HIPAA for 2017

Becky Walter, MCS-P, CMQP, CCCA
Who Regulates HIPAA?

Department of Health & Human Services (HHS) makes policy
Office Of Civil Rights (OCR) enforces
OIG Compliance vs. HIPAA Compliance

- HIPAA requires covered entities to have contingency plans that establish policies and procedures regarding protected health information
- HIPAA also administered by HHS
- Office of Civil Rights

- OIG Compliance relates to fraud and abuse
- Documentation, coding, billing and patient financial inconsistencies
- Medical necessity and erroneous payment demands
- Federal programs with extension through Office of Audit Services
FOR IMMEDIATE RELEASE
January 9, 2017

First HIPAA enforcement action for lack of timely breach notification settles for $475,000

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced the first Health Insurance Portability and Accountability Act (HIPAA) settlement based on the untimely reporting of a breach of unsecured protected health information (PHI). Presence Health has agreed to settle potential violations of the HIPAA Breach Notification Rule by paying $475,000 and implementing a corrective action plan. Presence Health is one of the largest health care networks serving Illinois and anesthesia. OCR’s investigation revealed that Presence Health failed to notify, without unreasonable delay and within 60 days of discovering the breach, each of the 836 individuals affected by the breach, prominent media outlets (as required for breaches affecting 500 or more individuals), and OCR.
Is it Mandatory?

- Federal laws with penalties for non-compliance
- State laws also apply
Pilot Program Exposed Issues

- In 2011-2012, OCR had a pilot program, Phase 1, auditing 115 covered entities.
- Based on those results, OCR is now implementing Phase 2 of the program.
Elements of HIPAA Compliance

- Privacy Standards
- Security Standards
- Breach Notification
- Education and Training
- Self-Auditing
- Non-discrimination
<table>
<thead>
<tr>
<th>Privacy Elements</th>
<th>Security Elements</th>
<th>Breach Notification Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice of privacy practices</td>
<td>Risk analysis</td>
<td>Risk assessment of Breach</td>
</tr>
<tr>
<td>Rights to request privacy protection for PHI</td>
<td>Access management</td>
<td>Notice to individuals</td>
</tr>
<tr>
<td>Access of individuals to PHI</td>
<td>Security incident procedures</td>
<td>Notification to media</td>
</tr>
<tr>
<td>Administrative requirements</td>
<td>Contingency planning and backups</td>
<td>Notification to Secretary</td>
</tr>
<tr>
<td>Uses and disclosures of PHI</td>
<td>Workstation security</td>
<td>Notification by BA</td>
</tr>
<tr>
<td>Amendment of PHI</td>
<td>Media movement and destruction</td>
<td>Law enforcement delay</td>
</tr>
<tr>
<td>Accounting of disclosures</td>
<td>Encryption</td>
<td>Burden of proof</td>
</tr>
<tr>
<td></td>
<td>Audit controls and monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrity controls</td>
<td></td>
</tr>
</tbody>
</table>
Privacy Compliance

1. Appoint a Privacy Officer
2. Define Minimum Necessary for Your Office
3. Write HIPAA Privacy Policies and Procedures
4. Customize Your NPP (Notice of Privacy Practices)
5. Implement Program and Train Your Team Members
6. Monitor Your Active Privacy Program
7. Business Associate Agreements In Place
Privacy Officer Responsibilities for ________________ (insert practice name)

Summary:

The Privacy Officer will oversee all activity related to the development, implementation, and maintenance of and compliance with the Practice’s policies and procedures involving patient privacy and access of protected health information (PHI). The Privacy Officer will understand and enforce compliance with the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations.

Performance Requirements:

The Privacy Officer will have or gain knowledge of federal, state, and healthcare privacy and compliance laws, rules, and regulations regarding protected health information (PHI). The Privacy Officer must be proactive, able to solve problems and exercise proper judgment in difficult situations. They must be able to organize and analyze data and be able to communicate results clearly to all practice employees and leadership.

Job responsibilities

- Act as the main contact for all patient privacy matters for this practice.
- Establish and maintain privacy policies and procedures in cooperation with the leadership of the practice.
- Coordinate with key personnel to ensure the organization has and maintains appropriate forms and notices. These notices include, but are not limited to, privacy and confidentiality consent, authorization forms, business associate agreements and public policy materials reflecting the organizations policies and procedures.
2. Minimum Necessary Standard

The Privacy Rule requires you to take reasonable action to limit the use or disclosure of PHI to the minimum necessary to accomplish your intended purpose.
3. Write HIPAA Policies & Procedures

- You are required to have written HIPAA Policies and Procedures in place for a valid HIPAA Compliance Program in your office...This includes keeping them up to date and active!
- What is commonly missed?
3. Common Uses and Disclosures: TPO

**Payment:** billing and collections activities; determination of eligibility

**Healthcare Operations:** Quality assurance, scheduling, auditing, and employee review

- No signed authorization required for:

  **Treatment:** Doctors can share information freely with each other
3. HIPAA Omnibus Rule - Disclosures

At the patients request, you may NOT disclose information to a patient’s health plan if they wish to pay out of pocket for their care. For Registered Medicare Providers also.
3. Write HIPAA Policies & Procedures

- Have internal policy & procedure for every area of PHI risk as well as for patient rights

- Include:
  - Faxes & emails
  - Phone calls
  - Neglect/abuse
  - Etc.
Sign-in Sheets

Policy

We provide sign-in sheets for our patients to sign when they arrive for their appointments.

Procedure

We provide sign in sheets, which are permitted by the privacy rule as long as the only information listed on them is the minimum necessary information. Sign-in sheets can only include the doctor’s name, patient’s name, appointment time, and patient’s time of arrival for the appointment. Other identifying information is prohibited. We allow no PHI on the sign in sheet.

Call Verification

Policy

We verify the identity of those to whom we speak on the telephone with any PHI is discussed during the call. This is done to ensure that the caller is the patient. We do not disclose any more than the minimum necessary during phone conversations unless we have authorization either by law or from the patient to disclose the information.

Procedure

When answering the phone, we make certain the person you’re speaking to is identified properly.

Phone Messages and Appointment Reminders
3. Write HIPAA Policies & Procedures

 Disclosure Logs and Accounting

- Patient may request accounting of all non-TPO disclosures
- Only non-TPO disclosures should be logged
- Not required for those with authorization, reporting neglect or abuse, law enforcement, or prior to 4/14/03
3. Write HIPAA Policies & Procedures

EOB’s and COB’s

• When coordinating benefits, blacken any other patient’s PHI on EOB
• Clear out anything that does not apply to the claim
• Otherwise is a violation of HIPAA law.
3. Write HIPAA Policies & Procedures

Destruction of Medical Records

- You are responsible for wrongful disclosures due to improper disposal of PHI.
- Shred, get receipt
- Erase
- Proper disposal
HIPAA Omnibus Rule - Marketing

• New rules limit circumstances when you can provide marketing communication to your patients WITHOUT written authorization
HIPAA Omnibus Rule - Marketing

1) the physician receives no compensation for the communication;
2) the communication is face-to-face;
3) the communication involves a drug or biologic the patient is currently being prescribed and the payment is limited to reasonable reimbursement of the costs of the communication (no profit);
4) the communication involves general health promotion, rather than the promotion of a specific product or service; or
5) the communication involves government or government-sponsored programs.

Physicians are still permitted to give patients promotional gifts of nominal value.
HIPAA Omnibus Rule - Copies

- Changes to timeframes and fees for patient’s written requests of PHI
- You have 30 days (with ONE 30 day extension)
HIPAA Omnibus Rule - Copies

- Must attempt to provide copies in electronic form if that is the request and if they are “readily reproducible”
- Otherwise, can be in another mutually agreed upon format
HIPAA Omnibus Rule - Copies

- You must consider transmission security when emailing PHI
- You can send in unencrypted email if the patient is made aware of risks and still requests
HIPAA Omnibus Rule - Copies

- New rule modified the costs to the patient for copies
  - include labor costs
  - supply costs such as copy, USB, CD
- Must follow state law for lower fee
4. Customize Your NPP (Notice of Privacy Practices)

- HIPAA gives your patients a right to be informed of the privacy practices of your office.
- HIPAA gives patients the ability to be informed of their rights concerning HIPAA privacy.
SAMPLE NOTICE OF PRIVACY PRACTICES

[Practice Name, Address, Phone]

Effective Date: [Insert effective date]

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

This Notice of Privacy describes how we may use and disclose your Protected Health Information (PHI) to carry out treatment, payment or health care operations (TPO) and for other purposes that are permitted or required by law. It also describes your rights to access and control your PHI. “Protected Health Information” is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health condition and related health care services.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

Treatment: We may use and disclose your personal information to provide you with treatment or services. For example, we may use your health information to prescribe a course of treatment or make a referral. We will record your current healthcare information in a record so, in the future, we can see your medical history to help in diagnosing and treatment, or to determine how well you are responding to treatment. We may provide your health information to other health providers, such as referring or specialist physicians, to assist in your treatment. Should you ever be hospitalized, we may provide the hospital or its staff with the health information it requires to provide you with effective treatment.

Payment: We may use and disclose your health information so that we may bill and collect payment for the services that we provided to you. For example, we may contact your health insurer to verify your eligibility for benefits, and may need to disclose to it some details of your medical condition or expected course of treatment. We may use or disclose your information so that a bill may be sent to you, your health insurer, or a family member. The information on or accompanying the bill may include information that identifies you and your diagnosis, as well as services rendered, any procedures performed, and supplies used. Also, we may provide health information to another health care provider, such as an ambulance company that transported you to our office, to assist in their billing and collection efforts.
HIPAA Omnibus Rule - NPP

• NPP must be updated
• Include:
  • New breach notification guidelines
  • Copy guidelines
  • Notice of Non-disclosure
  • Marketing uses
HIPAA Omnibus Rule - NPP

- Post in visible spot (bulletin board, etc.)
- Make copies available
  - Anyone who requests
- Post new NPP to website
Acknowledgement
(Notice of Privacy Practices)

• Document your Delivery or Intent
• Included in Auditing results
Notice of Privacy Practices Acknowledgement  
(Practice Name)

I understand that under the Health Insurance Portability and Accountability Act (HIPAA), I have certain rights to privacy regarding my protected health information. I acknowledge that I have received or have been given the opportunity to receive a copy of your Notice of Privacy Practices. I also understand that this practice has the right to change its Notice of Privacy Practices and that I may contact the practice at any time to obtain a current copy of the Notice of Privacy Practices.

__________________________________________  
Patient Name or Legal Guardian (print)  

__________________________________________  
Date

__________________________________________  
Signature

Office Use Only

We have made the following attempt to obtain the patient’s signature acknowledging receipt of the Notice of Privacy Practices:

[Signature Attempt Details]
5. Implement and Train Your Team Members

- Annual training required
- Keep Internal Policy Active and Updated
- Keep employment records separate from treatment records
- Fully enforce sanctions for failure to comply
<table>
<thead>
<tr>
<th>Incident</th>
<th>Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1: Accidental Breach</strong></td>
<td>Warning and Re-Education</td>
</tr>
</tbody>
</table>
| Possible Scenarios:  
  • Employee does not log off the computer after use  
  • Employee faxes the wrong PHI to another practice  
  • Employee forgets to get a signed acknowledgement of receipt of the Notice of Privacy Practices  
  • Employee emails PHI to the wrong email address | A verbal warning will be documented in the employee’s file on the disciplinary action form. Mandatory re-education and training will occur for the first offense. Continued offensives will lead to progressive disciplinary action up to and including suspension and termination. |
| **Level 2: Intentional Breach Without Harmful or Dishonest Intention** | Written Warning, Re-Education, and Possible Suspension |
| Possible Scenarios:  
  • Employee views patient records out of curiosity, not necessity  
  • Employee shares PHI because the information is interesting or gossip-worthy, but not for treatment  
  • Employee shares computer password  
  • Employee discusses confidential patient information in an unsecure area | A written warning will be documented in the employee’s file on the disciplinary action form. Mandatory re-education and training will occur for the first offense. Continued offensives will lead to progressive disciplinary action up to and including suspension termination. |
| **Level 3: Willful or Intentional Breach with Harmful or Dishonest Intentions** | Termination |
| Possible Scenarios:  
  • Using PHI for personal gain, such as marketing without an authorization  
  • Using PHI to cause harm, such as exposing information to unauthorized individuals out of spite or dislike of the owner of the PHI.  
  • Gives access to a restricted area to an unauthorized individual  
  • Gives access to PHI to an unauthorized individual | A disciplinary action form will be completed, termination will occur, along with possible referral to law enforcement. |
6. Monitor Your Active Privacy Program

- Conduct Initial Program Audit
- Conduct Regular Self-Audits
  - Privacy Program Audits
  - NPP Acknowledgement Audits
Audit Privacy in Patient Charts - NPP

Privacy Audit Form

Name of Office: ___________________________________________ Name of Provider: _________________

Name of person(s) doing research: __________________________ Date: __________________

Patient Name: ___________________________ Doctor: ___________________________
Medical Record #: ___________________________ Invoice #: ___________________________
Place of Service: ___________________________ Date of Service: ___________________________
Type of Service: ___________________________
Auditor’s Name and Telephone Number: ___________________________
Compliance Officer’s Name and Telephone Number: ___________________________

Does this file have a signed NPP acknowledgement? ☐ Yes ☐ No
Is all the PHI (except the patient’s name) on the inside of the chart? ☐ Yes ☐ No
Is the patient’s file properly protected and marked confidential? ☐ Yes ☐ No

If the answer to any of the above questions was No, complete the following.
Non-Compliance resulted from: ______________________________________________________
________________________________________________________________________________
________________________________________________________________________________
People Contacted: ___________________________________________
________________________________________________________________________________
What was discussed? ___________________________________________
________________________________________________________________________________
7. Business Associate Agreements

The Privacy Rule requires that you obtain satisfactory assurances from your business associate that they will appropriately safeguard the PHI it receives or creates on behalf of your office. The satisfactory assurances must be in writing in the form of a contract or other agreement between yourself and the business associate.
Who are Business Associates?

- Examples are billing companies, consultants, auditors, clearing house, attorney, collection agency, document shredders, answering service, contractors, software vendor, offsite record storage.
HIPAA Omnibus Rule - BAA

- You MUST review your relationships and determine if a BAA is needed
- Does your associate create, receive, maintain, store, or transmit PHI on your behalf?
SAMPLE BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "Agreement") is made and entered into effective as of ______________ [DATE], by and between [NAME OF PRACTICE] ("Client"), and [NAME OF BUSINESS] ("Business Associate"). The Business Associate shall perform Audit functions or activities on behalf of Client involving use and/or disclosure of PHI. The Business Associate, therefore, agrees to the following terms and conditions set forth in this HIPAA Agreement.

DEFINITIONS

Terms used in this Agreement that are specifically defined in HIPAA shall have the same meaning as set forth in HIPAA. A change to HIPAA which modifies any defined HIPAA term, or which alters the regulatory citation for the definition shall be deemed incorporated into this Agreement.

"Business Associate" shall mean the entity described above. Where the term "business associate" appears without an initial capital letter, it shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR § 160.103.

"Client" shall mean [NAME OF PRACTICE].

"Data Aggregation" shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR § 164.501.

"Designated Record Set" shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR §164.501.

"Electronic Protected Health Information" and/or "EPHI" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, and shall include, without limitation, any EPHI provided by Client or created or received by Business Associate on behalf of Client.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and any amendments hereto.

"HITECH" means the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.

"Individual" shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR § 160.103. It shall also include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

"Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information, and Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule"), that are codified at 45 CFR parts 160 and 164, Subparts A, C, and E and any other applicable provision of HIPAA, and any amendments thereto, including HITECH.

"Protected Health Information" and/or "PHI" shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR § 160.103.
HIPAA Omnibus Rule - BAA

• You no longer have to report failures of your BAs
• BAs are DIRECTLY liable for these violations
• BAs are responsible for their subcontractors
• BAs MUST comply with Security and Breach Notification rules
• YOU ARE RESPONSIBLE FOR THE AGREEMENT!!
7 Steps to Achieve Security Compliance

1. Appoint a Security Officer
2. Establish Policy for Protecting Electronic Systems
3. Maintain a list of Inventory
4. Conduct a Security Risk Analysis
5. Implement Proper Annual Training
6. Establish Usernames and Passwords
7. Monitor ongoing security processes
BREACH NOTIFICATION CHECKLIST

Timing

___ Discovery date recorded: ____________________________
___ Deadline for notifications (60 days post-discovery): ______________________
___ Law enforcement determination of notification delay (based on hindering criminal investigation or causing damage to national security); if so:
   ___ Documentation of determination
   ___ Extended deadline for notifications: ______________________

Identification Of Breach Data

___ Includes PHI: Y/N
___ PHI is encrypted/unencrypted/both/undetermined
___ Affected individuals have been identified

Determination of Urgency

___ Decision re: danger of imminent misuse of PHI/PHR data (if so, document decision and escalate notification procedures.)

Notice

___ Individual notice prepared, containing:
   ___ Brief description of what happened, date of breach, and date of discovery
   ___ Description of types of unsecured PHI involved (e.g., name, SSN, DOB, home address, account number, etc.)
   ___ Steps individuals should take for protection
   ___ Brief description of what we are doing to investigate the breach, mitigate losses, and protect against further breaches
   ___ Contact information for queries and to learn additional information, including toll-free number.
# HIPAA Risk Analysis Data Collection

This office utilized the following to collect data concerning what ePHI we house for our Risk Analysis:

<table>
<thead>
<tr>
<th>INFORMATION SYSTEM</th>
<th>STEP TAKEN TO OBTAIN INFORMATION</th>
<th>DATA COLLECTED</th>
<th>PERSON WHO COLLECTED DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practice Email</td>
<td>Asked all staff about email use for ePHI transmitting</td>
<td>Sample: email is sometimes used to send ePHI to patients. Job Titles that use email: Office Manager, Provider, Front Desk, Billing. Technical controls: email passwords/office manager keeps list. Non-technical controls: employee training on appropriate use.</td>
<td>Sally Sue Office manager</td>
</tr>
</tbody>
</table>

Compliance
### Risk Analysis Worksheet

<table>
<thead>
<tr>
<th>POTENTIAL RISK THREAT/ VULNERABILITY</th>
<th>CURRENT MEASURES</th>
<th>LIKELIHOOD</th>
<th>IMPACT</th>
<th>RISK LEVEL</th>
<th>NEW MEASURES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>LO-MED-HI</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Natural Threats**
1. Earthquakes
2. Landslides
3. Storm Damage (ice, snow, floods)
4. Tornadoes, hurricanes

**Environmental Threats**
5. Fire and smoke contamination
6. Building collapse or explosion
7. Power (blackouts, spikes, surges)
8. Utility problems (HVAC)
9. Broken or leaking water, sewer, or natural gas lines
10. Toxic materials release
11. Contagious disease epidemic
<table>
<thead>
<tr>
<th>Incident</th>
<th>Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1: Accidental Breach</strong></td>
<td><strong>Warning and Re-Education</strong></td>
</tr>
<tr>
<td>Possible Scenarios:</td>
<td>A verbal warning will be documented in the employee’s file on the disciplinary action form. Mandatory re-education and training will occur for the first offense. Continued offenses will lead to progressive disciplinary action up to and including suspension and termination.</td>
</tr>
<tr>
<td>- Employee does not log off the computer after use</td>
<td></td>
</tr>
<tr>
<td>- Employee faxes the wrong PHI to another practice</td>
<td></td>
</tr>
<tr>
<td>- Employee forgets to get a signed acknowledgement of receipt of the Notice of Privacy Practices</td>
<td></td>
</tr>
<tr>
<td>- Employee emails PHI to the wrong email address</td>
<td></td>
</tr>
</tbody>
</table>

| **Level 2: Intentional Breach Without Harmful or Dishonest Intention** | **Written Warning, Re-Education, and Possible Suspension** |
| Possible Scenarios: | A written warning will be documented in the employee’s file on the disciplinary action form. Mandatory re-education and training will occur for the first offense. Continued offenses will lead to progressive disciplinary action up to and including suspension termination. |
| - Employee views patient records out of curiosity, not necessity | |
| - Employee shares PHI because the information is interesting or gossip-worthy, but not for treatment | |
| - Employee shares computer password | |
| - Employee discusses confidential patient information in an unsecure area | |

| **Level 3: Willful or Intentional Breach with Harmful or Dishonest Intentions** | **Termination** |
| Possible Scenarios: | A disciplinary action form will be completed, termination will occur, along with possible referral to law enforcement. |
| - Using PHI for personal gain, such as marketing without an authorization | |
| - Using PHI to cause harm, such as exposing information to unauthorized individuals out of spite or dislike of the owner of the PHI. | |
| - Gives access to a restricted area to an unauthorized individual | |
| - Gives access to PHI to an unauthorized individual | |
Breach Reporting

Breaches Affecting Fewer than 500 Individuals

- If a breach of unsecured protected health information affects fewer than 500 individuals, a covered entity must notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered. (A covered entity is not required to wait until the end of the calendar year to report breaches affecting fewer than 500 individuals; a covered entity may report such breaches at the time they are discovered.) The covered entity may report all of its breaches affecting fewer than 500 individuals on one date, but the covered entity must complete a separate notice for each breach incident. The covered entity must submit the notice electronically by clicking on the link below and completing all of the fields of the breach notification form.

Breaches Affecting 500 or More Individuals

If a breach of unsecured protected health information affects 500 or more individuals, a covered entity must notify the Secretary of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. The covered entity must submit the notice electronically by clicking on the link below and completing all of the required fields of the breach notification form.

Notice to the Secretary of HHS
Breach of Unsecured Protected Health Information

This site is available as we continuously work to make improvements to better serve the public. Should you email scprvacy@hhs.gov or call us toll-free: (800) 368-1019, TDD toll-free: (800) 537-7697.

To file a breach report, please enter information in the wizard pages below. A field with an asterisk (*) before it is required.

---

General: Please supply the required general information for the breach.

* Report Type: What type of breach report are you filing?  
  - Initial Breach Report
  - Addendum
Section 1557

Section 1557 is the civil rights provision of the Affordable Care Act and prohibits discrimination on the basis of race, color, national origin, sex, age, or disability under “any health program or activity, any part of which is receiving Federal financial assistance ... or under any program or activity that is administered by an Executive agency or any entity established under [Title I of the Affordable Care Act].”12
Phase 2 Auditing Has Three Rounds

- OCR announced their “official” launch of the Phase 2 HIPAA audit program on March 21, 2016
- First round will be desk audits of covered entities
- Second round will be desk audits of business associates
- Third round will be on-site audits
Covered Entities

Every covered entity and business associate is eligible for an audit. This includes:

- individual providers
- organizational providers
- health plans
- clearinghouses
- business associates of these entities
What Are They Looking For?

- OCR will review the policies and procedures adopted and employed by covered entities and their business associates.
- Must meet standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.
How Will Auditees Be Notified?

• Email or USPS Mail: 2016 audit process will start with a simple email attempting to verify your address and contact information. An email is being sent to covered entities and business associates requesting that contact information be provided to OCR in a timely manner.
Search your email for something from

• OSOCRAudit@hhs.gov
Unfavorable Findings

• Should an audit report indicate a serious compliance issue, OCR may initiate a compliance review to further investigate.
Do You Feel Prepared For a HIPAA Audit Right Now?

Let’s Take a Poll
Audit Protocol — Updated April 2016

The Phase 2 HIPAA Audit Program reviews the policies and procedures adopted and employed by covered entities and business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These analyses are conducted using a comprehensive audit protocol that has been updated to reflect the Omnibus Final Rule. The audit protocol is organized by Rule and regulatory provision and addresses separately the elements of privacy, security, and breach notification. The audits performed assess entity compliance with selected requirements and may vary based on the type of covered entity or business associate selected for review. You may submit feedback about the audit protocol to OCR at OSOCRaudit@hhs.gov.

The protocol is available for public review and searchable by keyword(s) in the table below; export options will be made available soon.
<table>
<thead>
<tr>
<th>Audit Type</th>
<th>Section</th>
<th>Key Activity</th>
<th>Established Performance Criteria</th>
<th>Audit Inquiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>§164.520(c)(2)</td>
<td>Provisions of Notice - Certain Covered Health Care Providers</td>
<td>§164.520(c)(2) Specific requirements for certain covered health care providers. A covered health care provider that has a direct treatment relationship with an individual must: (i) Provide the notice: (A) No later than the date of the first service delivery, including service</td>
<td>Does a covered health care provider with direct treatment relationships with individuals provide its notice of privacy practices consistent with the established</td>
</tr>
</tbody>
</table>
HIPAA DENIAL

• HIPAA is something I can get to when I’m not busy...
• I did my HIPAA-thing in 2013, I’m all set.
• No one is REALLY going to check my program
• I’m a small provider
• HIPAA is too complicated, “they” don’t expect me to do this
Know Your State Laws

If your state privacy and confidentiality laws are more stringent than HIPAA laws, you must comply to which has the highest level of protection.
HIPAA Omnibus Rule - Vigorous Enforcement

- Unaware of violation - $100 to $50,000
- Reasonable cause violation - $1,000 to $50,000
- Willful neglect - $10,000 to $50,000
- Willful neglect - $50,000 to $1.5 million
- Multiple HIPAA violations - surpass $1.5 million.
HHS Settles with Health Plan in Photocopier Breach Case

Under a settlement with the U.S. Department of Health and Human Services (HHS), Affinity Health Plan, Inc. will settle potential violations of the HIPAA Privacy and Security Rules for $1,215,780. OCR’s investigation indicated that Affinity impermissibly disclosed the protected health information of up to 344,579 individuals when it returned multiple photocopiers to a leasing agent without erasing the data contained on the copier hard drives. In addition, the investigation revealed that Affinity failed to incorporate the electronic protected health information stored in copier’s hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the hard drives to its leasing agents.
Record Retention

• HIPAA related documents are retained for 6 years.
• Applies to authorizations, audit records, CA agreements, and contracts.
Where Are You with HIPAA?

• Initial development of program
• Initial program installed prior to 2009 (Hi-tech)
• Program installed, updated for Hi-tech, but needs to be updated for omnibus
• Completely up to date!
HIPAA is a Process...Not an Event

• Implementation requires commitment
• Ask for Help
• Realize it’s a Program, not just a Document
• Update what you have in place to meet the latest requirements
• Remember HIPAA also stands for: **Helping Increase Paperwork Across America!**
if you're making mistakes it means you're out there doing something

Neil Gaiman
Questions?
info@kmcuniversity.com