HIPAA HELPER

HIPAA

Protecting Patient Privacy

ASPIRUS™

Passion for excellence.
Compassion for people.

HIPAA-003 (juf 1/26/09)

PENALTIES FOR VIOLATIONS

HIPAA violations include but are not limited to:

- Failure to comply with HIPAA regulations
- Knowingly or wrongly disclosing or receiving Protected Health Information
- Obtaining information under false pretenses
- Obtaining information with the intent to:
    - Sell or transfer it
    - Use it for commercial advantage
    - Use it for personal gain
    - Use it for malicious harm

Civil penalties range from $100 per violation, per person, up to a limit of $25,000.

Criminal penalties can be as high as a $250,000 fine or a prison sentence up to 10 years.

PATIENT PRIVACY: EVERYONE'S RESPONSIBILITY

Everyone is responsible to respect the patient's right to privacy by:

- Keeping information confidential
- Resisting human nature to be curious and to share information about others
- Knowing that improper disclosure of Protected Health Information violates the law – **This includes accessing your own information.**
- Knowing Aspirus' privacy policies

The HIPAA Helper Reference Guide has been developed with input from the various teams involved in preparing Aspirus to be in compliance with the HIPAA Privacy Regulations. This booklet will provide facts and tips on how to respond to the most common questions about privacy practices. Where possible, there are references to related policies and procedures that will provide more thorough and in-depth information.

I hope you find this tool helpful and I thank you in advance for your contribution to assuring patients' rights to privacy and confidentiality of their protected health information.

Sandy Lakey, RHIA, CHP
Aspirus Privacy Officer

USE OF PHI FOR MARKETING PURPOSES

Under the Privacy Regulations, marketing is defined as communication about a product or service to encourage recipients of the message to purchase or use the product or service.

Communication is not considered marketing, and use of Protected Health Information (PHI) can occur without authorization, if made for one of the following purposes:

- Communications made by an organization for the purpose of describing the services offered or payment for such services.
- Communications made by a healthcare provider as part of the treatment, case management or care coordination of a patient, and for the purpose of furthering that treatment.
- Communication is a face-to-face encounter with the individual.
- Communication involves promotional gifts of nominal value provided by the covered entity such as sending calendars, pens or inexpensive sample products to generally promote the organization.

For more information, refer to policy #6531.

RESPONSIBILITY OF EMPLOYEES TO REPORT VIOLATIONS

It is the duty of all Aspirus employees to report incidents of non-compliance with the Privacy Regulations. Employees can do so confidentially by calling the **Business Ethics Hotline at Extension 72166 or 1-800-450-2339.**

This will put employees in touch with Aspirus' Privacy Officer.

For more information, see the Business Ethics Hotline Policy #6222.

Privacy Regulations allow healthcare providers to disclose to jailers Protected Health Information about an inmate which is necessary for the health of the inmate, the health of other inmates or the health of employees of the correctional institution.

From a practical standpoint, correctional facilities need to know the medical condition of their inmates because those facilities are responsible for the care of the inmates as well as the safety of others in the facilities.

RELEASE OF INFORMATION FOR RESEARCH PURPOSES

The use and disclosure of Protected Health Information (PHI) for research purposes has specific regulations under the Privacy Regulations. Research is not considered to be treatment, payment or healthcare operational activities; therefore, using or releasing PHI for research requires authorization from the study participant.

There are certain circumstances in which the requirement for obtaining authorization may be waived. This request must be reviewed and approved by the Institutional Review Committee of Aspirus and Aspirus Wausau Hospital.

Researchers can access PHI in several other specific circumstances such as work in preparation for research that uses only information in which the identity of patients is not known and that uses only a limited data set. However, in each of these situations, the research staff must follow guidelines for accessing, using and disclosing PHI.

More information can be found in the "HIPAA and Research: A Reference Guide" available from the Human Research Protections Coordinator at the Aspirus Health Foundation.

ASPIRUS MISSION AND VISION STATEMENTS

Aspirus Mission Statement

Aspirus is an integrated, community-governed healthcare system, which leads by advancing initiatives dedicated to improving the health of all we serve.We work collaboratively with others who share our passion for excellence and compassion for people.

Vision Statement

Aspirus is the region's health care system of choice. We deliver value, innovation, excellence and compassion.

WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a far-reaching federal law comprised of more than 1,500 pages of regulations. Much of the law has to do with assuring security of electronic transmission of patient information. However, for most people in healthcare, the regulations that protect patient privacy will have the most impact. In general, HIPAA is prescriptive and defines how information can be used and disclosed, rather than what is prohibited.

Aspirus organizations, clinics whose physicians practice at Aspirus organizations and other organizations which do business with Aspirus were required to be in full compliance with HIPAA Privacy Regulations by April 14, 2003.

PRIVACY REGULATIONS

HIPAA Privacy Regulations create national standards to protect medical records and other Protected Health Information (PHI) of individuals.

What is PHI?
Protected Health Information (PHI) is information that identifies the patient as an individual such as:

- Patient's name
- Any part of the patient's address
- Date of birth
- Admission and discharge date
- Telephone, fax number or e-mail address
- Medical record number, health plan number
- Social Security number
- Driver's License number

PATIENT'S RIGHTS UNDER THE PRIVACY NOTICE

When they first arrive at an Aspirus facility or begin to receive service from an Aspirus organization, all patients or clients will be given a Privacy Notice which outlines their rights. They will also receive an Acknowledgment of Privacy Notice to sign and have placed in their medical record.

The Privacy Rule gives patients the right to:
1. Receive the Privacy Notice
2. Access, inspect and copy their medical information
3. Amend their medical information
4. Request an accounting of disclosure of their medical information
5. Request restrictions on use and disclosure of their medical information
6. File a complaint

Access
Patients have the right to:
- Access or inspect their health record
- Obtain a copy of their health record (a reasonable fee for copying can be charged)

- Abortion in the following situations only
  a) medical emergency exists.
  b) pregnancy resulted from a sexual assault, sexual intercourse with a caregiver or abuse inflicted by minor's legal guardian.
  c) Psychiatrist or psychologist states in writing the minor will likely commit suicide rather than approach parent or legal guardian.

Even though parental consent is not required in the above exceptions, a parent still maintains access to the minor's records with respect to medical treatment.

Minors with divorced parents
Consent and record access remain consistent whether the parents are married or divorced. Unless denied physical placement, parents have the right to access their minor child's medical records and have the right to consent to medical treatment.

Aspirus' position is to accept in good faith a parent's representation of his or her right to access a minor child's medical record and consent to medical treatment, unless one parent indicates the other should be denied access or ability to consent. In that situation, burden will be placed on the parent to produce documentation confirming the stated position.

RELEASE OF INFORMATION ABOUT INMATES

Healthcare providers are permitted under both state law and Privacy Regulations to disclose healthcare information about inmates to prison or jail officials including prison nurses and physicians under the following guidelines:

Wisconsin State Statutes permit healthcare providers to give jailers a "written summary of services provided and a description of follow up care and treatment the prisoner requires."

CLERGY ACCESS

Unless the patient has requested Privacy Patient Status, the following information can be released to clergy who have proper identification:

- The patient's name
- The patient's location in the hospital
- The condition of the patient described in general terms
- The patient's religious affiliation (to clergy only)

Aspirus Wausau Hospital will provide clergy and/or their designees the information they need in order to minister to members of their church who are hospitalized. However, every patient has the right to request his or her religious affiliation not be disclosed or placed on the clergy listing. For more information, refer to policy # 6384.

RELEASE OF INFORMATION ABOUT MINORS

As a general rule, parents are responsible for their minor child's care and have access to their minor child's records until the child reaches the age of 18. There are exceptions, such as:

- Parents who have been denied physical placement rights.
- Parents or legal guardians who have a history of abuse or neglect, thus placing the child's safety at risk.

Parental consent to treatment

A parent must consent to medical treatment of a minor child except in the following circumstances:

- Emergency situations
- Emancipated minor, i.e. is married or previously married, has given birth, or has been freed from care, custody and control of parents
- Treatment of a sexually transmitted disease
- Treatment related to pregnancy or treatment of a newborn
- HIV testing

Amend

Patients have the right to:

- Request an amendment to their medical record which might clarify or challenge information in the record

They can do so by sending a written request to the Privacy Officer or the Health Information Management department of the Aspirus organization which holds the information.

The organization will review the request and determine if it agrees or disagrees with the amendment. The request for the amendment and the organization's response will then become part of the medical record.

Accounting Of Disclosures

Patients have the right to:

- Request an accounting of when and where their confidential health information was used or disclosed within the past six years

That list must contain:

- Date of disclosure
- Name of person or organization receiving the information and the address of the organization
- A brief description of what was disclosed and the reason for the disclosure

Exceptions are disclosure for treatment, payment or healthcare operational activities, authorized disclosures and other exceptions contained in the Privacy Regulations.

Restrictions

Patients have the right to:

- Request an organization restrict the use and disclosure of their Protected Health Information. The organization is not required under the Privacy Regulations to accept the request.

File A Complaint

Patients have the right to:

- File a complaint with the Privacy Officer of Aspirus
- File a complaint with Office of Civil Rights which is part of the U.S. Department of Health and Human Services.

DISCLOSURE OF PHI

Treatment

Healthcare organizations may, without the patient's authorization, use or disclose Protected Health Information for treatment, payment and healthcare operational activities. (Referred to as TPO.)

Examples of **treatment activities** are:

- A primary care provider may send a copy of an individual's medical record to a specialist who needs the information to treat the individual
- A hospital may send a patient's health care instructions to the nursing home where the patient is being transferred

Payment

Examples of **payment activities** are:

- A physician might send an individual's health plan coverage information to a laboratory which needs the information to bill for services it provided to the physician treating the individual.
- A hospital Emergency Department might give a patient's payment information to an ambulance service that transported the patient to the hospital in order for the ambulance service to bill the patient.

PRIVACY PATIENT STATUS IN THE HOSPITAL

A hospital patient has the right to request Privacy Patient Status, which would restrict disclosure of any information about the patient's admission and hospitalization.

Upon admission, each patient will receive a Privacy Patient brochure detailing his or her rights and the procedure to follow if the patient chooses to be designated as a Privacy Patient. The patient has the right to request this status at any time during his or her hospitalization.

Privacy Patient Status will:

- Restrict public disclosure of the patient's hospital admission
- Remove the patient's name from the hospital's directory
- Block any phone calls to the patient through the hospital Switchboard
- Require that no information about the patient be given to visitors inquiring at the Information Desk
- Initiate removal of the patient's name from outside the patient's room.

For more information about Privacy Patient Status, see Aspirus Wausau Hospital policy 6384.

RELEASE OF INFORMATION TO PERSONAL REPRESENATIVE

In general, the scope of the personal representative's authority to act for the individual under the Privacy Regulations derives from his or her authority under applicable law. When a person has broad authority to act on behalf of an individual in making healthcare decisions, such as a parent with respect to a minor child or a legal guardian of a mentally incompetent adult, the organization must treat the personal representative as the individual for all purposes under Privacy Regulations, unless an exception applies, such as cases of abuse, neglect or endangerment. This provision, in general, does not apply to Agents named in the Power of Attorney for Health Care (POAHC) documents.

reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy. For example, a hospital visitor may overhear a nurse's confidential conversation with another nurse. Or a visitor might glimpse at a patient's information on a sign-in sheet or nurse's station whiteboard. HIPAA Privacy Regulations are not intended to impede these customary and essential communications and practices and, thus, do not require that all risk of incidental use or disclosure be eliminated to satisfy its standards.

MINIMUM NECESSARY RULE

The Minimum Necessary Rule requires organizations to implement reasonable policies and procedures that limit how much Protected Health Information (PHI) is used, disclosed, and requested for certain purposes. These minimum necessary policies and procedures must also reasonably limit who within the organization has access to protected health information based on job responsibilities and the nature of the business.

TIPS FOR SECURING PROTECTED HEALTH INFORMATION (PHI)

- Turn documents containing PHI face down during the workday
- Secure computer before leaving it unattended (a protective screen saver should be running)
- Place PHI in a closed, secure location at the end of the day (such as files, drawers and cabinets, preferrably locked)
- Do not discuss patients where conversations can be overheard
- Do not share log-ins or passwords
- Question unfamiliar people in your area
- Close doors or curtains when administering patient care
- Do not discuss patients with family or friends

Operational

Examples of **operational activities** are:

- Conducting quality assessment and improvement activities.
- Review of competence or qualifications of health care professionals
- Conducting audits and reviews such as in the compliance program
- Business planning and development activities

PROTECTING PHI

Whiteboards

HIPAA Privacy Regulations allow the staff of covered organizations to take reasonable measures to protect patient confidentiality.

Use of whiteboards

Privacy Regulations **allow** use of whiteboards to track patient information.

Please keep these recommendations in mind:

- Choose a location outside plain view of the public. Whiteboards need to be convenient for the staff and physicians, but should not be accessible to the public.
- Whiteboards in patient rooms are acceptable, but consider carefully what information is written on them.
  For example, only use the patient's first name and last name initial.
- Only put on the board the minimum amount of information necessary for care of the patient.
- Check with your supervisor about whiteboard guidelines specific to your department.

Mail, Sign-in Sheets

Handling of Interoffice mail containing Protected Health Information

Preferably interoffice mail containing confidential information should be placed in a confidential envelope, but closed interoffice envelopes are acceptable, too. If using the pneumatic tube system, place a cover sheet over the information.

Use of Sign-In Sheets

Privacy Regulations allow use of sign-in sheets, but encourage healthcare professionals to take reasonable steps so that patients do not see the names of others on the sign-in sheet.

Voicemail

When leaving voicemail messages always identify yourself, the department/service or clinic you represent and the person you are calling. Also be sure to leave a call back number. During the patient's first visit, you might consider asking the patient his or her preference for leaving telephone messages. In addition:

- DO NOT leave test results unless previously arranged with the patient. It's better to say: "This is Jane with Dr. Smith's office. Please call me at 847-5555. Thank you."
- DO NOT specify the test or procedure. It's better to say: "This is Dr. Smith's office calling to remind Susan of her appointment Tuesday."
- DO NOT leave a message containing the diagnosis or procedure name. Use the word "appointment" instead.
- DO NOT leave messages with children.
- DO NOT leave detailed messages with family members, unless you have the patient's consent.

Use good judgment and professional discretion when leaving a message. For example, if it is late on a Friday afternoon and you can relieve a patient's anxiety by leaving more information about his or her results, this may be appropriate, rather than leaving the patient in suspense until you are available on Monday morning.

Public Areas

Privacy Regulations do not prohibit calling out patient names, but it is expected that you take reasonable steps to protect patient privacy such as calling out first name and last name initial or use Mr./Mrs. or Miss and the last name.

When discussing a patient's condition with family members or with another health professional in a waiting room, remember to speak quietly and, if possible, move to a more private area.

Here are some examples of permitted conversations in public areas:

- Speaking with someone to coordinate services at nurse's station.
- A healthcare professional discussing a patient's condition over the phone with the patient, another healthcare provider or a family member.
- A physician discussing a patient's condition or treatment regimen in the patient's room.
- Healthcare professionals discussing a patient's condition during training rounds or in an academic or training institution.
- A pharmacist discussing a prescription with a patient over the pharmacy counter, with a physician or with the patient over the phone.

USE OR INCIDENTAL DISCLOSURES OF PHI

Privacy Regulations permit certain incidental uses and disclosures of Protected Health Information when the organization has in place