

SPECTRUM[®]

HEALTHCARE RESOURCES

HIPAA Notice

HIPAA Compliance Statement

At SHR, understanding and complying with HIPAA standards is a key priority. SHR has studied the regulations and is taking appropriate action to comply with HIPAA standards.

SHR already maintains a heightened sensitivity to client and personal information. All SHR associates are expected to handle sensitive and personal information in a manner that ensures confidentiality. In addition, SHR senior management has committed resources to addressing HIPAA regulations. SHR will provide ongoing training to all employees.

SHR is dedicated to protecting the security and confidentiality of our clients' patient information. For more information on the TeamHealth/SHR HIPAA Compliance Program, contact Paul Gleis, Corporate Compliance at 865-293-5400.

What is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act. Portability guarantees health coverage when an individual's job changes. Accountability requires health care institutions to protect patient information. As a company we are required to take REASONABLE MEASURES to protect the privacy of patient's protected health information.

Does HIPAA apply to me?

HIPAA applies to everyone. If you work with patients, or with information about patients, you need to know about HIPAA. Even if you have no direct patient contact, the law still applies to you, simply because you work here. So, it's important that everyone knows about HIPAA.

What is Protected Health Information (PHI)?

Any information that identifies or could identify a person. The person could be living or dead. Information could be about the past, present, or future physical health, mental health, or condition of a person, written on paper, displayed or stored in a computer or spoken in conversation.

- Name
- Address
- SSN
- Relatives' names
- Employer names
- E-mail address
- Medical Record Number
- Health plan beneficiary number
- Telephone number
- Fax Number
- Birth date
- Certificate/license number
- Account number
- Finger/voice print
- Photographic images
- Internet Protocol (IPP address)
- Any unique identifying number, characteristic or code
- Any vehicle or device serial number
- Web UR

What do I do if I find papers that contain protected health information?

Papers that have protected health information on them should not be left out in the open or unattended. If you find papers that contain protected health information you should find the owner and return the papers to them or give them to your supervisor. Fax machines and printers that transmit protected health information should be located in a private area.

SPECTRUM[®]

HEALTHCARE RESOURCES

What can we do with PHI?

Covered entities are free to use PHI for the purpose of TREATMENT, PAYMENT and HEALTHCARE OPERATIONS. This includes things like ordering lab tests, billing, quality control and credentialing. Almost everything else requires patient authorization. One Exception: Disclosures required by law.

What is meant by "Use" & "Disclosure"?

The Privacy Rules of HIPAA limit both the use and disclosure of patient information. "Use" refers to what we do with information is given out to another institution to use. Patients typically give permission for use or disclosure of their information by signing a written form.

What patient information can I look at?

If it is not part of your job, it's not part of your business! If you are not involved in a patient's care you are not allowed to review their health information. NO ONE is allowed to look up information on friends, strangers, family members or even themselves.

What are patient's rights under HIPAA?

The HIPAA Privacy Regulations grant patients six (6) new rights in connection with their protected health information. Our organization will be implementing new policies and procedures to provide these rights to our patients.

1. Receive Notice of Privacy Practices

Patients will receive a notice describing Military Health Systems (MHS) privacy practices that is, when and why we use and disclose a patient's protected health information. The notice will give examples of disclosures we might make as well disclosures we are required by law to make.

2. Inspect and Receive a Copy of Their Protected Health Information

Patients have the right to inspect and receive a copy of their protected health information. There are limited exceptions to this rule-for instance, access to psychotherapy notes or information that may harm the patient or others may be denied. MHS procedures will assure that patient's requests for access to their information are handled properly.

3. Amend Their Protected Health Information

Patient's have the right to request that their protected health information be amended or corrected in those cases where the information is incorrect or incomplete, MHS will have procedures that outline how patient requests for amendments will be processed.

4. Request Restrictions on Disclosures

Patients have the right to request restrictions on how our organization uses and discloses their protected health information. MHS policies and procedures will spell out who such requests should be submitted to and how we will respond to such requests.

5. Request Alternative Means of Communication

Patient's have the right to ask that e communicate their protected health information by alternative means. For example, a patient may request that written correspondence from her doctor be mailed to a special post office box. MHS procedures will outline how these requests will be processed.

6. Obtain Accounting of Disclosures

Patients may get an accounting - a detailed listing - of all disclosures of their protected health information made during the six years prior to the date of the request. The accounting does not need to include any disclosures made to carry out treatment, payment of health care operations. MHS procedures will identify who will be responsible for providing these listings.

Violation of HIPAA

Unintentional disclosure of information can lead to civil fines up to \$100. Intentional disclosure of information can lead to criminal sanctions punishable up to \$250,000 and 10 years in prison. Violations of SHR's HIPAA Policies and Procedures will lead to disciplinary actions up to and including termination.

SPECTRUM[®]

HEALTHCARE RESOURCES

HIPAA SECURITY STANDARDS

Introduction

Effective April 21, 2005 Spectrum Healthcare Resources must comply with HIPAA security standards as they relate to the handling of Protected Health Information (PHI). SHR is required to maintain formal, documented policies and procedures to limit physical access while ensuring that properly authorized access is allowed. In general, users of PHI should have access only to the data he or she needs to perform his/her particular function. Please review the following to ensure that all employees are complying with the security standards for HIPAA.

Questions regarding HIPAA Security Standards should be directed to your SHR representative. Thank you for your assistance with this matter.

HIPAA Security Standards

1. Physical Safeguards

- Do not give your office key or fob to those who are not authorized to work in your area
- Question those who look like they do not belong in your work area
- Keep file cabinets containing PHI locked and limit who has a key to the cabinet
- Keep doors to offices with PHI locked and limit who has a key to the office
- Ensure that your computer view screen containing PHI is not visible to others
- Log off your computer when you are leaving your work station
- Lock your computer station when you are not physically present by pressing ctrl, alt, delete (simultaneously)

2. Technical Safeguards

- Do not give your password or user ID access to anyone else - Your user ID and password identify you as the user and can show everything you do on your computer
- As you may be required, from time to time, to download information from Spectrum Healthcare Resources Information Systems, keep all data downloaded to a floppy disc, PDA, or external memory device secure (under lock and key, encrypted or password protected)
- All faxes and e-mails must have the Spectrum Healthcare Resources HIPAA compliant language

3. Administrative Safeguards

- All employees are required to attend HIPAA training
- All employees are required to comply with all aspects of HIPAA including security standards
- Failure to comply with training or adhere to HIPAA standards will result in progressive disciplinary action, up to and including termination

HITECH

Promptly reporting HIPAA violations is even more of a critical concern now that it has been expanded to include HITECH, or Health Information Technology for Economic and Clinical Health. This new law includes some potentially serious penalties that can extend beyond the organization and personally impact the individuals responsible for a violation.

44 states now have their own breach laws, which may differ from the Federal laws. Some states, such as California, require a patient and state government notification within 5 days of the incident, even though the Federal law only requires notification within 60 days. When you discover a breach or violation, contact your SHR representative immediately.

If you access someone's information out of curiosity, you could be held personally responsible, not just the organization. HITECH includes civil and criminal penalties for both the organization and the individual responsible for the breach.

Remember that it's critical to notify your SHR representative immediately if you suspect there might be a breach. They may ask you for additional information to clarify the facts surrounding the situation. Your SHR representative will take it from there and work with you in a friendly and professional manner to resolve the situation.

ANNUAL RE-TRAINING ACKNOWLEDGEMENT FORM
Employees Only

I hereby acknowledge that I have read and understand the following training materials presented to me. I agree to protect and not disclose any Protected Health Information (PHI). I also understand that it is my responsibility to report any misuse or abuse of PHI. If I am uncertain or unclear on the “use” and “disclosure” of PHI, I understand it is my responsibility to contact my supervisor, the Human Resources Department, or the Corporate Compliance Hotline. I further acknowledge that any incident of non-compliance will result in disciplinary action up to and including termination, and may also result in civil and or criminal fines.

(Check those completed)

- HIPAA Guidelines & Security Standards
- OSHA Training on Blood-Borne Pathogens
- Joint Commission National Patient and Safety Goals
- Patient Bill of Rights and Responsibilities in the Military Health System (MHS)

OR

- I affirm that I have attended the above training at the MTF during annual training.

Printed Name

Signature

Date