MUNSON HEALTHCARE

Form #195 (02/15)

Confidentiality Agreement

It is the policy of Munson Healthcare and its affiliates (called "Munson" in this Agreement) that all employees, medical staff, students, volunteers, vendors, and any others who are permitted access, shall **protect and respect the privacy, confidentiality and security of all confidential information ("CI").**

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 that:

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 where 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 complete all required privacy and security training and annual HIPAA Healthstream training.
5. I will not maintain CI on a personal mobile device that is not encrypted and/or password protected.
6. I will not send CI by email unless properly encrypted.
7. I will not share passwords or allow EMR access to a computer under my login credentials.
8. I will not enter a restricted area in hospital without an official job related need or authorization.
9. 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.
10. 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.
11. I will safeguard all Munson and personal equipment from theft and improper use.
12. 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.
13. I understand that I am responsible for complying with all Munson privacy and security policies.
14. 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.
15. I understand that my duty to maintain the confidentiality of information as described here remains in effect even after leaving the Hospital.

I have read and understand the information noted above.

Your Signature_____Date_____

Print your Name_____Employee ID_____

Please see attached sheet for examples of privacy breaches/ Please note the examples are not all inclusive. There are other examples.

MUNSON HEALTHCARE

Form #195 (02/15)

Confidentiality Agreement

HIPAA Privacy Protected Health Information (PHI) includes:
Patient name, address, DOB, social security number, all content of the medical record, medications etc.

Munson Policy adds additional disciplinary consequences for privacy violations involving mental health records, substance abuse records, HIV status and other sensitive PHI.

Confidential Information is not to be shared inappropriately at work or away from work, via email, text, page, written format, social media, photos, video, verbal disclosure, fax or other.

Examples of Privacy Breaches:
-Using the EMR to keep track of medical problems and care of estranged family members.

-Using the EMR to check on patients you used to care for but are now discharged or moved to another floor.

-Announcing patient name or diagnosis loudly in a lobby area.

-Verbal disclosure of lab results to others who are interested, but who have no job related need to know.

-Visiting a patient on a restricted unit, such as Maternity, without their permission.

-Visiting a co-worker who is hospitalized, without their permission.

-Borrowing someone's password to access records or lending someone your password.

-Accessing a computer that is logged on under another's password.

-Disposing anything with a patient name on it in regular trash.

-Mailing or giving Discharge Instructions or medications to the wrong patient.

-Faxing PHI without FAX COVER SHEET and/or to the wrong Fax number.

-Asking patients or visitors invasive questions such as "Why are you here?" or "What surgery are you having?"

-Accessing charts of ex -husbands or ex- girlfriends, etc, out of curiosity or concern, or to use in custody battle.

-Accessing chart to see why your co-worker is in the emergency department.

-Disclosing patient presence in hospital after they had "opted out" of facility directory.

-Leaving paper charts or census sheets open and unattended. Leaving PHI in hall, restroom or library.

-Talking about your patients in a public place like the cafeteria or hair-dressers, or grocery store.

-Sending wrong H&P home with patient.

-Talking about medical information in front of patient's family without the patient's permission.