HIPAA and PHI General Guidelines.

PHI is defined as: 1) individually identifiable health information and 2) is used or disclosed to a covered Entity during the course of care. Examples are: email to a doctor's office for medicine or scripts, Appointment scheduling, MRI scans, test results.

POLICY:

PMR will reasonably safeguard PHI to limit incidental uses or disclosures. An incidental use or disclosure is a secondary use disclosure closure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure. For example: a conversation that is overheard despite attempts by the speakers to avoid being heard. All members of the PMR workforce will follow these guidelines in handling PHI to limit incidental uses and disclosures.

Minimum Necessary Standard

The minimum necessary standard states that you must make a reasonable effort not to use or disclose more than the amount of PHI necessary to accomplish your purpose. In other words, don't release more information than the recipient needs.

Guidelines to Guard Protected Health Information

Computer screens:

1. Computer screens at each workstation must be positioned so that only authorized users at that workstation can read the display. When screens cannot be relocated, filters, hoods, or other devices may be employed.

2. Computer displays will be configured to display a screen saver, when left unattended for more than a brief period of time. After 10 minutes, you will be required to re-enter your password. After 2 hours, you will be logged off the system completely. Any exceptions to this policy will require the approval of the Security Officer.

Conversations:

1. Conversations concerning Individual care or other PHI must be conducted in a manner that reduces the likelihood of being overheard by others.

2. Wherever reasonably possible, barriers will be used to reduce the opportunity for conversations to be overheard.

What if someone oversees or overhears information?

No *one can guarantee the privacy of health Information. But when you follow the Privacy Rule requirements on how to use and disclose health information, and if you have taken reasonable safeguards to protect that Information, you will be okay* because *this is considered an "incidental" use end disclosure*.

Copying medical records and other PHI:

1. When PHI is copied, only the Information that is necessary to accomplish the purpose for which the copy is being made may be copied. This may require that part of a page be masked.

Desks and countertops:

1. Provider reports and other documents which may display identifiers and other "keys" to information should be placed face down on counters, desks, and other places where individuals or visitors can see them.

2. Wherever it is reasonably possible to do so, medical reports and other documents containing PHI will not be left on desks and countertops after business hours. Supervisors will take reasonable steps to provide all work areas where PHI Is used in paper form with lockable storage bins, lockable desk drawers, or other means to secure PHI during periods when the area Is left unattended.

3. In areas where locked storage after hours cannot reasonably be accomplished, PHI must be kept out of sight. A supervisor must be present whenever someone who Is not authorized to have access to that data Is in the area,

Disposal of paper with PHI:

1. Paper documents containing PHI must be shredded when no longer needed. If retained for a commercial shredder, they must be kept in a locked bin.

Home office:

1. Any member of the workforce who is authorized to work from a home office must assure that the home office complies with all applicable policies and procedures regarding the security and privacy of PHI, including these guidelines.

Key policy: PMR has a strict key policy

1. The Compliance Officer will develop a list of which personnel, by job title, may have access to which keys. This includes 'keys to storage cabinets, storage rooms, and buildings.

2. All keys must be signed out.

3. Keys must be surrendered upon termination of employment.

4. The Compliance Officer will act to change locks whenever there Is evidence that a key is no longer under the control of an authorized member of the workforce, and its loss presents a security threat that Justifies the expense.

Records carried from one building to another:

1. When PHI is carried from one building to another, it must be signed out and signed in.

2. When a member of the workforce is transporting PHI from one building to another, it may not be left unattended unless it is in a locked vehicle, in an opaque, locked container. Locking the vehicle alone is not sufficient.

Record storage:

1. Areas where records and other documents that contain PHI are stored must be secure,

   a. Wherever reasonably possible, the PHI will be stored in locking cabinets.

   b. In the medical records department, access will be limited and strictly adhered to. Medical Records personnel will secure this department at the end of each business day.

Personal Digital Assistants and other devices:

1. Physical Medicine & Rehabilitation privacy and security policies apply to any PHI that is stored on a PDA, Laptop, Desk Computer, iPad, smart phone, telephone, television or any other form of PDA. This applies to all devices regardless of ownersh

2. Users of any form of PDAs are responsible for assuring that the PHI on their devices is kept secure and private.

3. Any loss or theft of any form of PDA must be reported to the Security Officer Immediately, including personally owned devices that have PHI stored on it.
4. Users of PDAs who store PHI on their devices will receive special training in the risks *of* this practice, and measures that they can take to reduce the risk, such as the use of passwords, encryption, working from the company server only etc.
5. Use of personal devices and work from home must be approved, in advance, by the Security Officer.

Printers and fax machines:

1. Printers and fax machines must be located in secure areas, where only authorized members of the workforce can have access to documents being printed. A PMR approved cover sheet must be used each time a fax is sent.

Workforce vigilance;

1. All members of the workforce are responsible to watch for unauthorized use or disclosure of PHI, to act or prevent the action, and to report suspected breaches of privacy and security policies to their supervisor, or the Compliance Officer (example of a breach: individual or visitor looking through PHI left on a counter).

Verifying the Identity and authority of a recipient:

1. Anytime health or personal information is requested or released – whether In person, over the phone, or by computer – you must verify his or her identity (that they are who they say they are). You must also verify their authority {that they have a right to see the Information they are requesting),

2. When a person calls you on the phone and tells you they are the patient, you verify this is true by asking for the last four digits of their social security number and/or their birth date.

Visitors:

Visitors to areas where PHI is being used must be accompanied by a member of

the Physical Medicine & Rehabilitation workforce at all times.

Our Policy Compliance Officer: Heather Pavell Is our Compliance Officer. She is responsible for the development and Implementation of the policies and procedures for Physical Medicine & Rehabilitation, as well as being responsible for employee education and documenting HIPAA complaints. Ms. Pavell's phone number is 201567-2277 and her email address is HPavell@rehabmed.net. She is located at The Physical Medicine and Rehabilitation Center, 500 Grand Avenue, Englewood, NJ 07631.

Sanctions for Violating Privacy and Security Policies and Procedures

POLICY:

Members of Physical Medicine & Rehabilitation workforce are subject to disciplinary action for violation of policies and procedures. Violations that jeopardize the privacy or security of PHI are particularly serious. This seriousness will be reflected in the nature of the disciplinary action, up to and including termination of employment.

1. All members of the workforce wlll be treated fairly and equitably in the imposition of sanctions for privacy and security violations.

2. Sanctions will be integrated Into Physical Medicine & Rehabilitation overall employee discipline policy. This policy will be in writing.

3. Disciplinary actions due to breaches of privacy or security of PHI will be documented, and the documentation must be retained for seven years. Disclosure of PHI in violation of policy is reportable under the accounting of disclosures of Protected Health Information policy.

4. No member of the workforce will be subject to sanctions for a disclosure of PHI made in good faith in accordance with the following policies:

    a. Disclosure of protected health information by "whistleblowers".

    b. Disclosures of protected health Information by workforce members who are the victims of a crime.

Disclosure of Protected Health Information by "Whistleblowers"

POLICY:

A member of the workforce of PMR is not in violation of the requirements of PMR policies regarding uses and disclosures of protected health information:

1. When the workforce member believes, in good faith, that PMR has engaged in conduct that Is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by PMR potentially endanger one or more individuals, workers, or the public; and

2. When PHI is disclosed to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or

conditions of PMR or to an appropriate health care accreditation organization, for the purpose of reporting the allegation of failure to meet professional standards or misconduct by PMR.

The PHI may also be disclosed by the workforce member to an attorney who is retained for the purpose of determining the legal options of the workforce member with regard to the conduct described above.

Disclosures of Protected Health Information by Workforce Members Who Are the Victims of Crime

POLICY:

A PMR workforce member who is the victim of a criminal act may disclose protected health Information (PHI) to a law enforcement office without violating PMR policies regarding the use and disclosure of PHI, provided that:

1. The PHI that is disclosed pertains to the suspected perpetrator *of* the criminal act; and

2. The PHI that is disclosed is limited to the following information:
   a. Name and address,
   b. Date and place of birth,
   c. Social security number,
   d. ABO blood type and RH factor,
   e. Type of injury,
   f. Date and time of treatment,
   g. Date and time of death, if applicable, and
   h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence of absence of fijclal hair (beard or moustache)t scars, and tattoos.

3. Other than the Information listed in number 2 above, no PHI related to the individual's DNA or DNA analysis, dental records or typing, samples or analysis of body fluids or tissue may be disclosed.

A disclosure made under this pollcy must be recorded for inclusion in any accounting of disclosures, to the extent that PMR is aware.

HIPAA Safeguards

Termination or Modification of Access to Protected Health Information: Electronic Systems

POLICY:

PMR will terminate access to Information systems and other sources of protected health Information (PHI), Including access to rooms or buildings where PHI is located, when a PMR employee, agent, or contractor ends his/her employment or engagement. PMR will terminate access to specific types of PHI when the status of any member of the workforce no longer requires access to those types of information.

Assignment of Security Responsibility

POLICY:

PMR recognizes the importance of specialized oversight for the development and implementation of the organization's security responsibilities. For this purpose, the Compliance Officer shall be assigned the responsibility to manage and supervise the execution and use of security measures to protect PMR data and to manage and supervise personnel in relation to the protection of this data. There will be:

1. An oversight process for systems certification.
2. A coordinated PMR contingency plan.
3. A process to oversee information access control standards.
4. Monitoring of internal audit controls of system records activity and respond to variances.
5. Maintenance of personnel authorization controls and clearance records.
6. Process to oversee Security Configuration Management.
7. Process to oversee Security Incident Procedures.
8. Process to oversee the Security Management Process including Risk Analysis and Risk Management provisions.
9. Coordinate termination and/or modification of access to information systems.
10. Provide technical assistance for universal security awareness training.
11. Process to oversee Media Controls.

Physical Access Controls

PMR will maintain strict physical access controls to Its Information systems at all times and under all conditions. This includes the physical security of electronic and paper data. Physical access controls Include the following:

1. Disaster Recovery.
2. Emergency mode operation.
3. Equipment and media control.
4. A facility security plan and procedures for verifying access authorizations prior to granting physical access.
5. Maintenance records.
6. Sign-in procedure for visitors to sensitive areas, and escorts If appropriate.
7. Testing and revision of physical access control plans periodically.

These controls are detailed in facilities security plan, which is maintained by the Security Officer.

Policies and Guidelines on Work Station Use and Location

Policy:

PMR will provide secure workstations containing computer or other devices with physical safeguards to minimize the possibility of unauthorized observation on or access to protected health information (PHI). Areas where sensitive information is regularly entered or utilized will be secured using barriers to prevent public viewing of PHI during normal working hours. Wherever feasible, these areas will be looked when not in use. Printers and fax machines will be located in the most secure areas available, and will not be located in or near areas frequented by individuals or the public.

Facsimile Machines and Protected Health Information

POLICY:

1. PHI may be transmitted by facsimile machine ("fax"), provided all other PMR policies and procedures regarding the disclosure of PHI are observed.

2. In order to reduce the potential for misdirected faxes, frequently used destination numbers will be preprogrammed into fax machines and tested before being used to transmit PHI.

3. To further reduce the possibility of misdirected faxes, each fax machine will display a key that identifies the destination for each pre-programmed fax number.

4. When PHI is faxed to a destination number that is not pre-programmed, the fax machine operation will double check the accuracy of the number in the machine's display before sending the fax.

5. All fax messages will include PMR approved cover sheet with the following statement that includes the confidentiality statement:

> Confidentiality Statement: The information contained In this facsimile Is privileged and confidential Information. This document may contain information which is protected under state and/or federal law. The Information contained is the Intended for the use of the individual or entity noted above. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver It to the Intended recipient, you are hereby notified that any dissemination, distribution, or copying of this Information is strictly prohibited. If you have received this communication in error, please notify us by telephone at 201-567-2277. Thank you.

6. Fax machines that are used to transmit or receive PHI shall be placed in secure locations. Whenever possible, fax machines used tQ receive PHI will not be used regularly for other purposes.

7. Transmittal sheets will be checked immediately after each transmission of PHI to assure that the information was sent to the correct number. If an error is detected, the sender must immediately act to correct the error, and report the error to the PMR Compliance Officer.

8. Transmittal sheets will be filed with the PHI that was transmitted, to document the recipient.

9. Use of fax machines with carbon rolls will be discontinued whenever reasonably possible. Carbon rolls will be disposed of in a way that makes it impossible to read the image on the film.

Electronic Transmission and Protected Health Information

POLICY:

PHI may not be transmitted by electronic transmission unless the sender is using a secure electronic transmission system. Employees may only send PHI using the PMR server. It is not secure to send PHI, that is not encrypted, via e-mail or other forms of electronic submission to other sources.

A secure email/electronic submission system has the following features:
The message cannot be intercepted. If the message is sent over an open network (e.g. the Internet) it must be encrypted, using an encryption standard approved by the Security Officer

1. The recipient of the message will know that the content has not been altered during transmission.
2. The recipient of the message will know the true Identity of the sender.
3. There are safeguards to lessen the possibility of sending the message to someone who is not authorized to receive it.
4. There are safeguards to reduce the likelihood that the message will be forwarded to someone who is not an intended recipient.
5. The e-mail/electronic submission will be linked to the individual's record in some way, either as a paper copy or an electronic file.
6. The system has been approved by the Security Officer as secure, in accordance with this policy.

"Instant Message" programs are inherently not secure and may not be used to transmit PHI.

Business Associate Contracts:

Our organization has identified its business associates and has contracts In place with each entity. Examples of business associates Include lawyers that see health Information to do their job, copying services, shredding services, transcriptions services, and many other vendors that see health Information.

Chain of Trust Agreements are also utilized by PMR. In any case where a vendor will have access to any electronic information, a Chain of Trust agreement must be in place.

Patient's Rights

Introduction

The Privacy Rule provides patients the right to know health care organizations handle their health information, and it provides patients the right to control some of those uses and disclosures.

The Privacy Rights of a Patient

The Privacy Rule provides certain rights to patients, some of which are new and some of which patients already have:

1. Right to Notice of Privacy Practices

Patients must be informed of the privacy practices of covered entities, in what is called the Notice of Privacy Practices {the Notice). The Notice explains how an organization handles health information and describes patients rights. The Notice must also provide Information on how the patient can enforce those rights in the organization and how to file a complaint with the organization and with the government.

Notice of Privacy Practices and Its Use

HIPAA mandates that patients have the right to receive notification of the privacy practices. The Notice of Privacy Practices is to be a public document and will be available to anyone who requests it.

Physical Medicine & Rehabilitation Center will use and disclose protected health Information only in conformance with the contents of the Notice of Privacy Practices. We will promptly revise a Notice of Privacy Practices whenever there is a material change to our uses or disclosures of Protected Health Information to our legal duties, to the patients' rights, or to other privacy practices that render the statements in that Notice no longer accurate.