For Munson Use Only

If used as a template, MUST change name of agency and details to reflect YOUR practice

HIPAA: Confidentiality and Systems Usage Breach Policy

POLICY: Workforce Members must protect patient and business information at all times. This policy outlines a consistent process for sanctioning breaches of confidentiality and inappropriate use of information systems, and supports MHC Policy on *HIPAA Privacy and Security Incident Management*. The purpose of this policy is to provide a fair, clear, and consistent sanctions system for employees involved in a privacy or security breach, as well as to comply with HIPAA recommendations for a Sanctions policy. Sanctions are an important part of the remedial action plan to prevent further privacy or security breaches. Human Resources and Management maintains final authority for disciplinary consequences, with input/recommendation from the Privacy and Security Officer.

A Security Review Board oversees organization compliance with HIPAA on a quarterly basis.

Workforce members' obligations to confidentiality are defined in MHC Policy 01.04, *Confidentiality of Patient Information*, as well as Munson Healthcare's *Confidentiality & Systems Usage Agreement*; permissible use and disclosure of PHI is described in policy 012.010, *Use and Disclosure of Protected Health Information*.

SUMMARY OF CONFIDENTIALITY AND SYSTEMS USAGE CONDUCT:
Confidential Information – whether communicated verbally or by handwriting, printed paper, or electronic format – must be acquired, accessed, used or disclosed only to specifically support a patient care need, a business need, a legal need, or with the express written authorization of the patient or his/her legal representative.

Workforce members must seek and disclose the minimum amount of confidential information necessary to carry out their duties. Access to the records of family members, friends, co-workers, or other individuals is strictly prohibited (unless there is a job-related need or proper
e-authorization is on file (see policy 012.015).

All system access must be under each individual's own ID; sharing of passwords or doing work under someone else's account is a violation of law and policy. Workforce members are responsible for all activity recorded under their own IDs.

Stricter state and federal laws require the most restrictive degree of confidentiality for mental health, substance abuse, certain infectious disease information and patients requesting to opt out of the facility directory. Note, the appendix of this policy includes key definitions regarding certain infectious diseases that may elevate the severity of breach of privacy.

PROCEDURE

Potential breaches identified by audits occurrence reporting, patient complaints, or any other means are reviewed, investigated, and documented by the Privacy Officer. Privacy Officer may consult with appropriate personnel such as Security Officer, Medical Director of Information Systems, employee's Manager, Risk Management, Legal Counsel and Human Resources. A breach is deemed to be a privacy breach when it meets HIPAA's Final Rule definition of Breach: The acquisition, access use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

Each acquisition, access, use or disclosure of PHI not permitted under the HIPAA Privacy Rule will be considered a Breach unless a Risk Assessment demonstrates that there is a low probability that the PHI has been compromised. Munson's Privacy Officer will conduct the Risk Assessment which will include consideration of the following four factors:

1. Whether the acquisition, access, use or disclosure violates the HIPAA Privacy Rule;
2. Whether the PHI involved was "unsecured"
3. Whether an exception to the definition of "breach" may apply and
4. Whether there was a low probability that the PHI has been compromised.

Low probability of PHI compromise will be determined by consideration and examination of, at a minimum, the following four factors:

1) The nature and extent of PHI involved, including the types of patient identifiers and the likelihood of re-identification
2) Who was the person who accessed the PHI and to whom was it disclosed?
3) Was the PHI actually acquired or viewed?
4) The extent to which the risk to the PHI has been mitigated.

All Risk Assessments that are conducted shall be documented and maintained by the Privacy Officer for seven years. If a low probability or risk cannot be demonstrated, or if Covered Entity decides to send the Breach Notification letter in lieu of an entire risk analysis, still, decision making process for both will be documented, with emphasis on identifying gaps in privacy or security and remedial action.

Every breach of confidentiality, security, and/or violation of information systems usage policy that violates HIPAA introduces the potential for corrective action. The focus is now on the risk to the PHI and not a "harm threshold" for the patient. When determining appropriate corrective action for a given violation, the Privacy and Security Officer, Human Resources, Management (and if needed, Risk Management and Legal Counsel) will consider several factors including but not limited to:

1. How sensitive is the PHI in nature? For example, social security numbers, credit card numbers, or information that could cause harm to the individual?

2. Was the PHI disclosed to another covered entity? Could reassurances be given that the PHI would not be further used or disclosed?
3. How many patients are affected? How much PHI was compromised? What is the likelihood that the patient could be identified?
4. What other facts does the forensic analysis, audits, or investigation reveal?
5. Does the person who breached PHI stand to benefit from the use of the PHI?

6. Does the breach meet any of the HIPAA exceptions for 1) unintentional or inadvertent disclosures not further disclosed or 2) person not able to retain PHI information?

7. Does the PHI involve mental health, substance abuse, sensitive infectious disease information, and patients requesting to opt out of the facility directory? **Breaches of this type may result in higher levels of disciplinary consequences.**

In the case of any sanction imposed on an employee, if corrective action already exists in the employee's personnel file, then the corrective action issued under this policy will be escalated in accordance with existing Human Resources corrective action policies.

Violations and resulting sanctions are evaluated based on the following guidelines:

1) Human Resources have the final authority regarding level of sanction deemed appropriate for employee and the situation. Employee's manager has input into this process.
2) The Privacy Officer will serve as a resource for investigation and audit detail.
3) The Privacy Officer will conduct the risk assessment to determine probability of risk to PHI, in collaboration with one of more of the following key personnel: Security Officer, IS Director, Risk Management, or Legal Counsel.

Sanctions are carried out as follows.

For employees and volunteers, the employee's manager and the Human Resources department, will implement the sanctions.

For members of the medical staff and their respective office staff, the Privacy Office and Medical Director of information Security determination of a breach level and recommendation for hospital-based sanctions will initially be made to a Medical Staff Advisory Committee consisting of the President and President-elect of the Medical Staff, the chair of the Physician Well-Being Committee, and the VPMA. This group will subsequently make a recommendation to the Medical Executive Committee (MEC). The MEC will act upon the recommendation of the group. The MEC will report back to the Privacy Office regarding sanctions imposed and exceptions approved. Any requests for appeal of sanctions by members of the medical staff will be handled by the MEC, as per current by-laws or policy.

PRIVACY AND SECURITY INCIDENT SEVERITY SCALE GUIDELINE WITH RECOMMENDED DISCIPLINARY ACTIONS			
	Risk of Compromised PHI and Consideration of Harm		
	Low risk of compromised PHI, and no harm to patient or organization **No BreachNotification required.**	**Moderate risk of compromised PHI, unknown harm to patient or organization: (cannot demonstrate low risk)** **Breach Notification Required**	**MAJOR** **Multiple patients affected/Multiple PHI/Major harm (or potential harm) to patient, or organization** **Breach Notification Required**
Encrypted, or meets a HIPAA exception. **UNINTENTIONAL: No known or believed intent; or inadvertent mistake; or carelessness.** **Note: if mobile device lost or stolen due to no fault of staff, Major harm consequence may be reduced to 1**	1	2	2
INTENTIONAL: Due to curiosity or concern; or negligence	2	2 - 3	4
MALICIOUS OR UNETHICAL intent including use of info in a domestic dispute; Personal financial gain; Willful or reckless disregard of policies, procedures or law.	4	4	4

DISCIPLINARY RECOMMENDATIONS:

1 (White): No Action, or a Verbal Warning with Re-education, or Process Improvement
2 (Yellow): Written Warning or Final Written Warning;
3 (Orange): Final Written Warning or Termination;
4 (Red): Termination.

APPENDIX:
KEY DEFINITIONS

Confidential Information constitutes either of the following:

Business Information: Any information regarding the business and operations of any of the Munson Healthcare system entities ("Entities") obtained during the course of your work or association with the Entities. This may include, but is not limited to, information concerning employees, physicians, financial operations, quality assurance, utilization review, risk management, research, procurement, contracting, and other operational information.

Protected Health Information ("PHI") means information that: (i) is created or received by a Health Care Provider, Health Plan, or Health Care Clearinghouse; (ii) relates to the past, present or future physical or mental health or condition of an Individual; the provision of Health Care to an Individual, or the past, present or future Payment for the provision of Health Care to an Individual; and (iii) identifies the Individual (or for which there is a reasonable basis for believing that the information can be used to identify the Individual).

Workforce or **Workforce Member** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Facility, is under the direct control of such Entity, whether or not they are paid by the Facility.

Certain Infectious Disease Information: Public Health Laws have been invoked from time to time when there is improper access to or disclosure of protected health information relating to a patient's infectious disease, when the improper access or disclosure causes great harm (or the potential for great harm) to that person.

Diseases such as sexually transmitted diseases (STDs) can cause harm to patients if the information is disclosed beyond patient care needs. Examples of STDs that elevate the potential or actual level of harm include:

Acquired Immunodeficiency Syndrome (**AIDS**)
Chlamydia trachomatis (**Genital infections**), (**LGV**)
HIV (**Confirmed positive HIV serology and detection tests; CD4 counts/percents and all viral loads on people already known to be infected**)
Neisseria gonorrhoeae (**Gonorrhea**)
Treponema pallidum (**Syphilis**)

This list is not all-inclusive and judgment should always be used about what other types of infectious diseases may be similar in nature.