Corporate Policies
Froedtert Hospital Policy

Title: **Confidentiality**
Policy Type: Corporate
Department: Administrative
Policy Number: CPA.0053
Origin Date: 5/25/94
Date Revised: 11/1/2007
Topic(s): Confidentiality, Privacy, Security HIPAA, PHI
Keyword(s): Confidential, Privacy, HIPAA, PHI, Protected Health Information, Compliance, Disclosure, Secure

Purpose: To define the responsibility of all individuals to comply with federal and state laws and Froedtert Hospital policies and procedures regarding proper use, disclosure and protection of confidential information.

Definitions: A. *Workforce*

For purposes of this policy only, workforce is defined as Froedtert Hospital staff members, volunteers, trainees, students (excluding residents, fellows and medical students), and other persons whose conduct in the performance of work for Froedtert, is under the direct control of Froedtert, whether or not they are paid by Froedtert.

B. Individuals

For purposes of this policy, an individual is defined as: Workforce, vendors, business associates, MCW physicians, residents, medical students and staff.

C. Business Associate

A business associate is a person or entity who, on behalf of the hospital, performs or assists in the performance of;

1. A function or activity involving the use or disclosure of PHI, or

2. Provides, other than as a member of the hospital's workforce, legal actuarial, accounting consulting, data aggregation, management, administrative, accreditation or financial services to or for the hospital.

D. Protected Health Information (PHI)

Any information, whether oral, written, electronic, magnetic or recorded in any form that:

1. Is created or received by Froedtert Hospital as a health care provider,

2. Relates to an individual's past, present or future

   a. Physical or mental health condition
   b. Health care treatment
   c. Payment for health care services, and

3. That either clearly identifies an individual (i.e., name, social security number or medical record number) or can be used to find out the person's identity (address, telephone number, birth date, e-mail address and names of relatives or employer).

I. POLICY

A. Certain individuals based on their role and responsibilities, may have access to confidential information which may include, but is not limited to the following:

1. Patient information (such as paper or electronic records, conversations, admission or discharge information, patient financial information, appointment, demographics and other PHI) for purposes of carrying out their job functions.

2. Information pertaining to staff members (such as salaries, employment records, disciplinary actions, etc.).

3. Froedtert Hospital business information (such as financial and statistical records, strategic plans, internal reports and documents, contracts, peer review information, communications, proprietary information including computer programs, source code, proprietary technology, etc.).

4. Third party information (such as insurance, business contracts, vendor and business partner's proprietary information, source code and other technology, etc.).

B. Accessing, Reviewing, Using and/or Disclosing confidential information is allowed only to carry out legitimate job functions. (Within the scope of specific job responsibilities, in accordance with Froedtert policies and procedures and as otherwise permitted or required by law.)

C. All individuals are responsible to follow the detailed policy statements listed above and will:

1. Not in any way disclose, copy, release, sell, loan, review, alter or destroy any confidential information outside the scope of their legitimate job responsibilities.

2. Not access or review your own protected health information. To obtain access to your own protected health information, staff members are required to follow the same process that all patients go through by requesting copies of the records through the HIM Department. See Corporate Policy CPM.0089 Protected Health Information (PHI), General Uses and Disclosures.

3. Not access, review, use or disclose patient information of family, friends, co-workers, VIP's or others unless it is to carry out legitimate job functions. Access to and/or copies of any medical record information, other than for legitimate job functions, must be processed through the HIM Department. Refer to Corporate Policy CPM.0089 Protected Health Information (PHI), General Uses and Disclosures.

4. Exercise reasonable caution when accessing, reviewing, using, discussing and/or disclosing confidential information and take reasonable safeguards to prevent others who do not require access to the information from inadvertently seeing and/or overhearing it.

5. Only discuss patient related information in a work related context. Individuals are not authorized to communicate patient information, including interesting or unusual cases with parties that do not have a business need to know.

6. Dispose of all written materials in any form or format containing any confidential information in accordance with Froedtert policy. (See Policy: CPM.0086 Protected Health Information (PHI), Disposal of.)

7. All departments that store, create or process confidential information must keep it reasonably secure from access by unauthorized persons.

8. Not have any individual rights to, or ownership of any information accessed or created by any individual during his/her relationship with Froedtert.

9. Not use, disclose, exchange or share computer passwords, access codes, key cards or any other security access code, badge or device with any other individual.

10. Not access the network, applications, computer systems or any other electronically stored data under another individual's user ID/login information.

11. Not store PHI on local hard drives or any mobile device unless it has been approved by the F&CH Information Technology Department.

12. Not make any unauthorized transmissions, inquiries, modifications or purging of confidential information. Individuals will not modify their workstation configuration, use or add software to his/her workstation without prior authorization from the F&CH Information Technology Department.

13. Practice good security measures such as keeping all electronic/mobile devices password protected and in a secure location.

14. Safeguard system access codes and accept responsibility for all activities undertaken using individual access codes. If the security of an individual's system access codes has been compromised, it is his/her responsibility to immediately change his/her password and report it to the F&CH Information Technology Security Department.

15. Promptly report to the Corporate Compliance Department, any concerns of activities that may compromise business or patient confidentiality. Froedtert will not retaliate against individuals who, in good faith, bring forth information of non-compliance. (See policy CPA.0062 Corporate Compliance Hotline.)

II. PROCEDURE

Confidentiality & Electronic Security Agreements:(Attached)

A. All members of workforce are required to sign a Confidentiality & Electronic Security Agreement upon hire and at least annually thereafter. Department leadership will review the agreement with staff members during the annual performance evaluation.

B. On site vendors and other individuals are required to sign the agreement if they will come into contact with patients and/or patient information. All individuals obtaining a Froedtert security badge or access card are required to review and sign a Confidentiality & Electronic Security Agreement in the Froedtert Security Department before any access cards or security badges are provided. Department managers should obtain a signed confidentiality agreement for those applicable vendors that do not go through security.

C. Confidentiality & Electronic Security Agreements will be stored as follows:

1. Froedtert staff- forms will be stored in personnel file in Human Resources.
2. Forms obtained by F&CH Information Technology Department (F&CH IT) will be stored in F&CH IT until they are scanned into the electronic storage database.
3. All other forms obtained for **non-Froedtert staff** will be stored in the Corporate Compliance Department until they are scanned into the electronic storage database.

Mail or Pneumatic Tube System:

A. All confidential information being routed through inter-departmental mail must be placed in an inter-office envelope. Always include the name and department of the recipient and sender on the outside of the envelope.

B. Tampering with incoming or outgoing mail is strictly prohibited.

C. All confidential information being routed through the Pneumatic Tube System must include the name and department of the recipient and sender. Use inter-office envelope when physically possible.

E-mail: Refer to the Corporate Policy, E-Mail Access-CPA.0047.

Wireless Paging:

A. As necessary to perform job functions, it is acceptable to include limited patient identifiers when sending wireless text pages to providers if it is for patient safety purposes and/or to deliver efficient patient care.

B. It is never acceptable to include HIV, sexually transmitted disease information or other sensitive test results or information through a wireless page.

C. Individuals are advised to exercise caution when sending text pages to limit the potential for improper disclosures.

D. Examples of acceptable data to include in a wireless page:

- Patient full name and non-sensitive diagnostic test result.
- Patient full name, room number and call back extension.
- Patient full name and date of birth.
- Patient full name and non-sensitive description of complaint or reason for page.

Overhead Paging:

Overhead paging in the hospital and clinics should not link a patient name with any type of hospital service. The announcement should alert the individual to dial an extension number where the message will be communicated in a confidential manner or announce that the patient should return to their nursing unit or service area (without specifying specific department name).

Verbal Disclosure of Patient information:

A. Professional discretion should be used when discussing patient identifiable information or sensitive business information over cellular, digital and/or analog phones, recognizing the vulnerability of incidental disclosure and the privacy and security of these devices.

Reporting suspected non-compliance:

It is the responsibility of each individual to promptly report any knowledge or suspicion of non-compliance or breach of confidentiality to the Corporate Compliance Department. For further details, please refer to the Corporate Policy: CPA.0062 Corporate Compliance Hotline.

Routine auditing and monitoring of appropriate staff member's access to confidential business and patient's protected health information will be conducted without notice.

Violations of Confidentiality Policy / Breach of confidentiality:

A. Any individual accessing, reviewing, using and/or disclosing confidential information owned and/or maintained by Froedtert is required to comply with Froedtert's policies and procedures. Failure on the part of any individual to comply with this policy may result in disciplinary action up to and including termination. Additionally, certain violations may be subject to reporting requirements to applicable state licensing/certification boards, and appropriate legal action.

Some Examples of Breaches of Confidentiality:

1. "Carelessness or Unintentional" –
   - Leaving a computer workstation unsecured before going to lunch.
   - Carelessly accessing the wrong patient's information.
   - Carelessly discussing confidential information in a public area and it's overheard by someone.
   - Accidentally faxing information to the wrong location.
   - Accidentally leaving a laptop containing Froedtert information, unattended in a public setting.
   - Leaving business or patient information sitting on the copy machine.
   - Throwing patient information in the regular trash can.

2. "Curiosity, Concern, Intentional " -
   - Accessing PHI of friend, family member, co-worker, acquaintance, VIP or other individual out of curiosity or concern.
   - Looking up an address in a Froedtert system so you can send a get well card.
   - Looking up appointment information for yourself or a family member.
   - Accessing confidential staff member employment information without a legitimate work related reason.
   - Taking pictures, videos or other recordings of patients without their written consent.
   - Looking up a co-workers information because they ask you to.
   - Sharing computer user ID/password with a new employee until they get their own.
   - Letting your spouse or children use your Froedtert issued Blackberry to play games.
   - Removing confidential information from the facility without proper authorization.
   - Looking up your own protected health information.
   - Talking about an unusual patient or case that you dealt with or heard about at work, with your family.

3. "Personal Gain or Malice" -
   - Using Froedtert business or patient information for personal benefit.
   - Selling patient or business information for a media story.

- Using confidential information for identity theft.
- Accessing patient's PHI to use against them in a legal / court proceeding.
- Accessing, reviewing, using or disclosing any confidential information without a business need.

B. Confidentiality breaches will be investigated by the Compliance Department and depending on the circumstances will likely include other departments as necessary. (i.e. Human Resources, Information Technology, Department Director, Risk Management, MCW, etc.) Based on the severity of the confidentiality breach, immediate account restrictions may be implemented.

C. If the confidentiality breach involves a staff member, the department director and human resources will determine appropriate disciplinary action.

D. Froedtert will work to minimize any harmful effects if there is a confirmed breach of confidentiality.

E**.** State and/or Federal Penalties associated with a Breach of Confidentiality:

Depending upon the severity of the breach or offense, state and/or federal penalties may apply. Examples of penalties associated are listed below:

- **Offense**: General penalty for failure to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) provision:
  Fines:
  - Up to $100 per person, per violation
  - Maximum of $25,000 per person, per violation

- **Offense**: Penalty for a wrongful disclosure of individually identifiable health information knowingly and in violation of HIPAA including any of the following:
  - Using a unique health identifier
  - Obtaining identifiable health information
  - Disclosing identifiable health information

  Fines: Up to $50,000 and/or up to one year imprisonment

- **Offense**: Knowingly misusing information under false pretenses

  Fines: Up to $100,000 and/or up to five years imprisonment

- **Offense**: Knowingly misusing information with intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm.

  Fines: Up to $250,000 and/or up to ten years imprisonment

Author / Director of Corporate Compliance and Internal Audit

Vice President, Chief Compliance and Project Officer

Executive Vice President/Operations