Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA Policy, Protection, and Pitfalls

Overview

- HIPAA Privacy Basics
  - What's covered by HIPAA privacy rules, and what isn't?
- Interlude on the "Hands-Off" Group Health Plan
  - When does this exception apply, when doesn't it apply, and what does it mean?
- Policies and Procedures
  - What do you have to have in place?
- Why does HIPAA matter?
  - Audits and potential penalties

HIPAA Privacy Basics

HIPAA Privacy Basics

- The Privacy Regulations were passed as part of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
- The Privacy Regulations require **"Covered Entities"** and **"Business Associates"** to follow certain rules when handling and securing certain health information called **"Protected Health Information"** (or "PHI")

HIPAA Privacy Basics

- **"Covered Entities"** are:
  - Health Care Clearinghouses
    - Convert paper medical claims into electronic claims
  - **"Health Plans"**
    - Provide or pay for cost of medical care
  - Health Care Providers
    - Furnish medical or health services or supplies

HIPAA Privacy Basics

- **"Health Plans"** include:
  - Group medical plans
  - HMOs
  - Insurers
  - Dental plans
  - Vision plans
  - Long term care policies
  - Health flexible spending arrangements
  - Most EAPs

HIPAA Privacy Basics

- HIPAA does **not** apply to:
  - Workers' Compensation
  - Life Insurance
  - Short Term Disability
  - Long Term Disability
  - AD&D
  - Business Travel Accident

HIPAA Privacy Basics

- **"Protected Health Information" ("PHI")** is:
  - Individually identifiable health information AND
  - Created or received by a Covered Entity (the plan) AND
  - Relates to
    - The past, present, or future physical or mental health of an individual; OR
    - The provision or payment for health care for an individual
- Applies to information in any format:
  - Paper
  - Electronic
  - Oral

HIPAA Privacy Basics

Individual Identifiers

- Social Security Number
- Medical record number
- Account and health plan beneficiary numbers
- Certificate, license numbers
- Vehicle ID or plate number
- URL or IP addresses
- Device identifiers
- Biometric identifiers
- Full face or comparable images
- Names
- Geographic units
- Dates
  - Month/day relating to any individual, including birth, treatment
- Ages over 89
- Phone, fax numbers
- E-mail addresses
- Any other unique identifiers

HIPAA Privacy Basics

- Examples of PHI:
  - List of member names, social security numbers and aggregate claim dollar amount
  - Enrollment information (once in the hands of the health plan)
  - E-mail with claim information for a specific member
  - List of members choosing COBRA coverage

HIPAA Privacy Basics

- Examples of information that is **not** PHI:
  - Enrollment information in the hands of the *employer*
  - Information kept to carry out employer's obligations under:
    - The Family & Medical Leave Act
    - The Americans with Disabilities Act
    - Similar laws
  - Records regarding:
    - Occupational injuries
    - Disability insurance eligibility
    - Fitness-for-duty exams

HIPAA Privacy Basics

- A **"Business Associate"** is:
  - A person who, on behalf of a covered entity **such as a health plan**
    - Uses/accesses/re-discloses PHI either:
      - To perform or assist in the performance of a plan function OR
      - To provide services to a Covered Entity
    - Examples:
      - **TPA (includes carriers acting as TPA)**
      - **Broker, consultant, attorney, accountant, other professionals**
      - **PBM, care management organization, EAP**
  - Covered Entities (the plan) must have Business Associate Agreements in place with Business Associates

HIPAA Privacy Basics

- Case scenarios:
  - Birth announcement
  - First responders who are employees of the employer treat an employee injured on the job
  - Employer wants to clarify something in a doctor's FMLA certification
  - Report from dental carrier about high dollar claims under the plan
  - Co-workers want to send flowers to employee with appendicitis

“Hands-Off” Group Health Plans

Limited Exception For Hands-Off Group Health Plans

- IF the group health plan is fully-insured
- AND the group health plan does not create or receive PHI except for:
  - Summary Health Information; and
  - Enrollment Information
- THEN the group health plan is not required to comply with various HIPAA privacy requirements
- The insurer or HMO remains subject to these privacy requirements

Limited Exception For Hands-Off Group Health Plans

- Hands-off plan sponsors are not required to do the following key tasks (among others):
  - Designate a privacy official
  - Train workforce members on HIPAA compliance
  - Create privacy safeguards
  - Create complaint procedures
  - Create HIPAA policies and procedures
  - Distribute a notice of privacy practices

What Can the Hands-Off Plan Sponsor Still Do?

- Assist employees with claim disputes
  - Must have authorization to receive PHI
- Help employees understand the plan
- Process enrollment, including payroll deductions
- Receive summary health information for certain purposes:
  - Obtaining premium bids
  - Modifying, amending, or terminating the plan

What If…

- What if the employer has a fully-insured group health plan, but also has a self-funded health FSA?
- What if the employer engages a third party that receives only summary health information and enrollment information for the purpose of getting pricing information and bids?
- What if the employer engages a third party that receives PHI besides summary health information and enrollment information?

HIPAA Policies and Procedures

HIPAA Policies and Procedures

- Your policies and procedures must address the following key topics (among others):
  - Use and disclosure of PHI
  - Individual Rights
  - Protecting PHI
  - Destruction of PHI
  - Transmission of PHI
  - Breach notification
  - Designation of Privacy Official

Use and Disclosure of PHI

- The Privacy Regulations create categories of uses and disclosures of PHI:
  - Required
  - Permissive
- Your HIPAA policies and procedures must address these rules

Use and Disclosure of PHI

- Required Disclosures
  - To individuals who request:
    - Access (inspection and copying of) his or her **own** PHI
      - Follow procedures, keep records
      - A note about family and friends
    - Accounting of disclosures of his or her **own** PHI
      - Plan is required to keep accounting of certain disclosures
  - To Department of Health and Human Services ("HHS")
    - Only to determine if a Covered Entity (e.g., a health plan) is in compliance with the Privacy Regulations

Use and Disclosure of PHI

- Permissive Disclosures
  - For Treatment, Payment, or Health Care Operations (TPO!)
    - Determining eligibility, coverage, contribution amounts
    - Coordination of benefits
    - Claims administration
    - Billing, resolving payment disputes, responding to customer inquiries about payments
    - Reviewing for medical necessity
    - Pre-certification review
    - Underwriting, other activities relating to renewal
    - Plan business planning and development
    - Plan customer services
  - "Minimum necessary" standard

Use and Disclosure of PHI

- Based on an authorization (if the "required" and "permissive" don't apply) . . .
  - Use form, follow procedures, keep documentation
  - Parent requests
    - Minor child –parent has right to child's PHI without authorization from minor child
    - Adult child—parent does NOT have right to adult child's PHI without authorization from adult child
  - Requests by authorized personal representatives
    - Don't be shy about asking for paperwork to prove authorized status

Use and Disclosure of PHI

- Request Made by Person Involved in Individual's Care
  - Must be family member, close personal friend, or other person identified by individual as being involved in care
  - If individual is present, use or disclose if:
    - The individual agrees;
    - The individual has an opportunity to object and does not object; or
    - You can infer individual does not object
  - If individual not present:
    - May disclose if in individual's best interests
      - e.g., in the case of emergency
      - e.g., individual is incapacitated and a spouse calls seeking assistance with payment of claims for the incapacitated individual

Use and Disclosure of PHI

- For Non-Health Plan Purposes
  - Individual authorization required
- Disclosure to Business Associate
  - Confirm Business Associate Agreement in place
- Disclosures for Legal and Public Policy Purposes
  - E.g., victims of abuse, neglect, domestic violence, judicial proceedings, law enforcement, etc.

Individual Rights

- Access (Inspection and Copying)*
- Accounting of Disclosures of PHI*
- Amendment or Correction of own PHI
- Confidential Communications
- Restriction on Use and Disclosure of own PHI

*previously addressed in this presentation

Individual Rights

- Notice of Privacy Practices
  - Contains uses and disclosures of individual rights as to PHI
  - Timing of distribution
    - Initial enrollment
    - Within 60 days of material change to notice
    - Tri-annual notice reminder requirement
  - Method of distribution
    - If company has an intranet, **must** be posted
    - May be distributed electronically if certain conditions met

Protecting PHI

- Maintain a secure reception area with a receptionist on duty and/or a locked door accessible only to Workforce Members via an electronic card or code mechanism
- Visitors will be escorted to their contact person and not left unattended

Protecting PHI

- All files containing PHI, including CDs and flash drives, are to be kept in a separate file area of human resources or an enclosed room or locked desk where access is limited to those Workforce Members who have access per the terms of the Privacy Policy

Protecting PHI

- Do not leave files, electronic storage media, or documents containing PHI on desktops, countertops, or work tables unattended
- Files or documents containing PHI may be kept at your desk provided that they are not left unattended on your desktop and are kept in locked drawers when not in use

Protecting PHI

- Documents containing PHI should not be left unattended on computers, copiers, fax machines, or printers
- Documents or electronic media containing PHI should not be deposited in trash cans, unsecured recycling bins, or other unsecured containers
  - PHI shall be destroyed in accordance with the Employer's document destruction policy

Protecting PHI

- Where reasonable and appropriate, PHI will be secured through the use of a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals
  - Encryption
  - Destruction
- Files containing PHI shall be clearly labeled as “private and confidential”

Protecting PHI

- Take care when discussing PHI to ensure that PHI is not discussed with any employee, individual, or third party who does not have access under the terms of the Employer's Privacy Policy
- When using the telephone to discuss PHI, take reasonable care to make sure that the party to whom you are speaking should have access to PHI
  - Make sure that you're speaking with either the individual who is the subject matter of the PHI or the individual's personal representative, or an individual designated by a Business Associate, insurance carrier, or a health care provider

Protecting PHI

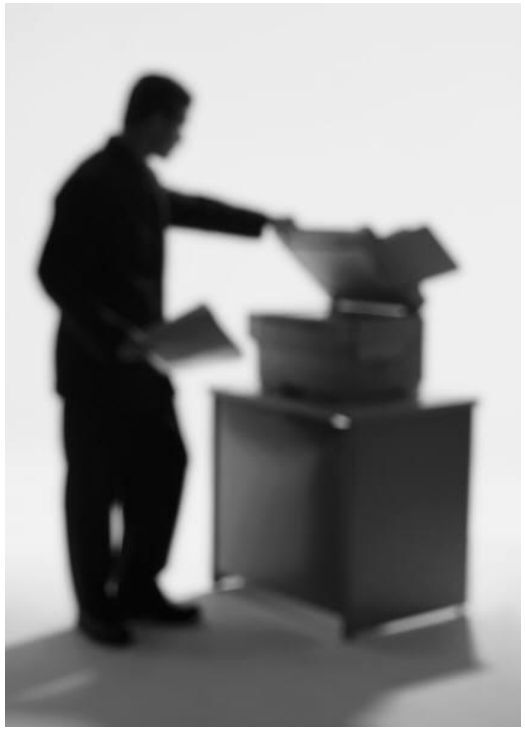
- PHI should not be discussed in public areas such as cubicles, elevators and lunch rooms or at social gatherings (note: it is acceptable for a person to disclose their OWN health information)

Destruction of PHI

- CDs, flash drives, or other electronic media containing PHI must be erased or destroyed
  - Electronic media must be cleared, purged or destroyed consistent with NIST guidelines
- Paper, film, or other hard copy media is to be shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed
  - Redaction is not an appropriate means of data destruction

Destruction of PHI

- Photocopiers with hard drives or other storage of information that are to be discarded or leased machines that are to be returned must have the hard drives erased using NIST standards before being disposed or returned



Transmission of PHI

- Mail
  - Incoming mail should be delivered in original sealed envelope to addressee
  - Outgoing mail should be clearly addressed to a specific person and marked confidential

Transmission of PHI

- E-mail
  - Incoming
    - Request that person sending limit people that are copied
    - Request that no individual identification in the subject line
  - Outgoing
    - File attachments must be password protected
    - No individual identification in subject line

Transmission of PHI

- Faxes
  - Incoming faxes with PHI should be received on a dedicated fax machine
  - Outbound faxes should be sent to a fax machine attended by the specific recipient; call first if necessary
- CD/Flash Drive/Other Electronic Media
  - Same as regular mail

Transmission of PHI

- Internet
  - Secure sites only (e.g., insurance carrier site with password access)
  - Verify appropriate security with service provider such as TPA
  - Confirm that a Business Associate Agreement is in place with the service provider

Notification of Breach

- What is a “breach”?
  - An unauthorized acquisition, access, or use or disclosure of unsecured protected health information in a manner not permitted by the HIPAA Breach regulations which compromises the security or privacy of such information
    - “Unsecured” means that the information was not destroyed or otherwise rendered unusable (e.g., encrypted)
  - Three permitted exceptions

Notification of Breach

Analysis of Breach

- Step 1: Did the incident include secured PHI? *If yes, then no breach.*
- Step 2: Is the acquisition, access, use or disclosure related to the incident permitted *(remember required and permitted uses and disclosure of PHI)* under HIPAA? *If yes, then no breach.*
- Step 3: Does the acquisition, access, use or disclosure related to the incident fit within one of the 3 exceptions? *If yes, then no breach.*
- Step 4: Can the health plan or Business Associate demonstrate there is a "low probability" that the PHI has been "compromised" after doing Risk Assessment? *If yes, then no breach.*

Notification of Breach

- Breach Analysis
  - Risk Assessment factors for Privacy Officer to consider:
    - Nature and extent of PHI involved
    - The unauthorized person who used the PHI or to whom the disclosure was made
    - Whether the PHI was actually acquired or viewed
    - The extent to which risk has been mitigated

Notification of Breach

- Notification of Breach Requirement
  - Breach of "unsecured PHI" (not destroyed or encrypted)
    - Notify each individual affected within 60 days of discovery
      - Generally first class mail
    - Notify HHS (OCR)
      - Immediately if 500+ individuals
      - Keep breach log and file annually if fewer than 500
    - Notify media if 500+ in one state

Why Does HIPAA Matter?

HIPAA Enforcement

- HHS must investigate complaint whenever preliminary review indicates willful neglect
- HHS may investigate in other situations
  - HHS will determine penalty amount on case-by-case basis on factors such as:
    - Nature and extent of violation and resulting harm
    - Number of individuals affected
    - Time period during which violation occurred
    - Size and financial condition of entity
    - Entity's history of compliance (or non-compliance)

HIPAA Enforcement

- HITECH Act authorized HHS to conduct audits
- Audit Pilot Program 2011-2012
  - On-site visits between 3 and 10 business days
  - Focus on achieving compliance
- Pilot Program is over
  - Get ready now for a strict audit program

HIPAA Audits

- What happens during an audit?
  - OCR analyzes processes, controls, and policies of covered entity
  - Key areas: http://ocrnotifications.hhs.gov/hipaa.html
    - NPP
    - Individual rights
    - Administrative safeguards
    - Uses and disclosures
    - Security of electronic PHI
    - Breach notification

HIPAA Audits

- What documents will be requested?
  - General information, organizational chart, identification of privacy officer, identification of PHI access
  - Notice of Privacy Practices
  - HIPAA policies and procedures, including breach protocols
  - Training documentation
  - Security policies, including encryption, access control, security incident management
  - Much, much more!

Top Five Issues in Investigated Cases

- 2013:
  - Impermissible uses & disclosures
  - Safeguards
  - Access
  - Minimum necessary
  - Mitigation
- Exact same list for 2012 and 2011.

HIPAA Penalties

- Enforcement
  - 4 tier structure for penalties:
    - No knowledge:
      Penalty per violation: $100 - $50,000
      Max penalty of identical provision per year: $1.5 million
    - Reasonable cause:
      Penalty per violation: $1,000 - $50,000
      Max penalty of identical provision per year: $1.5 million
    - Willful neglect, timely corrected:
      Penalty per violation: $10,000 - $50,000
      Max penalty of identical provision per year: $1.5 million
    - Willful neglect, not timely corrected:
      Penalty per violation: $50,000
      Max penalty of identical provision per year: $1.5 million

Thank you!

The intent of this presentation is to provide you with general information regarding the status of, and/or potential concerns related to, your current employee benefits issue. It does not necessarily fully address all your specific issues. It should not be construed as, nor is it intended to provide, legal or tax advice. Questions regarding specific issues should be addressed by the your organization's general counsel, tax advisor, or an attorney who specializes in this practice area.