HEALTH INFORMATION PRIVACY and SECURITY

Confidentiality Policy – Information concerning employees, physicians, patients or hospital business may not be accessed, used, or released by unauthorized individuals; or discussed with anyone without written authorization.

The HIPAA **Privacy Rule** sets national standards for the protection of patient information. The Privacy rule covers ALL forms of protected health information… **oral, written and electronic.**

Protected Health Information (PHI)

PHI is any **individually identifiable** health information (IIHI)

Any of the following information can be used to identify a patient:

- Name
- Addresses
- Dates
- Telephone or fax numbers
- Social Security Numbers
- Medical Records Numbers, Patient Account Numbers
- Insurance Plan Numbers
- Vehicle Information
- Certificate/License Numbers
- Medical Equipment Numbers
- Photographs, Fingerprints
- Email addresses, Internet addresses, Web Universal Resource Locators (URLs)
- Any other unique code, characteristic or identifier

Electronic Protected Health Information (EPHI)

EPHI is individually identifiable health information that is **transmitted by electronic media** or **maintained in electronic media**

All information that can identify a patient **must be protected**.

Permitted Uses and Disclosures

HIPAA allows for the provider of care to use and disclose health information for **Treatment, Payment** and **Operations (TPO).** Other permitted uses and disclosures allowed include those required by law, for public health, etc. Patients must sign an **authorization** for the use of their health information for non-TPO or other permitted uses and disclosures.

Under the **Minimum Necessary Rule** members of the workforce should only have access to the information they need to fulfill their assigned duties. (Workforce includes volunteers and students as well as anyone under the direct control of the health care provider, whether or not they are paid.)

The hospital must make reasonable efforts to **limit PHI** to the **minimum necessary** when using, disclosing or requesting information. **Minimum Necessary does not apply** when **disclosing** or **requesting** information for **treatment.**

Patient Rights

Patients have a right to know how their health information may be used or disclosed, and that they have certain privacy rights. These rights are communicated to our patients through a document called **Notice of Privacy Practices (NPP).**

Our Notice of Privacy Practices is distributed upon **registration** and a signed acknowledgement is obtained.

Patient rights allow patients to:

- Access and obtain a copy their medical record – Must refer to Health Information Management Department
- Request to amend their medical record. Must submit request in writing and directed to the Director of Health Information Management/Privacy Officer.
- Obtain a list of who we have disclosed their PHI to for up to the past six years
- Request other communications such as asking to have their bill mailed to an alternate address
- Request restrictions on the use or disclosure of their PHI. The hospital does not have to agree to restrictions. Restrictions are required to be in writing and must be reviewed by the Privacy Officer.

Facility Directory Restrictions

Patients **must** be given the opportunity **to agree** or **object** to be included in the **facility directory**

- Directory includes Patient Name, Location in Hospital and religious affiliation
- During Admission process, patient is asked “May we list your name and location in directory?” and “May we give your name and location to clergy?”

If patient chooses **to be included** in the directory:

- Location may be given to individuals who ask for the patient by name
- Religious affiliation can only be given to clergy

If patient chooses not to be included in directory:

- Patient name is marked as Confidential, “CONF” in the Information System.
- Caller/visitor is be told “I’m sorry, I don’t have any information for that name”

Involvement in the Individuals Care and Notification Purposes

Patients **must** be provided **the opportunity to agree to, prohibit or restrict** the **disclosure** of protected health information (PHI) **for involvement in their care and for notification purposes.**

We may disclose protected health information to a family member, close personal friend, or any other person named by the patient, if the information is relevant to that person’s involvement with the patient’s care or payment of the patient’s health care services.

We may also notify a family member, close personal friend, or any other person named by the patient of the patient’s location, general condition, or death, provided:

- the **patient agrees** to the disclosure(s);
- the patient has had the **opportunity to object** to the disclosure, and the patient did not express an objection; or
- the health care provider reasonably **infers** from the circumstances, using professional judgment, that the **patient does not object** to the disclosure.

If the hospital **suspects** that a patient is a **victim** of **domestic violence** or **abuse**, the hospital **should not disclose** information if there is reason to believe that the information could cause harm to the patient.

In the event that the patient does not have the opportunity to agree or object to the disclosure, the information can be disclosed using **professional judgment,** determining whether the disclosure is in the best interest of the patient and, if so, disclose only the PHI that is relevant to the person's involvement with the patient's health care.

Verification

Workforce members, who are authorized to disclose PHI, must verify the **identity** and **authority** of the person(s) requesting PHI if the identity is not known.

Providing for the security of patient information

We have to make sure all health information, no matter where it is, is secure. This includes information stored on computers. Everyone who uses a computer has a duty to keep health information secure.

Woman's Hospital **Workstation Use** policy states we must protect all patient information on computers by:

- Properly signing-on with individual IDs and passwords
- Signing-off of computers if you leave the work area for more than fifteen minutes
- Protecting computer screens from unwanted viewing
- Never leaving printers unattended when printing confidential information

Password Management

- Log on to the system you may have been given access to using only the ID provided to you and a valid password
- Do not share your password with any other person, including those who may ask
- Use of another person's login ID or password is prohibited
- Passwords must be changed whenever there is any indication of possible password compromise (Request new password from IS Help Desk or System Administrator
- Passwords must be not be written down unless the record can be stored securely
- Passwords must be composed of a mix of numeric and alphabetic characters
- Passwords must not be based on something that can easily be guessed

Proper use of e-mail

Woman's Hospital e-mail policy **prohibits transmission of patient information in an e-mail** message **outside** of the organization. **Patient name** is **prohibited** in the transmission of **internal e-mails**.

Proper use of fax

Faxing of patient information is only permitted in emergency situations. Always use the hospital's cover sheet.

Protection From Malicious Software

- All Woman's Hospital information systems must have installation and regular updating of anti-virus software
- If you are given access to an e-mail account, note the following:
    - Never open any file attachment to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete them by emptying your trash
    - Never download files or programs from unknown or suspicious sources

- Always check with a supervisor before using a floppy diskette from an unknown source
- Never open e-mail attachments when the file name ends with EXE, BAT, COM, VBS, VBE, SHS, VBX, PIF, SCR, LNK, EML, NWS, or SHS (For example, My pictures, EXE)
- If you suspect a virus or worm, notify the Information Security Officer by telephone, 8352 or e-mail

Log-In Monitoring

- If you have access to Woman's Hospital Information systems, note the following:
  - If information regarding your last log-in is inconsistent, report the discrepancy to the Security Officer
  - The number of unsuccessful log-in attempts are limited
  - Unsuccessful log-in attempts may be recorded and monitored

Safeguards

- Keep any documents, faxes, photocopies, reports, schedules, charts, patient boards, etc. hidden from unauthorized viewers
- Never leave file rooms unattended or unlocked.
- Do not discuss patient information with another caregiver in a location where another person may overhear the conversation.

Disposal of Patient Information

We have to handle and dispose of patient information carefully, such as using the **"Shred-it"** container instead of throwing patient information away.
RULE OF THUMB….NEVER dispose of patient information in any open area trash bin.

What are the consequences of not complying with the law?

A **breach** of privacy will subject the workforce to **disciplinary action** up to, and including termination.

It has always been against hospital policy to improperly use, disclose, share, or dispose of patient information in the wrong way. Under HIPAA, there are now fines and penalties for this.

Wrongful and willful disclosure of health information can result in fines from $100 per violation per person up to $25,000 for the identical violation per year. Criminal penalties for "wrongful disclosure" could result in jail sentences up to ten years and fines up to $250,000.

Reporting Violations

It is **EVERYONE's** responsibility to report violations. Any individual receiving an allegation of a breach or having knowledge or a reasonable belief that a breach of confidentiality of PHI may have occurred shall Immediately notify **the Director of Health Information Management/Privacy Officer.**

Rev. 1-25-06

Health Information Privacy and Security Training Documentation

Please sign and complete information below:

I received training regarding the HIPAA Privacy and Security Rules and the Hospital's privacy and security policies and procedures and I agree to comply with all Hospital policies and federal and state laws and regulations relating to the use and disclosure of protected health information. .

_____ _____

Name (Signature) Date

_____

Name (Print)

_____

Affiliation (school/company/and hospital department)