Confidentiality & Systems Usage Agreement

As a person having access to patient information, through your employment, association, or privileges with Munson Healthcare, Mercy Hospital Cadillac, and/or Mercy Hospital Grayling (hereinafter referred to as the “hospital(s)”), it is important that you understand and comply with hospital policy regarding security and confidentiality of patient information and the use of information systems. This Confidentiality & Systems Usage Agreement summarizes hospital policy.

DEFINITIONS

The name “Mercy” includes Mercy Hospital Cadillac, Mercy Hospital Grayling, and all organizations exchanging information with it, whether formally, informally, contractually, or otherwise affiliated.

The name “Munson” includes Munson Healthcare and all organizations exchanging information with it, whether formally, informally, contractually, or otherwise affiliated.

Otherwise affiliated may include: Charlevoix Area Hospital, Kalkaska Memorial Health Center, Ostego Memorial Hospital, Paul Oliver Memorial Hospital, and West Shore Medical Center.

Patient Information Any information regarding a patient obtained during the course of your work or association with the hospital(s). Such information may include, but is not limited to, financial and social data relating to patients, the medical record (i.e., documents relating to an individual’s medical history, diagnosis, condition, treatment or evaluation), business records, committee meetings and reports, physician office records, x-ray films, lab results, and incident reports.

Business Information Any information regarding the business and operations of the hospital(s) obtained during the course of your work or association with the hospital(s). 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.

Confidential information Patient information and Business information that is obtained during the course of your work or association with the hospital(s).

TERMS OF AGREEMENT

Confidential Information - whether communicated verbally or by handwriting, printed paper, or electronic (from a computer) format - must be accessed and 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. Special laws require the highest degree of confidentiality for mental health, substance abuse, and infectious disease information.

Conversing about and accessing confidential Information is a routine and necessary part of providing health services. However, reasonable measures must be employed to ensure that communication of and access to confidential Information in public areas (within and outside the facility/hospital/office) will not be heard or viewed by others who have no job related need to know. Appropriate precautions should be taken when accessing or transmitting confidential Information via computers, facsimile (fax), email, PDAs (palm pilots), printers, copiers, and the Internet.

You are responsible to seek and disclose the minimum amount of Confidential Information necessary to carry out your duties. You may not access the records of family members, friends, co-workers, or other individuals unless it is necessary for you to do your job (Exception: For Munson Medical Center employees, see policy 012.015). Your facility may or may not permit individuals who have access to health information systems to access their own electronic health information; refer to your facility’s policy.
You are responsible for all entries of data and information recorded into information systems under your user ID/password. You agree to not release your password to anyone else, or allow anyone else to access or alter information under your ID. You agree to not utilize anyone else's ID, password, or access device in order to access any information system. If you think your password may have been seen or used by someone other than yourself, reset it immediately; you may contact the Help Desk if you need help resetting your password.

The hospital maintains logs of access to information systems and reserves the right to audit, monitor, access, review and disclose information contained within such logs as necessary to assist customers and to determine and ensure that access to information systems is appropriate. Inappropriate activity will be investigated and corrective action will be carried out in accordance with existing disciplinary action policies.

If your employment or association with the hospital ends, you may no longer access any Munson or Mercy information systems. Your user ID(s) will be inactivated when you are no longer employed, associated with, or have privileges within the hospital(s). If your job classification or privileges change, you may be required to reestablish your access requirements and attend additional education. Your obligations to maintain confidentiality as described above continue even after a change or termination of employment, association, or privileges with the hospital(s).

Unauthorized purchase, installation, copying, access, alteration, erasure, or other unauthorized act pertaining to the hospitals' systems is prohibited. You may not make unauthorized copies of hospital-licensed software for any use, even when the software is not physically protected against copying. Use of hospital computers, including Intranet and Internet access, all clinical, administrative and business applications and electronic mail is intended only for job-related activities.

You are responsible for learning to use the facilities and systems that are required for your job duties. The hospital(s) provide education on many subjects, including specific topics and the use of certain information systems. You may be required to attend education classes on specific systems prior to being granted access. You are responsible for proper disposal of Confidential Information. Printed material with protected health information (PHI) on it must be disposed of using the Gray confidential bins or the blue bins, whichever are used in your department/agency for designated disposal of PHI. Where gray bins are available the blue bins are used for recycling of paper products without PHI. Departments handling Confidential Information further protected by state or federal law (such as Behavioral Health, Alcohol and Drug Treatment, and Infectious Disease) must first shred such documents before recycling. Call the Help Desk for assistance with eliminating or destroying Confidential Information on electronic media such as hardware and CDs. Employees of the hospitals refer to your facility’s electronic waste policy. This is policy 041.127 for Munson Medical Center.

By signing below, you are acknowledging that you have read and agree to follow hospital policy regarding confidentiality and the use of Information Systems. You are responsible for knowing and following policies. Consult your manager for copies of applicable policies and with any questions regarding your obligations under this agreement. If you are directly employed by the hospital, or use the hospitals' information systems for information storage, you also agree to provide authorized hospital representatives with any information necessary to unlock, decode, or otherwise make available upon demand, any and all information for which you are responsible if there is a legitimate need. If you breach the terms of this Confidentiality & Systems Usage Agreement, you may be subject to disciplinary action, in accordance with hospital policies and/or medical staff bylaws.

Your Signature:_______________________________________________________ Date:_____/_____/_______

Please Print Your Full Name:____________________________________________________________________

Your Work Phone:_______________________ Your Department:_______________________________________

Facility:_____________________________