CONFIDENTIALITY AGREEMENT

For protection and to respect the privacy, confidentiality and security of all confidential information ("CI"), this Confidentiality Agreement ("Agreement") is entered into by and between all employees, medical staff, students, volunteers, vendors, contractors and any others who are permitted access,

and *Munson Healthcare* (defined as the following entities, subsidiaries and/or affiliates: Munson Healthcare; Kalkaska Memorial Health Center; Munson Healthcare Foundations; Munson Dialysis Center; Munson Healthcare Cadillac; Munson Healthcare Charlevoix Hospital; Munson Healthcare Grayling Hospital; Munson Healthcare Manistee Hospital; Munson Healthcare Otsego Memorial Hospital; Munson Home Care; Munson Home Services; Munson Medical Center; Munson Medical Group; Munson Mobile Imaging, Inc.; Munson Services, Inc.; Munson Support Services; North Flight, Inc.; Paul Oliver Memorial Hospital, which shall be collectively referred to as "Munson".

CI includes:

1. Patient information (such as, medical records, billing records, and conversations about patients) *and*
2. confidential business information of Munson (such as, information concerning employees, physicians, hospital contracts, financial operations, quality improvement, peer review, utilization reports, risk management information, survey results, and research).

I UNDERSTAND AND AGREE TO ONLY ACCESS, USE OR DISCLOSE CI FOR JOB RELATED PURPOSES, AND WILL LIMIT ACCESS, USE OR DISCLOSURE TO THE MINIMAL AMOUNT NECESSARY TO PERFORM MY JOB.

FURTHER, I AGREE TO THE FOLLOWING:

1. I will protect the privacy and security of Munson information, including the electronic medical record (EMR) in accordance with all Munson policies.
2. I will not access the EMR out of curiosity or concern (for example, when a patient is a family member, friend, child, ex-spouse, co-worker, neighbor or VIP), but only for a job-related need.
3. I will not visit patients socially, for non work-related reasons, without first obtaining their permission.
4. I will not access my personal medical records on any MHC EHR (Electronic Health Record) to look up, or modify my own medical or billing records. This includes, but is not limited to viewing, adding, deleting updating appointments: charges, tasks, documents, notes, INBOX messages, etc. Instead, I will utilize the MHC Patient Portal for my personal needs.
5. I will complete any required privacy and security training and annual HIPAA Healthstream training.
6. I will not maintain CI on a personal mobile device that is not encrypted and/or password protected.
7. I will not send CI by email unless properly encrypted.
8. I will not share passwords or allow EMR access to a computer under my login credentials.
9. I will not enter a restricted area in hospital without an official job-related need or authorization.
10. I will not dispose of any paper or media with identifiable CI on it in the regular trash, but will use shredders, confidential bins or Information Systems to destroy materials.
11. I will immediately report to my supervisor any suspected privacy or security breach, or privacy error made in the course of normal scope of work.
12. I will safeguard all Munson equipment and data from theft and improper use, including personal equipment that may be used to access Munson resources.
13. I understand that any Munson device may be audited, including access to medical records, use of email and websites, and that there is no expectation of privacy.
14. I understand that I am responsible for complying with all Munson privacy and security policies.
15. I understand that all privacy breaches are investigated, documented and reported and that disciplinary consequences apply, up to and including termination. Civil fines or criminal penalties may also apply.
16. I understand that my duty to maintain the confidentiality of information as described here remains in effect even after my relationship with Munson, and/or access to Munson systems has ended.

I HAVE READ AND UNDERSTAND THE INFORMATION NOTED ABOVE.

Signature _____ Date _____

Printed Name _____ Employee ID_____

SEE NEXT PAGE FOR TIPS ON HOW TO AVOID A PRIVACY BREACH

GUIDELINES FOR AVOIDING A PRIVACY BREACH

DO:

1. You must have a work related need-to-know, prior to accessing, using or disclosing medical/billing records and your manager must agree on this job-related need.
2. Do utilize the Patient Portal for all medical information needs for yourself and others when there is no work-related need.
3. Do use confidential trash bins, or shredder, when disposing of any identifiable patient information.
4. Do use extra care when handing out, mailing, faxing or emailing PHI to make sure paperwork does not go to the wrong patient or location.
5. Do always use a fax cover sheet when faxing PHI and be sure to double check the fax number for accuracy prior to faxing.
6. Do always use [secure] in the email subject line when emailing PHI outside of mhc.net email. Be sure to double check the email address for accuracy prior to sending.
7. Do ask patient permission prior to discussion of any medical information in front of visitors.

DO NOT:

1. Do Not disclose patient information to anyone who does not have a job-related need – whether at work or at home, verbally or in writing, by text, photo or email or especially, by social media.
2. Do Not use the medical record to seek information on family, friends, spouses, children, ex-spouses or co-workers even if doing so is out of curiosity or concern. Remember that audits occur daily.
3. Do Not access the EMR using another person's password, or access a computer when another user is logged on.
4. Do Not use the EMR to check on the condition of a patient transferred from your department, floor, or facility unless you have a valid job-related need to know - and your manager agrees.
5. Do Not verbally disclose diagnostic results i.e., lab, cardiology, radiology, etc., to anyone who does not have a work-related need to know.
6. Do Not ask patients or coworkers you see at hospital why they are in the hospital, unless you have a work-related need to know.
7. Do Not visit patients, including co-workers (as patients), in the hospital unless they have invited you to, or you know with certainty they welcome visitors. It could be interpreted as an invasion of privacy.
8. Do Not access census sheets, whiteboards or patient lists where you are not currently assigned to work.
9. Do Not acknowledge the presence in the hospital of a patient who is opted out, (unless the patient has given out their privacy code to that person).
10. Do Not leave PHI in boxes or in unsecured areas such as public hallways, restrooms, unprotected storage, or other public areas.
11. Do Not discuss patients in public areas, such as the cafeteria or hallways, where conversations can be easily overheard.

MUNSON HEALTHCARE