

# Privacy & Security

HIPAA

PRIVACY & CONFIDENTIALITY

**movement for life**  
**physical therapy**

# What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") establishes a set of national standards for the protection of certain health information. These standards address the use and disclosure of individuals' health information "protected health information" ("PHI") by organizations ("covered entities") subject to the Privacy Rule, as well as standards for individuals' privacy rights to understand and control how their health information is used.
- Criminal and civil penalties apply to anyone who is in violation of this Law. ***Individuals, not just the organization, can have penalties brought against them.***
  - ***YOU ARE RESPONSIBLE FOR YOUR ACTIONS AND CAN BE HELD ACCOUNTABLE AS AN INDIVIDUAL***



# Privacy, Confidentiality & PHI

- “Individually identifiable health information” is information, including demographic data that relates to:
  - the individual’s past, present or future physical or mental health or condition,
  - the provision of health care to the individual, or
  - the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.
- Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

# Minimum Necessary

- PHI should only be accessed by team members on a need-to-know basis. This premise is also referred to as "*minimum necessary*."
- Minimum Necessary means each team member only needs to access the minimum amount of information necessary for them to carry out their job duties...nothing more!

# Question 1

You know a patient that is currently being seen in the office and being a part of the treatment team read her notes, despite the fact that you have never been directly involved in her care. Does this fall within the “need to know” category of information?

- Yes
- No

# Who must comply with HIPAA?

- HIPAA provides for the protection of individually identifiable health information that is transmitted or maintained in any form or medium. The privacy rules affect the day-to-day business operations of the following organizations that provide medical care and maintain PHI:
  - **Health Care Providers:** Any provider of medical or other health Services that bills or is paid for healthcare in the normal course of business. Health care includes preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, services, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual.
    - *This is us!*
  - **Health Care Clearinghouse:** Businesses that process or facilitate the processing of health information received from other businesses. It includes groups such as physician and hospital billing services.
  - **Health Plans:** Individuals or group plans that provide or pay the cost of medical care and includes both Medicare and Medicaid programs.

# We must comply with HIPAA.

- Regardless of your position or role in patient care, we are considered a “covered entity” and all areas of this Company are covered by HIPAA regulations.
- Release of PHI:
  - Even within the healthcare community, only minimum necessary PHI that is required to care for the patient can be shared. Information should only be shared with other medical providers known to be involved in the patient’s case.
  - Any information that needs to be released about a patient or his medical case may only be done within HIPAA guidelines.

# Permitted Uses and Disclosures

- There are four permitted uses and disclosures of PHI that do not require a patient authorization. These include:
  - Treatment (including contacting the patient with regard to appointments and other treatment related communication)
  - Payment of healthcare services
  - Health care operations
  - Permitted or Required by law (including court order/subpoena)
- PHI can be shared with family/friends involved in the patient's care if the patient does not object. This may be inferred, for example if the patient invites their spouse to be present at the evaluation, you can provide information openly during that time.
- PHI may be disclosed in an emergency situation when a patient may not be able to communicate themselves.



## Question 2

Does a physician need a patient's written authorization to send a copy of the patient's medical record to a specialist or other health care provider who will treat the patient?

- Yes
- No


# Question 3

Susan and Mike are both receiving therapy at the same time and Susan asks you, "What is wrong with Mike?" Can you release this information?

- Yes
- No

# Authorizations

- We have a new authorization form to release records to meet the new HIPAA standard.
  - Please be sure before releasing any information about a patient they have signed this form.
  - EXAMPLE: Sue's daughter calls to ask when Sue's next appointment is. Unless Sue has signed this form and included her daughter as someone we can release information to, we cannot provide the appointment date.
  - It is recommended to have each patient sign this form at the time of new patient intake.

 Attention: Medical Records  
1105 Walnut Street, #110  
San Luis Obispo, CA 93401  
Phone: (805) 387-7778  
Email: recordsrequests@movementforlife.com

**AUTHORIZATION FOR RELEASE OF INFORMATION**  
*Authorization is not required for the Use or Disclosure of Information Related to Treatment, Payment, Healthcare Operations or If Required by Law or Rules*

(1) Patient's Printed Name: \_\_\_\_\_  
Last First Middle Initial Suffix

Date of Birth: \_\_\_\_/\_\_\_\_/\_\_\_\_

(2) Central Valley PT will only disclose the protected health information you want disclosed. Check only one box to tell Central Valley PT the specific information you want disclosed/released:  
☐ I Do NOT release any information other than for treatment or payment (skip #s 3, 4, and 5)  
☐ I Limited Information (complete ALL Sections)

(3) Complete only if you selected "limited information". Please initial all that apply:  
\_\_\_\_ Evaluation/Examination \_\_\_\_ Attendance \_\_\_\_ Correspondence re: your Physical Therapy Services  
\_\_\_\_ Past Medical History \_\_\_\_ Treatments \_\_\_\_ Other: \_\_\_\_\_

(4) Complete only if you selected "limited information". I only authorize the release of information to the individuals/entities identified below by name:  
Spouse: \_\_\_\_\_ Attorney: \_\_\_\_\_  
Parent: \_\_\_\_\_ Employer: \_\_\_\_\_  
Friend: \_\_\_\_\_ School: \_\_\_\_\_  
Self: \_\_\_\_\_ Other: \_\_\_\_\_

(5) Check only one box indicating how long Central Valley PT can use this authorization:  
☐ I Disclose my information indefinitely (as long as Central Valley PT has custody of my files)  
☐ I Disclose my PHI for the following period beginning \_\_\_\_/\_\_\_\_/\_\_\_\_ and ending \_\_\_\_/\_\_\_\_/\_\_\_\_

(6) Please initial all items below indicating that you have read and understand the rights or information below:  
\_\_\_\_ I understand that this authorization does not expire unless I have indicated an expiration date above  
\_\_\_\_ I understand that I can refuse to give authorization without fear of retaliation or treatment limitations  
\_\_\_\_ I understand that if I give authorization I may revoke it at any time by notifying Central Valley PT in writing  
\_\_\_\_ I understand that the information used/disclosed as a result of my authorization may be subject to re-disclosure by the recipient and may not be protected by Federal privacy regulations once in the recipient's possession  
\_\_\_\_ I understand that if Central Valley PT requests my authorization it is required to tell me the purpose and to whom my PHI (protected health information) is being released to  
\_\_\_\_ I understand that I will receive a copy of this authorization after I sign it and before I sign, if I request it  
\_\_\_\_ Central Valley PT will not be compensated for using or disclosing my PHI, unless related to treatment/payment procedures, without specific permission from me after full disclosure of purpose and intent

# Question 4

An attorney's office calls and requests medical records to be faxed over to their office. The office does not have a release or subpoena on file and the receptionist requesting the information does not have one to fax you. Can you release this information?

- Yes
- No

# Release of PHI

- Before releasing any PHI
  - Verify the requesting entity's authority to request PHI
    - One of 4 approved disclosures
    - Appropriate patient authorization in place (see last slide)
- Verify fax, address, etc PHI being sent to
- *Do not send PHI via e-mail addresses outside of M4L domains*
- Keep log / record of all PHI released in the patient chart or Billing System notes

*\*Before any PHI is released (unless it is directly to a patient or treating physician), please get approval from the Records Dept\**

# Question 5

John is a 17-year old patient at your clinic. His mother comes into the office to request his medical records. She has a signed medical records release form. Can we release records to her without John's permission?

- Yes
- No

# Question 6

It is okay to send patients their medical records via e-mail?

- Yes
- No

# Individual Patient Rights

## **Each patient has the right:**

- To request a copy of our practice “Health Information Privacy Notice”
- To expect that all PHI will be protected per law.
- To view and request a copy of their PHI (access to PHI).
- To request revision of inaccuracies or to add information that has been omitted in their PHI.
- To restrict how their PHI is used and disclosed (except those noted on the prior slide – “Permitted Uses & Disclosures).
- To request confidential communication of PHI.
- To file a complaint related to compliance.



# Question 7

Your friend comes into the clinic to meet you for lunch and notices a patient, Tom, which he knows. He asks over lunch, “what is wrong with Tom?” Under HIPAA guidelines are you allowed to explain Tom’s condition?

- Yes
- No

# “Incidental” Disclosures

- No HIPAA violation if disclosure is “incidental”
- Examples of Incidental Disclosures
  - Overheard conversations
  - Leaving brief messages on a patient’s voice mail
- Voicemails for patients:
  - Reminder call example script:
    - “Hello, this is Sally calling from Avid Physical Therapy to remind you of your 10am appointment tomorrow, October 5<sup>th</sup>. Please call us at 494-6645 if you have any questions or need to reschedule.”
      - This script is appropriate unless the patient has specifically stated not to leave a message.
  - Follow up call for a no show or cancellation example script:
    - “Hello, this is Sally calling from San Luis Sports Therapy. Please call us at 543-7771. Thank you!”
      - We do not mention the reason for the call.

# Team Member Responsibilities

- **Each team member should understand and carry out our organizations privacy & security policies and procedures**
- **Report any violation of PHI data management or security breach**
- **Participate in ongoing organization training & education**
- **Our Health Information Privacy Notice:**
  - Should be available in the patient area (available in a binder in the waiting area)
  - On our websites
  - Offered or provided to each patient in it's full form. A signed acknowledgement that they were offered a copy of the notice should be retained in each patient chart.

# Question 8

Who should you notify should you witness or hear of a complaint regarding a privacy infraction?

- a. The patient's physician
- b. Your Office Director or the Privacy Officer
- c. No one, you don't want to draw attention to the matter

# Security of PHI

## Patient Privacy

- All PHI must be kept in areas so that it is kept private (patient charts, schedule, etc.)
- Utilize privacy curtains, knock on doors, avoid talking about patient cases in public areas of the office

## Discarding Patient PHI

- Always shred any documentation that contains PHI. Never discard PHI documents in the trash without shredding.
- If you should become aware of PHI being improperly disposed of, please notify your supervisor or the compliance officer.

# Question 9

You find patient records in the trash that have patient name, diagnosis, and initial evaluation results listed. What do you do?

- a. Remove the records from the trash and report this to your office director.
- b. Take out the trash and dispose of the records.
- c. Read the chart to see if there is anything important documented.
- d. None of the above.

# Security of PHI

## Chart Storage

- In offices that have after hour non-PT use, i.e. gym clients (or non-M4L employees completing cleaning services) ALL documents containing PHI must be securely put away and locked.
- Medical records/documents are not to leave the office under ordinary circumstances
- Company computers are to stay on premises except for clinic director use
- Charts must be retained for 10 years from the date of treatment,
  - For minors, charts need to be retained for 10 years past their 18<sup>th</sup> birthday

# Security of PHI

## Computers with PHI

- Do not share log-in or password information to your computer, e-mail, Google, Clinicient or ADP account or any database that may contain PHI.
- Log off of a computer when you are not using it.
- Log off and shut down computers at the end of the business day.
- Screen savers will be automatically set by the IT team. They are required as a means of security.

## Scanning

- Do not store PHI on hard drives of company computers, upload to Clinicient if needed or scan and send via email within company emails/company locations then delete.



# Security of PHI

## E-Mail

- Do not send e-mails containing any PHI outside of our company-sponsored e-mail accounts
- Do not e-mail patients/MD any PHI
- Do not use your personal e-mail account for any company business

## Social Media

- Please see the Employee Policy & Procedure Manual for our Social Media Policy
- Do not post any PHI on social media sites or communicate with patients about their condition/patient status

# Business Associates

- A Business Associate is anyone acting on behalf of a covered entity (us) whose function involves the use, disclosure or has exposure to PHI
- Examples: Shredding company, interpreters, DME/brace providers
- All Business Associates need to have agreements with our company
  - Should we enter into a new relationship with a vendor that has access to PHI, please notify the compliance officer so an agreement can be completed

# Privacy Concerns in the Workplace

Privacy pertains to co-workers as well...

- Employees are prohibited from providing any information regarding current or former employees, volunteers, seasonal, contractual, temporary or agency employees to co-workers or anyone outside of the company. These types of inquiries should be referred to the Human Resources Department.
- \* This includes employment verifications, references, medical information requests, etc.

# Question 10

There is a local high school athlete being treated in your office who is the starting quarterback of the school team. A local fan asks if you are seeing this patient and if he will be back for this week's CIF game. Are you allowed to release this information?

- Yes
- No