HIPAA Hiccups:
Common Misconceptions

Hays Companies
Spring 2018

Nicholas G. Karls
Associate Director of Research and Compliance
Hays Companies
nkarls@haysccompanies.com

Disclaimer

This presentation is provided for general information purposes only and should not be considered legal or tax advice or legal or tax opinion on any specific facts or circumstances. Readers and participants are urged to consult their legal counsel and tax advisor concerning any legal or tax questions that may arise. Any tax advice contained in this communication (including any attachments) is not intended to be used, and cannot be used, for purposes of (i) avoiding penalties imposed under the U. S. Internal Revenue Code or (ii) promoting, marketing or recommending to another person any tax-related matter.

First: Two Definitions

Covered Entity

Covered Entity (“CE”):

- Health Care Clearing Houses
- Health Care Providers
- Health Plans
  - Medical (includes Rx)
  - Dental, EAPs, and Vision
  - Health care flexible spending accounts (FSA)
  - Health reimbursement arrangements (HRA)

The employer is not a covered entity

- The employer-sponsored health plan is typically a covered entity

Protected Health Information

Protected Health Information (“PHI”):

- Health information

  +

- Individually identifiable

  +

- That is used or disclosed by a covered entity

  =

- Protected health information (PHI)

- If in electronic format = EPHI

Not All HI is PHI

Protected Health Information

What health information is not considered Protected Health Information?

- Employment records
- FMLA leave determination
- ADA reasonable accommodation
- Drug testing - Pre-employment physicals
- Life Insurance – Disability Insurance Information
- Educational records
- Worker's Compensation Records

Even if not regulated under HIPAA, protecting health information and confidential information is always a good idea & other laws may prohibit use and disclosure of this data

Policies and Procedures

HIPAA Policies and Procedures

"What do your policies and procedures say?"

- "Well, we have this Notice of Privacy Practices….."

The Notice of Privacy Practices (NPP) is not the same thing as formally adopted policies and procedures

- The NPP is a component of the policies and procedures

HIPAA Policies and Procedures

What does HIPAA require?

From 45 CFR §164.530(i)(1):

- A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. *The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity*, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

HIPAA Policies and Procedures

What does “reasonably designed” mean?

- It means that you must do an in-depth analysis of your activities as a plan sponsor to figure out the nature and extent of your interaction with Protected Health Information (PHI)
  - We use different interactive resources to help employers accomplish this analysis
  - Because there isn’t a one-size-fits-all solution, using sample documents without guidance is a rough route to go

Not Having Policies and Procedures for FSAs, HRAs, and Wellness Plans

FSAs, HRAs, Wellness

FSAs, HRAs, and Wellness plans are almost always treated like self-insured health plans

- Self-insured health plans have heightened obligations under HIPAA Privacy and Security
  - Exception for self-administered health FSA if there are less than 50 participants
- The plan has the authority to self-administer the plan
- Consistent issue for fully-insured employers with FSAs

Required Training

Required Training

This presentation does not count

45 CFR §164.530(b) states:

- A covered entity must train all members of its workforce *on the policies and procedures* with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

In other words, the training is based on your policies and procedures and not just on what HIPAA is and what it requires

Required Training

The final rules do not prescribe exact content for the training, but the preamble does state that recognizing and reporting HIPAA violations should be a part of the training

The timing for the training is as follows:

- Train applicable employees by the Covered Entity's compliance date
- Train new employees that require the training within a reasonable amount of time
- If there's a material change to policies and procedures, retrain within a reasonable amount of time

Document that the training was provided

Incident or a Breach?

Incident or a Breach?

Not every incident is a breach

- Breach: An unauthorized acquisition, access, use or disclosure of Protected Health Information (PHI) that compromises the information's security or privacy in a manner not permitted under the privacy rule

Incident or a Breach?

Determining whether a breach occurred requires a risk assessment:

1. The nature and extent of the PHI involved
2. Was unsecured PHI involved?
   - Secured PHI
     - PHI that is rendered Unreadable, Unusable or Indecipherable
     - Encryption or destruction
     - Encrypted electronic PHI does not require a risk assessment or breach notification
   - Unsecured PHI
     - PHI that is not secured by using a technology or methodology specified by HHS
     - Unsecured PHI is presumed to be compromised
3. The unauthorized person who used the PHI or to whom the PHI was disclosed, whether the PHI was actually acquired or viewed, and
4. The extent to which the risk to PHI has been mitigated

Incident or a Breach?

Not a breach if one of the following exceptions apply:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted…

- In layman's terms: Someone authorized in the HIPAA policies and procedures to work with PHI accidentally comes across PHI that they shouldn’t have and they don’t misuse that information

Incident or a Breach?

Not a breach if one of the following exceptions apply:

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted…

- In layman's terms: Someone authorized in the HIPAA policies and procedures to work with PHI accidentally discloses information to another authorized individual and they don’t misuse that information

Incident or a Breach?

Not a breach if one of the following exceptions apply:

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information…

- In layman's terms: there was no way for the information to be compromised (returned mail)

Not Using the Minimum Necessary

Minimum Necessary

The devil is in sending too many details

45 CFR §164.502(b)(1) states:

- When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Minimum Necessary

Before disclosing or using PHI, ask yourself, is all of this information absolutely required to accomplish the goals of the health plan?

- A common scenario: “John Doe from production is questioning whether our health plan really excludes liposuction. As you can see from the report sent over by BCBS, he went to an out-of-network provider last month and had his belly lipo-ed….”
- What additional information was in that BCBS report?
- How about: “Does our plan exclude liposuction? Are there situations where it may be covered?”

Thank You!