Protect Your Practice with Innovative Risk Management Techniques updated with HIPAA Hi-Tech Act and Omnibus Rule

Presented by:
Abbie Miller, MCS-P

Abbie Miller, MCS-P

• 16 years experience in a Chiropractic Office
• Medical Compliance Specialist for Physicians Certification
• Practice Performance Analyst
• Medicare Enrollment Specialist

First Line of Defense = Your Team

Five ways your Team can help
Reduce your Risk (and why you want them to)

• Audit Charges and Documentation on a Daily or Per Visit Basis
• Confidently Respond to Record Requests
• Recognize/Avoid HIPAA mistakes
• Write Office Policies to govern your actions
• Compile a Written Procedure Manual to make certain things get done properly

Ongoing Internal Auditing

Documentation Reviews

• Are all entries dated, timed and signed with names printed after the signature?
• Are the patient’s details recorded clearly on each page?
• Do note entries make reference to specific care plans?
• Are non-registered staff entries countersigned?

• Are all entries free of subjective opinion, jargon, abbreviation and offensive comments?
• Are any alterations or deletions initialed and still legible?
• Are all care plans in place and dated at the time of writing?
Be Prepared: Know What They Look For

- Signature may sink your ship UP FRONT
- Review your records as they do
- When records are missing important information, address it up front

Three Big Things

- Is this visit part of an episode of care?
  - If so, when did it start?
  - If so, what visit number is this?
  - If so, acute or chronic?
- What is the most recent exam for this visit?
- What diagnosis/plan goes with this visit?

Set Up a System

- Designate a frequency
- Coordinate with billing day
- Find a way to randomize
- “Pick a number!”
- Pre-billing audit
- Monthly compliance officer duties

Why Bother to Self-Audit?

- Self-audit can improve standards of documentation considerably and increase doctor and team member’s knowledge and confidence
- Self-auditing is used as a continuous improvement incentive for all clinical staff
- Self-audit can deliver an improvement in practice at no extra cost

Responding to Records Requests

- Does your documentation tell a believable clinical story that makes sense as to why you are still treating and why you should get paid?

Lack of Medical Necessity
Why Denials Occur

- Administrative
  - Incorrect ID number
  - Incorrect vital information of primary holder, patient, etc.
- Unsupported code
  - Therapy codes
  - Exam codes
- Medical necessity isn’t supported

What if Info is Missing?

- Don’t try to cram it in after the fact
- Summarize with a cover sheet style “Case Summary”
- Explain the detail that might have been left out
- Hope that they will add it to the record as an addendum, dated by you

How to Use a Case Summary

- Don’t try to cram it in after the fact
- Summarize with a cover sheet style “Case Summary”
- Explain the detail that might have been left out
- Hope that they will add it to the record as an addendum, dated by you

Avoiding HIPAA Privacy mistakes

Minimum Necessary Standard

- The minimum necessary standard requires you to evaluate your practices and enhance any safeguards as needed to avoid and limit unnecessary or inappropriate access to and disclosure of PHI.
Write HIPAA Policies & Procedures

Incidental Uses and Disclosures

- Unintentional
- Overhead phone conversations when answered at the front desk.
- A patient passing by another room where treatment is taking place
- Everyday operations

Accidental Disclosures

- Faxing or emailing PHI to the wrong destination
- Disclosing PHI to an unauthorized person
- If harmful, must be disclosed to the patient.
- Always included on non-TPO disclosure log

Emails

This email, including any attachments, may include PRIVILEGED AND CONFIDENTIAL information and may be used only by the person or entity to which it is addressed. If the reader of this email is not the intended recipient, or his or her authorized agent, the reader is hereby notified that any dissemination, distribution, or copying of this email is prohibited. If you have received this email in error, please notify the sender by replying to this message, and delete this email immediately.

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.
Write HIPAA Policies & Procedures

Marketing

- Encouragement of purchase of product or service that is not for treatment purposes
- Part of a treatment plan is ok...such as information on asthma if that is the DX on file
- Face to face ok: Product of the month

Write HIPAA Policies & Procedures

Use of Photographs

- Permitted but must be out of public view
- As part of a testimonial or other marketing effort, you must have authorization
- Can include in electronic or paper form

Write HIPAA Policies & Procedures

What’s OK?

- Sign in sheets: minimal information—name, time, etc.
- Verification of Callers: PHI over phone—Password, SSN, DOB, Zip, Maiden Name
- Social Security Number: use sparingly, or last four digits only

Write HIPAA Policies & Procedures

Phone Messages/ Appt. Reminders

- Reminders are good
- Postcards are ok
- Answering machines are ok
- Do not leave PHI on the call, or results of test
- OK to say that you are reminding of an appointment and date/time
- Should include that information in the NPP

Write HIPAA Policies & Procedures

More Common Sense

- Not required:—Private rooms—Soundproof rooms—Wireless encryption—Encrypted telephones
- A good idea:—Have patients wait a few steps back from counter—Curtains or screens—Speaking quietly—Files turned backward—Folders marked confidential—All faxes/email that contain PHI marked confidential—Fax machines secure locations

7 Steps to Achieve Privacy Compliance

1. Install 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. Train Your Team Members
6. Monitor Your Active Privacy Program
7. Business Associate Agreements In Place
Purpose of HIPAA Security

- Protect ePHI (Electronic Protected Health Information)
- Confidentiality
- Integrity
- Availability

Step 2: Understanding the Rules: Types of Safeguards

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

7 Steps to Achieve Security Compliance

1. Install a Security Officer
2. Understand the rules
3. Make a list of ePHI
4. Conduct a Risk Analysis
5. Implement policies & procedures
6. Deliver security awareness training
7. Monitor ongoing security processes

Timeline

- HIPAA - 1996
- HITECH - 2009
- OMNIBUS - 2013

HITECH Expansion

- Reach
  - Before: Covered Entities: healthcare organizations
  - Now: Covered Entities: expanded to business associates

HITECH Expansion

- Notification
  - Before: Loose notification requirements
  - Now: Strict notification requirements – 60 days requirement + public notice on website (and notifying HHS)
HITECH Expansion

- **Economics**
  - **Before:** 2003-2008 – 31,000 cases reported, no one fined; 
    - In 2009, CVS fined $2.25 M; Daily fine: $100/day
  - **Now:** Fines up to $1.5 M/year; regulators at HHS now benefit directly from fines levied — Daily fine: $50,000/day

HITECH Act

- Further expands the businesses covered by HIPAA Privacy and Security Rules by beefing up BA agreements
- Requires all to comply with new security breach notification rules
- Enhances penalties that can be handed down, and increases enforcement

Omnibus Final Rule

March 26, 2013
September 23, 2013

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.

Omnibus: Three Main Focuses

- Privacy, Security, and Breach Notification policies and procedures
- Notice of Privacy Practices
- Business Associate Agreements
**HIPAA Omnibus Rule - Breach**

- Redefines Breach
- Harder to avoid reporting a breach
- Redefines: “significant risk of financial, reputational, or other harm”

**HIPAA Omnibus Rule - Breach**

- Breaches presumed reportable unless after performing a risk assessment (applying four factors) it is determined there is “a low probability of PHI compromise”

**HIPAA Omnibus Rule - Breach**

1) Nature and extent of the PHI involved
   - Sensitivity of the information from a financial or clinical prospective
   - Likelihood the information can be re-identified

2) Who obtained the unauthorized access
   - Does this person have an independent obligation to protect the confidentiality of the information?

**HIPAA Omnibus Rule - Breach**

3) Whether the PHI was actually acquired or accessed
   - Was the exposed PHI actually accessed by anyone who may have had the ability to access or acquire

4) The extent to which the risk has been mitigated
   - Getting a signed confidentiality agreement from the recipient

**HIPAA Omnibus Rule - Breach**

- No need for independent entity to conduct risk assessment
- No need to conduct assessment if notification is made
- Take steps to reduce risks in future
- Must still adhere to requirements for individual notification, HHS notification, and media posting where applicable

**HIPAA Omnibus Rule - Disclosures**

At the patients request, you may NOT disclose information to a patient’s health plan if they have paid out of pocket for their care.
HIPAA Omnibus Rule - Marketing

- New rules limit circumstances when you can provide marketing communication to your patients WITHOUT written authorization

  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 provide access to EHR and other electronic records in electronic form of patient requests
- "readily reproducible"
- Otherwise, must be in another mutually agreed upon electronic format
- Hard copies only ok when individual refuses all e-formats

HIPAA Omnibus Rule - Copies

- Must provide access to EHR and other electronic records in electronic form of patient requests
- "readily reproducible"
- Otherwise, must be in another mutually agreed upon electronic format
- Hard copies only ok when individual refuses all e-formats

HIPAA Omnibus Rule - Copies

- New rule modified the costs that may be charged to the patient for copies
  - include labor costs
  - supply costs if the patient requests a paper copy
  - if electronic, the cost of any portable media (such as a USB memory stick or a CD)
- Must follow state law if a lower reimbursement rate is set.

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 - NPP

- NPP must be update NPP
- Include:
  - New breach notification guidelines
  - Updated patient rights concerning disclosures to health plans
  - Marketing using PHI

HIPAA Omnibus Rule - NPP

- Post revised NPP
- Make copies available
  - All new patients
  - Anyone who requests
- Post new NPP to website

HIPAA Omnibus Rule - NPP

- Post revised NPP
- Make copies available
  - All new patients
  - Anyone who requests
- Post new NPP to website

HIPAA Omnibus Rule - NPP

- Post revised NPP
- Make copies available
  - All new patients
  - Anyone who requests
- Post new NPP to website
Acknowledgement (Notice of Privacy Practices)

- Must make a good faith attempt to obtain a written acknowledgement that they have received a copy of your NPP.

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?

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 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!!

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.
**HIPAA Omnibus Rule - BAA**

- You have until Sept 23, 2014 to bring all BAA up to date and in conformance with new rules.
- Agreements in place prior to March 26, 2013 remain compliant until renewed or modified or Sept 23, 2014

**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

**New Rules – Game Changer?!**

“This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented,” said HHS Office for Civil Rights Director Leon Rodriguez. “These changes not only greatly enhance a patient’s privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates.”

**Does Enforcement Happen?**

Massachusetts provider settles HIPAA case for $1.5 million

Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (collectively referred to as “MEEI”) has agreed to pay the U.S. Department of Health and Human Services (HHS) $1.5 million to settle potential violations of the HIPAA Privacy and Security Rules. MEEI has also agreed to take corrective action to improve policies and procedures to safeguard the privacy and security of their patients’ protected health information and retain an independent monitor to report on MEEI’s compliance efforts. OCR’s investigation followed a breach report submitted by MEEI, as required by the HIPAA Breach Notification Rule.

**Does Enforcement Happen?**

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.
Take The Time
An active HIPAA Program is worth the effort!

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!

Record Retention

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

Train Your Team Members

• Ongoing training required, updates
• Access PHI on “need to know” basis
• Keep employment records separate from treatment records
• Fully explain sanctions for failure to comply.
Why do We Need to Write Policy

What Exactly is Policy

• Policy: This is how we do things here, and why we do them.

An Example of Policy

Sample Policy: Physician Education Policy

PURPOSE:
The purpose of physician and other practitioner education is to ensure all providers understand and comply with federal and state laws, statutes and regulations applicable to the delivery of health care in a clinical environment.

POLICY:
Physicians and other practitioners are required to attend all agreed upon and scheduled educational programs designed for providers. Education will be conducted subsequent to medical record audit activity and with a frequency to meet the needs of the provider. Provider compliance education will be conducted at least annually.

Why You Should Have a Standard Operating Procedure

What is SOP?

• SOP means Standard Operating Procedure
• This is the “way it is done”
• How we implement the policy we have decided upon
• No corporation operates without this for each position or job in the company
• Why do we try to do without?

Physical SOP Manual

• Define where your Physical SOP Manual is housed
• Decide who is responsible for each section of your SOP manual
• Define who will bring it to your team meetings
The KMCU SOP Flowchart

1. The person who performs the procedure writes out each steps as the steps are performed
2. Follow your own instructions the next time you perform this activity to verify the accuracy
3. Have another team member perform your duties while following your written instructions
4. Correct and clarify any areas of confusion, and re-test instructions, if needed
5. For ease of use, use lots of pictures, and illustrations and computer screenshots
6. For accuracy with repetitive processes an actual checklist is preferred
Team Meeting Accountability

- A regular part of your weekly team meeting should be a check-in on SOP Progress from each member of the team
- Everyone on the team is assigned a specific SOP to complete and a “by when.”
- Progress is reported weekly

Strategies for Better Defense

- Make a list of areas that are potential weaknesses and create policies/procedures
- Delegate and empower to share the work load among all members
- Train often and use a Training Log
- Operate under the “team functions better together” mentality. You’re all responsible for protecting the practice together!

Hold Regular Team Trainings

- Training together as a team helps build bonds
- Gain a shared understanding with unique strategies
- New ideas refresh energy in the practice
- Learn how to better serve patients

Need Help?

info@kmcuniversity.com