Name: Confidentiality Policy

Last Review Date: 06/13/2023

Next Review Date: 06/13/2026

Description: Confidentiality, Confidential, Privacy, Private, HIPAA, Compliance, PHI

Policy Number: FH-COM.062

Origination Date: 07/01/2014

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, in any format (paper, electronic, or video) created or received by a Workforce Member, Froedtert Health ("FH") or a FH Affiliate, or a department that is related to information that is not publicly available and that belongs to FH or is related to FH business operations.

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

1. Is created or received by a health care provider, a health plan, or a health care clearinghouse; and
2. 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
3. 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).

Note: 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.

C. Information Pertaining to Workforce: For purposes of this policy, Information Pertaining to Workforce means any information, in any format (paper, electronic, or video) related or pertaining to a FH Workforce Member that is used by Froedtert Health or a FH Affiliate to manage its Human Resources and related business operations. Examples include salaries, benefits/claims, employment records, corrective actions, social security numbers, workforce health, occupational health, and payroll information, etc.

D. Business Information: For purposes of this policy, Business Information

includes any information, in any format (paper, electronic, or video) created or received by Froedtert Health or a FH Affiliate that is proprietary in nature or is otherwise not publicly available and that belongs to FH or is related to FH business operations. Examples include but are not limited to FH financial, intellectual property, trade secrets, strategic, operations, contracts, research, internal communications such as emails or Power Point presentations, or other proprietary information or information that is not publicly available.

E. Froedtert Health, Inc. has designated itself and certain affiliates as "affiliated covered entity." Refer to the Designation of Affiliated Covered Entity FH-ADM.022 policy for definition.

F. Workforce Member - For purposes of this policy, Workforce Member includes any 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 a FH Affiliate.

G. All terms relevant to the HIPAA Privacy Rule are defined in the Corporate Policy: HIPAA Privacy Definitions. Froedtert Health, Inc.

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 their defined role and responsibility. A Workforce Member should not access, use, modify, retain, remove or destroy any information unless there is a legitimate business reason to do so as part of their employment with FH. Any personal use or misuse of such Confidential Information will be considered to be a violation of this Policy and may also constitute a potential violation of HIPAA.

C. Workforce Members do not have any individual rights to or ownership of any information accessed or created by the Workforce Member during their employment or relationship with FH.

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

E. Department leaders are required to validate that a signed Business Associate Agreement (BAA) is in place when applicable and prior to any access, use or disclosure of PHI by or to a third-party and in accordance with the Corporate Policy: HIPAA Business Associate Agreements (FH-SC.035).

F. Workforce Members have an obligation and responsibility to immediately report to FH Compliance any activities that may compromise the privacy and/or security of our Information Pertaining to Workforce, Business Information and/or PHI. FH will not retaliate against individuals who bring forth information of non-compliance. For more information on the reporting policy and procedures, refer to Corporate Policy: Compliance Reporting, Hotline and Non-Retaliation (FH-COM.025).

G. 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: Notification of Breach of Protected Health Information. (FH-COM.006).

H. Auditing and monitoring of system use and access is continuously conducted through an advanced privacy monitoring system.

Procedure:

I. Only the minimum necessary amount of Confidential Information should be acquired, accessed, used or disclosed when carrying out any given task. The following rules apply to Confidential Information:

<u>Access to and Use of Confidential Information:</u>

1. Workforce Members must not access, use, disclose, modify, retain, remove or destroy information beyond the scope of their job responsibilities and are only authorized to access the data elements necessary to carry out their legitimate job duties.
2. Workforce Members should ask another qualified staff member to provide care or services when the patient is a family member or friend. If no other qualified staff member is available, you may then provide care or services to the patient as you would any other patient. Inform your leader if a situation like this occurs.
3. Social Security Numbers (SSN) must only be acquired, accessed, used or disclosed when they are required to fulfill a business need. This includes having SSN on reports or other documents only when they are needed or required for billing, identification or other legitimate business purposes.

4. Confidential Information that is required to be disclosed should only

include the minimum amount of information necessary to satisfy the intended purpose of the request. This includes any reports, spreadsheets or databases that are created for FH's health care operations.

Disposal of Confidential Information:

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

Storing of Confidential Information Including Physical Environment Protections:

8. Storing of Confidential Information must be done in a location (both physically and electronically) that is only accessible to those who require the information.
9. Workforce Members should store the Confidential Information for only as long as required and in accordance with applicable law or regulatory requirements and FH's Record Retention policies. For example: 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 otherwise required by law or other requirement, or is specifically addressed in an 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.

10. Workforce Members must keep all Confidential Information stored/housed on devices, equipment, or on paper physically secure to prevent any unauthorized person from gaining access.

11. 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 by or accessible to others.

12. Workforce Members who are in roles where the removal of Confidential Information from the facility is authorized are responsible for the security of the information in their 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.

13. Confidential Information should not be left carelessly in conferences 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 it in the locked/secure recycle bins, or delivering it to the owner, when known).

14. Careful Dissemination of Confidential Information is critical in preventing errors and mishandling of information. To prevent the wrongful release of information when disseminating or handing out documents or other information which contain PHI or other Confidential Information, Workforce Members must first validate that they have the correct patient information prior to dissemination. For example, Workforce Members must:
a. Positively identify the recipient by validating identifiers (e.g. have the recipient state their name and date of birth in connection with patient care) prior to distributing any information.
b. Validate each page of the documents or information that is to be distributed to ensure all the information is correct and that no other information has been accidentally included.
c. When mailing Confidential Information, verify that all of the papers enclosed are correct and match the name addressed on the envelope prior to sealing the envelope. Workforce Members must also use the appropriate type of envelope or sturdy packaging to ensure:
(i) that documents are safely secured during the mailing process and (ii) that the envelope is properly addressed and sealed prior to mailing.
d. When emailing Confidential Information within FH, validate that the correct recipient(s) have been selected to receive the email. If the email is going to another organization outside of FH, (this does not include emails to/from the Medical College of Wisconsin (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 Corporate Policy: FH-IT.301 Appropriate Use of Information Technology).
e. 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. Do not open mail that is not addressed to you or to your department/area where you work.
f. Take appropriate actions when Confidential Information is misdirected within our health system 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 should contact/forward the information to FH Compliance for proper identification, delivery or disposal.
g. When faxing PHI or other Confidential Information, Workforce

Members must validate that they have the correct fax number, and use caution when entering the number in the fax machine to prevent errors. Whenever possible, frequently used fax numbers shall be pre-programmed into fax machines or systems with auto-fax functionality to eliminate errors in transmission. Appropriate fax cover sheets must always be used and the Corporate Policy Faxing of Protected Health Information (PHI) must be followed.
h. When a Workforce Member receives a complaint or they discover that Confidential Information was mishandled or accidentally released to an unintended recipient by them or others, they must immediately report the incident to their Leader and to FH Compliance.

15. Workforce Members must not email Confidential Patient, Business Information, or Information Pertaining to the Workforce to their personal email accounts or to the personal accounts of other FH Workforce Members. In the rare event that an exception may be required to email information to a patient's personal email account, permission must be granted by requestor's immediate Leader or FH Compliance.

<u>Computer and Other Electronic Security:</u>

16. Workforce Members must take appropriate actions to secure their computer workstation, laptop or mobile devices at all times and must secure their computer workstation or laptop before leaving it 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.
c. Be responsible for all activity and access that occurs under their userID/password and be accountable for any inappropriate activities that may occur.

d. Never share unique computer userID/password information or share ID badges with anyone.
e. Never allow anyone else to use a computer that they are logged into.
f. Never write their password down and leave it in a public or unsecured area where others may have access to it.
g. Never access a computer network, application or any other electronic information under another individual's userID/password.

h.Follow the FH IT approval process, proper remote access policies and all other policies and procedures in connection with the use of mobile devices that contain access to Confidential Information; they must also wipe any Confidential Information from the mobile device prior to end of employment.

i. Not make any unauthorized transmissions, inquiries, or purging of Confidential Information and must not modify the workstation configuration, or use or add software to workstations without prior authorization from FH IT and the appropriate Leader.
j. Not make any unauthorized modifications of Confidential Information. If Workforce Members are provided with directions or instructions that are in opposition to or in conflict 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 FH IT.

k. Not send Epic In-Basket/Staff messages to communicate with 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 all other patients (i.e. MyChart, phone calls, etc.). This includes sending Epic In-Basket/Staff messages to the provider regarding the Workforce Member's own health care.

l. Not post any Patient Information, including photographs or videos, on any Social Media site (Refer to Corporate Policy: FH-HR.004 Public Display with Social Media and to Corporate Policy: FH-COM.080 Patient Photography, Videotaping, Audio Recording and Other Media Imaging in all Environments of Care).

Paging, Instant/Messaging and/or Text Messaging Confidential Information:

17. When paging, instant messaging and/or sending texts of Confidential Information, Workforce Members must:

a. Never send Confidential Information via their personal phone, including Business Information or Information pertaining to the Workforce.
b. Never text patient orders.
c. When necessary to deliver timely information to care providers, include

only limited patient identifiers when sending messages through FH approved paging systems and/or approved instant messaging or texting applications. The intent is to provide necessary information to assist with safe and efficient care to patients. Examples of elements that may be considered for messaging include the minimum necessary of the following: patient full name, date of birth, medical record number, room number when needed, non-sensitive test results, description of complaint or reason for message.
d. Use caution when sending messages to prevent improper disclosures.
e. Never include mental health, HIV, sexually transmitted disease, or other highly sensitive information or diagnostic information.
f. Never send, retain, or store documents containing PHI or any Confidential Information on any instant messaging application other than those applications that have been authorized for use by FH's IT Security team.
g. Never include SSN's, Payment Card Information (PCI), or any other financial information (i.e. bank account numbers) on any instant messaging application.
h. Be mindful to provide only the minimum amount of information that is necessary.

<u>Verbal Disclosures of Confidential Information:</u>

18. When making verbal disclosures of Confidential Information, Workforce Members must:
a. Never discuss Confidential Business, Workforce, or Patient Information with others that do not have a business reason to know; including family members, friends and other staff members. Examples include:
i. 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.
ii. Do not share Workforce Members' salary, corrective actions or other confidential employment/benefit/claims related information with others.

iii. Do not share Confidential Business Information pertaining to our business such as budgets, strategic plans, transactions, trade secrets or other proprietary information or information not publicly available with others.
iv. Take appropriate precautions when talking to patients about their 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.
v. Speak softly in public areas, check-in areas and waiting areas to prevent others from overhearing Confidential Information.
vi. Close doors when possible to prevent others from overhearing Confidential Information they do not require and to maintain the patient's overall privacy.

vii. Use caution when having conversations in public areas such as elevators, dining locations, hallways and restrooms to prevent others from overhearing the conversation; this includes conversations conducted over speaker phone devices.
viii. Be aware of surroundings when discussing patient information in the space directly outside of patient rooms.
ix. Use professional discretion and judgment 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. Refer to Guidance provided on Scout - Verbal Communication with Patient's Family and Friends.
x. Be aware that information relevant to a patient's insurance claim or detailed bill may be discussed with the guarantor on the patient's account.

xi. Know that voice messages left for patients should generally include very limited and 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).

Reporting Suspected or Known Non-Compliance:
19. When reporting suspected or known non-compliance, is the responsibility of each Workforce Member to immediately report any knowledge or suspicion of non-compliance to FH Compliance. For further details on reporting, please refer to Corporate Policy: Compliance Reporting, Hotline and Non-Retaliation.

Sanctions for Violation of This Policy:
20. Any employee or employed provider who fails to comply with this Policy will be subject to appropriate disciplinary action under the corrective action policy applicable to them, up to and including termination of employment. Depending on the nature of the violation, the individual may also be reported to applicable state licensing boards, law enforcement, affected parties and/or other external agencies.
21. Individuals that are employed by third-parties subject to this policy, who fail to comply, will be subject to corrective action in accordance with their contract terms and/or employer's applicable policies. Depending on the nature of the violation, and the terms of our agreement with the third-

party, next steps may include retraining, removal of the individual, termination of access to our IT systems/applications, and/or termination of the agreement.

Assignment of Severity Levels by FH's Compliance Team:

22. Upon completion of a privacy investigation by FH's Compliance team, a severity level for each privacy violation will be assigned by FH's Compliance team to the incident based on the facts, unique circumstances, risk and severity of the incident. This severity level determination (Low, Medium or High) as set forth below will then be used by FH's HR Department in cooperation with the Leader of the person who is the subject of the privacy investigation to apply an appropriate sanction consistent with this Policy.

23. Low Severity Level: This category reflects unintentional mistakes or violations that occur when someone fails to follow what they learned or should have learned in training, and/or what they knew, or should have known from policies or procedures. Such violations may arise from carelessness, lack of knowledge, improper judgement, or human error. Examples include, but are not limited to:
• Patient registration errors;
• Accidental disclosures of PHI to the wrong recipient via handing out, email, mail, fax, prescriptions, etc.;
• Accidental access to a patient's PHI due to careless searching habits that is self-reported;
• Discussing PHI in public areas or talking in loud voices so that others can overhear the conversation;
• Leaving a computer accessible and unattended;
• Leaving detailed PHI on an unsecured answering machine;
• Disclosing PHI or a patient's location when the patient has opted out of the patient directory;
• Improper disposal of PHI.

24. Medium Severity Level: This category reflects instances where limited information was accessed, such as demographic information but not diagnostic or treatment information. In these instances, no information was taken or used for any personal reason but, unlike Low Severity Level instances, are not accidental in nature and may be viewed as more severe than a Low Severity Level in that the incident reflects a disregard for the training or FH policies and procedures. These incidents may create an elevated degree of privacy risk for the patient or organization because of the potential for information to be compromised but does not rise to the level of a High Severity Level infraction. Examples of Medium Severity Level privacy infractions include but are not limited to:
• Evidence identified by a Compliance staff member that an employee's colleague's, relative's, or acquaintance's limited demographic information was searched/accessed, but the access was likely a single or isolated incident and/or due to an error (e.g., human error) but was not reported to Compliance or Leadership and did not include access to the more sensitive patient information contained in the underlying medical record;

• Evidence identified by a Compliance staff member that a provider schedule or patient/department list was accessed beyond the scope of the employee's job duty, but not for personal use;
• Evidence identified by a Compliance staff member a of an isolated incident where Epic was used instead of the appropriate method/application to view information where there is also evidence that the employee would have otherwise had the right to be privy to the information via the appropriate method (MyChart Proxy, activated Power of Attorney (POA), currently directly involved in the patient's care or payment of care);
• Evidence of someone logging into FH's network resources (including Epic) to allow another individual access to PHI;
• Evidence that someone shared their Epic password or secured Froedtert account passwords or login credentials;
• Evidence that a Workforce Member inappropriately allowed someone else to use their login, or evidence that a Workforce Member used another Workforce Member's login;
• Evidence identified by a Compliance staff member of an isolated instance where a Workforce Member had a legitimate business purpose to search or review a record but looked at more information than what was necessary for a particular business purpose.

25. **High Severity Level:** This category reflects instances of Workforce Members intentionally, rather than accidentally, accessing confidential information of any patient out of curiosity without a legitimate business reason for doing so and in violation of FH Privacy Training and/or this Policy. Such access typically includes a violation of FH's policies, standards or training that may create (i) a higher degree of privacy risk for the patient because of the probability that PHI may have been compromised in violation of this Policy and/or HIPAA without the ability for the privacy risks to the patient to be mitigated; and (ii) a higher degree of risk of legal or reputational harm for FH. Examples include but are not limited to:
• Evidence that a Workforce Member intentionally accessed relatives, co-workers, high profile individuals such as sports stars or politicians, or other individual's PHI out of curiosity and without a legitimate business purpose such as treatment, payment or health care operations. This includes evidence identified by a privacy investigator that an employee searched for information in the medical record without a legitimate business purpose, such as viewing the diagnosis of a high profile individual, colleague, friend, relative, former spouse or domestic partner, or neighbor, where the employee would not have otherwise been privy to the information and/or the information was used or disclosed;
• Evidence that a Workforce Member accessed PHI out of curiosity and then re-disclosed it to the media, social media, or otherwise made it publicly available;
• Instances where someone deliberately used or disclosed PHI for malice, or personal gain, or other benefit;
• Instances where someone stole or attempted to steal health information to commit identity theft such as opening a credit card in another person's name;

• Instances where someone intentionally used or disclosed and/or delivered PHI to anyone to cause financial and/or reputational harm, or embarrassment to the individual;
• Evidence identified by a Compliance staff member of someone who assisted another individual in accessing, using or disclosing PHI for personal reasons, to snoop, or to view out of curiosity or for financial gain or other benefit;
• A repeated pattern of occurrences of any Low or Medium Severity Level violations in a one year period of time.

26. Breaches of confidentiality that constitute violations of HIPAA are subject to civil and criminal penalties. If it is determined that a violation of HIPAA has occurred, the Compliance team can factor it into the severity level to be applied.

Related Policies:
Appropriate Use of Information Technology Policy
Compliance Reporting, Hotline and Non-Retaliation
Corrective Action
CYBERSECURITY BASELINE POLICY
Designation of Affiliated Covered Entity
Disposal of Protected Health Information (PHI) and Other Confidential Information
Faxing of Protected Health Information (PHI)
HIPAA Business Associate Agreements
HIPAA Privacy Definitions
Information Integrity
Notification of Breach of Protected Health Information

Issuing Authority: FH Corporate Policy Committee

Distribution: Froedtert Health

Reference Type:

Additional Attachments: Confidentiality Agreement.docx

Content Details URL: http://fhpolicy.s1.fchhome.com/d.aspx?d=01e7l80rD46e

Constant Content File URL: http://fhpolicy.s1.fchhome.com/d.aspx?c=74Z04a76Ec3b

Expiry Date: 6/13/2073 12:00:00 AM