Patient Information Confidentiality

1. SCOPE

1.1. System-wide

1.2. Facilities and departments included in the scope are further defined in the Scope Definition Resource Guide if not specifically outlined above.

2. DEFINITIONS & EXPLANATIONS OF TERMS

2.1. Abbreviations:

- CMR: Combined Medical Records
- MCHS: Marshfield Clinic Health System
- PHI: Protected Health Information

2.2. Definitions:

- Minimum Necessary: The term Minimum Necessary is defined as limiting Protected Health Information ("PHI") access to those with a need to know and using, disclosing or requesting only that amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.
- "Need to Know": The term "Need to Know" is defined as an employee using (accessing) or disclosing PHI only when necessary to perform and complete his/her job responsibilities. This includes employees who are being treated as patients.
- Patient: All references to the "patient" in this policy mean the patient or her/his Personal Representative as defined in the Personal Representatives of Patients policy.
- Protected Health Information (PHI): The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information Protected Health Information.
  - ◊ Individually identifiable health information: information, including demographic data, that relates to:
    - the individual's past, present, or future physical or mental health or condition; **or**
    - the provision of health care to the individual; **or**
    - the past, present, or future payment for the provision of health care to the individual; **and**
    - that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual (e.g., name, address, birth date, Social Security Number).

3. POLICY BODY

Marshfield Clinic Health System respects and will protect every patient's right to have all information they share with health care professionals kept confidential.

Patient information, regardless of its media, i.e. written, verbal, or stored in paper, photograph, video, or electronic format, may be used for a variety of legitimate business purposes. Examples of information usage include, but are not limited to: patient care, quality review, education, research, public health, insurance administration, legal, and reimbursement. Regardless of its use, patients must be assured the information they share with health care professionals will remain confidential. Without such assurance, patients may withhold critical information, which could affect the quality and outcome of care, as well as the reliability of the information.

3.1. Conduct

a. Employees observing other employees violating patient confidentiality in or outside of MCHS must immediately report the incident to their manager, a Human Resources Manager, the Director of Employee Relations, the Privacy Officer or the Compliance Officer. Reporting of a potential PHI breach can be accomplished via RL Incident Reporting or other notification methods available from the Corporate Compliance intranet site.

b. All alleged violations of the Patient Information Confidentiality policy will be investigated by managers and/or appropriate personnel.

c. Managers must report their findings to the respective Privacy Officer, Human Resources Manager, Compliance Officer or Director of Employee Relations prior to determining disciplinary action, if any.

d. Employees found in violation of this policy are subject to disciplinary action, up to and including, immediate termination. See: Employee Conduct policy.

3.2. Employees may access PHI on a patient following the minimum necessary standard, only if they have a business need to know, as part of their assigned job duties or responsibilities.

3.3. Gossip, careless remarks, and idle chatter may be a breach of the patient's trust and right to confidentiality or unauthorized disclosure of PHI.

3.4. Employees are not authorized to access any portion of MCHS medical record [e.g. CMR, Patient Schedule, Patient Demographics, Cattails Dental, etc.] to obtain information on themselves, their spouse, or their dependents. While this information is about you and your family, and you may have the right to know, this information must be obtained through proper channels. Proper channels include calling the attending physician, health care provider, or the Health Information Management department. The Notice of Privacy Practices provides direction on the process to obtain copies of health information for you and/or your dependents. Employees are expected to follow the same procedure as non-employee patients. Physician use of the electronic medical record is governed by the Professional Staff Handbook.

With the exception of situations requiring emergency care, providers and staff should be discouraged from providing care to their immediate family members (e.g. parent, spouse, minor child). Providers are discouraged from ordering diagnostic testing or

performing procedures on themselves or immediate family members. Many health insurers do not reimburse services provided to immediate family members.

3.5. PHI may be disclosed only upon written authorization by the patient or his/her legal representative or where such disclosure is authorized by federal or state law, subpoena or court order, and in accordance with the "Authorization to Use and Disclose Protected Health Information" policy and/or other applicable MCHS policies.

3.6. Breaches of patient confidentiality or unauthorized disclosure of PHI are violations of this policy and have potential civil and/or criminal penalties under state and/or federal law including the Health Insurance Portability and Accountability Act (HIPAA). Violation of this policy may lead to discipline, up to and including, termination of employment.

3.7. Managers shall inform and educate employees about the Patient Information Confidentiality policy.

3.8. An employee who needs clarification of the Patient Information Confidentiality policy should speak with his or her manager or contact the Privacy Officer or Compliance Officer.

3.9. Security

a. Each employee has a password that enables him/her to access the computer system. This password must be kept confidential and may not be shared with anyone. Each time an electronic medical record is accessed, the time, date, location, and employee name are recorded in the audit system. This tracking system is capable of identifying potential abuse. Employees are responsible for all access while they are logged in. See Sec. 3.5 above. Security violations are also subject to disciplinary action, up to and including, termination of employment. See Network Passwords policy.

4. ADDITIONAL RESOURCES

4.1. References:

- Employee Conduct
- E-mail, Internet, and Telephone Communications
- Personnel Records
- Authorization to Use and Disclose Protected Health Information
- Network Passwords

5. DOCUMENT HISTORY

Version No.	Revision Description
1.0	Policy #449.0 transferred to the Document Control System
2.0	Minor Change: Section 3.4 addition of Cattails Dental and correction of Combined Medical Record spelling
3.0	Minor Changes: Grammatical changes to Section 3.4, hyperlink to Section 3.5.
4.0	Addition of second paragraph under Section 3.4, hyperlink of Network Passwords policy, and minor informational updates to second paragraph of policy body and Section 3.2.
5.0	Annual review. Updated Scope, logo, and policy links. Added to Section 3.1.a.
6.0	Updated Scope.
7.0	Updated Scope and logo. Updated formatting, setting metadata field, header, removed logo, added abbreviations, updated author and scope Updated link to Corporate Compliance Site

6. DOCUMENT PROPERTIES

Primary Author: Schilling, Stacy
Co-Author(s):
Approver(s): This document has been electronically signed and approved by: Schilling, Stacy C on: 10/8/2018 10:58:04 AM