Confidentiality Policy

description

Confidentiality, Compliance, PHI, Confidential, Confidentiality Policy

Policy Number

FH-COM.062

Purpose

A. To outline the responsibility, expectations and accountability for all Workforce Members to maintain and protect the confidentiality of patient, workforce and other business information at Froedtert Health (FH).

B. To describe the consequences for failing to comply with the rules, and expected behaviors or actions.

Definitions

A. Confidential Information - For purposes of this policy, confidential information includes any information not publicly available that belongs to FH or is related to FH business operations.

1. Patient's Protected Health Information (PHI): Any individually identifiable health information, whether oral, written, electronic, transmitted, or maintained in any form or medium that:

I. Is created or received by a health care provider, a health plan, or a health care clearinghouse; and

II. Relates to an individual's past, present, or future physical or mental health condition, health care treatment, or the past, present or future payment for health care services to the individual; and

III. Either identifies an individual (for example, name, social security number or medical record number) or can reasonably be used to find out the person's identity (address, telephone number, birth date, e-mail address, and names of relatives or employers)

IV. Protected health information excludes individually identifiable health information contained in employment records held by a covered entity in its role as employer; in addition to any person who has been deceased for more than 50 years.

2. Information Pertaining to Workforce: Examples include salaries, benefits/claims, employment records, corrective actions, social security numbers, workforce health, occupational health, and payroll information, etc.

3. Business Information: Examples include FH financial, strategic, operations, contracts, research, internal communications or other proprietary information or information not publicly available.

B. Froedtert Health Affiliate (FH Affiliate) - For purposes of this policy, Froedtert Health Affiliate refers to: Froedtert Memorial Lutheran Hospital, Inc.; Community Memorial Hospital of Menomonee Falls, Inc.; St. Joseph's Community

Hospital of West Bend, Inc.; Froedtert & The Medical College of Wisconsin Community Physicians, Inc.; West Bend Surgery Center, LLC; Froedtert Surgery Center, LLC; Waukesha Surgery Center, LLC; Drexel Town Square Surgery Center, LLC; Menomonee Falls Surgery Center, LLC; Inception Health, LLC; and Exceedent, LLC. . Any other entity that becomes controlled by FH after adoption of this policy also may be considered a FH Affiliate.

C. Workforce Member– For purposes of this policy, FH or FH Affiliate employee, volunteer, student, temporary worker or other persons whose conduct in the performance of work is under the direct control of FH or a FH Affiliate, whether or not they are paid by FH or FH Affiliate.

D. All terms relevant to the Privacy Rule are defined in the Corporate Policy FH-COM.031- HIPAA Privacy Definitions.

Policy

A. All Workforce Members have a legal and ethical responsibility to protect and secure the privacy and confidentiality of information regarding our patients, staff and business activities.

B. A Workforce Member may be granted access to Confidential Information as necessary to fulfill the requirements of his/her defined role and responsibility.

C. A Workforce Member who has access to, or comes into contact with any Confidential Information is only authorized to acquire, access, use, disclose, remove, copy, alter, or destroy information within the scope of our policies and only for the sole purpose of carrying out his/her approved and legitimate job duties and never for personal reasons, curiosity, malicious use, unethical motivation or for any other unapproved purpose.

D. Workforce Members are prohibited from accessing, reviewing, using, copying, printing, disclosing or removing his/her own PHI. The approved methods for obtaining access to one's PHI is to contact the health provider directly, request copies of the medical information from the Health Information Management Department, or by accessing information through the MyChart portal. It should be noted that appointment information, provider schedules and billing information is considered PHI.

E. Workforce Members are prohibited from accessing, reviewing, using, copying, printing, disclosing or removing the PHI of any family members, friends, co-workers, neighbors, patients in the media, VIPs, or any other individual for any personal reason or other non-legitimate job duty related purposes. It should be noted that appointment information, provider schedules and billing information is considered PHI.

F. Workforce Members do not have any individual rights to or ownership of any information accessed or created by the workforce member during his/her employment or relationship with FH.

G. FH employees are provided proper training and education regarding the confidentiality rules, regulations and expected behaviors and are required to complete all mandatory education within the specified timeframe. A Confidentiality Agreement must be signed by each FH employee upon hire and as required throughout his/her employment. Signed Agreements for employees are retained in the Human Resources Department.

H. A Confidentiality Agreement must be signed by each FH volunteer, student, temporary worker, medical staff member, resident and others when obtaining an identification badge from FH Affiliate Security Department. Signed agreements will be forwarded to the FH Compliance Department.

I. Department leaders are required to validate that a signed Business Associate Agreement is in place when applicable and prior to any access, use or disclosure of PHI and in accordance with the HIPAA Business Associate Agreements Policy FH-SC.035. Additionally, department leaders may decide to request certain contractors or other on site vendors

to sign the FH Confidentiality Agreements due to the sensitive information they may come into contact with during their business engagement. Those agreements are to be stored in the departmental files and retained for 6 years after the engagement has ended.

J. Workforce Members have an obligation and responsibility to immediately report to the FH Compliance Department (FH Compliance) any activities that may compromise the privacy and/or security of our staff, business and/or patient information. FH will not retaliate against individuals who, in good faith, bring forth information of non-compliance. For more information on the reporting policy and procedures, refer to Corporate Policy FH-COM.025 Compliance Reporting, Hotline and Non-Retaliation.

K. FH Compliance is responsible for and will investigate and respond as appropriate to all reported concerns related to privacy and confidentiality. If a breach of our patient's Confidential Information has occurred, FH Compliance will follow all applicable rules and regulations regarding breach notification which are outlined in the Corporate Policy: FH-COM.006 Notification of Breach of Protected Health Information.

L. Routine auditing and monitoring of system use and access may be conducted at any time and without notice. A Workforce Member's system access may be revoked at any time.

M. FH will administer appropriate and consistent sanctions and will take corrective action against those Workforce Members who do not follow the rules, regulations and expected behaviors or actions.

Procedure

A. Only the Minimum Amount of Confidential Information should be acquired, accessed, used or disclosed when carrying out any given task. For example:
1. Workforce Members must not access, use or disclose information beyond the scope of his/her job responsibilities and are only authorized to access the data elements necessary to carry out his/her legitimate job duties. Staff who are unsure of the scope of their job duties or authorization to access PHI are required to seek immediate clarification from their leader.
2. Social Security Numbers will not be acquired, accessed, used or disclosed unless it is required to fulfill a business need. This includes having Social Security Numbers on reports or other documents when it is not needed or required.
3. Electronic security access is granted in accordance with the Workforce Members role and responsibility and in accordance with FH Information Technology policies and procedures.
4. Reports, spreadsheets and databases will only contain the data elements necessary to fulfill the business purpose and will be strored in a secure environment and for the appropriate length of time.

B. Disposal of Confidential Information must be done in a manner that ensures that the information cannot be identified, recovered or reconstructed and done in accordance with Corporate Policy: FH-COM.030 Disposal of Protected Health Information and Other Confidential Information. Workforce Members are required to use the locked/secure recycle bins or other authorized manner of disposal for the disposal of all Confidential Information. Confidential Information must never be discarded in regular trash bins or dumpsters.

C. Storing of Confidential Information must be done in a location (both physically and electronically) that is only accessible to those that require the information. Only store the information as long as required and in accordance to the Record Retention policies and regulatory requirements. For example:
1. Confidential Information in electronic format should not be stored on a shared or public drive, local hard drive, non-encrypted USB, mobile device, personal device or any other device that is not in compliance with FH Information Technology policy and procedures.
2. Departments should not indefinitely store data, internal reports, spreadsheets or other databases that are used for a

specific departmental use to track productivity, quality monitoring or for other internal purposes. (Unless required by law or other requirement, or is specifically addressed in a FH Affiliate record retention policy) Departments should perform regular maintenance of their electronic and physical space to assure that only the necessary data and information is retained.

D. Physical Environment Protections:
1. Keep all Confidential Information, devices or equipment that contain confidential information physically secure to prevent any unauthorized person from gaining access.
a. Areas that do not have the capability of being locked during off hours must have an established process to assure that Confidential Information is not left easily viewable or accessible by others.
b. Workforce Members that are in roles where removal of Confidential Information from the facility is authorized, are responsible for the security of the information in his/her possession. Confidential Information, including laptops, should never be left in an unlocked vehicle or in plain sight, or left unattended in a public location where others may steal, view or access it.
c. Confidential Information should not be left carelessly in conference rooms, restrooms, dining locations, photocopiers or other publicly accessible locations. Any Workforce Member who discovers Confidential Information in a public location, is responsible for securing the information (e.g. disposing in the locked/secure recycle bins, or delivering to the owner, when known.)

E. Careful Dissemination of Confidential Information is critical in preventing errors and mishandling of information.
1. When disseminating or handing out documents or other information which contain PHI or other Confidential Information, Workforce Members must validate that they have the correct information prior to dissemination. For example, Workforce Members must:
a. Positively identify the patient or staff member by validating identifiers (name and date of birth) prior to distributing any information.
b. Validate each page of the documents or information that is to be distributed to ensure that all the correct information is enclosed and that no other information has been accidentally included.
2. When mailing information, verify that all of the correct papers are enclosed and match the name addressed on the envelope prior to sealing the envelope. Ensure that the envelope is properly addressed and select the appropriate type of envelope or sturdy packaging to ensure it will safely secure the documents during the mailing process.
3. When emailing Confidential Information within Froedtert Health, validate that the correct recipients have been selected to receive the email. If the email is going to another organization outside of Froedtert Health, (this does not include emails to/from MCW), type SECURE in the subject line to force the email to be encrypted. For additional information regarding emailing of confidential information, refer to the Email and Internet and Usage Policy FH-IT.025.
4. When routing Confidential Information throughout the health system, information must be protected to the extent possible to maintain its confidentiality. For example, only use the approved inter-office envelopes and complete all of the fields of information required on the outside of the envelope so it is properly delivered.
a. If Confidential Information is misdirected and the recipient is unaware of who the owner or intended recipient is, the recipient may either dispose of the information in a locked recycle bin, or forward the information to the FH Compliance Department for proper identification or disposal.
5. When faxing PHI or other Confidential Information, Workforce Members must validate that they have the correct fax number, and to use caution when entering the number in the fax machine to prevent errors. Appropriate fax cover sheets must always be used and the Corporate Faxing Policy FH-HIM.010 must be followed.
6. When a Workforce Member receives a complaint or they discover that Confidential Information was mishandled or accidentally released to an unintended recipient, they must immediately report the incident to his/her Leader and to the FH Compliance Department.

F. Computer and other Electronic Security
1. Workforce Members must secure the computer workstation when it is left unattended. They must also:
a. Alert other Workforce Members when they discover their workstations not properly secured.
b. Notify Department Leader and/or FH Compliance if non-compliant practices continue.
2. Each Workforce Member is responsible for all activity and access that occurs under his/her UserID/password and will be held accountable for any inappropriate activities that may occur.
a. Never share unique computer UserID/password information or share ID badges with anyone.

b. User must never allow anyone else to use a computer that they are logged into.
c. Never write your password down and leave it in a public or unsecure area where others may have access to it.
d. Never access a computer network, application or any other electronic information under another individual's UserID/password.

3. Workforce Members will not email Confidential Information to any personal web email accounts. For any exceptions, discuss with your immediate Supervisor or the Compliance Department.
4. Workforce Members with mobile devices that contain access to Confidential Information must follow the FH Information Technology approval process, proper remote access policies and all other policies and procedures, in addition to wiping confidential information from the mobile device prior to end of employment.
5. Workforce Members may not make any unauthorized transmissions, inquiries, modifications or purging of Confidential Information and will not modify the workstation configuration, or use or add software to workstations without prior authorization from the FH Information Technology Department and the appropriate Leader.
6. If Workforce Members are provided direction or instruction that is in opposition with computer and/or electronic security policies or rules, or if they become aware of a situation that compromises the security of our systems or unique UserIDs/passwords, Workforce Members are responsible to immediately report the incident to the FH Information Technology Department.
7. Workforce Members should not send in-basket messages to staff members who are receiving care as a patient. Any patient who happens to be a staff member should receive communication in the same manner as al other patients. (i.e. MyChart, phone calls, etc.)
8. Workforce Members will not post any patient information, including photographs or videos, on any Social Media Site.

G. Paging/Messaging Confidential Information
1. When necessary to deliver timely information to care providers, it is acceptable to include limited patient identifiers when sending messages through pagers. The intent is to provide necessary information to assist with safe and efficient care to patients. Workforce Members must:
a. Use caution when sending messages to prevent improper disclosures.
b. Never include mental health, HIV, sexually transmitted disease, or other highly sensitive information or diagnosis information.
c. Provide the minimum amount of information that is necessary.
d. Examples of acceptable elements for messaging: Patient full name, date of birth, medical record number, room number, non-sensitive results, description of complaint or reason for message.

H. Verbal Disclosures of Confidential Information requires Workforce Members to comply with the following guidelines:
1. Never discuss confidential business, workforce, or patient information with others that do not have a business reason to know; this includes family members/friends. Examples include:
a. Do not share interesting or unusual patient situations with others who do not have a business need to know the information. This also includes inappropriate and unprofessional comments or gossip about patients, co-workers or others.
b. Do not share staff members' salary, corrective actions or other confidential employment/benefit /claims related information with others.
c. Do not share confidential business information, transactions, trade secrets or other proprietary information or information not publicly available with others.
2. Care teams must take precautions when talking to patients about his/her health, care and treatment in the presence of others. Request patient visitors to step out of the inpatient room prior to discussing Confidential Information with the patient.
3. Speak softly in public areas, check-in areas and waiting rooms to prevent others from overhearing the information.
4. Close doors when possible to prevent others from overhearing information they do not require and to maintain the patient's overall privacy.
5. Use caution when having conversations in public areas such as elevators, dining locations, hallways and restrooms to prevent others from overhearing the conversation.
6. Care teams should be aware of surroundings when discussing patient information in the space directly outside of

patient rooms.
7. Professional discretion and judgment should be used when discussing patient information with patient's family or friends. When possible, obtain patient's verbal consent prior to disclosing relevant information. In the event the patient is unable to consent, use professional judgment and keep the patient's best interest in mind by sharing information only with family or friends who are currently involved in the patient's care and by limiting the information to what they need to know about the current episode of care.
8. Information relevant to a patient's insurance claim or detailed bill may be discussed with the guarantor on the patient's account.
9. Voice messages may be left for patients and should generally include very basic information. Do not leave messages with specific health information on a voice message. Examples of acceptable information to be left on a voice message are:
a. Name of the facility calling
b. Name of the individual calling
c. Contact information
d. General comment or statement which describes the purpose of the phone message.
e. Information about an appointment may include instructions the patient needs to know to be prepared for the appointment and to avoid the appointment from being cancelled. (i.e. eating, drinking, medication restrictions)

I. Reporting Suspected or Known Non-Compliance
1. It is the responsibility of each Workforce Member to immediately report any knowledge or suspicion of non-compliance to the FH Compliance Department. For further details on reporting, please refer to corporate policy- FH-COM.025 Compliance Reporting, Hotline and Non-Retaliation.

J. Sanctions for Breach of Confidentiality
1. Any Workforce Member who fails to comply with the confidentiality rules, policies and/or laws is subject to corrective action up to and including immediate termination of employment or business relationship.
2. Other actions such as remediation education, root cause analysis or other activities may be assigned to the leader and/or Workforce Member, depending upon the incident and severity of the violation.
3. Depending on the violations, reporting to applicable state licensing boards, law enforcement, affected parties and/or other external agencies may apply.
4. Upon completion of an investigation, a severity level is assigned to the incident based on the facts, circumstances, risk and severity of the incident. The following are common examples of privacy violations and what severity level they may fall into, depending upon the circumstances involved.
a. Level 1 Severity: Generally involve lower risk infarctions that are typically accidental or careless acts that result in non-compliance or breach of confidentiality. This may include patterns of failure to validate information, such as patient identifiers prior to distributing, mailing, faxing or handing out patient information or other confidential information. Any of these examples may escalate to a higher level severity infarction depending upon the particular facts and circumstances involved.
(i) Patterns of accidental or careless actions, disregard of policy and procedures or overall poor performance by a workforce member will result in corrective action. Root cause analysis and re-education may be required.
b. Level 2 Severity: Moderate risk or severity of infractions which are prohibited acts, where despite training, an individual does not follow policies. Typically these incidents are not accidental in nature and may be viewed as a more egregious action that results in non-compliance or breach of confidentiality. This may include actions such as accessing patient information beyont the scope of defined job role; but not deemed as curiosity or for personal reasons, accessing provider schedules, removing PHI or other confidential information from the facility for legitimate purpose but it is subsequently lost or stolen, disclosing patient information or location when the patient has opted out of the patient directory, computer username/password violations Any of these examples may escalate to a Level 3 Severity, depending upon the particular facts and circumstances involved.
(i) FH will hold staff member accountable by following the Corrective Action Policy, which may include corrective action or termination of employment or business relationship. Root cause analysis and re-education may be required.
c. Level 3 Severity: Higher risk or severity infraction which involve willful intent, unethical actions, reckless and/or irresponsible acts or complete disregard of the rules. This may include actions such as the use, access or disclosure of patient or confidential information without a legitimate business purpose/job duty. Some examples include: snooping in records, reviewing records for personal reasons, curiosity, inappropriately disclosing confidential information to others that do not require the information, gossiping about patients or others, unethical acts or malicious

actions such as identity theft, fraud, personal gain, custody battles, defamation of character, and estranged relationships (i) FH has no tolerance for these actions or behaviors and will take immediate corrective action, including the termination of employment or business relationship. Root cause analysis and re-education may be required.
5. Breaches of confidentiality that constitute violations of HIPAA are subject to civil and criminal penalties. The tiered civil money penalties range between $100 and $50,000 per violation, and potentially may be in excess of $1,500,000 for identical violations in a calendar year, determined based on the nature and extent of the violation, the nature and extent of the harm resulting from the violation, and the history of prior non-compliance and the level of culpability.

Issuing Authority

FH Corporate Policy Committee

Distribution

Froedtert Health

category

Compliance,