GREENSFELDER
ATTORNEYS AT LAW

18th Annual Sleep Medicine Conference KENTUCKY SLEEP SOCIETY Patient Confidentiality and Regulatory Compliance

Jayme R. Matchinski
Greensfelder, Hemker & Gale, P.C.
October 14, 2016
Louisville, Kentucky

Learning Objectives:

1. Define appropriate use of date encryption requirements.
2. Outline appropriate use of patient information to meet HIPAA guidelines.

GREENSFELDER
ATTORNEYS AT LAW

Encrypting Data to Meet HIPAA Compliance

A covered entity must, in accordance with § 164.306 . . . Implement a mechanism to encrypt and decrypt electronic protected health information US CFR § 164.312(a)(2)(iv).

- If your sleep labs choose not to encrypt data, the HIPAA Security Rule states that a covered entity must implement an equivalent solution to meet the regulatory requirement.
- HIPAA regulations leave encryption open to interpretation since covered entities vary when it comes to network usage, depending on the type and size of business.

GREENSFELDER
ATTORNEYS AT LAW

Key Recommendations for Data Encryption:

- Don’t use public FTP (File Transfer Protocol) if your sleep lab needs to transfer patient data to and from payers or other business associates.
- Combine two methods of encryption – send encrypted files over an encrypted connection.
- For remote access to applications and data in cases of telecommuting or working from remote locations, use a VPN (Virtual Private Network). This network creates a temporary encrypted connection that only exists during the time of use.
- Always use SSL (Secure Sockets Layer) (**http://www.onlinetech.com/secure-hosting/technical-security/ssl-certificate**) for web-based access to any sensitive data.
- Keeping sensitive data on a portable device is not recommended – it is better to store your data in an offsite location with a secure environment, such as a HIPAA compliant data center (**http://www.onlinetech.com/company/michigan-data-centers/compliance/hipaa-compliant-data-centers**) with the proper physical and network security in place to protect PHI and prevent a data breach.

GREENSFELDER
ATTORNEYS AT LAW

HIPAA and HITECH

- HIPAA – Enacted in 1996 to protect the privacy and security of certain health information
  - ***Privacy Rule*** – Sets national standards for the protection of health information
  - ***Security Rule*** – Specifically applies to *electronic* protected health information
- HITECH – Strengthens HIPAA enforcement and penalties and instituted breach notification procedures

Phase 2 of HIPAA Audit Program

- On March 21, 2016, U.S. Department of Health and Human Services (DHHS), office for Civil Rights (OCR) announced the official launch of Phase 2 of its HIPAA Audit Program.
- OCR has been sending communications to Covered Entities and Business Associates to obtain or verify their contact information.
- Upon verification, OCR will distribute screening questionnaires to gather data about the size, type, and operations of potential auditees.

Phase 2 of HIPAA Audit Program

- OCR will create audit pools based on the responses to these questionnaires. The OCR will select a random sample of Covered Entities and Business Associates for desk audits.
- After desk audits are completed in 2016, OCR may conduct more extensive on-site audits.
- OCR may initiate a compliance review to investigate any serious compliance issues revealed during the audit.

HIPAA Privacy - Summary

- Limits the uses and disclosures of patient information
- Creates individual rights to inspect, copy, amend, request restrictions, file complaints and receive notice of privacy practices
- Requires agreements with business associates to safeguard information
- Requires privacy policies and procedures
- Requires implementation of “reasonable safeguards”
- Requires training of all employees

HIPAA Security - Summary

- Covered entities must:
  - ✓ ***Ensure the confidentiality***, integrity, and availability of all ePHI they create, receive, maintain or transmit;
  - ✓ ***Identify and protect*** against reasonably anticipated threats to the security or integrity of the information;
  - ✓ ***Protect*** against reasonably anticipated, impermissible uses or disclosures; and
  - ✓ ***Ensure compliance*** by their workforce.

"You can't just walk in and ask to access patient records. HIPAA would call that fantasizing."

GREENSFELDER
ATTORNEYS AT LAW

HIPAA Definitions

- ***Covered Entity***
  - A health plan
  - A healthcare clearinghouse
  - A healthcare provider who transmits any health information in electronic form

HIPAA Definitions

- ***Protected Health Information ("PHI")*** – Any information that is created or received by a healthcare provider and relates to the past, present or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present or future payment for the provision of healthcare to an individual that is:
  - Transmitted by electronic media;
  - Maintained in electronic media; or
  - Transmitted or maintained in any other form or medium.

Common Issues

1. Minimum Necessary Rule
2. Uses and Disclosures
3. HIPAA Privacy: Safeguards for PHI
4. Individuals' Rights
5. HIPAA Security: Safeguards for ePHI
6. Business Associates

Common Issues

GREENSFELDER
ATTORNEYS AT LAW

Minimum Necessary

- When using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the **minimum necessary to accomplish the intended purpose of the use, disclosure or request**
- **Reasonable Efforts** – Covered entities should evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. It is intended to reflect and be consistent with, not override, professional judgment and standards

Minimum Necessary

- **Exceptions**
  - Disclosures or requests by a healthcare provider for treatment
  - Uses or disclosures made to the individual
  - Uses or disclosures made pursuant to a valid authorization
  - Disclosures made to the Secretary of HHS
  - Uses or disclosures required by law
  - Uses or disclosures required for complying with HIPAA

Uses & Disclosures

- ***General Rule*** – A covered entity may not use or disclose PHI unless a patient authorizes it or it is otherwise permitted by the Rule
- Permitted Uses/Disclosures mean that you are “permitted” to use or disclose PHI without the need for patient authorization – use sound judgment

Uses & Disclosures

- Examples of permitted uses/disclosures include:
  - treatment, payment or operations
  - required by law (*i.e.*, Patient and Advocacy system)
  - public health activities (*i.e.*, reporting to the CDC)
  - law enforcement (only if certain conditions are met)

Uses & Disclosures - Treatment

- ***Treatment*** – The provision, coordination or management of healthcare and related services by one or more healthcare providers, including the:
  - Coordination or management of healthcare by a healthcare provider with a third party;
  - Consultation between healthcare providers relating to a patient; or
  - Referral of a patient for healthcare from one healthcare provider to another

Uses & Disclosures - Treatment

- Examples of Treatment
  - A laboratory faxes, or communicates over the phone, a patient's medical test results to a physician
  - A physician may mail or fax a copy of a patient's medical record to a specialist who intends to treat the patient
  - A hospital may fax a patient's health care instructions to a nursing home to which the patient is to be transferred

Uses & Disclosures - Treatment

- Examples of Treatment
  - A doctor may discuss a patient's condition over the phone with sleep tech
  - A doctor may orally discuss a patient's treatment regimen with a sleep tech who will be involved in the patient's care
  - A physician may consult with a sleep tech or another physician by e-mail about a patient's condition

Uses & Disclosures - Payment

- ***Payment*** – Includes:
  - Obtaining reimbursement for healthcare services
  - Determining eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts)
  - Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related healthcare data processing

Uses & Disclosures - Payment

- ***Examples of Payment***
  - A hospital may contact persons other than the patient to obtain payment for healthcare services
  - A physician practice may engage a debt collection agency to perform certain debt collection services on its behalf
  - Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
    - Name and address;
    - Date of birth;
    - Social security number;
    - Payment history;
    - Account number; and
    - Name/address of the health care provider/health plan.

Uses & Disclosures - Operations

- ***Health Care Operations*** – Includes:
  - Quality assessment and improvement activities
  - Reviewing the competence and qualifications of healthcare professionals
  - Conducting or arranging for medical review, legal services, and auditing functions
  - Business planning and development
  - Business management, etc.

Safeguards

- Certain uses and disclosures are inevitable and permissible during another permissible or required use or disclosure, ***as long as the covered entity has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure***

Safeguards

- ***Safeguards*** – Must maintain reasonable and appropriate administrative, physical and technical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule
- It is not expected that a covered entity's safeguards guarantee the privacy of PHI from any and all potential risks

Safeguards

- ***Examples***
  - Shredding documents containing PHI
  - Securing medical records with lock and key and/or passwords
  - Limiting access to keys and/or passwords
  - Speaking quietly when discussing a patient's condition with family members in a waiting room or other public area
  - Avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality

Access

- A covered entity is ***required*** to disclose PHI if:
  - An individual requests his/her own PHI
  - When requested by HHS to investigate or determine HIPAA compliance
- Records contained in a ***designated record set***

Access

- ***Designated Record Set*** – That group of records a covered entity uses to make decisions about individuals, medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.
  - ***Except***
    - Psychotherapy notes;
    - Information compiled for legal proceedings;
    - Laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access; or
    - Information held by certain research laboratories

Access

- **Timing**: HIPAA Covered entities must act on a request for access no later than ***30 days*** after receipt of the request; *regardless of where the records are stored*
  - **One *30 day*** extension is permitted
- **Form**: If records are stored electronically and a patient requests the records in an electronic format, they must be furnished in the form requested, if readily producible

Amending PHI

- An individual has a right to have his/her PHI/record in a designated record set amended
- Denials – A covered entity may deny the request for an amendment if:
  - The PHI was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
  - The PHI/record is not part of the designated record set;

Amending PHI

  - The PHI is not available for inspection by the individual; or
  - The PHI is accurate and complete
- May require requests be in writing and provide reason to support toe requested amendment
- Covered entity has ***60 days*** after receipt of the request to grant or deny the amendment, or request a 30 day extension
- If the request is accepted, the covered entity must make reasonable efforts to inform, and provide the amendment to, those persons identified by the individual as having received the PHI and business associates
  - Reasonable time

Amending PHI

- If the request is denied, the covered entity must provide timely, written denial and include:
  - The basis for the denial,
  - The individual’s right to submit a written statement disagreeing with the denial,
  - A statement that, if the individual does not submit a statement of disagreement, the individual may request the covered entity provide the individual's request for amendment and the denial with any future disclosures How the individual may complain to the covered entity or the Secretary (includes name and phone number of contact person)

Requesting Restrictions

- Individuals have a right to request a restriction on the uses and disclosures of their PHI
- Covered entities **may** agree to comply with the restriction; however, if there is an agreement to comply, the covered entity **must** comply, unless emergency treatment is required
  - Does not restrict required or permitted disclosures
- If the individual pays for a service out-of-pocket and in full and requests restrictions on the disclosure of PHI, the covered entity **must** comply

Requesting Restrictions

- Restrictions terminate upon any of the following:
  - The individual agrees or requests, in writing
  - The individual agrees orally and the oral agreement is documented
  - The covered entity informs the individual that it is terminating the agreement to restriction
- Restrictions must be documented

Confidential Communications

- A covered entity must permit individuals to request, and must accommodate reasonable requests, to receive communications of PHI by alternative means or at an alternative location
- May require the request be made in writing, but cannot require an explanation

Accounting of Disclosures

- An individual has a right to receive an accounting of disclosures of PHI in the 6 years prior to the date on which the accounting is requested
- Exceptions include disclosures made:
  - To carry out treatment, payment, or operations
  - To individuals of PHI about themselves
  - Incident to a permitted use or disclosures
  - Pursuant to an authorization
  - Facility directories
  - National security or intelligence purposes

Accounting of Disclosures

- To correctional institutions or law enforcement officials
- As part of a limited data set

- An accounting must include:
  - The date of the disclosure;
  - The name of the entity/person who received the PHI and, if known, the address of each person/entity;
  - A brief description of the PHI disclosed; and
  - A brief statement of the purpose of the disclosure

Accounting of Disclosures

- Within 60 days after receipt of the request for an accounting of disclosures, the covered entity must:
  - Produce the accounting; or
  - Request a 30 day extension
- The first request within a 12 month period must be provided free of charge, thereafter, a cost-based fee may be charged if the individual is informed in advance of the fee

Notice of Privacy Practices

- Individuals have a ***right*** to adequate notice of the uses and disclosures of PHI that may be made by the covered entity and the individual's rights and the covered entity's legal duties with respect to the PHI
- Must be available upon request to any person

Notice of Privacy Practices

- If you have a website, the notice must be prominently posted
- Must document compliance with this requirement by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgement of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgement

Administrative Safeguards of ePHI

- ***Workforce Training*** – A covered entity must provide for appropriate authorization and supervision of its workforce, must train its workforce on its security policies and procedures and have sanctions against those who violate the policies and procedures
- ***Evaluation*** – Periodic evaluation of the policies

Administrative Safeguards of ePHI

- ***Device and Media Controls*** – Covered entities must implement policies and procedures governing the receipt, transfer, removal, disposal and re-use of hardware and electronic media that contain ePHI into and out of a facility and the movement of these items within the facility.

Physical Safeguards of ePHI

- *Workstation Use* – Covered entities must implement safeguards for all workstations that access the ePHI and restrict access to authorized users

"WARNING. You have violated HIPAA! An email notification has been sent to a federal agency, your supervisor, and your mother."

GREENSFELDER
ATTORNEYS AT LAW

Technical Safeguards of ePHI

- ***Access Control*** – Implement technical policies and procedures to allow access only to those persons or software programs that have been granted access rights to ePHI
  - Unique user identification – Assigning a unique name/number for identifying and tracking users
  - Emergency access procedures – Implementing procedures for accessing ePHI during emergencies

Technical Safeguards of ePHI

- ***Access Control*** – Technical Policies
  - Automatic logoff* – Terminating a session after a certain amount of time of inactivity
  - Encryption and decryption* – Implementing mechanisms to encrypt and decrypt ePHI

** Denotes those implementation specifications that are not required per se; covered entities may determine whether the implementation specification is reasonable and appropriate for that covered entity. If it is not, the Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.*

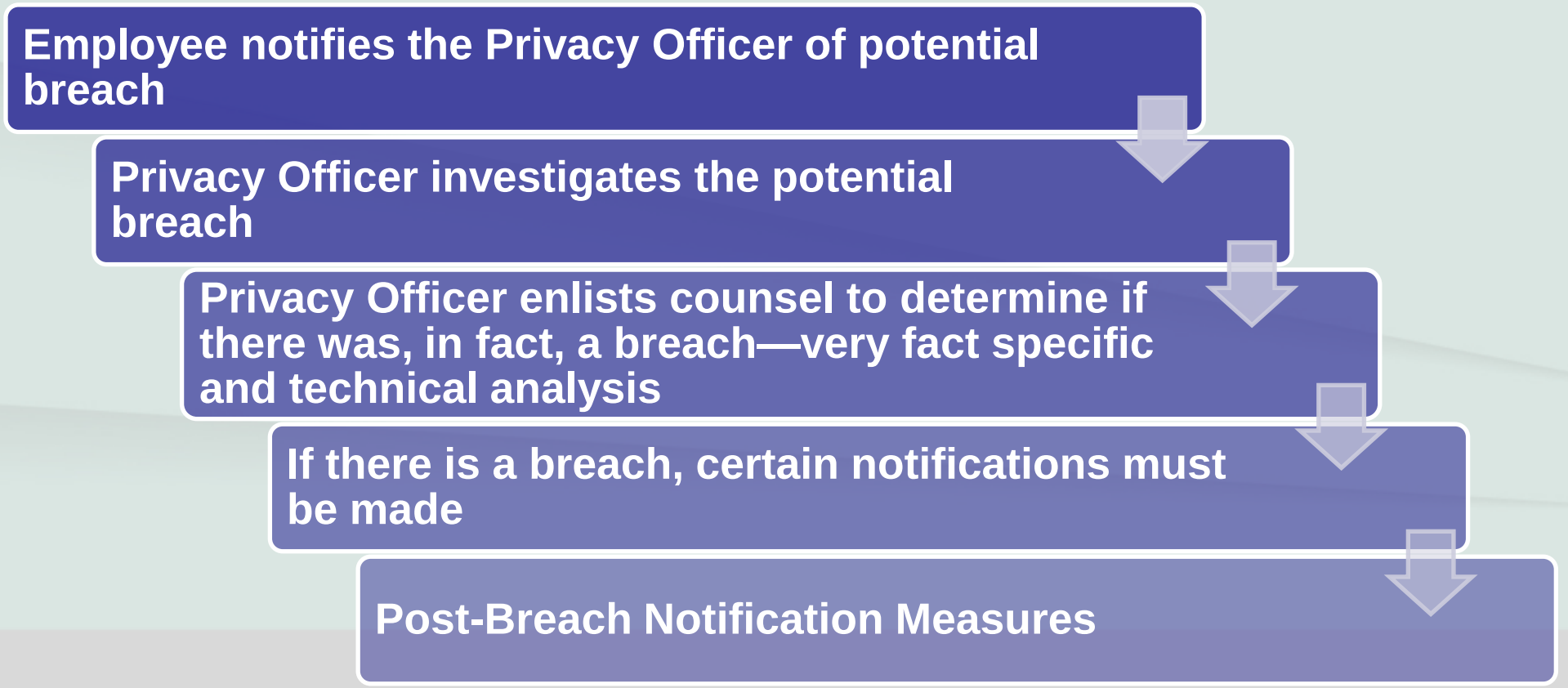
Safeguarding ePHI

- ***Audit Controls*** – Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI
- ***Integrity Controls*** – Implement policies and procedures to protect ePHI from improper alteration or destruction

Safeguarding ePHI

- ***Person or Entity Authentication*** – Implement procedures to verify that a person or entity seeking access to the ePHI is the one claimed
- ***Transmission Security*** – Implement measures to guard against unauthorized access to ePHI that is being transmitted electronically

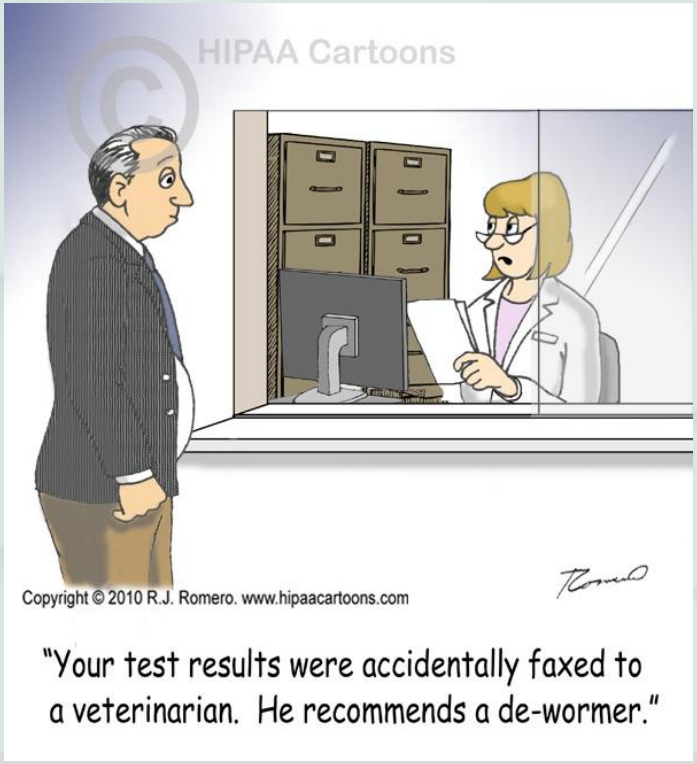
Breach Notification - Process



GREENSFELDER
ATTORNEYS AT LAW

Breach Notification

Notice to Individuals – Notice must be provided without unreasonable delay and no later than ***60 days*** after the breach is discovered via first class mail unless the individual has specified a preference for e-mail



GREENSFELDER
ATTORNEYS AT LAW

Breach Notification

- ***Notice to the Media*** – For breaches of **more than 500** individuals in one state, prominent media outlets must be notified
- ***Notice to HHS*** – Covered entities must notify HHS of the breach
  - **500+ Individuals** – Notify HHS and individuals at the same time
  - **<500 Individuals** – Notify HHS no later than **60 days** after the end of the year the breach was discovered
  - Form: **http://ocrnotifications.hhs.gov/**

Breach Notification - Strategy

- What should you do if you suspect that there has been a breach that might require reporting?
  - ✓ Recommend that you immediately contact your legal counsel for advice
  - ✓ Determination of whether the breach requires notification under the Rule is fact specific and requires analysis
  - ✓ Provide assistance with documentation and notification requirements put you in best position possible

Post-Breach Notification Steps

- ✓ Review your policies and procedures and update them, if necessary
- ✓ Institute greater safeguards and protective measures to prevent recurrence
- ✓ Consistently enforce disciplinary measures for employees that are involved in the breach/inappropriate access of PHI
- ✓ Train/Retrain your staff on HIPAA compliance
- ✓ Perform internal audits to ensure compliance with your policies and procedures

Questions?

Jayme R. Matchinski

(312) 345-5014

jmatchinski@greensfelder.com

GREENSFELDER
ATTORNEYS AT LAW