Home Health Student Internship Requirements

☐ Student Internship Application

☐ Home Health Release form

☐ Background consent form complete and fingerprinting results received. Please keep in mind that students are expected to pay for fingerprinting via money order at the time of the fingerprinting appointment. Human Resources will contact you to set up the appointment.

☐ Confidentiality Agreement

☐ HIPAA Education and Quiz

☐ Student Online Safety Education complete. Allow 45 minutes to complete.

☐ Per Education Affiliation Agreements with schools, your school must be able to provide documentation of updated immunizations, negative TB results, and proof of flu shot (10/1-3/31). Be sure to verify with your school that they have record of this information.

☐ License or Certification (if applicable)

☐ Send complete packet, along with background consent forms to Human Resources **before** your internship begins. Your internship supervisor will notify you when you have been cleared by Human Resources to begin your internship.

Welcome to Munson Home Health! Please note that this packet must be complete and submitted to Human Resources **before** you can begin your internship. If you require computer access, please notify your manager.

Home Health Student Internship Application

Full Legal Name:_____

Email Address:_____ Phone Number:_____

Date of Birth:_____ Social Security No:_____

School Name:_____ School Contact:_____

Internship Department at Munson Home Health:_____

I require a Munson computer login to complete my job duties:___Yes___No

Internship Start Date:_____ Internship End Date:_____

Have you ever been convicted of, or plead guilty or nolo contender (no contest) to any criminal offense (misdemeanor or felony)?_____Yes_____No

I request that I be granted access to provide services at Munson Home Health under the supervision of my sponsoring manager. Munson conducts criminal record checks. Falsification of this or any other information could prohibit the ability to provide services. Convictions may include, but are not limited to any alcohol driving offenses, retail fraud, and any and all convictions other than a minor traffic offense. I permit Munson Home Health to conduct a criminal record check without liability arising from obtaining this information.

I understand that I cannot work at any Munson Home Health facility until the entire Student Packet is complete and turned in to Human Resources.

Signature:_____ Date:_____

HR Approval: _____

MUNSON HOME HEALTH

MUNSON HEALTHCARE

Release and Waiver of Liability

In consideration of an educational experience at Munson Home Health, the undersigned individual:

- Hereby acknowledges that there are dangers and risks of personal injury or illness inherent in observing the care and treatment of patients, in exposure to bodily fluids and other specimens, and otherwise.
- Hereby acknowledges that Munson Home Health is not responsible for any personal injury, illness, or other damage of any kind relating to my experience or exposure to patients, bodily fluids or other specimens.
- Hereby acknowledges that any bodily or personal injury, illness or other damages of any kind arising out of or related to the educational experience will not be covered by workers compensation insurance or any other insurance coverage provided to Munson Home Health.
- Hereby assumes full responsibility for any risk of bodily or personal injury, illness, or other damages of any kind arising out of or related in any way to the educational experience at Munson Home Health, including any risks caused by the negligence of Munson Home Health.
- Hereby releases, waives, forever discharges and covenants to hold harmless Munson Home Health, its officers, directors, employees, insurers, and agents of and from all liability for any all loss or damage, and any claim or demand on account of personal or bodily injury arising out of or related in any way to the educational experience at Munson Home Health, including any/all loss or damage, claim or demand arising out of the negligence of Munson Home Health.

_____

Student Name (Print)

_____ _____

Student Signature Date

_____

Parent/Legal Guardian's Name (Print)

_____ _____

Parent/Legal Guardian's Signature Date

(required if student/intern is under 18)

STATE OF MICHIGAN
DEPARTMENT OF LICENSING AND REGULATORY AFFAIRS

MICHIGAN WORKFORCE BACKGROUND CHECK CONSENT AND DISCLOSURE

MCL 333.20173a, MCL 330.1134a, and MCL 440.734b require that a health facility/agency that is a:

- psychiatric facility
- ICF/MR
- nursing home
- county medical care facility
- adult foster care facility (AFC)
- hospital that provides swing bed services
- home for the aged
- home health agency
- hospice

Shall not employ, independently contract with, or grant clinical privileges to an individual who regularly has direct access to or provides direct services to patients or residents in the health facility/agency or AFC until the health facility/agency or AFC conducts a fingerprint-based criminal history check.

An individual who applies for employment either as an employee or as an independent contractor or for clinical privileges with a health care facility/agency or AFC and has received a good faith offer of employment, an independent contract, or clinical privileges shall give written consent at the time of application for the health care facility/agency or AFC to conduct a criminal history check, including a state and Federal Bureau of Investigation (FBI) fingerprint-based check, and shall give a written statement disclosing that he or she has not been convicted of a crime that would prohibit employment.

NOTE: Throughout this form:

- "Employee" includes persons independently contracted with and/or those granted clinical privileges.
- Clinical privileges do not apply to adult foster care facilities.

Health Facility or Agency

Licensee Name:_____ **Date:**_____

Employment Applicant Name:_____

Facility Name/License Number:_____

The health facility/agency or AFC:

a. May not knowingly employ a worker, having direct access to patients or residents, who has been convicted of a disqualifying crime or has been the subject of a state or federal agency substantiated finding of patient or resident neglect, abuse, or misappropriation of property.* "Direct access" means regular access to a patient or resident, or to a patient's or resident's property, financial information, medical records, treatment information, or any other identifying information.
b. May terminate the background check or decide not to hire the individual at any stage of the process.
c. Must ensure that any background check information provided will only be used for the purpose of determining an individual's suitability for employment in a long-term care setting.
d. Must retain verification of compliance with background check requirements.
e. Will make the final employment decision.

* This does not include a finding of abuse, neglect, or misappropriation (financial exploitation) substantiated under the Michigan Mental Health Code or Adult Protective Services Act.

Part 1 – Consent to Conduct Background and Criminal Record Checks

As a condition of being considered for employment:

a. I hereby consent to and authorize the health facility/agency or AFC to conduct a background check that includes a search of state and federal abuse and neglect registries and databases, in addition to a fingerprint-based search of state and federal criminal history records. I understand that this consent extends to the release and sharing of such information with the Michigan Departments of Licensing and Regulatory Affairs and State Police.

b. I further understand the Michigan State Police (MSP) and the Federal Bureau of Investigation (FBI) may also retain the submitted information and fingerprints as permitted by the Federal Privacy Act of 1974 (5 USC § 552a(b)) for routine uses beyond the principal purpose listed above. Routine uses include, but are not limited to, disclosures to: governmental authorities responsible for civil or criminal law enforcement, counterintelligence, national security, or public safety.

c. I hereby authorize the release of any relevant information to the health facility/agency or AFC to be used to conduct the background check as required under MCL 333.20173a, MCL 330.1134a, and MCL 440.734b.

d. I understand, except for a knowing or intentional release of false information, the health facility/agency or AFC has no liability in connection with a background check conducted under MCL 333.20173a, MCL 330.1134a, and MCL 440.734b or the release of criminal history record information for the purposes of making an employment decision.

e. I understand that the health facility/agency or AFC will make the final employment determination. I also understand that the health facility/agency or AFC may terminate the background check or decide not to hire me at any stage of the process.

f. I understand that the health facility/agency or AFC, in denying employment to an applicant, and reasonably relying on information obtained through a background check, is provided immunity from any action brought by an applicant due to the employment decision.

g. I agree to provide the information necessary to conduct a criminal background check.

_____ _____

Signature of Applicant Date

Part 2 – This employment applicant information is required to process a complete and accurate criminal record check.

EMPLOYEE PERSONAL INFORMATION

First Name:

Middle Name:

Last Name: Suffix:

OTHER NAME (S) USED (MAIDEN NAME, ALIAS)

First Name:

Middle Name:

Last Name: Suffix:

Date of Birth: Country of Citizenship:

Place of Birth (City, State/Province):

Height: Weight: Hair Color: Eye Color Gender: ☐ Female ☐ Male

Race: ☐ Asian ☐ Black ☐ Hispanic ☐ Native American ☐ Pacific Islander ☐ White ☐ All

Social Security Number:

ADDRESS

Street Address:

City: State: Zip Code: County:

Phone Number:

Job Title: Conditional Hire Date:

RESIDENCY

Driver's License or State/Canadian ID Number:

State/Prov. License/ID Number

Has this employment applicant resided in Michigan continuously for the past 12 months? ☐ YES ☐ NO

PROFESSIONAL LICENSE(S) /CERTIFICATION(S)

1. License/Certification Number:
2. License/Certification Number:
3. License/Certification Number:

Part 3 – Employment Applicant Disclosure Statements

The following convictions and/or findings may disqualify you from working in a long-term care facility/agency or AFC. "Conviction" includes any plea of guilty or nolo contendere (no contest), which may include cases that resulted in a deferred sentence or delayed sentence.

a. **Relevant Crime Described under 42 USC 1320a-7** – The crimes include patient abuse, health care fraud, and any crimes related to the unlawful manufacture, distribution, prescription, or dispensing of a controlled substance.

b. **Felony** – Any felony, or an attempt or conspiracy to commit any felony.

c. **Misdemeanor** - Any state or federal crime that is substantially similar to the misdemeanors described below:

- Any misdemeanor involving the use of a firearm or dangerous weapon with the intent to injure, the use of a firearm or dangerous weapon that results in a personal injury, or a misdemeanor involving the use of force or violence or the threat of the use of force or violence.
- Any misdemeanor for assault if there was no use of a firearm or dangerous weapon and no intent to commit murder or inflict great bodily injury.
- Any misdemeanor involving criminal sexual conduct.
- Any misdemeanor involving abuse or neglect, torture, or cruelty.
- Any misdemeanor involving home invasion.
- Any misdemeanor involving embezzlement, larceny, fraud, theft or second or third degree retail fraud.
- Any misdemeanor involving negligent homicide.
- Any misdemeanor involving the possession, use or delivery of a controlled substance.
- Any misdemeanor involving the creation, delivery, or possession with intent to manufacture or deliver a controlled substance.

d. **Any finding of Not Guilty by Reason of Insanity**

e. **A substantiated finding of patient or resident neglect, abuse, or misappropriation of property resulting from an investigation conducted in accordance with 42 USC 1395i or 1396r**

Listed below are all offenses that I have been convicted of, including all terms and conditions of sentencing, parole and probation, and/or a substantiated finding of patient or resident neglect, abuse, or misappropriation of property.

Offense	Date of Conviction/Finding	City	State	Sentence	Date of Discharge

I certify that the above statements are correct and complete to the best of my knowledge.

Signature of Applicant _____ Date _____

Part 4 – Conditional Employment

If the health facility/agency or AFC determines it necessary to employ me pending the results of the state and federal criminal history background check, I understand the following:

a. If the background check reveals disqualifying information my employment will be terminated for good cause, unless and until I successfully prove that the disqualifying information is inaccurate, expunged or set aside.
b. If I knowingly provided false information regarding my identity, criminal convictions, or substantiated findings of patient or resident neglect, abuse, or misappropriation of property, I may be guilty of a misdemeanor punishable by imprisonment for not more than 93 days and/or a fine of not more than $500.00.
c. I understand that as a condition of continued employment, I am required to report in writing to the health facility/agency or AFC immediately upon being arraigned on a felony charge or convicted of one or more of the criminal offenses as described in MCL 333.20173a, MCL 330.1134a, and MCL 440.734b, or upon becoming the subject of an order or dispositional finding of "Not Guilty by Reason of Insanity", or upon being the subject of a state or federal agency substantiated finding of patient or resident neglect, abuse, or misappropriation of property. Reporting of an arraignment is not cause for termination or denial of employment.

_____ _____

Signature of Applicant Date

Part 5 – Applicant Rights

a. I understand that upon my request, the health facility/agency or AFC can provide a copy of any disqualifying record information found on any of the relevant registries or databases.
b. I understand that if I believe the results of any disqualifying information found on any relevant registry is inaccurate, it is my responsibility to contact the agency that maintains the registry to correct the registry information.
c. I understand that if I believe the results of the criminal history fingerprint record are inaccurate, or if the conviction contained in the criminal history record is one that may be expunged or set aside, I may file an appeal with the Department of Licensing and Regulatory Affairs.

_____ _____

Signature of Applicant Date

Part 6 – Disclaimer

The State of Michigan is not responsible for any additional information, requirements, or use of any substitute forms that the above named health facility/agency or AFC provides to the applicant.

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.

HIPAA Employee Brochure

Mission Statement
Munson Healthcare and its partners work together to provide superior quality care and promote community health.

Values
Patients
People
Accountability
Respect
Stewardship
Compassion

Privacy, Our Mission, and Our Values
Federal laws were established that require all health care providers to take significant measures to safeguard patient privacy. Building upon our culture of protecting patient confidentiality, Munson Healthcare is undertaking efforts to comply with these laws. Our efforts uphold the Munson values of Respect and Stewardship, and support the trusting patient relationships that are so critical to providing quality care.

While these new federal laws were established, in part, to ensure patient privacy, they also simplify the sharing of health information for the coordinated care of patients in our communities. As stewards of the health information that is entrusted to us, we believe that protecting patient privacy is simply the right thing to do. Your commitment to protecting patient health information will ensure our success, and allow us to continue providing superior quality care.

Sincerely,

Ed Ness
President and CEO
Munson Healthcare

Table of Contents

Brief Overview of HIPAA
The Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA, was created by the federal government to promote the portability of health insurance (that is, to help individuals gain health insurance coverage, even with pre-existing health conditions) and to protect against fraud and abuse.

Passed with bipartisan support, the law also includes provisions aimed at improving the efficiency of health care and ensuring that the privacy of individuals (our patients) is protected. These provisions promote the use of electronic transactions (e.g. claims) while protecting the privacy and security of health information. These particular rules fall under a category of HIPAA law called "Administrative Simplification", and Covered Entities are obligated to comply with the Administrative Simplification rules. Covered Entities are health care providers, health plans, and health care claims clearinghouses.

HIPAA'S ADMINISTRATIVE SIMPLIFICATION RULES INCLUDE THE FOLLOWING PARTS:

- **Privacy.** The privacy regulations govern who has access to Protected Health Information (PHI). They ensure that PHI is used appropriately by creating a national minimum standard of privacy (state laws can be more stringent). The privacy regulations also give patients specific rights regarding their health information. The deadline to comply with the privacy regulations is April 14, 2003.
- **Security.** The security regulations govern how health information is protected. They establish safeguards for Protected Health Information (PHI), including, for example, ensuring that access to PHI is authorized and audited, and encrypting (or scrambling) the content of PHI that is transmitted over the Internet. The deadline to comply with the security regulations is April 21, 2005.
- **Electronic Data Interchange (EDI).** The EDI regulations promote electronic transactions to increase efficiency and save costs in the administration of health care delivery and its payment systems. The extended EDI compliance date is October 16, 2003.

HIPAA has been called the most significant federal legislation in decades to impact the health care industry. In our role as a leading health care system, it is essential for Munson Healthcare to act in accordance with HIPAA standards and to meet compliance deadlines.

The Benefits of HIPAA
HIPAA supports a new way of doing business in the Information Age. This provides an opportunity to improve how we deliver health care and creates benefits for patients, our organizations, and the health care industry.

For *patients*, HIPAA reduces the chance for inappropriate use and disclosure of information related to patient care. Patients gain an understanding of the ways in which health care organizations use and disclose their personal information. Patients also learn about their rights regarding those uses and disclosures. The HIPAA rules also simplify the ability for providers to share health information with other providers; the true benefit is realized through improved care to the patients that providers mutually serve.

HIPAA is a public policy affirmation of our Value of Respect, particularly as it applies to patient confidentiality. The law is also geared toward improvement in the accuracy and efficiency of health care transactions related to treatment and payment. These factors work to enhance patient confidence and reinforce a positive public image for Munson Healthcare.

The *health care industry* as a whole benefits from the increased use of electronic transactions and from the existence of minimum standards for protecting patient information.

HIPAA Concepts: Workforce Education
HIPAA requires that we educate our entire workforce about HIPAA and the confidentiality policies and procedures that we have implemented. By definition, the workforce includes physicians, employees, volunteers, and other individuals, such as contractors, who act in roles as if they are employees, whether on a part-time or full time basis. This education is required of such workforce members regardless of the amount of contact they have with patients or PHI (although those who have more patient or PHI contact will learn more about HIPAA than those who don't regularly work with patients or PHI).

HIPAA Concepts: Protected Health Information
Protected Health Information (PHI) is medical information that could reasonably identify an individual. Medical information is considered Protected Health Information if it includes **any** of the following information (in oral, paper, or electronic form):

. Names
. Street address, city, county, full zip code (with some qualifications)
. Dates directly related to an individual (e.g. birth date, admit/discharge date, dates of service)
. Telephone and fax numbers
. Email addresses
. Social Security Numbers
. Medical record numbers
. Health plan beneficiary numbers
. Account numbers
. Certificate/license numbers
. Vehicle identifiers (e.g. license plate numbers)
. Device identifiers and serial numbers
. Web Universal Resource Locators (URLs)
. Internet protocol (IP) address numbers
. Biometric identifiers (e.g. finger and voice prints)
. Full face photographic images
. Any other unique identifying number, characteristic, or code

Every member of the work force, even those who don't deal directly with patient information, should have an understanding of what PHI is and the ways in which it must be protected.

HIPAA Concepts: Use and Disclosure
The sharing of PHI is essential to providing and paying for health care services. HIPAA describes the sharing of PHI as either a Use or Disclosure. Use is defined as the sharing of PHI *internally* within an organization. Examples include the creation of a hospital bill or the sharing of a medical record between caregivers when treating a patient.

A Disclosure is defined as the release of PHI *outside* an organization. An example would be the sharing of medical dictation with an external vendor, such as a transcription service or a collection agency.

The Privacy rule covers electronic, paper, and oral uses and disclosures of Protected Health Information.

HIPAA Concepts: Treatment, Payment, and Operations
The vast majority of uses and disclosures of PHI are for one of three reasons:

- **Treatment.** The provision, coordination, or management of health care and related services by a health care provider
- **Payment.** Activities by a provider or health insurance plan to obtain or provide reimbursement for the provision of health care; the activities of a health insurance plan to obtain premiums, determine coverage, and provide benefits
- **Health Care Operations.** A wide range of activities defined in the privacy regulations, such as:
  - quality assessment and improvement
  - credentialing, performance evaluation, training of health professionals
  - medical review, legal services, audits
  - underwriting, premium rating
  - business management, administration, planning and development.

There are uses and disclosures of PHI that fall outside of these three areas. Examples include some marketing activities and disclosures to entities such as life insurance companies, public health departments, or law enforcement agencies. HIPAA applies more restrictions to these types of uses and disclosures.

HIPAA Concepts: Notices of Privacy Practices; Acknowledgement
HIPAA requires that health care organizations provide patients with a Notice of Privacy Practices. The Notice must be easy to read and understand, and it must be posted in public areas where patients are likely to see and read it, including an organization's website.

This Notice informs patients how their PHI may be used and disclosed by the organization to carry out treatment, payment, and health care operations. It explains patients' rights and how to exercise them. It provides the name of a contact person if the patient wants more information or wishes to file a complaint.

The Notice should be provided to patients the first time they visit a health care organization on or after April 14, 2003 (the date the Privacy Rule is to be enforced). Most importantly, the organization must make a good-faith effort to obtain a written Acknowledgement that the patient has received a copy of the Notice. Patients do not have to agree with the Notice.

HIPAA Concepts: Opportunity to Agree or Object
HIPAA requires that patients be given the opportunity to verbally agree or object to certain uses and disclosures of their PHI.

Patients must be given the opportunity to agree or object to being included in a Facility Directory; that is, the patient must specify whether or not he wants visitors and callers to know of his presence in the hospital. Individuals who inquire about a patient by name may only know of the patient's location and general condition. Clergy may also be privileged to a patient's religious affiliation and need not ask for patients of a given affiliation by name, provided the patient elects to have his name included in the Facility Directory.

Patients must also be asked if the hospital/treating facility may disclose information to other individuals (e.g., family members, friends, roommates, etc.) who are involved in the patient's care. That is, care providers generally should not make assumptions that patients want individuals who are with a patient or related to a patient to be involved in discussions about their care.

HIPAA Concepts: Authorization

A written Authorization from the patient is required for some of the small minority of uses and disclosures that fall outside of treatment, payment, and health care operations. Research and some marketing activities require authorization. Authorization must always be obtained to release a patient's psychotherapy notes.

Once an Authorization is signed, a patient has the right to revoke or cancel it at any time. HIPAA specifically states that the patient's care cannot be conditional upon a patient's signing of an Authorization.

Certain other specific uses and disclosures outside of treatment, payment, and operations do not require a written Authorization. For the most part, such disclosures are required by law and pertain to reporting certain incidents to law enforcement officials, public health agencies, or health oversight agencies.

HIPAA Concepts: Patient Rights

HIPAA provides patients (or members of health plans) with several basic rights that inform and empower them.

Munson Healthcare has developed policies and procedures to ensure that these rights are respected and delivered.

1. The patient has the right to receive a Notice of Privacy Practices (see page 5).
2. The patient has the right to inspect and copy his or her PHI used by the organization. The organization is obligated to provide this information in a timely manner.
3. The patient has the right to amend his or her PHI kept by the organization. This right may be denied based upon certain criteria. The organization is responsible for documenting the request and its outcome.
4. The patient has the right to restrict the use and disclosure of his or her PHI. This right may be denied based upon certain criteria. The organization is responsible for documenting the request and its outcome.
5. The patient has the right to authorize or to reject the use or disclosure of his or her PHI for certain activities that do not fall within treatment, payment, and operations. Care cannot be conditional upon an Authorization (see page 5).
6. The patient has the right to request and receive an accounting of uses or disclosures of his or her PHI for certain activities that do not fall within treatment, payment, or operations, such as reporting of infectious disease, births, and deaths to public health authorities; reporting of suspected abuse or other suspected criminal activity to authorized officials; and, reporting of an employee's non-job related access to, use, or disclosure of a patient's health information.
7. The patient has the right to request where and how confidential communications containing his or her PHI are made. The organization is responsible for complying with reasonable requests.
8. The patient has the right to file a complaint directly to the organization or to the Secretary of Health and Human Services about the organization's privacy practices and/or suspected violations of HIPAA's privacy regulations. The organization is responsible for investigating the complaint and responding to the patient in a timely manner.

HIPAA Concepts: Incidental and Oral Communications
Health care providers often need to discuss patient information in places such as the Emergency Department or a semi-private room, where privacy is often difficult to achieve. From time to time, these discussions may result in an "incidental" disclosure of PHI.
The goal of the privacy regulations is not to prevent discussions related to treatment, but rather to ensure that the organization -- and its employees -- are doing what is reasonable to protect a patient's PHI. Whenever possible, conversations containing PHI should be avoided in public places such as hallways, elevators, lounges, and cafeterias.

HIPAA Concepts: Minimum Necessary
HIPAA requires that organizations take reasonable steps to allow access only to the minimum PHI necessary to perform a specific task or job. This minimum necessary standard applies to both internal uses as well as external disclosures. The minimum necessary standard is not intended to impede patient care and therefore does not apply to treatment.

To fulfill the minimum necessary standard, employees should have access to information tailored to their specific job responsibilities. External vendors also will receive information based upon the specific task or job that they perform for the organization.

HIPAA Concepts: Business Associates
Business Associates are external persons or entities that use or receive PHI from a Munson Healthcare organization to assist with a specific task or job. Business Associates may include lawyers, independent contractors, consultants, auditors, billing companies (including clearinghouses), quality review companies, transcriptionists, and information system/data processing vendors.

Munson Healthcare must develop written contracts that clearly state the permitted uses and disclosures of PHI by each Business Associate. Consistent with the minimum necessary standard, Business Associates should receive only the PHI needed to perform a specific activity or task for the organization, and they may not use the information for purposes outside of the written contract.

HIPAA Concepts: Privacy Official
HIPAA requires that organizations create the new role of Privacy Official. The Privacy Official's primary responsibility is to oversee an organization's compliance with HIPAA privacy regulations. This individual serves as a champion for privacy issues. He or she ensures that the organization implements appropriate policies and procedures, responds to employee questions and concerns, and resolves privacy-related complaints.

HIPAA Concepts: Safeguards
HIPAA requires organizations to implement and maintain appropriate safeguards to protect PHI from unauthorized access and unauthorized uses and disclosures. Through its privacy and security policies, Munson Healthcare is working to implement safeguards, such as:

- Improved authentication/log-on mechanisms
- Implementation and monitoring of audit trails and logs that identify potential incidents of unauthorized access to PHI
- Adequate measures for destroying PHI in paper and electronic form
- Verification of the identity of persons requesting PHI.

Reporting Privacy Concerns

The new privacy regulations are complex, and you will likely have questions from time to time. As a member of Munson Healthcare's work force, you are responsible for seeking answers to questions or concerns, including possible violations of law, regulations, policies, and procedures.

When seeking answers to your questions or concerns, consider the following guidelines::

1. First, contact your supervisor.
2. If you are not comfortable asking your supervisor or not satisfied with the answer, contact a higher-level manager.
3. If you are still not satisfied, contact your local Privacy Official.

FAQ

What is HIPAA?
HIPAA is a law created by the federal government to promote the portability of health insurance and to protect against fraud and abuse. Other major provisions promote the use of electronic transactions while protecting the privacy and security of health information. Although HIPAA initiatives may be motivated by public policy, Munson Healthcare does not view compliance as the only reason for our efforts. Our commitment to Respect Privacy is simply the right thing to do, and it requires a long-term commitment from every Munson Healthcare employee.

Why is HIPAA significant?
Here are three ways in which HIPAA is significant:

- The regulations include patient confidentiality and privacy protections, which greatly increase patient rights and provider responsibilities regarding health care information.
- The regulations require health care providers to process certain electronic business transactions in a standardized and efficient manner.
- The regulations give the government significant additional authority to regulate health care providers and payers.

Are there penalties for non-compliance with the law?
Yes, under the law, there are potential penalties for non-compliance. These penalties include fines, criminal sanctions, and even imprisonment in the most severe cases. In addition, there are potential penalties that are not legal in nature, such as loss of reputation in the community.

Is there a problem in our health care industry with protecting patient information?
Yes. There have been many documented instances where PHI was treated inappropriately:

- In Washington, international hackers stole 5,000 patient record files from an academic medical center.
- An employee in Michigan told a friend that one of his patients had AIDS. That friend had known the patient for years and subsequently told other friends about the patient.
- A medical student in Texas was paid for disclosing questionable medical practices to local attorneys so that the attorneys could find easy cases to win.

Does HIPAA apply to volunteers and temporary staff?
Yes. HIPAA applies to all members of the Munson Healthcare work force. Work force members include physicians, employees, temporary workers, students, and volunteers.

I work in the ER. What happens if someone is unable to sign an Acknowledgement due to his or her medical condition?
No problem. Our commitment to helping people who need medical attention is our first priority. Continue to treat the patient. You may obtain the Acknowledgement as soon as it is reasonably practical.

I'm worried that HIPAA requirements will prevent me from providing quality patient care by limiting my access to information or persons to whom I can speak. What should I do?
Increased privacy and security protections are not intended to interfere with the communication of health information when used for treatment. If you need access to information for legitimate treatment purposes, it should be available to you. If you are asked to share information for legitimate treatment purposes, please share it.

I'm not sure if a specific activity or task is considered part of operations as defined by HIPAA. What should I do to find out?
There are several useful sources for this information. Ask your supervisor, refer to organizational policies, or ask your Privacy Official.

I never deal with patient information. Why should I care about HIPAA?
Through our commitment to Respect Privacy and patient confidentiality, it is every employee's job to know how to apply the organization's policies in case you do come into contact with patients or patient information. For example, from time to time, we all see patients that we know, like friends, neighbors, and relatives. If you see a patient that you know, it is important for you to respect that patient's privacy, for example, by not seeking information about why the patient is at your facility.

How do I handle a patient who will not sign an Acknowledgement for the Notice of Privacy Practices?
Explain to the patient that he or she does not have to agree with the Notice in order to sign the Acknowledgement. Rather, the patient is signing the Acknowledgement to confirm that he or she has received the Notice. If the patient still does not sign the Acknowledgement, simply record that you made a reasonable effort to obtain an Acknowledgement from the patient.

I often hear other employees having patient-related conversations in the cafeteria. Should I do anything about this? If so, what?
As long as the conversations you hear do not include identifiers and cannot reasonably be linked to a specific patient, the conversation is OK. If the conversation can be linked to a patient, you may want to say something to the people having the discussion. If you feel uncomfortable addressing the issue directly, talk to your supervisor, contact your Privacy Official, or follow existing occurrence reporting procedures.

I filed a privacy complaint several weeks ago and have not heard what was done about it. How can I find out what's been done?
Contact your Privacy Official.

A patient wants to change his medical record. What should I do about this?
Under HIPAA, a patient has a right only to amend his or her medical record, not to change it. This means a patient cannot remove information from the record. If a patient wishes to amend his or her medical record, follow your organization's appropriate policy.

I'm afraid I will lose my job if I tell someone about a privacy violation in my department. How can I be sure that the organization will protect me?
It is Munson Healthcare policy that no one is allowed to retaliate in any form against an individual reporting a privacy concern in good faith.

I want to use Protected Health Information in a manner not currently described in the Notice of Privacy Practices. What should I do?
Consult your HIPAA leadership to determine if the use falls within treatment, payment, or operations. If the use is not described in the Notice of Privacy Practices, then you must obtain an authorization from the patient prior to using the PHI. An alternative would be to revise the Notice to add the additional use, if it is a permitted use. You may not use the PHI until the Notice is revised, distributed to patients, and posted throughout the organization.

I am developing a relationship with a new vendor. Does HIPAA impact what I need to do?
Yes. HIPAA requires that you know what type of information will be disclosed to the vendor. If the vendor is using Protected Health Information provided by us, then we may have to establish a contractual relationship that includes specific language. Your HIPAA leadership can provide guidance on where to obtain the necessary contractual language. Share only the minimum necessary information that allows the vendor to complete its specific task or job. Also, new relationships will require us to consider whether changes to our Notice of Privacy Practices are necessary.

Quick Tips for Using and Disclosing Patient Information
When asked for patient information, you should consider two things:
1. Who is asking for the information?
2. Why do they need it?

Here are some examples of common requests and how they should be handled:

Who's Asking?	Why?	Requirements
Provider (physician, hospital, nursing home, other provider)	To treat the patient	No Authorization is needed. Minimum necessary does not apply.
Provider	For billing purposes	No Authorization is needed. Release the minimum amount of information needed.
Payer (health plan, insurance company)	For payment purposes	No Authorization is needed. Release the minimum amount of information needed.
Family member	To help in caring for the patient	No Authorization is needed, but the patient should be asked and given an opportunity to object or limit the information shared.
Media	For a news story	Refer this request to Public Relations.
Attorney	For a lawsuit	Written patient Authorization or a valid subpoena is required. Follow your organization's policy and procedure in this circumstance.
Patient's Employer	To obtain the results of drug testing	Written patient Authorization is required. Follow your organization's policy and procedure in this circumstance.

Remember: When in doubt, check with your supervisor or your organization's Privacy Official before disclosing any information.

Munson Healthcare
HIPAA General Awareness Quiz

Your Name:_____ **Date:**_____

Department: _____

1. Why should I care about HIPAA?
   a. It is required by Federal law
   b. It supports our Value to Respect patients' privacy
   c. Every employee must know how to apply the hospital's HIPAA policies
   d. Our patients and MHC staff who become patients deserve privacy and respect.
   e. All of the above

2. Which of the following types of Workforce Members are not required to learn about HIPAA?
   a. Volunteers
   b. Physicians
   c. Employees
   d. None of the above

3. PHI stands for:
   a. Prohibited Health Information
   b. Protected Health Information
   c. Psychotherapy Health Information
   d. Public Health Information

4. PHI is any health information that could reasonably be used to identify the patient.
   a. True
   b. False

5. It's OK to share PHI with the friends or neighbors of a patient if you all belong to the same church group.
   a. True
   b. False

6. The Notice of Privacy Practices:
   a. informs patients how their PHI may be used by the hospital
   b. provides the name of a contact person if the patient wants to file a privacy complaint
   c. must be offered to every patient and posted in a public place in the hospital
   d. all of the above

7. Under HIPAA, patients have the right to decide whether or not they want callers and visitors to know of their admission to the hospital.
   a. True
   b. False

8. HIPAA compliance includes taking reasonable measures to ensure that conversations about patients are not overheard by people who have no need to know.
   a. True
   b. False

9. Under HIPAA, if you access a patient's health information for unauthorized or non-job related reasons, we would be required to notify patient of this breach if major harm (emotional, financial or reputational) occurs (upon the patient's request).
   a. True
   b. False

10. Under HIPAA, the term "Minimum Necessary" means:
    a. that you do as little work as possible every day
    b. that every employee can have access and share only to the amount of PHI necessary.
    c. that physicians cannot request a patient's entire medical record to treat the patient
    d. none of the above

11. Under HIPAA, it's important to check policy or ask supervisor if a given disclosure of PHI:
    a. will require a change to our Notice of Privacy Practices
    b. requires patient authorization
    c. requires a written contract with a business associate
    d. all of the above

12. We can assume it's okay to discuss a patient's health information in front of family members and/or friends.
    a. True
    b. False

13. The penalties for an institution and/or employee with a serious HIPAA violation may include:
    a. fines
    b. imprisonment
    c. termination of employment
    d. loss of reputation in the community
    e. all of the above

How to Access the Orientation Education

Go to this link: Orientation Education

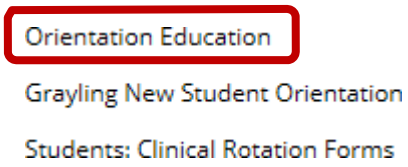
or

Go to the following internet web page: http://www.munsonhealthcare.org/

1. Scroll down and click on FOR EMPLOYEES

2. Place mouse on “New Hire Hub”:

3. Select “Orientation Education” from the dropdown menu.



Allow approximately 1 hour to complete the education. You are required to complete this training before starting your work with Munson. If you have any difficulty, please contact Human Resources at 231-935-2279