MARATHAS BARROW WEATHERHEAD LENT LLP

HIPAA Privacy Overview

Benefit Advisors Network

Stacy H. Barrow
sbarrow@marbarlaw.com

February 8, 2017

GCG EMPLOYEE BENEFITS INSURANCE RISK MANAGEMENT WEALTH MANAGEMENT

Benefit Advisors NETWORK smart partners

Overview of Presentation

- HIPAA Overview
- To Whom and to What Do the Rules Apply?
- Penalties for Violations
- What is Protected Health Information (PHI)?
- What are the Basic Rules?
- Selected Topics in HIPAA Privacy

Benefit Advisors NETWORK smart partners

HIPAA Overview

- HIPAA is a federal law that was enacted in 1996
- Final rules were issued by HHS in late 2000, amended in 2002
  - Compliance with the 2000 HIPAA privacy rules was required by April 14, 2003
- Changes to HIPAA were made under American Recovery and Reinvestment Act of 2009 – added section dealing with privacy, security and health information technology, referred to as the HITECH Act
- On January 25, 2013 HHS released its "omnibus" HIPAA/HITECH regulation, implementing changes to:
  - HIPAA Privacy, Security and Enforcement Rules
  - Interim breach notification guidance
  - Certain changes to the HIPAA Privacy Rule as required by GINA

Benefit Advisors NETWORK smart partners

HIPAA Overview

- OCR Phase II Audits to Begin Soon on Covered Entities and Business Associates
- In preparation, pay extra attention to areas of “heightened risk”
- These include:
  - Risk assessment
  - Individuals’ right to access their PHI
  - Authorizations
  - Minimum necessary use and disclosure
  - Notice of privacy practices
  - Breach notification and incident response
  - Access controls
  - Encryption

Benefit Advisors NETWORK smart partners

To Whom Do the Privacy Rules Apply?

- The HIPAA Privacy rules apply (although sometimes in different ways) to all "covered entities":
    i. health plans;
    ii. health care clearinghouses; and
    iii. health care providers who transmit any health information in electronic form in connection with one of the transactions covered by HIPAA.
- The rules also apply to a health plan's "Business Associates"
- Many organizations that have health information are not subject to HIPAA
    - Examples include: employers, workers compensation carriers, many state agencies like child protective service agencies

Benefit Advisors NETWORK smart partners

Covered Entities: Health Plans

- What is a Health Plan under HIPAA?
  - Employer sponsored health plans are “health plans” under HIPAA (includes FSAs)
    - Exception for FSAs with fewer than 50 participants that are self-insured and self-administered
  - HMOs and health insurers are also health plans under HIPAA. Those fully-insured plans are responsible for HIPAA compliance and employers are also responsible
- What is NOT a health plan under HIPAA?
  - Pension and Disability insurers or benefits are **NOT** covered by HIPAA
  - Life, property or casualty insurers or benefits are **NOT** covered by HIPAA
  - Workers’ compensation insurers or benefits are **NOT** covered by HIPAA

Benefit Advisors NETWORK smart partners

What Type of Benefits Are Covered?

- Medical (physicians, hospitals)
- Vision
- Dental
- Hearing
- Behavioral Health
- Substance Abuse
- Prescription Drug Coverage

Benefit Advisors NETWORK
smart partners

HIPAA Penalties

Violation Category	Per Violation Penalty	Annual Cap for All Violations of an Identical Provision
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect-Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect-Not Corrected	$50,000	$1,500,000

Benefit Advisors NETWORK smart partners

HIPAA Violations in the News

- Massachusetts Eye and Ear Associates Inc. settles HIPAA data breach with HHS for $1.5 Million
  - An employee's unencrypted personal laptop containing electronic protected health information of patients and research subjects was reported stolen. The laptop contained patient prescriptions and clinical information for 3,621 individuals.
- Emory Healthcare: Data breach after the organization misplaced 10 backup disks containing PHI for 315,000 patients.
- Howard University Hospital: Notified approximately 34,503 patients of a potential disclosure of their PHI when a laptop which was password protected was stolen from a contractor's vehicle.
- Anthem: Breach affected nearly 80 million customers, and included names, taxpayer IDs, birthdays, medical IDs, street addresses, email addresses, and employment data, including income.

Benefit Advisors NETWORK smart partners

HIPAA Violations in the News

- Advocate Health Care Network – settled for $5.55M
  - Largest to date against a single entity
  - 3 breaches affected PHI of 4M individuals
  - ePHI disclosed names, CC numbers, clinical info…
  - Inadequate BAA's, lax security, unencrypted laptop left in unlocked car overnight
- Catholic Health Care Services of the Archdiocese of Philadelphia – BA to nursing homes
- $650k settlement, 2 year corrective action plan
- Employee's smartphone stolen (no password or encryption)
- Had info on 412 residents, including SSN, medical procedures

Benefit Advisors NETWORK smart partners

HIPAA Violations in the News

- First enforcement for lack of timely notification settles for $475,000
- Health care network in Illinois reported a breach on 1/31/14 that had occurred on 10/22/13 (101 days)
  - Company discovered that paper-based operating room schedules, which contained the PHI of 836 individuals, were missing from a surgery center
  - The information included names, DOB, medical record numbers, dates of procedures, types of procedures, surgeon names, and types of anesthesia
  - OCR found that the company failed to notify, *without unreasonable delay* and within 60 days of discovering the breach
  - Settlement sought to balance the need to emphasize the importance of timely breach reporting with the desire not to disincentive breach reporting altogether

Definition: Protected Health Information (PHI)

- The HIPAA Privacy Rules apply to Protected Health Information
- Protected Health Information (PHI) is **individually identifiable health information** in any form – paper, oral, electronic, that is created, maintained or received by a Covered Entity
- PHI excludes employment records held by an employer in its role as an employer (*e.g.,* physician's note submitted by employee documenting reason for absence from office)
- Under the Omnibus Rule, Covered Entities must protect PHI of deceased individuals for at least 50 years

Benefit Advisors NETWORK smart partners

What is Health Information?

- Health information includes any information created by a health care provider, health plan, employer, school, or university that relates to:
  - the past, present, or future physical or mental health or condition of the individual;
  - the provision of health care to the individual; or
  - the past, present or future payment for health care to the individual

Benefit Advisors NETWORK smart partners

What Makes Health Information Individually Identifiable?

- Name
- Dates: birth, admission to hospital, discharge from hospital, death
- Telephone and fax numbers
- Social Security Number
- Account number
- Vehicle identifiers including license plates
- Web URLs and IP address numbers
- Genetic Information
- Geographic unit (certain zip code information excepted)
- Ages over 89
- E-mail and other addresses
- Medical record numbers and health plan numbers
- Certificate or license number
- Device identifiers and serial numbers
- Biometric identifiers, including finger and voice prints and full face and other identifying photographic images

Benefit Advisors NETWORK smart partners

Examples of PHI

- Information that is PHI:
  - Claims related information (e.g., EOBs, calls from employees to the plan, etc.)
  - Summaries of claims information from vendors that include identifiers
  - List of plan participants
- Information that is not PHI:
  - Doctor's note provided to manager (e.g., sick leave purposes)
  - Health information contained in FMLA or ADA requests
  - De-identified information (e.g., aggregate claims statistics)

Benefit Advisors NETWORK smart partners

HIPAA Privacy: The Basic Rules

- An employer's health plan(s) can use and disclose PHI for most routine uses and disclosures for payment for treatment and the operations
- Most other uses or disclosure of PHI require a signed, written authorization
- An employer's health plan(s) have to give certain rights to individuals. For example, right of access by a participant to his or her records, right to propose a change to the record, and accounting of disclosures. The handling of these rights can be delegated to the third-party administrators.
- Administrative Requirements: Training, privacy officer, privacy notice, many policies, procedures and sanctions for violations

Benefit Advisors NETWORK smart partners

Typical Allowable Uses and Disclosures Without Any Written Permission

- Enrollment
  - use internally, or
  - disclose to the employer's health plan's vendors
- Eligibility
  - use internally, or
  - disclose to the employer's health plan's vendors, or
  - disclose to health care providers
- Claims adjudication and payment
- Pre-certification and referral
- Coordination of benefits
- Utilization review
- Review of status of claims payment
- Use of de-identified information

Benefit Advisors NETWORK smart partners

The Key Requirements

- Training
- Privacy Officer
- Privacy Notice
- Authorization
- Minimum Necessary
- Safeguards
- Participants' Rights as Individuals
- Vendors - Business Associates
- Handling Complaints
- Employee Sanctions
- Policies & Procedures

Benefit Advisors NETWORK smart partners

Mandatory Training Under Privacy Rule: Why are We Listening to This?

- An employer's health plans must train all participants of its workforce with access to PHI ("HIPAA Personnel") regarding HIPAA privacy policies and procedures, as necessary and appropriate for the participants of the workforce to carry out their job duties
  - Each new participant of the workforce with access to PHI must be trained within a reasonable period of time after their hire date
- All training must be documented

Benefit Advisors NETWORK smart partners

Privacy Officer

- Under HIPAA, all health plans must have a privacy officer
- The privacy officer is responsible for developing and implementing policies and procedures necessary to comply with HIPAA privacy rules, including training
- Employers must also designate a contact person to answer questions and receive complaints about HIPAA's privacy rules, and to obtain the forms necessary for a participant to exercise any of his or her rights under HIPAA
- Fully insured plans that do not receive any PHI (other than Summary Health Information) have a limited HIPAA obligation
  - Among other things, such plans avoid the need to name a privacy officer, deliver a privacy notice (the carrier does it on behalf of fully insured plans), or maintain privacy policies and procedures (and train their employees on them)

Benefit Advisors NETWORK smart partners

Privacy Notice

- Notices can be delivered by e-mail, if a participant agrees to electronic notice
- The privacy notice must be distributed upon enrollment to all new participants
- An employer's intranet may include a copy of the privacy notice
- Participants are entitled to paper copies upon request
- An employer's health plans cannot substantially change their information policies and procedures before updating its notice to reflect those revisions
- At least once every 3 years, an employer's health plans must remind participants of the availability of the privacy notice

Benefit Advisors NETWORK smart partners

Privacy Notice – Omnibus Rule Changes

- Under the Omnibus Rule, the Notice of Privacy Practices must now include the following information:
  - That the sale of PHI and the use of such information for paid marketing require authorization from the individual
  - That other uses and disclosures not described in the Notice of Privacy Practices will be made only with authorization
  - That Covered Entities must notify affected individuals of breaches of their PHI
  - That individuals can restrict disclosures to their health for services for which they pay "out-of-pocket" (applicable to providers' privacy notices)

Benefit Advisors NETWORK smart partners

Privacy Notice – Omnibus Rule Changes

- Notice of Privacy Practices under the Omnibus Rule
  - Health plans that underwrite – notice must state that the plan cannot use or disclose genetic information for underwriting purposes
  - Covered Entities that contact individuals for fundraising – notice must state that individuals have the right to opt out
  - Covered Entities that maintain psychotherapy notes – notice must state that most uses and disclosures of psychotherapy notes require authorization
  - Health plans that do not post the notice of privacy practices to their website must provide information about any material change to cover individuals within 60 days of the change

Authorizations

- Written authorization is not required if PHI is being used by the plan for treatment, payment or health care operations purposes (or for other disclosures permitted by the privacy rules)
- An employer should seek a written authorization from the individual before releasing the individual's PHI to most third parties
- An employer should seek authorization from individuals before using PHI for reasons other than payment or health care operations
  - For example, if an employer wants to use the plan's own health plan records to see if a participant is entitled to disability benefits, participant must sign an authorization

Benefit Advisors NETWORK smart partners

Interaction with Participants and Family

- Individuals may ask for assistance with plan benefits
  - If (1) disclosure is to a family member involved in the individual's care or payment for that care, (2) disclosure is limited to that family member's involvement in the care or payment and (3) the individual has not objected to the disclosure to the family member, then it's okay to disclose, but preferable to refer to your outside administrators
  - With a complete authorization, or another legal document, such as a general power of attorney, an employer could disclose anything to the family member

Benefit Advisors NETWORK smart partners

What Can I Discuss?

- Employees can always pass on information from a spouse to the plan or, if for purposes of payment or operations, to the plan's vendors
- You can discuss the medical claims of a child (under 18) with either parent (subject to limited exceptions - e.g., records protected under federal laws on family planning), unless the employer is notified that it is not appropriate to so share the information (e.g., domestic abuse)
- You may disclose PHI to family members of a deceased participant who were involved with the participant's care or payment for their care, so long as such disclosure is not contrary to any prior expressed preference of the individual that is known to the plan

Benefit Advisors NETWORK smart partners

“Minimum Necessary” Rule

- The “Minimum Necessary” Rule
  - Whenever the health plans use or disclose PHI or requests PHI from another plan or a physician, it “must make reasonable efforts to limit [PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure or request”
  - Thus, the minimum necessary rule covers
    - HR Department’s use of information
    - Disclosure
    - Requests for disclosure

“Minimum Necessary” Rule

- The minimum necessary rule does not apply to:
  - Disclosures to or requests by a health care provider for treatment
  - Disclosures to the individual or pursuant to an authorization
  - Disclosures to government for enforcement of privacy rules
  - Other uses or disclosures required by law

Benefit Advisors NETWORK smart partners

Limiting Employee Access to PHI

- Employers must identify those persons or classes of persons in its "HIPAA workforce" who need access to PHI to carry out their duties:
  - Privacy Officer
  - Other members of the HR Staff to the extent that they handle benefits issues, as necessary
  - Members of the IT Department may have access to PHI
- Only HIPAA Personnel may have electronic and physical access to PHI—all others should avoid seeing (or using) PHI
  - HIPAA Personnel may use and disclose the Plan's PHI only for plan administrative functions
  - The amount of PHI disclosed must be limited to the minimum amount necessary to perform the relevant plan administrative functions
  - Generally, HIPAA Personnel may not disclose PHI to employees other than other HIPAA Personnel

Benefit Advisors NETWORK smart partners

Safeguards to Protect Privacy

- PHI may not be filed in the same files as any other employee HR information, including personnel records, and electronic access must be restricted to only HIPAA Personnel
- HIPAA Personnel have their own computer passwords and user domain account passwords accessible only to HIPAA Personnel, and they may not share passwords
- Lock cabinets and doors to offices that contain health plan records
- Be cognizant of discussions—discuss PHI only in a "controlled environment"
- Take precautions—if you are in a position to hear, take precautions not to hear if you have no need to hear

Benefit Advisors NETWORK smart partners

Individual Rights

- Right to Inspect and Copy PHI in the plan's records
- Right to Propose an Amendment to Correct PHI in the health plan's records
- Right to remove non-paid claims from PHI data set
- Right to an Accounting of Disclosures
- Right to Request Restrictions on PHI Use & Disclosure
- Handling of these rights may have been delegated to vendors

Individual Rights

- Copying and proposing amendments
- Participants and dependents have the following rights under HIPAA:
  - To access, inspect and copy their health information records in the health plan's records
  - To copy any enrollment, payment, claims adjudication, and case or medical management records system that includes PHI and that is maintained by or for the health plans or used in whole or in part by the health plans to make decisions about individuals
  - Right to propose an amendment to the PHI or a record about the participant (or dependent) in the health plan's record sets

Individual Rights

- Accounting of disclosures
- Participants have a right to request from the health plans an accounting of the disclosures of their PHI
- An employer must keep a log of disclosures of PHI made within 6 years prior to the request, and be able to give that log to a participant upon request
- An employer may require HIPAA Personnel to keep track of additional disclosures

Benefit Advisors NETWORK smart partners

Individual Rights

- Confidential Communications
- HIPAA grants adult dependents (e.g., spouse, adult children) the right to request that the plan send them communications (including any EOB that the plan may mail out) by alternative means or at alternate locations from the mailing address of the named insured
- Privacy notice advises participants of this right
- The health plans only needs to accommodate the request if the request is reasonable and the individual specifies that the disclosure of all or part of the health information would endanger the individual (e.g., domestic abuse)

Benefit Advisors NETWORK smart partners

What is a Business Associate?

- Definition:
- A person who (i) performs for or on behalf of a covered entity, or assists a covered entity, in performing an activity or function involving use or disclosure of health information (e.g., claims processing, utilization review, billing), or (ii) provides legal, actuarial, accounting, management, administrative, accreditation or financial services where the provision of such services involves the disclosure of health information from the entity or another business associate of the entity
- Includes anyone with health information from your health plans (could include attorneys, consultants, TPAs, auditors, computer software service companies)
- Includes: Benefits Brokers and others

Benefit Advisors NETWORK smart partners

What is a Business Associate?

- The Omnibus Rule expanded the definition of business associate:
  - One who, other than in the capacity of a member of a covered entity's workforce creates, receives, maintains, or transmits PHI
  - Includes a "subcontractor" of a business associate who creates, receives, maintains, or transmits PHI on behalf of the business associate
- Under the Omnibus Rule, business associates include:
  - Patient Safety Organizations; Health Information Organizations
  - E-Prescribing Gateways; others that provide data transmission services to a covered entity with respect to PHI and that require access on a routine basis to such PHI, including those that store PHI and have access (e.g., hosting providers)

Benefit Advisors NETWORK smart partners

What are the Business Associate Rules?

- General Rules
  - Need specific HIPAA-dictated language in a contract with all business associates
  - Language includes privacy protections as well as the extension to service providers of individuals' HIPAA rights.
  - So, when entering into a new agreement with a third party administrator or a benefits consultant to audit your vendors, the Privacy Officer must arrange to have this language in your agreement

Benefit Advisors NETWORK smart partners

What are the Business Associate Rules?

- Privacy and Security Requirements under HITECH Act (2009)
- Under HITECH, all of the HIPAA rules apply directly to business associates, including penalties
  - Previously, HIPAA applied only to “covered entities” – health plans, health care providers, and clearinghouses
  - HIPAA applied indirectly to business associates – through business associate agreements
  - Business associates, like brokers and consultants, perform PHI-related functions for group health plans

Benefit Advisors NETWORK smart partners

Enforcement of Agency Law

- The Omnibus Rule makes Covered Entities liable for business associates (and business associates for their subcontractors) under federal common law of agency
- Whether a business associate is an agent is fact specific, considering the terms of the business associate agreement and the totality of circumstances regarding the relationship
- Critical factors:
  - Covered Entity's control and authority to control manner and method (i.e., give interim instructions)
  - Whether Covered Entity is delegating a HIPAA obligation

Benefit Advisors NETWORK smart partners

Handling Complaints

- The Privacy Notice advises everyone that they have a right to complain, about violations of their HIPAA rights
- If an employee (or covered dependent) complains his or her health plan privacy rights have been violated, the person complaining should be directed to the Privacy Officer, or if any employee wants to complain about a health plan privacy violation by someone else (including by your vendors), all those receiving such a complaint should make a written report to the Privacy Officer
- The HIPAA Policies must include forms for making privacy complaints.
- All complaints should be investigated by the Privacy Officer
- Retaliation for making privacy complaints is prohibited

Benefit Advisors NETWORK smart partners

Employee Sanctions for Violations

- Employers are required by HIPAA to have and apply appropriate sanctions against the health plan's workforce who fail to comply with the plan's privacy policies and procedures or the privacy requirements of HIPAA
- In other words, if the members of the HR Department do not follow the HIPAA privacy policies they could be disciplined, up to and including termination of employment

Benefit Advisors NETWORK smart partners

Policies & Procedures

- HIPAA requires the establishment and maintenance of HIPAA Policies & Procedures
- All who handle PHI should retain a copy of the Policies & Procedures
- All who handle PHI should be familiar with the requirements of the Policies & Procedures

Benefit Advisors NETWORK smart partners

Breach Notification Rules

- Notification Requirement Upon Breach of "Unsecured" PHI applies:
- PHI is "unsecured" if it is not rendered "unusable, unreadable, or indecipherable to unauthorized individuals"
  - "Secured" PHI acts as a safe harbor
- ***NEW*** Under the omnibus rule, an impermissible use or disclosure of PHI is presumed to be a reportable breach unless the covered entity or business associate, as applicable, demonstrates through a documented risk assessment that there is a low probability that PHI has been compromised
- Notice must be provided "without unreasonable delay" but in no event later than 60 days from discovery of the breach or the date breach reasonably should have been discovered

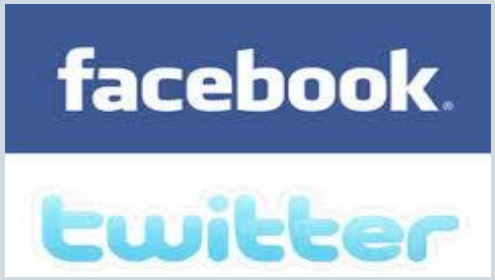
Benefit Advisors NETWORK smart partners

Breach Notification Rules

- The Omnibus Rule articulates four factors that a risk assessment must consider:
  - The nature and extent of the PHI (e.g., sensitivity of data, likelihood of re-identification);
  - The unauthorized person to whom the PHI was used/disclosed;
  - Whether the PHI was actually acquired or viewed; and
  - Mitigation efforts (e.g., encrypting data)

Privacy Breach

- A privacy breach can occur when information is
- Physically lost or stolen
  - Paper copies, films, tapes, electronic devices
- Misdirected by others
  - Verbal messages sent to or left with the wrong voicemail
  - Mislabeled mail
  - Misdirected email
  - Wrong fax number
  - Placed on intranet, website, Facebook, Twitter
  - Not using secure email
    - If data is not de-identified it is easy to have an inadvertent violation



Benefit Advisors NETWORK smart partners

Breach Notification Rules

- Content of Notice
  - Brief description of what happened, date of breach, and date of discovery of breach (if known)
  - Types of unsecured PHI involved in breach (e.g., full name, SSN, DOB, home address, account number)
  - What individuals should do to protect themselves from potential harm from breach
  - Actions covered entity taking to investigate, mitigate losses, and protect against future breaches
  - How to find more information

Benefit Advisors NETWORK smart partners

Breach Notification Rules

- Nature of notification
  - If business associate discovers breach, must notify covered entity (i.e., the group health plan) so it can notify affected individuals
  - Previously, contractual obligation to disclose "security incidents;" now direct statutory notification obligation
  - Covered entity may contract with business associate to handle administrative details on its behalf; pay for notifying affected individuals

Breach Notification Rules

- If covered entity experiences breach, must give notice to affected individuals (at last known address) or by e-mail (if specified as preference)
- If contact information for individual insufficient or out of date, and if 10 or more individuals, notice must be posted on covered entity's website for 90 days or broadcast in local media and active toll free number for 90 days; if urgency required "because of possible imminent misuse," notice must be by telephone or other means, as appropriate
- If breach involves 500 or more individuals, must immediately notify HHS and prominent media outlet

Action Items

- Report breaches to HHS annually and keep internal logs of breaches
- Meet the safe harbor for treating PHI as “secured” or implement breach notice policies and procedures
- If applicable, amend and distribute HIPAA privacy notice with revised information; send copies to business associates
- As necessary, sign amended or new BA agreements
- Conduct HIPAA Audit of policies and procedures to honor requests and general compliance
- Update policies and procedures for marketing restrictions, minimum necessary standard
- Implement training

Benefit Advisors NETWORK smart partners

MARATHAS BARROW WEATHERHEAD LENT LLP

QUESTIONS?

GCG Financial, LLC
info@gcgfinancial.com
www.gcgfinancial.com

Stacy H. Barrow
sbarrow@marbarlaw.com
(617) 830-5457