MARATHAS BARROW WEATHERHEAD LENT LLP

HIPAA Privacy & Security Overview

Benefit Advisors Network

February 6, 2019

Stacy H. Barrow

sbarrow@marbarlaw.com

(617) 830-5457

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

Overview of Presentation

- HIPAA Core Concepts
- Uses and Disclosures of PHI
- Individual Rights of Participants
- Safeguards for Protecting PHI
- Breach Notification Requirement

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
  - Access to health care (e.g., portability, special enrollment, nondiscrimination)
  - "Administrative Simplification" rules (e.g., privacy, security, coding for health care transactions)
- The purpose of HIPAA's Administrative Simplification rules were to improve efficiency and effectiveness of the health care system by standardizing the electronic exchange of administrative and financial data

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

What is HIPAA?

- HIPAA 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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

HIPAA Privacy Rule & Security Rule

- The HIPAA Privacy Rule and Security Rule protect individually identifiable health information.
  - **Purpose of the Privacy Rule:** Sets rules for how a covered entity may use and disclose PHI and gives participants certain rights regarding the protection of and access to their PHI
  - **Purpose of the Security Rule:** Protects against reasonably anticipated threats of uses or disclosures of electronic PHI (e-PHI) that are not allowed by the Privacy Rule. Requires a covered entity to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

What is the Covered Entity?

- 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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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 eligible 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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

What Type of Benefits Are Covered?

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

Consequences of Non-Compliance

- Significant civil, monetary and criminal penalties for failure to comply with HIPAA
  - Rules enforced, including civil monetary penalties, by the Office of Civil Rights, not the DOL or the IRS
  - Criminal action prosecuted by Department of Justice
- Potential litigation for breach of HIPAA rules
- Notification of breaches
- Employers may discipline any employee who violates HIPAA

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

Consequences of Non-Compliance

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

OCR Phase II Audits

- OCR Phase II Audits in process on Covered Entities and Business Associates
- 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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

HIPAA Violations in the News

- **Catholic Health Care Services of the Archdiocese of Philadelphia**: BA to nursing homes
  - First settlement with BA; $650k settlement (June 2016); 2 year corrective action plan
  - Employee’s smartphone stolen (no password or encryption)
  - Had info on 412 residents, including SSN, medical procedures
- **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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

HIPAA Violations in the News

- **Presence Health:** First enforcement for lack of timely notification settles for $475,000 in February 2017
- 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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

HIPAA Violations in the News

- **Lessons Learned from these and other settlements**
  - Don’t use unsupported software (i.e., out-of-date versions) and apply patches regularly and promptly
  - Train workforce that snooping is forbidden and a HIPAA violation
  - After routine IT maintenance, always check that firewalls are reactivated and security settings are appropriate
  - Wipe any hard drives (which many copiers have) before reselling or returning to leasing companies
  - Implement strong policies and procedures regarding taking PHI offsite, handling while offsite and protecting it from others (family members, neighbors, visitors in the home, etc.)
  - Never leave PHI or a device containing PHI in a vehicle unless the PHI or device is secured
  - Review business associate agreements (and subcontractor BAAs) to make sure they’ve been updated for legal requirements and any changes in the services to be rendered by the business associate

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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)

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

What About Enrollment Information?

- Enrollment information (including premium contribution amounts) has special, dual status—it is not PHI in the hands of the employer, but it is PHI in the hands of the insurance carrier or covered entity
- Only authorized employees and business associates may have access to PHI and only for plan administration purposes

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

Examples of PHI Use That Require Authorization

- Authorization required when:
  - Disclosing PHI to an FMLA administrator so he/she can determine if an employee is eligible for FMLA leave
  - Giving a manager PHI about an employee's medical condition so he/she can make an ADA accommodation

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

HIPAA Privacy: The Basic Rules

- An employer's health plan(s) may use and disclose PHI for Treatment, Payment, and health care Operations of the plan ("TPO Purposes")
- 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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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)

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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)

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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
  - Contact your ***Privacy Officer*** <u>before</u> disclosing PHI to anyone claiming to be a personal representative of a participant
    - ***Privacy Officer*** will confirm that the individual has met all legal requirements to be a personal representative

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

“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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

"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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

“Minimum Necessary” Rule

- Only use PHI when it’s necessary to perform your job duties
- Use only the minimum necessary PHI to perform your job duties
- Follow your employer’s HIPAA policies and procedures for confidentiality and security
- Do not disclose PHI to other employees that are not authorized to receive it
- ***Ask*** if you have questions about what you can and can’t disclose

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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
  - 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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

Limiting Employee Access to PHI

- Employers must identify those persons or classes of persons in its workforce who need access to PHI to carry out their duties (“Authorized Employees”):
  - Privacy Officer
  - Human Resources to the extent that they handle benefits issues related to the employer’s group health plan
  - Members of the Information Technology department may also have access to PHI

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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)

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

Individual Rights

- If you are contacted by a participant who wants to exercise one of these rights, contact your Privacy Officer
- These are not absolute rights
- In most cases, the participant's request should be forwarded to the applicable insurance carrier or claims administrator
  - TPAs are generally required to respond to such requests per the client's Business Associate Agreements with them
- 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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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)

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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, the Privacy Officer must arrange to have this language in your agreement

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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
- 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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

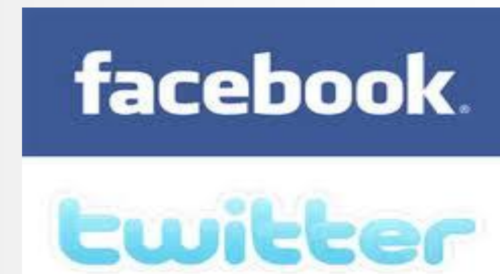
Breach Notification Rules

- 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)

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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



© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

Safeguards for Hard-Copy PHI

- Clean desk rule—PHI should not be left out and unattended
- Dispose of material containing PHI by means of secure trash bins designated for shredding
- Do NOT use intra-office mail to transmit PHI
- Lock all file cabinets containing PHI

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

Safeguards for Oral PHI

- Only discuss PHI in your office or a conference room with the door closed
  - If you work in a cubicle area and must discuss PHI in your cubicle area, do not use identifiers and use appropriate volume
- Only discuss PHI with other authorized workforce members or business associates.
- Remember—the minimum necessary rule applies

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

Safeguards for Emailing PHI

- Avoid using email to transmit PHI:
  - When transmitting e-PHI to a vendor, use a vendor secure website instead of email when possible
  - Upon receipt of an email with PHI from a participant which requires a response that contains PHI, respond by telephone to the extent possible
- If you must use email to transmit PHI:
  - do not use identifiers to the extent possible (in the message and the subject line);
  - delete the email chain below your message;
  - use caution regarding recipients (e.g., reply all); and
  - if the email must be sent outside the company, use encryption where possible

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

Safeguards for Electronic PHI

- Physical safeguards:
  - Computer screens should be out of sight from others – if you work in a cubicle, use a privacy screen
  - Log-off from your computer when you leave your workstation for any amount of time
  - Don't save unencrypted files with PHI to your laptop hard drive
  - Create strong password and do NOT share them
  - Do NOT file PHI in the same files as any other employee HR information, including personnel records
- Never download PHI to your personal computer or send it to your personal email address

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

When is a breach considered discovered for purposes of the notice deadline?

- A breach is considered "discovered" as of the first day that it is known (or reasonably should have been known) to the plan
- Employers have an obligation to report breaches they cause
- *This means it is critically important that you report to the Privacy Officer as soon as you think a breach MAY have occurred—The time to respond may start ticking at the time YOU discover the breach*

If something happened but you are not sure if it would be considered a breach, tell the Privacy Officer and the situation will be evaluated

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

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

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

Questions?

Stacy Barrow

sbarrow@marbarlaw.com

(617) 830-5457

The information provided in this slide presentation is not, is not intended to be, and shall not be construed to be, either the provision of legal advice or an offer to provide legal services, nor does it necessarily reflect the opinions of the firm, our lawyers or our clients. No client-lawyer relationship between you and the firm is or may be created by your access to or use of this presentation or any information contained on them. Rather, the content is intended as a general overview of the subject matter covered. Marathas Barrow Weatherhead Lent LLP is not obligated to provide updates on the information presented herein. Those viewing this presentation are encouraged to seek direct counsel on legal questions. © Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.

© 2019 Marathas Barrow Weatherhead Lent LLP. All Rights Reserved.