faith and does not result in further use

   – Nurse has a patient in the emergency department and he doesn’t know his medication.

   – She goes to the computer and looks up the patient’s records “Clinton Curtis Calloway” and then discovers that the patient has the same name as his father

   – She has accessed the wrong one by mistake and logs off
Three Exceptions to the Definition of Breach

2. Unintentional access, disclosure, or use of information by employee or person acting under the authority of the CE or BA
   - Medical Records employee drops off records of Mary Smith to ICU instead of CCU
   - Nurse tells clerk “wrong chart” and she takes the records back

3. Unauthorized disclosure to one unable to retain such information
   - Patient handed wrong discharge instructions and nurse retrieves before she can see of example of returned mail
Limited Data Sets (LDS)

- LDS is PHI that excludes direct identifiers such as patient name, address, fax number, SSN, MR number, health plan number, photo, etc.

- The final rule eliminated the exception for unauthorized use or disclosure of data that excludes the 16 LDS direct identifiers, date of birth and zip code.

- The final rule will require the hospital or CE to do a breach risk assessment if a limited data set is used or disclosed in an impermissible manner even if the limited data set excludes the zip codes or birth date.
If PHI is Breached (Not New)

- Patient is to be notified of breach timely and never later than 60 days after discovery of the breach
  - The breach is discovered on the first day the breach is known or should have been known to any employee other than the person who committed the breach
  - Contains the information to be included in the breach
  - Include toll free number and web site
  - If breach less than 500 then complete a log and send in annual report
  - If police ask to delay notification can do if oral request for 30 days or in writing for the time specified by the official
Please Remember

- Remember to encrypt all lap tops
- Portable devices are a great privacy and security vulnerability
- Not just lap tops but tablets and smart phones have been the culprit in a large number of recent high profile breaches
- Do a mobile device risk analysis and design, install, and monitor your P&Ps
- Design a mobile device HIPAA plan so you don’t end up notifying patients of breaches later on
19 Unique Identifiers

- In the past, when hospital had to report a breach, there was no requirement to include which identifiers were associated with it.

- Even though these were evaluated during the risk assessment especially SSN or MR number.

- Now new rule requires that the unique identifiers must be included with each risk assessment.

- The identifiers are consistent with the ones published in the original HIPAA rule.

- Includes name, email address, SSN, telephone number,
19 Unique Identifiers

- All ages over 90 or dates indicating age
- Fax number, MR number, account numbers
- Health plan number, certificate or license number
- Vehicle identification number or serial number including license plate number
- Internet IP address, device identification or serial number, URLs, biometric devises, full face picture
- All geographic subdivisions smaller than a state (street address, city, county, precinct) (Note: ZIP code must be removed, but can retain first 3 digits if the geographic unit to which the zip code applies contains more than 20,000 people)
- For dates directly related to the individual, all elements of dates, except year (i.e., DOB, admission date, discharge date, DOD)
Access to PHI
Right to an Electronic Copy
Patient Access to PHI

- A patient has a right of access to their medical record information
- The patient can come to the hospital and inspect their PHI
- Patients can ask for a copy of their PHI
- The final rule made significant changes to this section
- Patient can ask for an electronic copy if the format is readily producible
  - Patient asks for it on a CD or a flashdrive
Patient Access to PHI

- Patient signs a HIPAA compliant authorization form
- If you have ePHI you can not just offer them a hard copy
  - Exception: If all of your medical records are in paper and you have no electronic medical records then you can offer a paper copy
  - If the patient rejects all of the offers of the electronic format then you can give a hard copy
- If not available in that format then a copy of the in at least one readable electronic form
- The hospital or CE does not have to go out and purchase software or hardware to accommodate various request
  - Patient asks for a copy in word but the hospital can provide a PDF copy
Authorization for the Use or Disclosure of Protected Health Information

I authorize the use and/or disclosure of my protected health information as described below:

1. My authorization applies to the information described below. Only this protected health information may be used and/or disclosed pursuant to this authorization: ____________________________________________
   ____________________________________________
   ____________________________________________

2. I authorize the following persons (and or class of persons) to make the authorized use and/or disclosure of the specified protected health information: ____________________________________________
   ____________________________________________
   ____________________________________________

3. I authorize the following persons (or class of persons) to receive my protected health information: ____________________________________________
   ____________________________________________

4. This authorization expires upon ________________________________ (insert date or event triggering expiration).

5. I understand that once my protected health information is used and/or disclosed pursuant to this authorization, it may no longer be protected by the privacy regulations and may be subject to re-disclosure by the recipient(s).

6. I understand that I have a right to revoke this authorization at any time. My revocation must be in writing as described in the Notice of Privacy. I am aware that my revocation is not effective to the extent that I have authorized the use and/or disclosure of my protected health information and such use and/or disclosure has been relied upon by authorized recipients. I also understand
Patient Access to PHI

- Patient can request copy to go to them or can have hospital send to someone else
  - Authorization must clearly identify the individual and where to send the record
- Electronic copy must include all electronic PHI held by the hospital or CE unless only specific information is requested
  - Patient does not want an entire copy of their records but only the discharge summary or H&P
Patient Access to PHI

- If available in mixed media where some of the medical records are paper and other electronic, can provide a combination

- If patient wants emailed to them and it is not unencrypted can still do this as long as hospital or CE advises the patient of the risk that it could be read by a third party

- If patient gives you a flash drive or CD or other device and hospital has security concerns about plugging in the external portable media may refuse to use the patient’s devices
  - May not be able to charge them if you use a hospital flash drive or device
Patient Access to PHI

- The hospital or CE can charge for a copy of the PHI
  - Must be reasonable cost-based fees and can’t include the cost of new technology
- Costs may not include a retrieval fee
- Cost based fees can include:
  - Labor costs for copying
  - Cost of supplies such as flash drives or discs
  - Postage if patient asks for it to be mailed
Patient Access to PHI

- States could implement a lower cost but not higher costs since federal regulation and preemption doctrine
- Final rule reduced the total time to get patients a timely copy of their records
- Removed from 90 to 60 days by removing provision allowing an extra 30 days if PHI not maintained on site
- Hospital has 30 days to get PHI with one time extension up to 30 days including reason for delay and expected date of completion
  - State law can be more stringent if they want
Marketing, Fundraising, and the Sale of PHI
Marketing

- Marketing is defined as:
  - A communication about a product or service that encourages recipients of the communication to purchase or use the product.

- Many new changes in the regulations:
  - Final rule implements the HITECH restrictions on the use of PHI for marketing and adds more restrictions.

- The general rule is that if it meets the definition of marketing and the hospital gets payment from a third party you need an authorization:
  - Unless it meets one of the exceptions to the rule.
  - Authorization must mention hospital has been paid.
Marketing

- Hospital will have to rewrite their policies and procedures to conform to the new regulations
- Hospitals should train staff
- Remember the fraud and abuse laws still apply
- Identify any arrangements in existence that may need to be terminated or amended to comply with the new marketing restrictions
- Remember the marketing regulations as hospitals and other CEs enter into new agreements when they receive payment from third parties for refill reminders, or other communications to patients to purchase or use a product or service
Marketing

- An authorization for marketing will not be needed if;
  - There is a **face to face** communication
    - Such as the patient is in the room with the provider talking to them
    - Talking to the patient on the phone is not a face to face communication and neither is email
    - A face to face communication is allowed even if the hospital or CE receives payment
Marketing

- An authorization for marketing will not be needed if:
  - A *promotional gift* of nominal value provided by the hospital
    - The hospital gives the patient a pen with the hospital’s name on it
    - A patient is given a free mug, or calendar
    - The hospital gives patients a blanket with the hospital name on it
Marketing Exceptions

- There are four exceptions to the rule that you need an authorization for marketing:
  
  1. A refill reminder or other communication about a drug or biologic that is currently prescribed to the patient
     - As long as the hospital or CE doesn’t get financial remuneration for it
     - Hospital can get the actual cost reimbursed (no profit) of sending it out by the drug company such as labor or postage
     - A generic pharmacy company may pay a pharmacy a cost based fee to encourage patients to switch to a genetic drug to save the patient money
     - Communications to remind the newly diagnosed patient with CHF to take their medication to prevent unnecessary readmissions
Marketing Exceptions

2. A communication about the hospital or CE’s own health related products and services as long as the hospital does not receive financial remuneration

- Hospital sends patients information about their new mammogram screening center or women’s health center
- The hospital is opening up a new OB unit
- The hospital has expanded their ED area and added a new urgent care center
3. The hospital or CE can contact the patient for case management or care coordination regarding alternative treatments, therapies, health care providers and related functions

- Discharge planning nurses call all patients who have been discharged from the hospital to reinforce their discharge instructions to prevent unnecessary readmissions

- The anesthesiologist calls the patient at home who had anesthesia yesterday to complete the post-anesthesia assessment within the 48 hours time frame

- The ED nurse calls the patient to let them know their culture was positive for a STD
Marketing Exceptions

4. A communication for treatment of the patient by a healthcare providers or to direct or recommend alternative therapies, therapies, health providers

- It can’t be marketing

- The hospital or CE can not receive financial remuneration for the communication

- A physician recommends the patient with back pain to the PT clinic and to see an anesthesiologist in the pain clinic and the physician is not paid to make the recommendations
If the marketing involves financial remuneration from a third party then the hospital or CE must include this information in the authorization form:

- A new glucometer comes on the market and the company pays the hospital to send patients information on it.

“Financial remuneration” is defined to include payments in exchange for making the marketing communication:

- It does not include non-financial benefits such as in-kind benefits provided to the hospital.
- Drug company gives you free brochures that hospital can share with their patients.
Other Marketing Exceptions

- Communications promoting health in general that does not promote a product or service
  - Information to promote a healthy diet
  - Information to encourage weight loss in obese patients
- Communication about government and government sponsored programs
  - Social worker helps the patient qualify for Medicare or Medicaid
- Communications that do not involve PHI
  - Such as when the hospital buys a mailing list not derived from PHI and uses it to promote a third party product
What Costs Are Permitted?

- Recall the drug manufacturer could pay a hospital, pharmacy, or other CE to send the patient a refill reminder but it has to be at cost.

- In other words the hospital, pharmacy store, or other CE could not make money on it.

- Would include the cost of labor, supplies, and postage to make the communication.

- There can not be any other financial incentives beyond the costs of making the communication.
  - So no free Carribean cruises or Hawaiian vacations.
Refill Reminders Guidance Issued

- OCR issued guidance on refill reminders and HIPAA under HITECH Act
- Issued FAQ sheet and Fact sheet
- Explains refill reminder exception
- Guidance at www.hhs.gov/ocr/privacy/
- General rule is you need an authorization before can use PHI can be used in a marketing communication
- But had an exception for communicating about refill reminders
The HIPAA Privacy Rule and Refill Reminders and Other Communications about a Drug or Biologic Currently Being Prescribed for the Individual

Background

The Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual’s written authorization before his or her protected health information can be used or disclosed to make a marketing communication to the individual. In general, marketing means to make a communication to an individual about a product or service that encourages the individual to purchase or use that product or service. Often, the lines between a marketing communication and a communication for a treatment or health care purpose unavoidably overlap, as a necessary part of providing treatment and health care services and benefits to encourage or advise individuals to purchase or use certain health-related products or services. For this reason, the Privacy Rule includes important exceptions to what is considered marketing to ensure essential healthcare communications are not impeded. One important exception concerns communications about refill reminders and other communications about a drug or biologic currently being prescribed to the individual (“refill reminder exception”).

How the Refill Reminder Exception Works

The Privacy Rule expressly excludes from the definition of “marketing” refill reminders or other communications about a drug or biologic that is currently being prescribed for the individual, provided that financial remuneration received by the covered entity in exchange for making the communication, if any, is reasonably related to the covered entity’s cost of making the communication. See paragraph (2)(i) of the definition of “marketing” at 45 CFR 164.501. Financial remuneration means payment to a covered entity (or business associate, if applicable) from or on behalf of a third party whose product or service is being described. Financial
Refill Reminders Guidance Issued

- Exception for drug currently being prescribed
- Provided remuneration is reasonable and related to the cost of making the communication
- Exception includes information about generic equivalents & their drug delivery device (insulin pump)
- Communication about a recently lapsed prescription within the last 90 days
- Encouraging patient to get their Rx refilled
- Not for new meds, to get patient to switch to a different drug or for adjunctive drugs
Marketing

- If hospital or other CE does not receive any remuneration it can make communications about treatment and healthcare operations without an authorization
  - Case management, care coordination, etc.

- In summary, if the hospital or other CE receives financial remuneration about reasonably related costs
  - Then need a patient authorization
  - Authorization must note that the hospital is receiving financial remuneration
Fundraising

- The final rule made several changes to fundraising
  - It clarifies and expands the type of information that be used and disclosed for fundraising purposes
  - It makes other changes to help patients avoid unwanted mailings, phone calls and other fundraising solicitations
- Hospitals or other CEs that do any fundraising will have to revise their P&Ps to reflect the new standards
- Hospitals or other CEs should educate staff on the new regulations
Fundraising

- Changes not as significant as the ones we just looked at regarding marketing
- Good news is the new regulations are more flexible
- Concern under the old regulations that they restricted the hospital or other CE activities to be able to target fundraising communications
  - Patient who is cured from breast cancer may want to contribute to the new breast cancer center
  - Patient who has a stroke and recovered fully may want to support and donate for the new stroke center the hospital is building
Fundraising

- Hospitals were concerned about contacting a patient for fundraising who had a bad outcome
  - Hospital may not want to contact patient or family to donate money if patient had a bad outcome such as died from the stroke or heart attack
  - Hospitals wanted to be sensitive regarding patients with bad outcomes but previously could not use this data
  - If the hospital or CE meets the special conditions then the PHI can be used and disclosed to the BA without a patient authorization form
Fundraising

- Remember, you need to add to the NPP that the patient may be contacted for fundraising purposes and the patient has a right to opt out

- If a patient has opted out (revoked) and doesn’t want to receive fundraising information the hospital or CE may not make any further communications regarding fundraising
  - Strict compliance with opt-out requirement and reasonable efforts are no longer acceptable

- With every fundraising communication, the patient must be given a clear and conspicuous opportunity to not receive any more fundraising communications (opt out)
Fundraising

- A hospital or other CE cannot condition treatment or payment on the patient to require them to receive fundraising communications.

- New rules continue to allow the hospital or CE to use and disclose to the BA the following information for fundraising:
  - Demographic information (name, address, other contact information, age, gender, and date of birth)
  - Dates of health care provided to an individual
  - For example, hospital wants to build a new wing and hires fundraising company (BA) to raise the money.
Fundraising

- New regulations permit new types of PHI to be used for fundraising purposes which can be disclosed to the BA
  - Department or service information such as cardiology, oncology, or the emergency department
  - Treating physician information
  - Outcome information include the death or not so favorable outcome of the patient
  - Health insurance information
Fundraising

- Remember, if the patient opts out and doesn’t want to receive any more communication you must honor this.
- The hospital or CE may provide the patient with the method to opt back in if they change their mind.
- The hospital or CE can choose the method to opt out:
  - Can’t impose an undue burden on patient.
  - Can’t impose more than a nominal cost on patients who want to opt out.
  - Patient can opt out of all or just for specific campaigns.
Fundraising

- Permissible choices to allow a patient to opt out could include
  - A toll free number the patient can call (not required but HHS recommends)
  - An email address
  - Return of a preprinted prepaid postcard
  - But could not require the patient to write a letter
- Making a donation after the patient opted out and asked not to receive any more correspondences is not an appropriate opt back in method
Sale of PHI

- First time there is a definition

- The sale of PHI means:
  - A disclosure of PHI where the CE or BA directly or indirectly receives remuneration from the recipient of the PHI in exchange for the PHI unless the disclosure is for one of the following eight exceptions
  - The sale of PHI includes access, license, lease, or transfer of the ownership of the PHI
  - De-identified data is not PHI
Sale of PHI

- The **general rule** is that the hospital or CE or BA has to obtain the patient’s authorization for the sale of the patient’s PHI
- It is also important to note that remuneration includes both financial and in-kind which is different than the marketing rule
- Make sure you update your P&P to reflect the new regulations
- Train your staff
Sale of PHI

- Make sure your BA agreements do not involve payment for data but instead the fair market value of their services.

- Ensure that research activities only involve reasonable cost-based fees to cover the cost to prepare and send or transmit PHI.

- The following two activities are not considered a “sale”:
  - Payments for grants, contracts related to research activities.
  - Exchange of PHI through health exchange network if paid fees are assessed on participants.
Sale of PHI Exceptions

1. Public health purposes as allowed in the privacy rules

2. Research purposes where the remuneration received is the cost to prepare and transmit the PHI

3. Treatment and payment purposes

4. Sale, transfer, merger, or consolidation of all or part of the hospital or CE and related due diligence
Sale of PHI Exceptions

5. Services rendered by a BA under a BA agreement at the request of the hospital or CE

6. Disclosures to provide patients with access to their PHI or an accounting of disclosures

7. Other disclosures as required by law

8. Other purposed allowed by HIPAA where there may be a transfer of compensation as the result of the disclosure
   - The copying fee for medical records
   - But must be cost-based fee
Decision Tree for Safe of PHI

1. Is there a direct or indirect remuneration?
   - If the answer is no then it is allowed
   - If the answer is yes go to step 2

2. Is there an exchange of PHI
   - If the answer is no then it is not prohibited
   - If the answer is yes go to step 3

3. Does one of the exceptions apply?
   - If no then prohibited unless an authorization is obtained
   - If yes then not prohibited
Deceased Individuals
Deceased Individuals

- A hospital or CE may disclose a deceased’s patients PHI to a family member or other person involved in the care or payment prior to death
  - PHI that is relevant to the person’s involvement
  - Unless the disclosure is inconsistent with any prior expressed preferences of the patient
- The final rule limits the amount of time a deceased patient’s PHI must be protected to 50 years
  - This is not a record retention period
  - So if someone had MR older than this they are not protected
Deceased Individuals Guidance

Health Information of Deceased Individuals

45 CFR 160.103, paragraph (2)(iv) of the definition of “protected health information”

Background

The HIPAA Privacy Rule protects the individually identifiable health information about a decedent for 50 years following the date of death of the individual. This period of protection for decedent health information balances the privacy interests of surviving relatives and other individuals with a relationship to the decedent, with the need for archivists, biographers, historians, and others to access old or ancient records on deceased individuals for historical purposes. During the 50-year period of protection, the personal representative of the decedent (i.e., the person under applicable law with authority to act on behalf of the decedent or the decedent’s estate) has the ability to exercise the rights under the Privacy Rule with regard to the decedent’s health information, such as authorizing certain uses and disclosures of, and gaining access to, the information. With respect to family members or other persons involved in the individual’s health care or payment for care prior to the individual’s death, but who are not personal representatives, the Privacy Rule permits a covered entity to disclose the relevant protected health information of the decedent to such persons, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the covered entity.

How the Rule Works

The HIPAA Privacy Rule applies to the individually identifiable health information of a decedent for 50 years following the date of death of the individual. The Rule explicitly excludes from the definition of “protected health information” individually identifiable health information regarding a person who has been deceased for more than 50 years. See paragraph (2)(iv) of the definition of “protected health information” at § 160.103. Thus, for example, a HIPAA covered entity that maintains health or medical records, correspondence files, physician diaries and casebooks, or photograph collections that contain identifiable health information on individuals who have been deceased for more than 50 years may use or disclose the information without regard to the Privacy Rule because the information is not considered protected health information.

During the 50-year period of protection, the Privacy Rule generally protects a decedent’s health information to the same extent the Rule protects the health information of living individuals but does include a number of special disclosure provisions relevant to deceased individuals. These include provisions that permit a covered entity to disclose a decedent’s health information: (1) to alert law enforcement to the death of the individual, when there is
Deceased Individuals Guidance

- Protects information when a patient dies for 50 years after their death
- Balances needs of historians, families, archivists etc.
- During 50 year protection personal representative of decedent can exercise this right
- Physicians or hospitals can disclose after 50 years because information no longer protected
- Can use if suspicious death, coroner case, OPO, research on PHI of decedent, for payment of bill etc.
Immunization Records
Immunization Records

- The final rule allows the hospital, physician, or other CE to provide information about immunizations to the school.
  - If the school is required to have proof of immunizations prior to admitting the student.
- The PHI disclosed must be limited to the immunization.
- Written authorization is not required.
The physician or CE is required to obtain an oral or written agreement from the parent.

- Need to document the permission such as the phone call.
- A signature of the parent is not required.
- Can be from the individual if an adult or emancipated minor.
- Can be an email and again document it in the child’s medical record.
Student Immunizations

45 CFR 164.512(b)(1)(vi)

Background

The HIPAA Privacy Rule strikes an important balance between protecting the privacy of individuals’ protected health information (PHI) and allowing the disclosure of PHI in a number of circumstances to those responsible for ensuring public health and safety. One circumstance involves the disclosure of student immunization information to schools. Schools play an important role in preventing the spread of communicable diseases among students by ensuring that students entering classes have received various immunizations. Most States have “school entry” laws, which prohibit a child from attending school unless the school has proof that the child has been appropriately immunized. Some States allow a child to begin school provisionally for a certain period of time while the school waits for the necessary immunization information. Typically, schools ensure compliance with State requirements by requesting immunization records from parents, who then request them from their child’s health care provider. To ensure schools are able to receive the necessary documentation of immunization in a timely manner and admit children without undue delay, the HIPAA Privacy Rule permits a covered health care provider to disclose proof of immunization directly to a school that is required by law to have such proof prior to admitting a student, with the oral or written agreement of a parent or guardian.

How the Rule Works

The Privacy Rule permits a covered health care provider to disclose proof of immunization about a student or prospective student to a school that is required by State or other law to have such proof prior to admitting the student, provided the health care provider obtains and documents the agreement to the disclosure from either:

- A parent, guardian, or other person acting in loco parentis of the student, if the student is an unemancipated minor; or

- The student himself or herself, if the student is an adult or emancipated minor.
Student Immunizations

- Can report to school when information is required to attend school with oral or written agreement of parent
- Student can authorize if adult or emancipated minor
- Parent or guardian or loco parentis of minor
- Does not need HIPAA authorization form or the signature of the parent
- Can be a written request or pursuant to a phone call
- Has section on FAQs
# Immunization Records

## 2013 Recommended Immunizations for Children from Birth Through 6 Years Old

<table>
<thead>
<tr>
<th>Age</th>
<th>HepB</th>
<th>HepB</th>
<th>RV</th>
<th>DTaP</th>
<th>Hib</th>
<th>PCV</th>
<th>IPV</th>
<th>Influenza (Yearly)*</th>
<th>MMR</th>
<th>Varicella</th>
<th>HepA*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Birth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 month</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 months</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 months</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 months</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12 months</td>
<td></td>
<td>HepB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 months</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18 months</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19-23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-3 years</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-6 years</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Notes:
- If your child misses a shot, you don’t need to start over. Just go back to your child’s doctor for the next shot. Talk with your child’s doctor if you have questions about vaccines.

### Footnotes:
- Two doses given at least four weeks apart are recommended for children aged 6 months through 18 years of age who are getting a flu vaccine for the first time and for some other children in this age group.
- Two doses of HepA vaccine are needed for lasting protection. The first dose of HepA vaccine should be given between 12 months and 23 months of age. The second dose should be given 4 to 16 months later. HepA vaccination may be given to any child 12 months and older to protect against HepA.” Children and adolescents who did not receive the HepA vaccine and are at high risk should be vaccinated against HepA.

### Additional Information:
- If your child has any medical conditions that put him at risk for infection or is traveling outside the United States, talk to your child’s doctor about additional vaccines that he may need.

For more information, call toll free 1-800-CDC-INFO (1-800-232-4636) or visit http://www.cdc.gov/vaccines
GINA
The Genetic Information Nondiscrimination Act of 2008
GINA

- GINA is a federal law that protects individuals from genetic discrimination in health insurance and employment (hiring, firing, and promotions)
  - It prevented insurance companies from charging a higher premium to a healthy person based solely on their genetic predisposition
  - Woman has the BRCA\textsubscript{1} gene that puts her a higher risk for getting breast cancer
  - An employee was fired after the hospital found out her father died from Huntington’s chorea
- It was enacted May 21, 2008 and new regulations include changes to comply with GINA
Genetic Information

- Adopts the definition from the GINA 2008

- Genetic information is:
  - The individual’s genetic tests (a type of medical test to test for genetic disorders)
  - The genetic tests of a family member
  - Family medical history
  - It is not the sex or age of any individual

- Clarifies that tests such as a CBC, cholesterol, HIV test, liver tests, or tests to detect the present of drugs or alcohol are not genetic information
Genetic Information

- The final rule prohibits the use of genetic information for underwriting
  - Except for long term care plans
  - Except the use of genetic information is allowed when the person is seeking a particular benefit and the genetic information is needed to determine the medical appropriateness of providing the benefit
    - Woman with BRCA1 is requesting the insurance company to approve surgery for a mastectomy when there is no cancer present

- Genetic information include information about a fetus or embryo
CMS, CLIA, and CDC Changes to Lab Test Results
Lab Test Results

- The patient now has the right to get a copy of their lab results from the lab that runs the test
- Use to be the patient could only get a copy of their lab tests from the physician or ordering practitioner
- This amended the federal CLIA law and the HIPAA law
- So patient can now get their lab results directly from the lab
Lab Allowing Access to Lab Results

BILLING CODE 4120-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

42 CFR Part 493

Office of the Secretary

45 CFR Part 164

[CMS-2319-F]

RIN 0938-AQ38

CLIA Program and HIPAA Privacy Rule: Patients’ Access to Test Reports

AGENCY: Centers for Medicare & Medicaid Services (CMS), HHS;

Centers for Disease Control and Prevention (CDC), HHS; Office for Civil Rights (OCR), HHS.

ACTION: Final rule.

SUMMARY: This final rule amends the Clinical Laboratory Improvement Amendments of 1988 (CLIA) regulations to specify that, upon the request of a patient (or the patient’s personal...
Research

Brief Discussion
Research

- Research is defined to mean a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

- Can not condition treatment or payment on signing an authorization to permit the use of the patient’s PHI in research (unchanged).
  - Except that an authorization for a research study may condition or limit access to the study related treatment on signing on authorization to use PHI for that study only.
  - Hospital is doing a research study on the use of a new drug for prostate cancer and no right to obtain the experimental drug unless you are in the study.
A conditional authorization is one that conditions the provisions of the research related treatment on obtaining an authorization to disclose PHI for research purposes.

- So patient participates in the research project has to agree the results can be used.

There was a change in the rule regarding combining conditional and unconditional authorizations into a single authorization form:

- The hospital, physician, or other CE can combine conditional and unconditional authorizations into one single authorization form if certain criteria are met.
Research

- The unconditional component can be used for any type of research activities
- The compound authorization must clearly differentiate between the conditional and unconditional elements of the form
- Must clearly allow the patient to opt-in to the unconditional elements
- Still requires the authorization to include a description of each purpose or disclosure of PHI
  - Must identify a specific study for which the PHI will be used and not a general description
Research

- The preamble states the intended purpose is adequately described if it would be reasonable for the individual to expect that his PHI could be used or disclosed in the future research purposes.
  - Patient is taking an experimental anticoagulant and study looks at no reoccurrence of a DVT or pulmonary emboli and maintaining INR. Other data is collected and a later study evaluates if any increase blood pressure or weight gain from taking the drug.
  - This may extend to PHI not yet collected at the time the authorization was signed.
The hospital, physician, or CE can use a separate checkbox to signify that the person has opted in to the unconditional activity using one line for the signature.

The CE can describe the unconditional research activity on a separate page of a compound authorization and cross reference the relevant sections to minimize using repeat language so less confusing.

CE and IRBs will have broad discretion now to determine what is an adequate description of future research for consent and authorization.
Research

- Hospitals, physicians, or CE will need to revise P&P
- Will need to distinguish between conditional and unconditional request for consent or authorizations
- Determine when it is appropriate to include both conditional and unconditional permission into a single authorization form
- Clearly distinguish the conditional and unconditional permission to potential research subjects when a single consent or authorization is used for both
Office for Human Research Protections (OHRP)

OHRP Informed Consent Frequently Asked Questions

These FAQs provide guidance that represents OHRP's current thinking on these topics and should be viewed as recommendations, unless specific regulatory requirements are cited. The use of the word "must" in OHRP guidance means that something is required under HHS regulations at 45 CFR part 46. The use of the word "should" in OHRP guidance means that something is recommended or suggested, but not required. An institution may use an alternative approach if the approach satisfies the requirements of the HHS regulations at 45 CFR part 46. OHRP is available to discuss alternative approaches at 240-453-6900 or 866-447-4777.

Commonly Used Abbreviations

CFR — Code of Federal Regulations
FDA — Food and Drug Administration
FWA — Federalwide Assurance
HHS — Health and Human Services
IEC — Independent Ethics Committee
IRB — Institutional Review Board
AHRQ Toolkit to Facilitate Consent

- AHRQ toolkit to facilitate the process of obtaining informed consent
- Also information on the HIPAA authorization for potential research subjects
- Available at http://www.ahrq.gov/fund/informedconsent/
The AHRQ Informed Consent and Authorization Toolkit for Minimal Risk Research

The Agency for Healthcare Research and Quality (AHRQ) has developed the Informed Consent and Authorization Toolkit for Minimal Risk Research to facilitate the process of obtaining informed consent and Health Insurance Portability and Accountability Act (HIPAA) authorization from potential research subjects. This toolkit contains information for people responsible for ensuring that potential research subjects are informed in a manner that is consistent with medical ethics and regulatory guidelines.

Contents

Background
Why a Toolkit?
Development of This Toolkit
Informed Consent, HIPAA Authorization, and Adult Health Literacy
How To Improve Informed Consent and Authorization
Improving the Process
Adapting New Processes and Documents in Your Institution
Improving the Informed Consent and Authorization Process
Using the Tool for Researchers' Certification of Consent and Authorization
Improving the Forms
Sample Documents for Informed Consent and HIPAA Authorization (English and Spanish versions)
Adapting and Testing AHRQ Sample Documents
Regulatory Requirements
Resources
Other Resources From the Department of Health and Human Services
References

AHRQ Publication No. 09-0093-0F
Current as of September 2009

Select to download print version PDF File (300 KB), PDF Help.
The End! Questions??

- Sue Dill Calloway RN, Esq. CPHRM, CCMSCP
- AD, BA, BSN, MSN, JD
- President of Patient Safety and Education Consulting
- Board Member Emergency Medicine Patient Safety Foundation at www.empsf.org
- 614 791-1468
- sdill1@columbus.rr.com
- Additional resources on Business Associates and BAAs
OIG Criticizes OCR Oversight Security Rule

 Audit (A-04-11-05025)

11-21-2013
The Office for Civil Rights Did Not Meet All Federal Requirements in Its Oversight and Enforcement of the Health Insurance Portability and Accountability Act Security Rule

Complete Report

Download the complete report

Adobe Acrobat Reader® is required to read PDF files.

Summary
The Office for Civil Rights (OCR) did not meet certain Federal requirements critical to the oversight and enforcement of the Health Insurance Portability and Accountability Act Security Rule (Security Rule). OCR had not assessed risks, established priorities, or implemented controls for its Federal requirements to provide for periodic audits of covered entities to ensure their compliance with Security Rule requirements. In addition, OCR’s Security Rule investigation files did not contain required documentation supporting key decisions made because management had not implemented sufficient controls, including supervisory review and documentation retention, to ensure investigators follow investigation policies and procedures for properly initiating, processing, and closing Security Rule investigations. Further, OCR had not fully complied with Federal cybersecurity policies and procedures.

http://oig.hhs.gov/oas/reports/region4/41105025.asp
Department of Health and Human Services

OFFICE OF
INSPECTOR GENERAL

THE OFFICE FOR CIVIL RIGHTS DID NOT MEET ALL FEDERAL REQUIREMENTS IN ITS OVERSIGHT AND ENFORCEMENT OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT SECURITY RULE

Inquiries about this report may be addressed to the Office of Public Affairs at PublicAffairs@oig.hhs.gov

Thomas M. Salmon
Assistant Inspector General

November 2013
A-04-11-05025
Business Associates and BA Agreements
Who is a Business Associate?

- A BA could be;
  - An auditors, accountants, lawyers, consultants, accrediting agencies like TJC, DNV Healthcare, AOA, CIHQ, NCQA, CAP, CARP, billing firms, management, utilization review organizations, data processing company, financial services, collection of unpaid hospital bills et al.,
  - It is not a member of the hospital or CE’s workforce
- Providers like hospitals must have a contract, called a Business Associate Agreement (BAA) with Business Associate (BA) that limits how they use information
Business Associates (BAs)

- There were many changes related to BAs
- The final rule revises the BA definition to include:
  - An individual or entity that “creates, receives, maintains, or transmits PHI for a function or activity” on behalf of a CE or organized health care arrangement (OHCA),
  - But other than as a part of the workforce of the CE or OHCA
  - Clarified that downstream contractors from BAs that touch PHI may also be considered BAs
- BAs are subject to the Breach Notification rules
- BAs are subject to the civil (four tiers) and criminal penalties like hospitals and other CEs
BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (this “Agreement”) is made and entered into by and between Washington University, a benevolent corporation created by special act of the Missouri General Assembly, on behalf of itself and/or its affiliated organization(s) (collectively referred to herein as “Covered Entity”) and __________________________, a __________________________ corporation (“Business Associate”).

RECITALS:

A. Covered Entity may Disclose or make available to Business Associate, and Business Associate may Use, Disclose, receive, transmit, maintain or create from or on behalf of Covered Entity, certain information in conjunction with services being provided by Business Associate to or on behalf of Covered Entity.

B. The parties are committed to compliance with the Health Insurance Portability and Accountability Act of 1996 and regulations promulgated thereunder, as amended from time to time (collectively “HIPAA”).

C. The purpose of this Agreement is to satisfy the obligations of Covered Entity under HIPAA and to ensure the integrity and confidentiality of “Protected Health Information” Disclosed or made available to Business Associate and certain information that Business Associate Uses, Discloses, receives, transmits, maintains or creates from or on behalf of Covered Entity.

AGREEMENT:

NOW, THEREFORE, in consideration of the foregoing recitals and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions.

A. “Breach Notification Rule” shall mean the provisions of 45 C.F.R. Part 160 and 164, Subpart D, entitled “Notification in the Case of Breach of Unsecured Protected Health Information.”
SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS
(Published January 25, 2013)

Introduction

A “business associate” is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A “business associate” also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity’s obligation with respect to individuals’ requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate is to carry out a covered entity’s obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation; (7) require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or
Business Associates

- BAs are directly subject to certain security standards
  - Added additional security rules for BAs

- BAs are subject to the privacy requirements in HITECH

- Minimum necessary rules now apply to BAs
  - Hospital contracts with company to make copies of the medical records and request is received for information related to child abuse information
  - Can’t just copy entire chart. Would need to abstract out information related to what constitutes the child abuse
Business Associates

- Makes the hospital or other CE liable for violations of the BAs that are acting as their agent as previously discussed

- BAs not subject to all of the privacy standards such as the NPP requirement

- Expands the definition of BA to include subcontractor

  - Hospital contracts a company to do audits and they sign a BAA. Some of the work is more detailed than what the BA can do so they hire a forensic specialist who is a subcontractor of the BA
Business Associates

- The final rules specify the following are BAs
- New rule regulates data center operators and vendor that maintain or transmit PHI even if they do not actively access the PHI
- E-prescribing gateway
  - E-prescribing is an electronic way to send prescriptions to the pharmacy through automated data entry process using e-prescribing software and a transmission network (the hub or gateway for transmission) such as SureScripts or RXHub
What is a "business associate" under HIPAA?

The term "business associates" refers specifically to a person or organization that conducts business with the covered entity that involves the use or disclosure of individually identifiable health information. Business associates include those that perform services on behalf of the covered entity, such as claims processing, data analysis, utilization review, and billing, or provide services to the covered entity, such as legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. To be a business associate, the work of an organization must deal directly with the use or disclosure of protected health information.

The HITECH Act also specifies that an organization that provide data transmission of PHI to a covered entity and that requires access to PHI on routinely will be treated as a business associate. Such an organization may include: a Health Information Exchange Organization, a Regional Health Information Organization (RHIO), an e-Prescribing

www.hrsa.gov/healthit/toolbox/HealthITAdoption/toolbox/PrivacyandSecurity/associateshipaaa.html
Business Associates

- The final rules specify the following are BAs (continued):
  - Other persons that provide data transmission services with respect to PHI and that require access on a routine bases to such PHI
  - Health information organization (HIO)
    - Government lead non-profit organization that provides information about ARRA 2009 as it pertains to EHRs development for incentive payments
    - OCR did not define this in the rule since industry is still evolving but mere conduit is not a BA
Business Associates Subcontractor

- The definition of BA includes a subcontractor
  - Subcontractor is defined as a person to whom a BA delegates function, activity, or service other than in the capacity of a member of the workforce of the BA
  - In other word, the subcontractor is not an employee of the BA
  - The surveyor is an employee of the TJC so they are a BA and not a subcontractor
- BA includes the subcontractor who receives, creates, maintains or transmits PHI on behalf of the hospital or CE
Business Associates

- The BA and not the hospital or CE would be responsible for entering into a BAA with the subcontractor
  - An example would be a BA who gives PHI to a third party to use it for a project and the third party is a subcontractor
  - There must be a HIPAA compliant BAA between the BA and the subcontractor
  - So the bottom line is that subcontractors are BAs
- The revised rule specify that the BA’s permitted and required uses and disclosures of PHI
Subcontractors

- So the subcontractor is subject to the HIPAA provisions just like any BA

- So the BA and subcontractor must comply with
  - The applicable security rule regarding PHI
    - Includes the security standards, administrative, physical, technical safeguards, organizational requirements, P&Ps, and documentation requirements
  - Must report breaches of unsecured PHI
  - BA must enter into downstream BAA with subcontractor
  - The BA has to follow the privacy rules that apply to the hospital or CE’s if the BA is carrying out the hospital’s obligations
Subcontractors BA Agreements

- The hospital or CE is not responsible to have a BAA with the subcontractor
  - The hospital just has a BAA with their BA
- The BAA between the BA and the subcontractor can not give the subcontractor more authority then what the hospital gave them
  - So the BA can not permit the subcontractor to use PHI or disclose PHI in a manner the BA was not allowed to do
- Each BA in the chain (downstream) can have no more than what the previous one had
Business Associates Revisions

- The hospital or CE will need to rewrite their BAA

- There is a new definition of breach
  - So if your old BAA defined breach or outlines an assessment of breach and discusses the harm threshold it is out of date with the new rules

- The minimum necessary rule now applies to BAA so only want to disclose what is absolutely necessary for the intended purpose

- May want to add that BA must enter into a BAA with any subcontractors

- Section that BAs have to comply with the security rule regarding ePHI
Business Associates Does Not Include

- A health care provider with respect to disclosure concerning treatment of the patient
  - ED doctor calls doctor on call to discuss patient’s care

- A government agency to determine eligibility or enrollment in a government health plan that provides public benefits and is administered by another government agency for collecting PHI
  - An example is Medicare or Medicaid

- A CE participating in an OHCA that performs a specific service, function or activity on behalf of such OHCA (Organized Health Care Arrangement)
Business Associates Compliance Date

- As previously discussed, the effective date to be in compliance with the new rules is September 23, 2013.

- However, there is an exception for grandfathered BAAs until September 23, 2014 if the following rules are met:
  - If you currently have a BAA in existence before the new rules were published on January 25, 2013 and
  - You must also have to have a BAA that was current with the existing rules which would be compliant with the changes that were made in the HITECH 2009 law.
Business Associates Compliance Date

- If you enter into a new BAA on or after March 26, 2013 then you do not get the year extension and must be in compliance September 23, 2013

- If you change or modify a BAA on or after March 26, 2013 then you do not get the year extension and must be in compliance September 23, 2013

  - So a BAA that is revised or renewed between March 26, 2013 and September 22, 2013 have to be in compliance with the new rule
Business Associates

- OCR now has direct enforcement authority with regard to the BAs and subcontractors
- BAs and subcontractors are now subject to the HIPAA civil and criminal penalties
- So revise your BAA if missing required BA provisions
- Be mindful of agency law analysis when revising
- Take steps to cure any breach or end the violation and if unsuccessful terminate the BAA
- Amend your P&P to reflect the new rules
- Train your staff
HIPAA - Collaborative of Wisconsin

(Site best viewed at 1024x768)

HIPAA COW is a non-profit organization open to entities considered to be Covered Entities, Business Associates, and/or Trading Partners under HIPAA, as well as any other organization impacted by HIPAA regulations.

WHAT'S NEW

HIPAA COW Spring Conference - April 12, 2013, Click on the Events tab at left for more information

2012 Annual Report

HIPAA COW Example Policy and Procedure Template - This example policy and procedure (P&P) template was developed to assist organizations to create a P&P template for their own organizations.

HIPAA COW Resources Grid - A complete listing of all deliverables on this site

NIST 2012 HIPAA Conference Presentations

HIPAA COW Privacy Breach - Privacy Officer's Responses & Investigation Checklist - This checklist has been created to provide outlined guidance in responding to a large scale/impact privacy breach due to loss, theft, or other unauthorized access, use, or disclosure of patient protected health information (PHI). More detail is provided in the HIPAA COW Breach Notification Policy.

RECENT HIPAA NEWS:


OCR Audit Protocol: The Department of Health and Human Services Office of Civil Rights has posted HIPAA Audit Protocols on it's website: http://ocrnotifications.hhs.gov/hipaa.html 7/8/12

RECENTLY UPDATED:

HIPAA COW Risk Analysis Toolkit
Privacy and Security Toolkit

Health information security and medical privacy are of utmost importance in today’s healthcare environment. HIMSS provides guidance and resources to assist healthcare entities navigate many of the complex and rapidly evolving issues that are facing the healthcare industry.

The HIMSS Privacy and Security Committee guides the implementation of strategic initiatives that promote the privacy and security of healthcare information and management systems. Its goal: “By 2014, all entities who use, send, or store health information meet requirements for confidentiality, integrity, availability and accountability based on sound risk management practices, using recognized standards and protocols.”

HIMSS has launched several work groups that are actively involved with industry changing activities to achieve this goal.

Latest News & Announcements

New Privacy White Paper and Blog Posting
The HIMSS Privacy and Security Committee chose the topic of Patient Trust as the focus of the HIMSS Blog for Thursday, June 7, 2012, to discuss the release of a new white paper titled “Understanding the Role of Trust in the Protection of Privacy,” written by Ken Hartman, HIMSS PBS Committee member.

This latest addition to the HIMSS Privacy & Security Toolkit is the result of the PBS Committee’s desire to increase understanding of privacy as a separate and distinct concept from Security. The paper discusses why it is important to understand the linkage between trust and privacy, and delves into the more personal issues of vulnerability, fairness, and competence.

Social Media in Healthcare: Privacy and Security Considerations
Toolkits

www.himss.org/ASP/topics_pstoolkitsDirectory.asp?faid=569&tid=4

Privacy and Security

Overview
HIMSS Annual Security Survey Results
Legal and Regulatory
Information Systems Security
Medical Identity Theft
Privacy Impact Assessment
Privacy & Security for RHIOs/HIEs
Privacy and Security for Personal Health Records
Privacy & Security Committee, Task Forces and Work Groups
Resources from our Corporate Members
Medical Device Security
Privacy & Security Toolkits
News

Privacy & Security Toolkits

Be prepared for healthcare IT challenges with HIMSS Privacy and Security Toolkits. Each Toolkit contains resources, best practices and case studies on a variety of important privacy and security topics. Begin exploring today!

Privacy & Security Toolkit
Outlines general principles and examples of how healthcare entities can manage the privacy and security of their electronic information to meet compliance requirements.

Privacy & Security Toolkit for Small Provider Organizations
Smaller organizations will find guidance in this toolkit for implementing an appropriate set of policies and procedures for their organization.

Patient Identity Integrity Toolkit
Learn about patient identity integrity and the many issues involved in reliably and safely matching patient identity across systems.

Risk Assessment Toolkit
Learn how to conduct security risk assessments and implement a risk management process in your healthcare organization.

Mobile Security Toolkit
Manage the security of mobile technologies in your healthcare IT environment based on industry best practices.

Cloud Security Toolkit
Understand cloud computing and its associated security challenges to make informed information security decisions for your healthcare organization.
Center on MR Rights and Privacy

About the Center

The Center on Medical Record Rights and Privacy is based at Georgetown University's Health Policy Institute, a non-partisan multi-disciplinary group of faculty and staff dedicated to conducting research on key issues in health policy and health services research. The Center is dedicated to raising public awareness of the rights and responsibilities associated with medical records and other health information.

The Center focuses on a range of topics related to consumers' rights to their own medical records and privacy protections afforded to this information. The Center has expertise in the Health Privacy Rule issued under the Health Insurance Portability and Accountability Act (HIPAA), the Fair and Accurate Credit Transactions Act as well as state laws that address medical record rights and privacy. The Center provides information on

New and Notable

- Report on State Medical Record Access Laws
- Report on State Law Requirements for Patient Permission to Disclose Health Information
- Releasing Clinical Laboratory Test Results: Report on Survey of State Laws
- Report on State Prescribing Laws: Implications for e-Prescribing
This presentation is intended solely to provide general information and does not constitute legal advice. Attendance at the presentation or later review of these printed materials does not create an attorney-client relationship with the presenter(s). You should not take any action based upon any information in this presentation without first consulting legal counsel familiar with your particular circumstances.
Do you have a question that you would like answered during the Q&A session? Simply follow the instructions below.

You may enter your question in the chat box in the webinar room.

OR

If you are listening to the conference via streaming audio through your computer, you must dial in on the telephone at 1-877-776-3544 to ask your question live. After dialing-in (or if you are already dialed-in):

1. Press *1 on your touchtone phone. If you are using a speaker phone, please lift the receiver and then press *1.

2. If you would like to withdraw your question, press *1.
Thank you for attending!

- Sue Dill Calloway RN, Esq., CPHRM
- AD, BA, BSN, MSN, JD
- President of Patient Safety and Education Consulting
- Chief Learning Officer of the Emergency Medicine Patient Safety Foundation at www.empsf.org
- 614 791-1468
- sdill1@columbus.rr.com