TMCAH
Safety Packet 2024

Patient's Rights and Responsibilities

All patients and their families possess basic rights and responsibilities. These include:

The Right To:

a. Be treated with consideration, respect, and full recognition of the client's dignity and individuality, including privacy in treatment and personal care and respect for personal property and including being informed of the name, licensure status, and staff position and employer of all persons with whom the client/resident has contact, pursuant to RSA 151:3-b.
b. Receive appropriate and professional care without discrimination based on race, color, national origin, religion, sex, gender identity, disability, or age, nor shall any such care be denied on account of the patient's sexual orientation.
c. Participate in the development and periodic revision of the plan of care, and to be informed in advance of any changes to the plan or intent to discharge except as provided in RSA 151:26-a, III.
d. Be informed that care is evaluated through the provider's quality assurance program.
e. Refuse treatment within the confines of the law and to be informed of the consequences of such action, and to be involved in experimental research only upon the client's voluntary written consent.
f. Voice grievances and suggest changes in service or staff without fear of restraint, discrimination, or reprisal.
g. Be free from emotional, psychological, sexual, and physical abuse and from exploitation by the home health care provider.
h. Be free from chemical and physical restraints except as authorized in writing by a physician.
i. Be ensured of confidential treatment of all information contained in the client's personal and clinical record, including the requirement of the client's written consent to release such information to anyone not otherwise authorized by law to receive it. Medical information contained in the client's record shall be deemed to be the client's property and the client has the right to a copy of such records upon request and at a reasonable cost.
j. Be informed in advance of the charges for services, including payment for care expected from third parties and any charges the client will be expected to pay.

Responsibilities – The patient and/or family has a responsibility

a. Give accurate and complete health information.
b. Create and maintain an environment that is safe and free from sexual or other forms of harassment by the client or others in the home. For the purposes of this subparagraph, an environment is unsafe if conditions in and around the home imminently threaten the safety of the home health care provider personnel or jeopardize the home health care provider's ability to provide care.
c. Participate in developing and following the plan of care.
d. Request information about anything that is not understood, and express concerns regarding services provided.
e. Inform the provider when unable to keep an appointment for a home care visit.
f. Inform the provider of the existence of, and any changes made to, advance directives.

The Mission Statement of Tufts Medicine Care at Home provides for the organization's ethical standards.

TMCAH Mission Statement: Empower people to live their best lives by reimagining healthcare, advancing knowledge and pioneering discovery.

Our commitment to excellence begins with our commitment to the highest ethical standards. No organization can achieve its mission without the commitment to each and every employee. It is through our employees that we succeed in reaching our goals. TMCAH provides general guidance and direction regarding ethical and legal business practices and behavior. It is the foundation of our Corporate Compliance Program. Every employee is expected to be familiar with, understand and follow the principles set forth in the Code.

Since the importance of ethical and legal behavior cannot be understated, TMCAH requires annual compliance training for all staff members

What do we mean by compliance?

Compliance means following a rule or request. In the healthcare setting, when we speak of compliance we mean following the rules, regulations, policies and laws created by the government, insurance companies and payers.

What do we mean by ethical behavior?

We simply mean doing the right thing. Ethical conduct goes beyond what is allowed by laws and regulations. It takes into account the Core Values the agency has adopted.

What is the philosophy regarding compliance and ethical behavior?

We will fully comply with all applicable federal and state laws, regulations, standards and other compliance requirements at all levels of government and with state practice acts. We will not pursue any business opportunity that requires unethical or illegal activity.

How do we inform its employees of our commitment to ethical and legal conduct?

The Code of Ethical Conduct describes our commitment to the highest ethical and legal standards and provides guidance to our staff regarding issues that may be faced. The Code of Ethical Conduct is available in the electronic policy management system, MCN/Ellucid.

What is the Corporate Compliance Program?

The Corporate Compliance Program is our practical means of monitoring activities to make sure they follow our Code of Ethical Conduct.

The Program includes the elements of an effective compliance program as defined by the U.S. Federal Sentencing Guidelines. The elements of our Compliance Program are:

- Written standards of conduct and policies and procedures.

- Designation of a Corporate Compliance Officer with direct access to the Board of Directors.
- Education and training for all new hires, with annual training for all staff.
- Processes to receive anonymous complaints and to allow complaints from staff without fear of retaliation, such as a hotline.
- Systems to respond to allegations of wrongdoing and to enforce disciplinary action against employees who have violated the Code of Ethical Conduct.
- Audits to identify potential problem areas.
- Effective means to take corrective action to remedy and weaknesses that may be found within our processes that could lead to violations of our Code of Ethical Conduct.

Why do we have a Corporate Compliance Program?

We have established our Corporate Compliance Program to assist our organization in promoting our commitment to the highest ethical and legal standards. The Corporate Compliance Program provides education related to our Code of Ethical Conduct and other topics related to compliance as needed, conducts investigations into alleged wrongdoing, and performs monitoring activities, such as audits, to assess areas of risk within the organization. It is through this pro-active approach that we are able to maintain the highest ethical standards.

How do I know if a decision I make meets the requirements of our Code of Ethical Conduct?

It is sometimes difficult to determine what the right decision is. There could be two possible actions to take, both with their benefits and drawbacks. If you take a moment to consider your options and ask yourself a few questions it may make your decision easier.

- Is there a law or regulation that governs this situation? (If there is, then the law should be followed at all times.)
- Is there an internal policy or procedures that govern the situation? Would my action be consistent with the Code of Ethical Conduct?
- How would my actions be seen by someone outside the organization?
- Would I feel comfortable explaining my actions to my friends and family?
- What would the most ethical person I know do?

What is the rationalization trap?

Sometimes it is difficult to choose the "right" decision. Doing the right thing is not always easy. We have faced situations where we are tempted to take the easy way out even if it is not the best way. Try to avoid these excuses for behavior that might not meet the requirements of our code.

- All the other hospitals are doing it this way
- No one will ever know
- I don't have time to do it the right way
- I saw my supervisor doing it the other day
- That policy isn't meant to apply to me
- After all I have given the organization, I deserve something in return

Who can help me when I am not sure if a situation meets the requirements of our Code of Ethical Conduct?

If you need help figuring out if there is a law, regulation, policy, procedure or standard that would affect a situation you are faced with, there are many resources available to you.

- Discuss the situation with your supervisor
- Contact the Compliance Officer
- Contact Human Resources
- Contact the Compliance Hotline 1-833-668-8387

Who is the Corporate Compliance Officer?

The Corporate Compliance Officer reports directly to the CEO/President and has access to the Board of Directors.

What is my responsibility when it comes to Compliance?

EVERY employee is required to follow the Code of Ethical Conduct. That means we all must obey all laws and regulations that govern our organization. We are also required to conduct our activities under the highest ethical standards. If you are aware of the violation of the Code of Ethical Conduct, it is your OBLIGATION to report it. Violations of our Code of Ethical Conduct are taken very seriously and may lead to disciplinary action up to and including termination.

What types of laws and regulations are we generally talking about when we talk about Corporate Compliance?

The number of laws and regulations that apply to healthcare organizations are too numerous to count. Many of the laws and regulations that are usually thought of in terms of compliance are put forth by the federal government. Healthcare fraud has become the focus of many national investigations over the past few years. Frequently, the investigations focus on the intricate regulations related to filing claims for payment of services. There are other laws and regulations that may impact the general healthcare staff on a day-to-day basis.

What is the False Claims Act?

The Federal Government enacted the False Claims Act (FCA) to prohibit the knowing submission of false or fraudulent claims to the federal government, including Medicare. Penalties for violating the FCA can be up to three times the amount of the payment received on the claim, plus additional amounts up to $11,000 per false claim. False claims can also result in exclusion from the Medicare and/or Medicaid programs.

How do we prevent violations of the False Claims Act?
We have established policies and procedures that reinforce our commitment to the highest ethical standards when it comes to submitting claims for payment to any payer. These policies and procedures are available via the Chief Financial Officer and in the electronic policy management system. Consistent with the FCA, we encourage employees, vendors and contractors to report to us suspected improper conduct without fear of retaliation.

What is healthcare fraud?

Generally, when you hear the term healthcare fraud it is referring to an intentional deception or misrepresentation that could knowingly result in benefit to the individual or the organization the individual represents. Some examples of fraud include:

- Billing for services or supplies that were not actually furnished
- Signing blank records
- Falsifying information on records
- Selling Medicare numbers
- Offering incentives to Medicare patients to receive services when the same incentives are not offered to non-Medicare patients
- Offering bribes, payment or incentives in exchange for healthcare referrals
- Misrepresenting services as covered and medically necessary when they are in fact not.
- Assigning diagnoses and procedures codes based upon coverage requirements and not based upon the actual services performed and the actual patient diagnosis

What is healthcare abuse?

Abuse is very similar to fraud. In healthcare, abuse consists of practices that lead to unnecessary costs to healthcare payers. Abuse is different from fraud in that with abuse there is no evidence that the act was committed intentionally and knowingly. Some examples of abuse are:

- Charging excessively for services and supplies
- Providing medically unnecessary services or services that do not meet professional standards
- Billing Medicare based upon a higher fee schedule than other payers
- Billing Medicare as primary when it is really secondary

What are some of the actions all healthcare workers should take to prevent fraud or abuse?

Much of the information that is entered into our computer systems ends up on the claims we submit for payment to the Medicare program. So, although you may not actually be the person who sends the claim out, the information you record may impact the information submitted for payment.

- Make sure that the charges entered are for services and supplies that were actually rendered to the patient you are charging. Make sure there is adequate documentation in the patient's medical record to support the charges
- Make sure that the information entered in the medical record and the computer is accurate and complete. All entries in the medical record must be signed
- If registering a patient, make sure you complete the Medicare Secondary Payer Questionnaire accurately and completely
- Do not charge patients differently based upon the type of insurance coverage they have
- Protect confidential healthcare information, including patient insurance numbers and Social Security numbers
- Do not enter into arrangement with physicians that will reward them financially for the number of referrals

- Do not disguise medically unnecessary services as medically necessary by inaccurate charging of the service provided, inaccurate documentation in the medical record, or inaccurate reporting of the patient diagnosis code
- Immediately report any instances of suspected fraud or abuse to your immediate supervisor, the Compliance Officer or the Compliance Hotline

What is a conflict of interest?

A conflict of interest exists when your judgment could be affected because you have a personal interest, other than your compensation from our agency, in the outcome of a decision over which you have influence or control. When we say personal interest, we mean that you or a member of your family could obtain financial gain as a result of the decision. Our decisions on vendors we do business with must not be influenced by gifts from the vendor.

Under no circumstances, should an employee accept cash gifts or gift certificates from any company doing business with or seeking to do business with the agency.

A potential conflict of interest exists when you or a member of your family works for or has a financial relationship with:

- A company that does business with
- A company that is seeking to do business with
- A company that competes with

What is my responsibility when it comes to reporting a potential conflict of interest?

If you think you have a conflict of interest based upon either your relationship with another company or the relationship of your family member with another company, complete the Conflict of Interest Disclosure Form.

- Employees and workforce members are required to complete the form annually with their annual performance review
- Conflict of Interest disclosures are discussed with the appropriate Executive Team Member

What is HIPAA?

The Health Insurance Portability and Accountability Act is a federal law that addresses many different aspects of health care. For all healthcare professionals, HIPAA sets out standards regarding protection of confidential patient data. Every day that you report to work you have access to confidential information regarding our patients. We are required to take every precaution to protect the confidentiality of patient data.

- Access patient information only to the extent that it is required in order to fulfill our job responsibilities
- Use only legitimate and authorized means to collect patient information and, whenever possible, obtain it directly from the patient
- Do not reveal any patient information unless it is as part of a legitimate business or patient care purpose
- Do not discuss health information about a patient with any person unless it is in connection with your work, permitted by law and authorized by the agency.
- Be aware of your surroundings and guard against visitors and third parties needlessly overhearing patient health information
- Protect the confidentiality of our patient's medical records by accessing them only for legitimate patient care or business purposes
- Remember that employees who are treated in our facilities are our patients. Their records and health information are just as confidential as non-employees. Access their records only for legitimate business purposes.

What do you mean when you refer to fair and equitable treatment of employees?

We recognize that the most important asset the organization has is its employees. We will provide all employees non-discriminatory terms, conditions and privileges of employment in accordance with the law, regardless of race, color, religion, national origin, sex, sexual orientation, age, disability or any other factor protected by applicable law.

What do I do if a government agency asks for information?

First of all, we will comply with all requests for information as required by law. All requests from any regulatory agency should be complied with accurately and timely and in accordance with the laws that govern such requests.

Requests from government agencies are sometimes received as part of your normal job functions. For example, if you work in Medical Records, you may get requests from the Medicare program for patient records before a claim is paid. These types of requests are referred to as routine requests. Routine requests should be handled as part of your normal job function, and, of course should be completed timely and accurately.

Non-routine requests might be notification of an investigation, a subpoena, an affidavit, a warrant or a request for a list of records. We will respond to these requests. As an employee when you receive such a request, your first obligation is to notify Medical Records. Employees must not obstruct any investigation into the business or legal practices. We will always

cooperate fully and completely with any valid and appropriate government inquiry concerning the business or legal practices.

How do I report a suspected violation of our Code of Ethical Behavior?

It is every employee's responsibility to be the eyes and ears of the Corporate Compliance Program. The organization's reputation depends upon you doing your part to report any questionable ethical actions or suspected violations of our Code of Ethical Behavior. Reporting suspected violations in good faith gives us the opportunity to investigate the matter and take corrective action, if warranted. Supervisors are encouraged to listen to their employees' concerns and to take the appropriate action. Your supervisor should be your first contact for reporting suspected violation. If you are not comfortable speaking with our supervisor or you don't feel that your supervisor took appropriate action, you may go to the next-level manager. If you are not comfortable discussing your concern with your next-level manager or you do not feel that the problem was dealt with appropriately, you may contact one of the following:

- Human Resources
- Corporate Compliance Officer
- Compliance Hotline

What is the Compliance Hotline?

The Compliance Hotline is another way to report suspected violations. It is available 24 hours a day, 7 days a week. You may report concerns to the Hotline using your name or anonymously. Anonymity is protected to the fullest extent possible.

Who should use the Compliance Hotline?

The Compliance Hotline is not meant to replace your normal reporting mechanisms and it is not intended for the reporting of Human Resource issues. It should be used only in those situations where you are not comfortable reporting a concern to your supervisor or next-higher level manager or if you feel that appropriate steps have not been taken to address your concern. The Compliance Hotline number is: 978-552-4300.
Thank You.

Reference: Baptist Hospital Corporate Compliance Manual
Revision: 6/3/2011

CONFIDENTIALITY

(Policy # 1521)

Confidentiality Statement

I, the undersigned, acknowledge and agree that:

1. One of the most serious responsibilities of all employees is the patient's right to privacy. I will not disclose information concerning a patient's treatment without authorization to other providers unless they require the information to carry out their duties.
2. In the course of performing assigned tasks or exercising clinical privileges I may have access to patient, organizational, and employee information. Such information is the property of Tufts Medicine Care at Home Parent, Inc. (TMCAH). This information may contain data that is confidential in nature. Maintaining confidentiality is essential in my access to and use of patient and employee information.
3. This access to information may also include access to various electronic information systems which include, but are not limited to, personal computers, organization, clinical, and financial electronic information systems, local and wide area networks as well as Internet access. Access to these various systems will be permitted according to approved policies and procedures.
4. If permitted access, I will use this access only to obtain information that I am authorized and required as part of my job duties or exercise of clinical privileges to access. I will not redisclose information except to those authorized.
5. Information Systems USER ID(s) and passwords issued to me are the equivalent of my signature and must remain confidential and known only to me. I understand that my password(s) is representation that I personally retrieved, transmitted, or verified information. I will not reveal my USER ID or password to anyone unauthorized.
6. All activity on information systems owned or maintained by TMCAH, including electronic mail and voice mail, will be monitored for compliance with security standards. TMCAH specifically reserves the right to review all entries made on any system(s) as well as attempts to access the system(s).
7. If I have reason to believe that the confidentiality of my password(s) has been compromised, I will contact my supervisor and/or the Information Systems manager immediately, so that my password(s) may be inactivated and a new password(s) assigned to me, and other appropriate corrective action taken.
8. In accepting employment and/or clinical privileges, I agree to adhere to all policies and procedures of TMCAH dealing with information, integrity, and security and understand that it is my responsibility to become familiar with the information and security policies and procedures. #1521 Page 3 of 3
9. In the event that remote access to the information systems owned and/or maintained by is TMCAH authorized for the performance of assigned tasks and/or clinical privileges granted by TMCAH: a) No organizational, patient, or employee information is to be stored or left out where it can be observed by unauthorized persons. b) All back-up or printed material such as drafts and copies of patient, organizational, and employee information will be treated with the same degree of security as the final document. c) All virus scanning software required by the Information Systems Department will be used as prescribed. d) No informational, patient, or employee information is to be placed on the Internet system without encryption and authentication processes approved for use by the Information Systems Department. e) I will be subject to all remote access physical security requirements prescribed by the Information

Systems Department. f) All organizational, patient, and employee information is the property of TMCAH and remains subject to all the policies that govern its use. The Information Systems Department will monitor all activity and specifically reserves the right to access, review and audit any system(s) and delete any organizational or patient information that is not appropriate to be on the system(s) used in the remote access of information. g) All organizational, patient, and employee information is the property of TMCAH. I further understand that actions which violate the intent of this statement shall be brought to the attention of management for appropriate action in accordance with the applicable disciplinary policies and may include a written warning, suspension, and termination of employment and/or privileges. (Refer to Policy #4000 - "Privacy Violation Disciplinary Process.")

INCIDENT\COMPLAINT REPORTING

Identification and reporting of complaints and incidents gives our organization an opportunity to improve customer satisfaction, increase knowledge of operations and to improve performance through changes to systems policies or procedures, and the dissemination of information.

Reportable incident may include:

- Any deviation from law, regulation, policy, or patient care plan
- Patient, Employee, Customer and Privacy complaints
- Patient or staff accidents
- Unusual or unintended response to treatment

Patient, employee and customer complaints represent important opportunities for the organization to increase its understanding of the quality of service delivery, customer perceptions, privacy practices, and knowledge of operations. All patients, customers (patients, physicians, discharge planners, community resources, etc.) and employees are encouraged to voice concerns and grievances. In addition, they are entitled and encouraged to make recommendations for changes in agency policies and services without coercion, discrimination, and reprisal.

If a complaint is not resolved and the patient, employee or customer is not satisfied, the Director of Quality Improvement and/or designee will inform the complainant of the option to contact the Joint Commissions' Office of Quality Monitoring at (800) 944-6610 or complaint@jointcommission.org.

Employee may also voice concerns to the Joint Commission Office of Quality Monitoring for unresolved concerns/complaints at 1-800-994-6610 or email complaint@ jointcommission.org

They may also contact:

- US Department of Health and Human Services 1-877-696-6775
- Massachusetts Home Health Hotline 1-800-462-5540
- New Hampshire Home Health Hotline 603-271-4592

Corporate Responsibilities/Employee Standards of Conduct

Introduction
Tufts Medicine Care at Home has developed a Standard of Conduct policy in order to maintain an environment consistent with our Vision, Mission and Core Values. The Standards clearly state TMCAH's expectations for the manner in which employees, volunteers and students should conduct themselves in order to promote and protect the integrity of Tufts Medicine Care at Home.

Policy Statement
The Standards of Conduct are considered to be an extension of the Tufts Medicine Care at Home's Core Values:

- To respect the dignity and earn the trust of every person we serve and work with
- To offer services which are accessible and highly responsive to people's needs and expectations
- To achieve effective outcomes with state-of-the-art services provided with compassion and with dedication to quality
- To nurture our staff's creativity and invest in their personal and professional development
- To promote a corporate environment that fosters open communication
- To adhere to the highest standards of ethical conduct
- To provide leadership in forging new partnerships to provide a comprehensive, seamless system of health care services
- To manage our financial and human resources responsibly to ensure that our services are cost effective and meet our highest standards for clinical outcomes and client satisfaction

Standards of Conduct
The following six standards constitute the basis for Tufts Medicine Care at Home's Standards of Conduct.

Quality of Care:
The major focus of Tufts Medicine Care at Home in meeting patients' needs is caring for the whole person in his/her intellectual, emotional, spiritual and physical dimensions.

- **We treat the person** rather than the disease
- **We encourage patients and families to participate** in decisions regarding their care by providing them with access to information about their care in a manner that they can understand
- **We respect** and maintain the dignity of every patient and strive to provide care in a manner sensitive to cultural differences and individual desires
- **We provide appropriate care** based on the patient's medical need, without regard to race, religion, national origin, age, gender, sexual orientation, disability, ability to pay, or any classification protected by law
- **We provide medically necessary care** that is properly documented in the patient's medial record
- **We maintain competencies** related to our job responsibilities and exercise appropriate judgment and objectivity when providing patient care

- **We mandate** that all employees maintain therapeutic relationships with our patients and adhere to the agency's professional boundaries.
- **We report situations** that compromise quality through the appropriate, established channels, and correct such situations as soon as possible
- **We are committed to maintain** accreditation by the Joint Commission and/or other such accrediting bodies

Laws and Regulations:

Tufts Medicine Care at Home will operate in accordance with all laws and regulations. These laws and regulations apply to areas such as patient referrals, employment, physician relationships, billing and payment practices, the environment, health and safety and dealing with payers and regulatory agencies.

- **We refrain** from any conduct that may violate federal or state laws, including those related to federal program fraud, abuse and false claims
- **We prohibit** any type of payment for or receipt of money or benefits for the purpose of inducing referrals in violation of the anti-kickback statute, Stark physician self-referral law, or other federal or state statues or regulations
- **We recruit**, hire, train, promote, assign, transfer, lay off, recall and terminate employees based on an evaluation of work performance, their demonstrated skills and competencies, experience and conduct without regard to race, religion, national origin, age, gender, sexual orientation, disability, or any classification protected by law
- **We provide** employees with the necessary training and education to perform their duties in accordance with applicable laws and regulations
- **We make certain** that cost reports or other information required to be provided to any federal, state or local government agency are filed accurately and in conformance with the applicable laws and regulations to the best of our knowledge and understanding
- **We do not engage** in activities that jeopardize the tax-exempt status of the organization, including certain lobbying and political activities, or activities that further the private or personal interests of an individual rather than our charitable purpose. We refrain from activities that violate the antitrust laws.
- **We follow** applicable environmental, health and safety requirements
- **We report** any practice or condition that we believe may violate laws, rules or regulations, safety standards, internal policies or Standards of Conduct to appropriate levels of management in a timely manner
- **We take steps** to ensure that our billing and coding are in compliance with our policies, and with federal and state laws and regulations, and are supported by appropriate documentation, including the medical record

Human Resources:

Tufts Medicine Care at Home strives to cultivate a work environment where employees are highly regarded; where they are treated honestly and respectfully; where their health and safety are protected; where they are motivated to reach their potential; where they are given an opportunity for personal and career learning and advancement; where they are provided with the tools necessary to do their job well; where there are safe and adequate procedures for resolving conflicts; and where employees are recognized and rewarded for their achievements without prejudice or discrimination.

- **We do not tolerate** any form of harassment or unlawful discrimination, as unprofessional conduct such as intimidating and disruptive behavior
    - Types of intimidating/disruptive behavior: verbal outbursts, physical threats; condescending language; body language (example – invading personal space, aggressive/rude gestures); disruptive behavior such as assault and other criminal behavior. Anyone who witnesses unprofessional behavior as described above should notify their supervisor/manager and/or Human Resources.
    - Tufts Medicine Care at Home Incident Report should be completed. As indicated, the procedure outlined in the agency's Performance Improvement will be followed.

- **We seek to be a responsible employer** by providing opportunities for professional satisfaction, pride of work and career growth
- **We keep employees informed** of activities and events that affect their specific work environment and performance of their job duties
- **We provide training** opportunities for employees to assist them in obtaining and maintaining certifications or licensures necessary for the performance of their job duties
- **We maintain** a drug free workplace and will not tolerate the use or possession of illegally acquired drugs and/or alcoholic substances while employees are on duty
- **We function** in an environmentally responsible manner, providing for the health and safety of our employees as well as our patients and the community
- **We provide** a grievance process to report and resolve conflicts without fear of retribution

Business and Ethical Practices:
Tufts Medicine Care at Home is committed to ethical business conduct and integrity. Employees must represent Tufts Medicine Care at Home accurately and honestly and must not do anything that purposefully defrauds anyone. Record keeping and billing for services provided to the patients must be accurate. Business is conducted in a manner that is consistent with the organizations' tax-exempt regulations. Tufts Medicine Care at Home employees who have knowledge/concern regarding business or ethical practices have an obligation to report the matter immediately to his/her supervisor or the agency's Corporate Compliance Officer.

- **We do not engage** in unethical or illegal activities in the pursuit of business opportunities
- **We act in good faith** and in the best interest of Tufts Medicine Care at Home at all times in the performance of our job duties
- **We appropriately document** the care that is provided
- **We prohibit** false documentation in the medical record (example – "false representation of any document, clinical or business")
- **We submit claims** only for medically necessary services provided
- **We do not steal** or misappropriate confidential or proprietary information belonging to another person or entity
- **We use resources** and assets only to further the Mission of Home Health Foundation
- **We do not offer**, give, solicit or receive any form of bribe, kickback or other inappropriate gift or payment

- **We make certain** that payments and other transactions are properly authorized by management and properly documented
- **We prepare** all financial documents, including financial statements, cost report, accounting records, expense reports, and time sheets accurately
- **We deal** with payers and regulatory agencies honestly and accurately

Confidentiality:
Tufts Medicine Care at Home employees, volunteers and students must keep organizational, patient and employee information in the strictest confidence. In keeping with the Health Insurance Portability and Accountability Act (HIPAA) Professional Ethical Guidelines all employees, volunteers, students must maintain the privacy and security of protected health information.

All employees, volunteers and students are expected to keep confidential information about other employees and the proprietary business practices of the organization.

All employees, volunteers and students requiring access to any Tufts Medicine Care at Home organizational patient or employee information must sign a confidentiality statement. Confidentiality policies and procedures are included as part of new employee orientation and for all employees annually. Breach of agency or patient confidentiality may result in disciplinary action up to and including dismissal;

- **We protect and respect** the confidentiality of our patients and their medical information
- **We only reveal** personal or confidential information concerning patients for legitimate patient care purposes, unless authorized by patient or otherwise permitted by law
- **We only share** confidential information regarding the operations of Tufts Medicine Care at Home with employees when they have a legitimate need to know the information in order to perform their job responsibilities
- **We will maintain** confidential information, including financial data in a confidential, secure manner according to relevant polices and applicable law

Conflict of Interest:
Tufts Medicine Care at Home's members of the Board of Trustees and Management shall exercise the utmost good faith in all transactions touching upon their duties of the Tufts Medicine Care at Home. An Annual Disclosure Form is completed by each member of the Board of Trustees and Management in order to identify potential areas of conflict;

- **We avoid** engaging in any activity, practice or act that appears to conflict with the interest of Tufts Medicine Care at Home
- **We do not solicit** or accept money, gifts, favors, services, entertainment or other things of value
- **We abstain** from any decision or discussion affecting Tufts Medicine Care at Home that might represent a conflict of interest when serving as a member of an outside organization or board
- **We do business** only with individuals and companies based on the best interest of Tufts Medicine Care at Home
- **We will avoid** any appearance of impropriety (wrong doing) when dealing with employees and referral source

- **We avoid** outside employment, consulting arrangements or personal investments if they interfere with our job responsibilities or unduly influence the decisions we are required to make on behalf of Tufts Medicine Care at Home.

Employee Reporting Responsibility:
Any Employee has the responsibility to report immediately to their Supervisor/Manager or the Corporate Compliance Officer if they have any knowledge or facts that they believe might be a suspected violation related to Prescription Drug Fraud, Waste and Abuse. Additionally, if there are any questions regarding the information provided, refer to you Supervisor/Manager or the Corporate Compliance Officer.

Whistleblower Protections
- Definition – An employee, former employee, or member of an organization who reports misconduct to people or entities that have the power to take corrective action.
- Individuals can report fraud anonymously.
- Employers cannot threaten or retaliate against whistleblowers

Exclusion Lists
Human Resources will check the Office of Inspector General and General Services Administration exclusion lists (regarding conviction of a criminal offense related to health care fraud) for all new employees and at least once a year thereafter to ensure that beneficiaries are not included on such lists.

Confidential Methods for Reporting Fraud, Waste and Abuse (FWA)
Office of the Inspector General
- By Phone: **1-800-HHS-TIPS (1-800-447-8477)**
- By TTY: **1-800-377-4950**
- By E-mail: HHSTips@oig.hhs.gov
- Centers for Medicare & Medicaid Services (CMS)
- By Phone: **1-800-MEDICARE (1-800-663-4227).**
- By TTY: **1-877-486-2048**

2024 Home Care National Patient Safety Goals
The purpose of the National Patient Safety Goals is to improve patient safety. The Goals focus on problems in health care safety and how to solve them.

- **Identify patients** correctly NPSG.01.01.01 Use at least two ways to identify patients. For example, use the patient's name and date of birth. This is done to make sure that each patient gets the correct medicine and treatment.
- **Improve staff communication** NPSG.02.03.01 Get important test results to the right staff person on time.
- **Use medicines safely** NPSG.03.04.01 NPSG.03.05.01 NPSG.03.06.01 Before a procedure, label medicines that are not labeled. For example, medicines in syringes, cups and basins. Do this in the area where medicines and supplies are set up. Take extra care with patients who take medicines to thin their blood. Record and pass along correct

information about a patient's medicines. Find out what medicines the patient is taking. Compare those medicines to new medicines given to the patient. Give the patient written information about the medicines they need to take. Tell the patient it is important to bring their up-to-date list of medicines every time they visit a doctor.

- **Use alarms safely** NPSG.06.01.01 Make improvements to ensure that alarms on medical equipment are heard and responded to on time.
- **Prevent infection** NPSG.07.01.01 Use the hand cleaning guidelines from the Centers for Disease Control and Prevention or the World Health Organization. Set goals for improving hand cleaning.
- **Identify patient safety risks** NPSG.15.01.01 Reduce the risk for suicide.
- **Improve health care equity** NPSG.16.01.01 01 Improving health care equity is a quality and patient safety priority. For example, health care disparities in the patient population are identified and a written plan describes ways to improve health care equity.
- **Prevent mistakes in surgery** UP.01.01.01 UP.01.02.01 UP.01.03. Make sure that the correct surgery is done on the correct patient and at the correct place on the patient's body. Mark the correct place on the patient's body where the surgery is to be done. Pause before the surgery to make sure that a mistake is not being made.

Internet Use

Tufts Medicine Care at Home owns the computer systems and all data contained on them, may record or monitor system use at any time, and may inspect or remove any file at any time. The agency reserves the right to inspect any and all files stored in private areas of the network in order to assure compliance with policy. No employee may use the agency's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code. The agency may authorize internet access to only those employees who demonstrate a legitimate business need. Any employee who obtains a password or ID for an Internet resource must keep that password confidential. Agency policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites. Computing resources are not to be used for personal commercial purposes or for personal financial or other gain.

The following uses of e-mail by individuals or organizations are considered inappropriate and unacceptable at Tufts Medicine Care at Home, Inc. In general, e-mail shall not be used for the initiation or re-transmission of:

- Chain mail that misuses or disrupts resources - E-mail sent repeatedly from user to user, with requests to send to others.
- Harassing or hate-mail - Any threatening or abusive e-mail sent to individuals or organizations that violate agency rules and regulations.
- Virus hoaxes.
- Spamming or e-mail bombing attacks - Intentional e-mail transmissions that disrupt normal e-mail service.

Ethics

Tufts Medicine Care at Home addresses ethical issues relating to patient care through the Vehicle of an Ethical Consultation. This consultation is available to assist all staff, patients and families, physicians, as well as those who are involved in decision making when appropriate.

The request for an Ethical consultation may be made by completing the Request for Ethics Consultation Referral Form on MCN/Ellucid. Evenings and weekends the Clinical Supervisor may be contacted. The clinical Supervisor will then contact the appropriate Vice President.

(Policy# 2072)
Patient/Family with Ethical concerns may contact the Ethics Committee Chairperson @ 978-552-4756.

The Ethics Committee Chairperson clarifies the concern with the person requesting the consult. If the request is determined to be outside the scope of the Ethics Committee, the requesting party will be informed and alternative avenues will be suggested.

Tufts Medicine Care at Home has established an Ethics Committee. The role of the Ethics Committee is to support patients, families and the agency's employees as they work together to find solutions/directions/guidance relative to ethical concerns.
Goals of the Ethics Committee:

- To serve as a forum for discussion and consultation of Ethical concerns.
- To provide Ethics education to Agency staff and the community.
- To assist in the formulation of Tufts Medicine Care at Home policies and procedures related to Ethical issues.

The Ethics Committee Chairperson will be responsible to follow-up with the person(s) who requested a case consultation, in order to discuss findings/recommendations relative to the review process. The Ethics Committee Consultations are advisory and makes recommendations only. The Ethics Committee has no enforcement power. However the case consultation does provide a rational and non-judgmental forum for discussion and for exploration and clarification of values, bioethical principles and alternatives.

The Ethics Committee is advisory committee reporting to the Tufts Medicine Care at Home's President/CEO. The President/CEO will inform the Board of Trustees concerning policies and issues addressed by the Ethics Committee as indicated.

Areas of Conflict that may give rise to Case Consultation include:

- Refusal of treatment
- Forgoing/withdrawing of life-sustaining treatment
- Do not resuscitate (DNR) issues
- Informed consent
- Confidentiality
- Family member/significant other disagreement regarding care of the patient
- poor communication between caregivers and patient and family

- Determining capacity to make decisions
- Drug diversion, misuse of drugs
- Lack of understanding options
- Advance Directives
- Palliative sedation

Advanced Directives for Health Care

TMCAH respects the patient's right to self-determination and to formulate advanced directives for health care. An **advanced directive** is a general term for several legal documents, which directs health care in the event the patient is unable to make health care decisions. These instructions may identify an individual to act as the patient's agent to carry out that individual's wish regarding health care decisions. All patients will be provided information concerning their **right to accept or refuse medical treatment and to formulate advanced directives.**

The existence and location of any advanced directive will be documented in the patient's medical record and a copy will be requested for the medical record. The name and telephone number of the designated agent will be recorded in the medical record. **A patient may revoke an advanced directive or the authority of an agent at any time,** either verbally or in writing, or by any action indicating revocation. The clinician should document revocation of an advanced directive in the medical record and notify the physician and the agent. **An employee of the agency may not act as a witness to the execution of a patient's advanced directive.**

Upon agency receipt of notice from the attending physician that appropriate medical criteria are present and that the patient has been determined to lack the capacity to make or communicate health care decisions, the agency will implement a valid patient advanced directive. **The agent has no authority until this determination is made.** The clinician will document in the medical record that an advanced directive is in effect.

If a patient who has been determined by the physician as incapable of making health care decisions **objects to a decision made by the agent, the patient's decision shall prevail unless the patient is determined to be incompetent by a court order.** The clinician should follow the patient's wishes and notify the physician and the Clinical Manager.

Detailed copies of the Massachusetts and New Hampshire laws regarding advanced directives are available in the Clinical Director's office. There are differences between the Massachusetts and New Hampshire regarding the formulation of advanced directives.

Massachusetts:

The Health Care Proxy is the legally recognized document, which allows competent adults (age 18 or older) to appoint an agent to make health care decisions should they be unable to make or communicate such decisions.

- A valid health care proxy must (1) be in writing, (2) be signed by the patient in front of two witnesses neither of whom are designated as agent, and (3) identify the patient and agent and indicate that the patient intends the agent to have authority to make healthcare decisions on the patient's behalf should he or she be unable to do so.

New Hampshire:
There are two advance directive documents legally recognized in New Hampshire- the Living Will or the Durable Power of Attorney for Health Care.

- The **Living Will** allows a person (age 18 or older) of sound mind to provide written instructions concerning the **withholding or withdrawing of life sustaining procedures in the event the person is in a terminal condition or permanently unconscious.** The Living Will comes into effect **only** if the patient is diagnosed and certified in writing to be in a terminal condition or permanently unconscious. Two physicians who have personally examined the patient, one of who is the attending physician must make the determination.

- The **Durable Power of Attorney for Health Care** authorizes an agent to make health care decisions should the patient be unable to make or communicate such decisions. The agent's authority becomes effective only after the attending physician certifies in writing in the medical record that the patient lacks the capacity to make health care decisions. Despite the Durable Power of Attorney for Health Care being in effect, treatment may not be given or withheld over the objections of the patient without court order.

SUSPECTED ELDER AND DISABLED ADULT ABUSE, NEGLECT, AND EXPLOITATION REPORTING
Definitions:

- **Disabled Adult**

A person between the ages of 18 to 59, inclusive, who is mentally or physically disabled and as a result of such mental or physical disability is wholly or partially dependent on others to meet his/her daily living needs.

- **Elder**

A person who is 60 years of age or older.

- **Abuse**

Any act or omission by a person that is not accidental and harms or threatens to harm an elder or a disabled adult physically, mentally, emotionally or sexually.

- **Neglect**

An act of omission which results or could result in the deprivation of essential services necessary to maintain the minimum mental, emotionally or physical health of an elder or disabled person. Self neglect is included.

- **Exploitation**

The illegal use of an elder's or disabled person's property or person for another person's profit or advantage, including but not limited to, situations where a person obtains money, property, or services from an elder or disabled person through the use of undue influence, harassment, duress, deception or fraud, for the purpose of taking unjust advantage of another for one's own benefit.

Procedure

- All agency staff is informed of the mandated Elder and Disabled Persons Abuse, Neglect and Exploitation Policy at the time of orientation to the agency.

- All paraprofessional staff is required to attend an inservice on recognizing and reporting elder and disabled person abuse, neglect and exploitation at least once per year.
- All agency staff will participate in an annual written safety test which includes a review of elder, disabled person abuse, neglect and exploitation.

Professional Reporting

When a professional provider knows or suspects that an elder or disabled person is being neglected, abused, or exploited they are mandated to verbally report findings to the proper state authorities as soon as possible. If the abuse poses an imminent threat to the patient's safety, the provider shall also immediately make an oral report to the police department of the town in which the alleged abuse occurred. A written report must be completed and sent to the proper state authorities within 48 hours.

Paraprofessional Reporting

When a paraprofessional knows or suspects that an elder or disabled person is being neglected, exploited or abused, the paraprofessional must immediately verbally report this to their supervisor; their supervisor will then assist them in contacting the proper state authorities as soon as possible. If the abuse poses an imminent threat to the patient's safety, the supervisor shall immediately make a verbal report to the police department of the town in which the alleged abuse occurred. The supervisor will assist the paraprofessional in filing the written report.

Patient Transfer

When the patient/family is involved in issues of abuse/neglect/exploitation/misappropriation and/or current Department of Public Health or other investigations, the clinical manager will report this information verbally and in writing to the administrator of the receiving facility/agency.

Massachusetts Patients

Elders

- A verbal report is made to Elder Services of Merrimack Valley, Inc. 24 hours a day via the Elder Abuse Hotline at: 1 (800) 922-2275; or ESMV at: 1 (800) 892-0890 during regular business hours (8:00 a.m. – 5:00 p.m., Monday – Friday).
- All verbal reports are followed up with a written report within 48 hours using the Elder Abuse Mandated Reporter Form – Attachment #1.
- The completed report is then mailed to Elder Services of Merrimack Valley, Inc., 360 Merrimack Street, Building #5, Lawrence, MA 01843.

Disabled

- A verbal report is made to the Disabled Persons Protection Commission (DPPC) 24 hours a day at 1-800-426-9009 V/TTY.
- All verbal reports are followed up with a written report within 48 hours using the Disabled Persons Protection Commission's Reporting Form – Attachment #2.
- When completed, written reports are mailed to Intake Unit, Disabled Persons Protection Commission, 300 Granite Street, Suite 404, Braintree, MA 02184 Fax: 617-727-6469.

New Hampshire Patients

Elders and Disabled

- All Verbal reports are made to the Bureau of Elderly and Adult Services, (800) 949-0470 or (603) 271-7014.

Non-Mandated Referral

- **Intimate Partner/Domestic Relations Abuse**
  Domestic violence is a health care issue. HHVNA is committed to developing a receptive climate for the early detection and effective intervention for patients experiencing intimate partner/domestic relation's abuse. Using a self-reporting screening tool, all patients will be screened for risk of abuse and neglect at start of care (SOC) and at resumption of care (ROC).
  Note: Able persons between the ages of 18-59 years are not subject to reporting when they are the victims of domestic violence. Patient permission must be obtained to refer for services.

Contact Numbers:

- **New Hampshire: National Domestic Violence Hotline 800-799-7233**
- **Massachusetts: Massachusetts Domestic Violence Hotline 800-992-2600**

CHILD ABUSE REPORTING, SUSPECTED

All professional licensed personnel are mandated by law to report child abuse/neglect/exploitation. The agency requires that all Home Care Aides report all suspected cases of child abuse/neglect/exploitation to their supervisor. The Manager is available for consultation/assistance with questionable abuse/neglect patients.

Definitions:

- **Child**
  A person under the age of 18.
- **Abuse**
  The non-accidental commission of any act by a "caretaker" which causes or creates a substantial risk of harm or threat of harm to a child's well-being.
  The commission of a sex offense against a child as defined in the criminal law.
- **Neglect**
  Failure by a "caretaker", either deliberately or through negligence, to take actions necessary to provide a child with minimally adequate food, clothing, shelter, medical care, supervision or other essential care.
  Physical dependence of the child upon an addictive drug at birth
- **Physical Injury**
  Death; or fracture of a bone, a subdural hematoma, burns, impairment of any organ, and any other such nontrivial injury; or soft tissue swelling or skin bruising, depending upon such factors as the child's age, circumstances under which the injury occurred and the number and location of bruises; or addiction to a drug or drugs at birth; or failure to thrive.
- **Emotional Injury**
  An impairment to or disorder of the intellectual or psychological capacity of a child as evidenced by observable and substantial reduction in the child's ability to function within a normal range of performance and behavior.
- **Exploitation**
  Taking unjust advantage of another for one's own benefit.

Procedure

- When abuse/neglect/exploitation is suspected, the clinician is to make an oral report by calling appropriate Department of Children and Families (DCF) office (MA) or Division of Children, Youth and Family Services (DCYF) office (NH). In the case of the Home Care Aide, they are to notify their supervisor who will assist with filing the complaint.
- Clinical staff will document the reporting of suspected abuse/neglect/exploitation and the findings of follow-up reports in a visit note or call log, as appropriate.

Massachusetts: The report must be called into the Department of Children and Families (DCF) Statewide Hotline.

- A written report (51A) MUST follow up the verbal report within 48 hours.
- DCF will send a follow-up notification to the reporter of disposition of the case after it has been screened. The follow-up report will be included in the medical record.

Hotline (Statewide)	24 Hour Hotline	(800) 792-5200

New Hampshire: The report must be called in to the Department of Child and Youth Services (DCYF) Central Intake number during business hours.

- A written report, "*Report of Suspected Abuse/Neglect/Exploitation: Elder, Disabled Adult, Child; New Hampshire Residents*" is required by the agency to follow up the verbal report.

Central Intake	Monday – Friday 8:00 a.m. – 4:30 p.m.	(603) 271-6556 (800) 894-5533 (in state calls only)
Easter Seals (covering for DCYS)	After Hours and Weekends	(800) 685-8772
	If there is an emergent danger to a child during off hours, the local police in the area in which the child resides need to be contacted.	

Other Resources

National Call Center for At-risk Youth		(800) 872-5437
Helping Parents	MA	(800) 882-1250
	NH (only)	(800) 750-4494
Parental Stress – Available 24 Hours/Day 7 Days/Week	MA	(800) 632-8188
	NH (only)	(800) 750-4494
Families First Health and Support Center	NH	(603) 422-8208 (press 2 for support)

HOME AND PERSONAL SAFETY AWARENESS

You need to know how to:

A - Be **AWARE** of potentially unsafe conditions and always practice your skill safely.
C - **CORRECT** the condition and notify the appropriate person.
T - **TAKE** precautions to avoid future problems

Typical hazards:

- Inadequate lighting in all areas– not enough or too much causing a glare
- Cluttered pathways, loose carpets, wet or highly waxed floors, and electrical/telephone cords
- Defective or poorly maintained equipment, stairs, handrails, furniture
- Incorrect use of tools and using furniture as a ladder
- Improper storage or labeling of medications, cleaning fluids/chemicals, oily rags, rubbish
- Leaving sharp objects unprotected and firearms unsecured, within easy reach
- Unrestrained household pets
- Family violence
- Be aware of the special safety hazards in each area and alert appropriate person(s) to potentially hazardous conditions.

Fire Safety

Fires are a leading cause of injury and death in health-care facilities
Fire Hazards in Homecare include:

- Smoking
- Oxygen, compressed gases (gas cylinders), mechanical respirators
- Flammable substances, such as paint thinner, solvents, alcohol and ether
- Faulty electrical equipment or wiring and improper use of extension cords
- Combustibles such as rubbish, latex gloves, rags, linens, drapes
- Grease from cooking
- Lint from laundry

Take part in all training programs and drills

- Know where the exits are located.
- Plan emergency routes for quick exit. Know the escape routes (posted throughout the office.)
- Identify locations of smoke detectors, and telephones.
- Know the telephone number of your location.
- Learn how to operate the fire extinguishers in the home or office, if they are available, and know where they are located.
- Don't open doors without first testing for heat radiating from them.
- Remember to touch walls and doors with the back of your hand, instead of your palm.
- Stay close to the floor to avoid inhaling too much smoke.
- AVOID SHOUTING - remain calm at all times.
- Walk - don't run - to the nearest emergency exit!
- Meet in the building parking lot away from emergency equipment.

- Re-enter only upon notification by emergency personnel.

Help Prevent Fires…

- Inspect your work area for hazards regularly
- Keep combustibles and flammables away from heat
- Keep combustibles that can spark out of areas where oxygen is used
- Dispose of rubbish properly
- Help enforce smoking rules.
- Display “Oxygen in Use” sign.

R.A.C.E.

In case of a fire, remember **"RACE"**

R: Remove any patients from immediate danger

A: Activate the **Alarm**.

Pull the fire pull station nearest the fire location.
Alert other employees in the immediate area.

C: Confine the fire.

Close all vents, windows, and doors.
Turn fans off.
Shut down electrical and gas equipment.

E: Evaluate/Evacuate/Extinguish

Evaluate the type and extent of the fire and the type of material burning. If necessary, **evacuate** to a safe area.
If the fire is small and isolated, attempt to **extinguish** the fire, using the appropriate extinguisher.

P.A.S.S.

Fire Extinguisher Instructions
Operation of Fire Extinguisher: "PASS"

P - Pull the safety pin
A - Aim the nozzle
S - Squeeze the handle
S - Sweep from side to side at base of fire

The different kinds of fire extinguishers

A - Ordinary combustibles
B - Flammable liquids & gases
C - Electrical equipment & appliances
D - Certain combustible metals, such as magnesium, titanium, potassium, sodium

The ABC fire extinguisher is the most common at the agency.

ELECTRICAL SAFETY

Electricity is everywhere in our homes and offices, and it only takes one old or poorly wired plug to prove just how powerful it is. Each year healthcare workers suffer pain, injuries, and death from shocks or fires caused by electricity.

Danger signs:

- Fraying power cords
- Overloaded sockets
- Hot plugs & sockets
- Water near electric
- Flickering lights

Manage electricity safely by taking these sensible precautions:

- When planning to use electrical equipment, assess for the appropriate number of outlets.
- Order the home equipment from a Durable Medical Equipment supply company that is Joint Commission certified.

Examine all cords and plugs routinely. Report to your supervisor and the medical supply company any plugs that are damaged or heat up when in use.

- Keep cords away from heat and water.
- Don't run cords under rugs or through doorways.
- Always use grounded, three-holed electrical outlets.
- Be sure you know what to do in the case of a power outage.

REMEMBER

If you have a patient on life support/ventilator

- Notify the local power company at time of admission
- Tell them whether you have an emergency generator or battery pack, and how long it will last
- If a power outage occurs, that home will be listed as *High Priority* with the Power Company

HAZARD COMMUNICATION PROGRAM
"Right to Know"

- OSHA requires the agency to have a written Hazardous Communication Policy to alert employees of hazardous chemicals in the workplace.
- Manufacturers provide the agency with Material Safety Data Sheets (MSDS) for each hazardous chemical supplied to us. The MSDS provides information for employees if they come in contact with a hazardous chemical.
- If you should have an exposure to a chemical, contact your manager/supervisor immediately. Your manager/supervisor will obtain the relevant information in order to treat the exposure if indicated.
- MSDS information is available through the Agency's Facilities and Supply
- Coordinator and/or on-line at the manufactures' web site.

ERGONOMICS AND BACK SAFETY

Slips, Trips & Falls

Slips, trips and falls are a common cause of injuries on the job. Many falls can be avoided by becoming aware of your environment and potential hazards.

Injuries are often caused by:

- Wet floors
- Uneven floor surfaces
- Loose carpets or scatter rugs
- Electrical cords
- Poor lighting
- Glare from too much light
- Cluttered or obstructed work area or passageways

Suggestions to prevent slips, trips and falls:

- Pay attention to your step
- Don't rush
- Wear sensible shoes with adequate traction and support
- Clean up fluid spilled on the floor

BACK SAFETY

Back injuries are common among home healthcare workers. They can be associated with improper methods of lifting, pulling, pushing, carrying, bending or twisting. Back injuries often result from years of abusing one's back causing weakness and stress to the soft tissue and bony structures. Back injuries can be associated with poor posture. Disc compressive forces are higher in sitting than standing erect. If a worker's seated posture is poor, the disc compressive forces can be greater than those measured during standing with a flexed trunk!! Overtime, high disc compression forces can cause disc damage.

Back Biomechanics:

- Body position affects the amount of load (force) on the spine.
- Holding/carrying an object close to the body lowers the load on the back.
- Leaning forward from your waist will increase the load on the low back.
- Body positions creating load on the lumbar spine listed chronologically from the **LEAST to the MOST amount of LOAD:**
- Supine lying
- Erect standing
- Supported, erect sitting
- Standing with trunk forward bent at waist
- Slouch sitting

To Avoid Back Injury:

- Use safe lifting techniques.
- Maintain proper sitting and standing posture.
- Stay physically fit.

Good Posture:

- Involves training your body to sit, stand and walk in positions creating the least strain on supporting muscles and ligaments.
- Helps decrease abnormal wear on joint surfaces.
- Prevents fatigue.
- Decreases stress on the ligaments holding the spine together.

Good Posture Requires:

- Good muscle flexibility.
- A balance in strength of your back and abdominal muscles.
- Awareness of your own posture. Looking in the mirror is helpful!!

ERGONOMIC SAFETY

Adapting equipment, procedures and work areas to fit the person helps prevent injuries and improve efficiency.

Common ergonomic injuries and their causes:

- **Strains and sprains:** most often to the back, fingers, ankles, and knees due to improper lifting or carrying objects.
- **Musculoskeletal Disorders:** most often to fingers, wrist, neck, and back from repetitive motion for long duration, poor posture, awkward posture.
- **Eye strain, headaches and fatigue:** due to poor lighting, neck posture or noise

Hints for Good Standing Posture:

- Avoid slouching and the military stiff posture.
- Think of elevating your chest bone toward the ceiling.
- Hold your shoulders slightly back and your head neutral.
- Keep your earlobes in line with the middle of your shoulders.

Hints for Good Driving Posture:

- Keep your back supported including the lumbar (low back) area. May need to use a lumbar roll.
- Sit with your seat slightly reclined back at 100-110 degrees (less lumbar disc compression force) rather than the 90-degree upright posture.
- Sitting with your seat slightly reclined back at 100-110 degrees with lumbar support helps decrease disc compressive forces.
- Position headrest to support back of your head.
- Position seat toward steering wheel so knees are bent and you are not stretching to reach gas/brake pedal.
- Knees should be at the same height or higher than your hips

Ergonomic Hints for Workstation:

- Sit with back and buttocks supported against chair. Use additional low back support if needed to maintain your normal lumbar curve.
- Move chair close to work so you don't slouch and reach excessively.
- Sit with seat slightly reclined back.

- Adjust chair height so elbows are bent at 90 degrees.
- Keep upper arm and elbow close to body.
- Keep feet flat on floor. Use footrest if necessary.
- Position monitor directly in front of you, with the top line of your characters at, or just below eye level.
- Keep the tools (mouse, phone) you use often within easy reach.
- Don't pound the keyboard.
- Sit at least an arm's length from monitor.
- When using keyboard, keep wrist flat (not bent up or down) and straight (not bent left or right).
- Reduce screen glare by using a glare filter or changing screen position or lighting.
- Get up, walk tall and stretch often.

Lifting Safely:

- Plan the move. Check for tripping hazards.
- Assess the object (size, weight, shape).
- Get help or use a mechanical lifting aide if the object is too heavy or an unusual shape.
- Stand close to the object.
- Use the ***Power Position*** by bending at the hips and knees, keep the lower back in an inward (arched) position and keep your buttocks out.
- Grip object firmly.
- Tighten abdominal muscles.
- Lift with your legs, not your back. Push up from your knees.
- Avoid fast, jerky movement.
- Keep object close to your center of gravity, decreasing stress to back and shoulder muscles.
- To change directions- turn your feet. Do not twist your trunk.

PERSONAL SAFETY

Even though you may be exposed to many hazards everyday, you can handle and avoid risks by being alert and aware of your surroundings, by following basic safety rules and by using your common sense.

Traveling safety tips:

- Follow safe driving rules and posted speed limits**.**
- **Use a seat belt at all times while driving as per agency.**
- Keep your vehicle in good repair. Make sure the spare tire is useable and keep the gas tank at least half full.
- Keep an auto survival kit in your vehicle.
- Keep doors locked and windows closed at least to earlobe level.
- Park within site of your destination and in a well-lighted area. Avoid parking near trucks, vans, shrubs and tall hedges.
- Look around and inside the vehicle before entering. Have keys ready to unlock the vehicle’s door.

- Drive to the nearest police, fire station or well –lighted gas station if you need assistance.
- Carry a spare vehicle key on your person.

Defensive driving:
Defensive driving saves money, time and *lives.* Be prepared to drive defensively.

- Do not mix driving with alcohol or other drugs.
- Be alert for impaired Drivers. Do not challenge aggressive drivers. Make every attempt to get out of their way.
- Allow a safe distance between vehicles. Follow the 2 - 3 seconds rule.
- Get your emotions in check before you drive.
- Anticipate driver mistakes at intersections and highway ramps.
- If you're tired, pull of the road for some exercise, fresh air or a cup of coffee.
- Be aware of medications that you are taking that could affect you driving ability.
- Uncorrected vision or hearing impairments, uncontrolled epilepsy, heart disease and diabetes can increase your chance of an accident. *Consult your physician.*

Bad weather driving conditions:
Rain, fog and snow make driving treacherous and make it difficult for drivers to see each other.

- Use your low beam headlights, drive slower and leave more distance between vehicles
- Puddles on the road can result in your vehicle hydroplaning (tire loose traction with the road)
- If your vehicle goes into a skid, take your foot off the accelerator. Do no hit the brakes. Turn the steering wheel in the direction you want the vehicle to go. Use moderate turns of the wheel until you come out of the skid.
- Slow down your vehicle as you approach shaded areas, bridges and overpasses in the winter. These sections freeze first and stay frozen longer after the sun hits them.

Safety Tips before the Visit:

- Know the patient's history of violence, substance abuse or mental illness.
- Notify the scheduling department of changes in your schedule.
- Avoid unsafe areas; "safety" of the neighborhood may change according to the time of day.

Make arrangements with the Manager/Supervisor for security services as needed.

- Know exactly where you are going.
- Get accurate directions
- Have a map of the area with you
- Have the family watch for your arrival if possible and watch to see if you get safely back in your vehicle.
- Have money to buy gas or make a telephone call.
- Keep purse and valuables out of sight.
- Dress appropriately and within guidelines of the agency. Always wear your identification badge.
- For routine visits, the patient or the family needs to restrain their pet.

Visiting safety tips:

- Before getting out of your vehicle, check the surrounding area – activities of people, condition of buildings, etc. If you feel uneasy, do not get out of your vehicle. Contact the office from a safe place or from your cell phone.
- Always project confidence with your body language. Dress simply and limit jewelry. Keep one arm free.
- Avoid persons who are loitering by walking to another area.
- Be alert to building surroundings, elevators and body language of persons you encounter. Strong eye contact may discourage trouble.
- Always knock on the door before entering a person's residence. Call out and identify yourself.
- If a situation appears unsafe for any reason, leave the area and contact the office, police or both.
- Do not attempt to break up a domestic argument, which can become explosive.
- Be prepared to defend yourself if you come across an aggressive or assault situation. Be trained to recognize and divert increasing hostile behavior.
- If you are threatened, you can scream; kick their shin, instep or groin; act insane; yell "FIRE" or "NO" loudly; or blow a whistle.

BASIC RULES FOR VIOLENCE PREVENTION:

- Treat people always with respect.
- Check ahead of time if client has history of violent behavior.
- Safely store all objects that could be used as a weapon away from violent persons.
- Vary your daily routine if possible.
- All threats and potential sources of trouble should be reported. Take all threats seriously.
- Trust your feelings.
- Call for support at first sign of trouble, or if you have any doubts.
- Try to spot trouble before it starts.
- Always follow proper security procedures in all circumstances.

Stay calm, alert and in control of yourself.
Think before you act.
Work as a team.

EMERGENCY MANAGEMENT PLAN

PURPOSE: To provide continuous care for TMCAH patients and appropriate support in the event of an internal or external emergency without endangering staff safety.

- To minimize and control loss, damages and liabilities
- To facilitate recovery to normal operations with minimal delay
- To support local hospitals and facilities in caring for victims of terrorism, bioterrorism and disasters.
- To coordinate services and resources with the Massachusetts Emergency Management Agency, New Hampshire Office of Emergency Management and the state Departments of Public Health in declared emergencies.

DEFINITION: "Emergency Management" is defined as a need for immediate action which includes implementation of procedures to assure that health care and safety needs of the patients and staff are prioritized and met to the extent possible during emergent events. Emergency management also includes the actions to be taken to continue priority functions, protect assets and plan for recovery.
Policy: Tufts Medicine Care at Home employees will follow the emergency management plan when providing care and support to patients during an internal or external emergency based on patients' needs.

Tuft Medicine Care at Home has identified the following priorities in an emergency situation:

- Provision of care to priority patients and maintaining staff safety.
- Plan for discharge of those patients who can be safely managed without TMCAH services.
- Plan for the ability to admit and service those patients that are discharged from area healthcare facilities.
- Provide assist with public health activities as staffing resources allows.

OVERVIEW
The emergency management plan is directed toward the following events/conditions as identified in the Hazard Vulnerability Analysis. (See "Attachment B")

- **Internal Events**
  - Telecommunication Interruption/Failure
  - IS Failure
  - Utility Interruption/Failure
  - Fire
  - Smoke/Water Damage
  - Epidemic/Major Illness of staff
  - Public Relations Issues
- **External Events:**
  - Severe weather hazards
  - Widespread utility failure
  - Community Emergencies: widespread fire, transportation accident
  - Hazard Materials Spill, Radiological Disaster, Chemical Accident
  - Terrorism/Bioterrorism
  - High rate of discharge from acute care facilities
  - Pandemic illness

These internal and external events have the potential to initiate the emergency management plan. The plan is not specific event driven, but plans the functions, operations and recovery based on the impact of the event on the infrastructure of TMCAH. The infrastructure scenarios include the following:

- Technology hardware problem
- Power outage ≤ 4 Hours
- Power outage ≥ 4 Hours
- Facility Unavailable ≤24 Hours but power is still on
- Facility Unavailable ≥ 24 Hours but power is still on

- Facility Unavailable with no power
- Facility Available, power is on but personnel are not permitted to travel

LIFE SAFETY
Life Safety functions and activities are three-fold in purpose:
- Patient Care Priorities
- Planning Activities
- Employee Safety

Patient Care Priorities
All patients will be assessed on admission and on an ongoing basis to determine the need for priority visits in the case of emergency. Prioritization is documented in the medical record. A current patient census with priority designation is accessible to managers and emergency management team.

Clinical Prioritization:
Priority #1 - Essential Care Required
- Patient is diabetic, unable to self inject
- Patient requires infusion therapy which requires supervision/assessment
- Patient requires treatment(s) which must be continuous to be effective
- Patient without caregiver or with elderly, frail caregiver who could not care for the patient in a disaster/emergency.
- Patient dependent on electrical equipment or oxygen for survival
- Patient lives in an unsafe home that would not survive a weather event (i.e. trailer, summer cottage)
- Other: For example, fragile family situation

Priority #2 - Non-Life Threatening
- Patient requires intermittent skilled care and assessment, but has available resources and support.
- Patient lives alone, significant interruption of services would impact patient's ability to meet basic needs and safety.

Priority patient information is entered in the electronic medical record system, and a master list of priority patients will be maintained and for planning purposes.

Planning Activities
As most emergency management situations involve weather hazards; there is an opportunity for planning based on weather forecasting information. The Clinical Director, clinical managers, supervisors are responsible for performing the planning activities. **Planning** for agency services that may be limited or interrupted due to weather includes the following:
- Preparing priority patient visit list
- Scheduling available staff
- Establishing back up communication strategies
- Identifying management team for emergency

- Education/informing patients of plans for weather emergency
- Communication of emergency plans to staff

OCCURRENCE PROTOCOLS:
The following information is intended to provide a brief description of actions to take for a specific occurrence.

- **Weather Related/Natural Disasters (Snowstorm, Hurricane, Tornado, Flood, etc.)**
    - Weather related events can be planned based on weather forecasting. Visiting and office staff is alerted to the potential initiation of the emergency plan. Staff available for visits will be identified, patients prioritized and assigned. TMCAH staff members will make every reasonable effort to reach the assigned patient. Patients may be advised that regular schedules for health care staff may temporarily be revised due to the weather event. TMCAH staff will contact the office if unable to reach patient's homes. Every reasonable attempt will be made to notify patient's family or contact person regarding the inability to service the patient. If health care needs cannot be provided in the home, the patient may be transported to the nearest hospital, health care facility or emergency shelter.

- **Fire & Explosion in a Patient's Residence**
    - TMCAH staff will be familiar with fire escape route(s) appropriate to patient's abilities. At the first sign of fire/smoke/, proceed immediately to the safest exit with the patient. Once away from danger, call the Fire Department. **IF THE PATIENT CANNOT BE MOVED, CLOSE THE DOOR OF THE PATIENT'S ROOM AND GO TO THE NEAREST TELEPHONE TO CALL THE FIRE DEPARTMENT.**

Fire in TMCAH Office Sites
The individual discovering the fire/smoke will call sound the alarm. TMCAH staff will follow the direction of the CEO or designate to evacuate the building.

Radiological Disaster or Chemical Accident
Each office will follow local nuclear disaster plan procedure. TMCAH will maintain a list of patients living within ten (10) miles of a nuclear plant along with the designated emergency shelter location, evacuation plan and contact numbers. In the event of a radiological/chemical accident, TMCAH will follow local, state or Federal Emergency Management instructions. As described previously, the Incident Commander will be responsible for maintaining communication with Emergency Management Agency officials. This communication may include sharing information about the priority status of patients in the affected area so that rescue/evacuation plans may be planned for this population.

Power/Utility Outages
Based on the extent of the outage, organization services will continue as scheduled. Field staff will attempt to contact the agency via available communication devices to report patient's status and support systems available. Staff members will assure to the extent possible that patient's immediate personal and health care needs are met. If repair time of the utility is unknown or anticipated to be lengthy, staff will assist family and caregivers to set up alternate means of

contacting and/or servicing the patient. The emergency plan may be implemented based on the extent and projected loss of power/utility.

Epidemic or Major Illness of Staff
Based on the extent of the illness, the emergency management plan may be initiated. At minimum, the VP of Clinical Services will assess staff availability and patient priorities. TMCAH will make efforts to utilize temporary help from supervisory personnel, on–call or per-visit staff. Staff may be requested to increase their visits, if possible.

High Rate of Discharge from Acute Care Facilities
In the event that an unusually high rate of discharge from an acute care facility takes place (labor action, or emergent event) the VP of External Relations and VP Clinical Services will make every effort to provide and coordinate services to all patients, and determine the number of referrals that the organization can accept with current staffing levels. The clinical managers in conjunction with the nursing staff will review patient caseloads, assess needs and establish priorities for visits.

Public Relations Issue
An event, in or out of the work environment, which may have a grave or significant effect on the Tufts Medicine Care at Home reputation, membership or portion thereof. Examples of such a crisis situation: death (sudden or violent or after a long illness) of an employee, significant illness or bodily injury to an employee.

Terrorist Event
In the event of a terrorist event, TMCAH will initiate the Emergency Management Plan and the Incident Command System. The Incident Commander will coordinate resources and services in conjunction with local, state and federal authorities in conjunction with the Massachusetts Terrorism Incident Response Plan and New Hampshire Office of Emergency Management.

RECOVERY AND RESTORATION
The President/CEO or designee will have the authority to declare the emergency over. With this declaration, the EMT will establish priorities for resuming operations. This assessment includes but is not limited to:

- Determining site of operation (may move to temporary/alternate location)
- Emergency financial operations
- Repair and restoration of facilities and equipment
- Utility repairs and restoration
- Property safety
- Inventory of damage

The President/CEO or designee will:

- Notify insurance carriers
- Notify regulatory agencies of current agency status

Other resources may be utilized for assistance in recovery and restoration. The resources include trade and advocacy associations/organizations.

Visiting Staff
During recovery, staff will continue with visit schedule(s) according to prioritization with direction from clinical managers. If communication remains disrupted/impaired, visiting staff will utilize the following:

- Contact answering service for updates
- cell phones
- Tiger Text
- E-mail
- Access voice mail for updates
- Listen to radio stations for instructions:
    - WCCM 1490 AM (English)
    - WNNW 800 and/or WHAV 1110AM (Spanish)

INFECTION CONTROL

Infection control is taking steps to prevent illness to yourself and others. Preventing infections can help a person to recover more quickly or stay healthy as possible.

The method by which infection moves is referred to as the route of transmission. A germ, such as a virus, bacteria, fungus or parasite, spreads infections, which multiply in a person, animal, plant, food, soil or water. A person who does not have resistance to the germ is a susceptible host. Different germs enter through different routes. Germs may enter through direct contact, such as when people touch each other, kiss, have sex, etc. They may also enter a person through indirect contact such as a food, water, feces, bandages or other substances, contaminated by a germ. Some enter through droplets produces by a sneeze or cough and other germs are carried in the air.

Standard Precautions is based on the principle that **all** blood and body fluids are potentially infectious. Standard precaution includes the use of Personal Protective Equipment (PPE) by staff whenever there is a chance of exposure to **any bodily fluid with the exception of sweat**. PPE includes: gloves, aprons, gowns, masks, face shields or goggles to protect patients and staff from infection. TMCAH provides appropriate personal protective equipment to all staff that is at risk to exposure.

In addition to **Standard Precautions you may also need to use Transmission Based Precautions** when infections are spread by different means.

Transmission Based Precautions include:

- **Droplet Precautions:** For patients known or suspected to have serious illnesses transmitted by large particle droplets (5 mm or larger). These illnesses include influenza, meningitis, pneumonia, mumps, rubella, epiglottitis, and sepsis. Large droplets do not remain suspended in the air and do not travel more than 3 feet from an individual. Droplets may be spread when a patient is coughing, sneezing, or during procedures such as suctioning. When caring for patient on droplet precautions home care staff and other individuals should wear a surgical mask, face shield, gown and gloves.

- **Airborne Precautions:** For patients known or suspected to have serious illnesses transmitted by Airborne Microorganisms: such as, Measles, Varicella, Tuberculosis. If a patient is known or suspected to have active pulmonary or laryngeal Tuberculosis staff entering the home must be fit tested by the agency for a National Institute for Occupational Safety and Health certified N95 Respiratory Device.
- **Contact Precautions:** For patients' known or suspected to have serious illnesses easily transmitted by direct patient contact or by contact with items in the patient's environment. These include gastrointestinal, respiratory, skin, or wound infections colonized or infected with Mult resistant bacteria such as Methicillin Resistant Staphylococcus Aureus (MRSA) and Vancomycin Resistant Enterococcus (VRE). Other examples are: Clostridium difficile infection (C-Diff), Escherichia coli 0157:h7, Respiratory Syncytial Virus and scabies. In addition to wearing gloves as outlined in Standard Precautions, staff should wear a clean non sterile gown when providing care for a patient requiring contact precautions when there is substantial contact with patient, environmental surfaces, or items in the patient's room or if the patient is incontinent or has diarrhea, an ileostomy, colostomy or uncontained wound drainage.

When caring for a patient that requires Transmission Based Precautions contact your manager/supervisor, the infection control nurse or refer to Isolation Precautions for more information.

HAND HYGIENE

Good hand hygiene is the single most important action you can take to reduce transmission of microorganisms to patients and staff. Adherence to hand hygiene (i.e. hand washing or use of alcohol-based hand rubs) has been shown to reduce transmission of antimicrobial resistant organisms (e.g. Methicillin resistant staphylococcus aureus or Vancomycin resistant enterococci) and reduce overall infection rates.

Hand Hygiene will be performed:

- When visible dirt, blood or body fluids are on the hands of the health care worker (HCW)
- When there is no visible dirt, blood, or body fluids in the following clinical situations:
    - Before and after direct patient contact;
    - After removing gloves;
    - Before handling invasive device for insertions;
    - After contact with blood, body fluids, mucous membranes, non-intact skin, and wound dressings
    - Before entering clinical bag
    - After using restroom
    - Before handling medication or food
- Staff providing direct care to patients:
    - May not wear artificial fingernails or extenders,
    - Will maintain natural nail tips no longer than 1/4 inches,
    - May not wear nail jewelry, and
    - Will maintain nail polish so that it is not cracked, chipped or scratched.

Procedure

Hand washing:
Hand washing is required when hands are visibly soiled or contaminated with proteinaceous substances such as urine, blood or other body fluids.

- Wet hands under warm running water avoiding use of hot water. Repeated exposure to hot water may increase the risk of dermatitis.
- Keep hands below elbows and apply liquid non-antimicrobial or antimicrobial soap.
- Rub the hands together for a minimum of 15 seconds. Be sure to scrub between fingers, around the fingertips and nails and around and under any rings. Rinse under running water.
- Dry hands with a disposable paper towel. Do not use any cloth product in the patient's home to dry hands.
- Turn off water faucet using paper towel to avoid decontamination.
- Discard the used towel in a trash container.

Hand Hygiene also includes cleaning hands with alcohol-based hand wash or rub when hands are not visibly soiled. Alcohol-based hand rubs significantly reduce the number of micro-organisms on skin, are fast-acting and cause less skin irritation. The agency will provide alcohol rubs that have a concentration of at least 60% ethanol or isopropanol alcohol.

- **Hand hygiene** will be performed:
- Before entering or re-entering the clinical bag (after patient contact)
- Before and after patient contact
- Between tasks and procedures on the same patient
- After handling contaminated equipment
- Before glove donning and after each glove removal
- After contact with patient bodily fluids or excretions, mucous membranes, non-intact skin or wound dressings - unless hands become visibly dirty

Hand hygiene will be performed using the following procedure:

- Apply manufacturer's recommended amount to one palm.
- Vigorously rub hands together, spreading the solution thoroughly over both, particularly around nail beds and under jewelry.
- Continue until hands are completely dry. Un-evaporated alcohol can be ignited by static electricity. Do not run hands under water at this point.
- Store products away from heat or flame.
- Some gels can leave a residue after 5-10 applications. Washing with soap and water at that point solves the problem.
- Use of sterile or clean gloves does not eliminate the need for rigorous hand hygiene. Hand antisepsis is required before and after glove use. Likewise the use of hand hygiene/antisepsis does not eliminate the need for using gloves.
- Alcohol-based antiseptic hand rubs significantly reduce the number of micro-organisms on the skin and causes few incidents of skin irritations.
- Use a hand lotion or cream to help minimize the potential irritation associated with hand hygiene agents (the use of petroleum-based hand lotions or creams may adversely affect the integrity of latex gloves.)

Respiratory Hygiene/ Cough Etiquette

The following measures to contain respiratory secretions are recommended for all individuals with signs and symptoms of a respiratory infection.

- Cover nose/mouth with your elbow when coughing or sneezing;
- Use tissues to contain respiratory secretions and dispose of them in the nearest receptacle after use;
- Perform hand hygiene (e.g. hand washing with an non-antimicrobial soap and water, or use alcohol-based hand rub, or antiseptic hand wash) after having contact with respiratory secretion and contaminated objects/material;
- Provide tissues and no-touch receptacles for tissue disposal;
- Provide conveniently located dispensers of alcohol –based hand rub; where sinks are ensure that supplies for hand washing are available.

BLOODBORNE PATHOGENS

Tufts Medicine Care at Home (TMCAH) has developed a Bloodborne Pathogen Exposure Control Plan (ECP) to protect you as an employee who may have had an occupational exposure to blood and body fluids as a result of performing your job duties and to provide appropriate treatment and counseling.

If an employee is determined to be at risk for occupational exposure to blood or other potentially infectious materials (OPIM) the employee must comply with the procedures and work practices outlined in the ECP. Copies of the ECP are located in the Infection Control Manual, which is part of the Emergency Plan located in the electronic policy management system, MCN/Ellucid.

Bloodborne Pathogen is the term that includes any pathogenic microorganism that is present in human blood or other potentially infectious material (OPIM) and can infect and cause disease in persons who are exposed to blood containing the pathogen.
OSHA identified the following Bloodborne Pathogens:

- HIV Human Immunodeficiency Virus
- HBV Hepatitis B Virus
- HCV Hepatitis C Virus
- Malaria
- Syphilis

AIDS is a disease caused by the **Human Immunodeficiency Virus (HIV).** The body substances containing the greatest amount of the virus are blood, spinal fluid, peritoneal fluid, vaginal secretions, pericardial fluid, pleural fluid, synovial fluid, amniotic fluid, semen and breast milk. The virus is transmitted through sexual contact, percutaneous exposure, and perinatal exposure, by absorption through mucous membranes and through non-intact skin. It is not spread through ordinary business, social or household contact.

The **Hepatitis B Virus (HBV)** is classified as a DNA virus. The body substances containing the Hepatitis B virus are blood, urine, vaginal secretions, saliva, semen, and most body fluids. The virus is transmitted through sexual contact, percutaneous exposure, perinatal exposure, by absorption through mucous membranes and non-intact skin. It is not spread through ordinary business, social or household contact.

The **Hepatitis C Virus (HCV)** is classified as an RNA virus of the liver. The virus is transmitted through blood and blood products. Currently there is no vaccine effective against HCV. IV drug use is the most common mode of transmission, accounting for 43% of infections. Other common causes include transfusions, heterosexual exposure, occupational risk, regular hemodialysis or other high-risk behaviors such as obtaining a tattoo or acupuncture treatment. It is not spread through ordinary business, social, of household contact.

Tuberculosis

Mycobacterium Tuberculosis is carried in airborne particles and generated when individuals with pulmonary or laryngeal TB sneeze, cough, speak or sing. The normal air current keeps them airborne and can spread the particles throughout a room or building. Infection occurs when a susceptible person inhales these particles containing Mycobacterium Tuberculosis. The probability that a person will become infected with Mycobacterium Tuberculosis TB depends upon the concentration of infectious particles in the air and the duration of the exposure. Groups known to have a higher prevalence of Tuberculosis infection include:

- Medically under served individuals
- Homeless Individuals
- Prison inmates
- Intravenous Drug Users
- Foreign born clients from area of the world with high prevalence (i.e. Asia, Africa, the Caribbean and Latin America)
- Contacts with individuals with Tuberculosis
- Immunocompromised patients (i.e. HIV, immunosuppression therapy, and cancers)

A diagnosis of Mycobacterium Tuberculosis will be considered in any patient with:

- persistent cough (greater than 2-3 weeks in duration)
- bloody sputum
- night sweats
- weight loss
- anorexia
- fever

Biohazard Material

- All specimens are considered potentially hazardous. All specimens are placed in a clear-labeled zip lock plastic bag prior to transport. The sealed plastic bag is placed in a leak-proof container that is labeled as biohazardous for transport.
- All home-generated infectious waste is placed in a closeable, leak-proof bag and double bagged prior to disposal to prevent leakage during handling, storage and transport.
- Other regulated waste will be disposed of according to (Policy #1931)

Cleaning and Disinfecting

- All equipment and working surfaces are properly cleaned and disinfected after contact with blood or other potentially infectious materials.
- When environmental surfaces in the home care setting are visibly contaminated with blood or body fluids, clean with an agency-approved disinfectant using Standard Precautions before leaving the client's home.

Patient Laundry

- All laundry is treated as contaminated, handled as little as possible and with a minimum of agitation.
- Appropriate PPE will be used when handling dirty laundry.

Occupational Exposures

An exposure that might place a healthcare worker at risk for HBV, HCV, or HIV infection is defined as an injury (e.g., a needle stick or cut with a sharp object) or contact of mucous membrane (e.g., eyes, nose, mouth) or nonintact skin (e.g., exposed skin that is chapped, abraded, or afflicted with dermatitis) with blood, tissue, or other body fluids that are potentially infectious.

Following initial first aid of cleansing or irrigation of the injured site, the employee will immediately inform their manager/supervisor of the incident and will be directed to go to the Occupational Health Center or Emergency Department closest to where the exposure occurred and. Tufts Medicine Care at Home provides occupational health services through the following health care providers to all employees for agency related illnesses or injuries:

- Lowell General Emergency Department
- Tufts Medical Center Emergency Department
- Melrose Wakefield Hospital Emergency Department
- Circle Health Urgent Care –Locations in Dracut, Westford, or North Billerica
- Convenient MD- any location
    - Make sure to let the receptionist know, the account associated with our protocol is under Tufts Medicine.

An unusual occurrence report form must be completed along with a blood borne pathogen exposure report and a worker's compensation report with your manager/supervisor.

STAFF WITH COMMUNICABLE DISEASE

Any staff having signs/symptoms of a communicable disease (anything that spreads is communicable) or diagnosed with a communicable disease must notify their supervisor/manager who will immediately contact the infection control nurse. Staff must present to the manager/supervisor written documentation from the doctor or Occupational Health Services of clearance to return to work.

Sharp Safety

Only agency approved safety needle and lancets should be used during patient care. **Patient and family education** regarding correct needle and lancet disposal is also the key in preventing unwanted exposure. Sharps are placed in a leak proof, puncture resistant and rigid container. If household container used, label the container **"NOT FOR RECYCLING".** Broken glassware, which may be contaminated, will be picked up using mechanical means, such as a brush and dustpan or tongs, and disposed of in a puncture-resistant container.

PACE (A Program of All-Inclusive Care for the Elderly)
All you need in one place… Where You Are At the Center

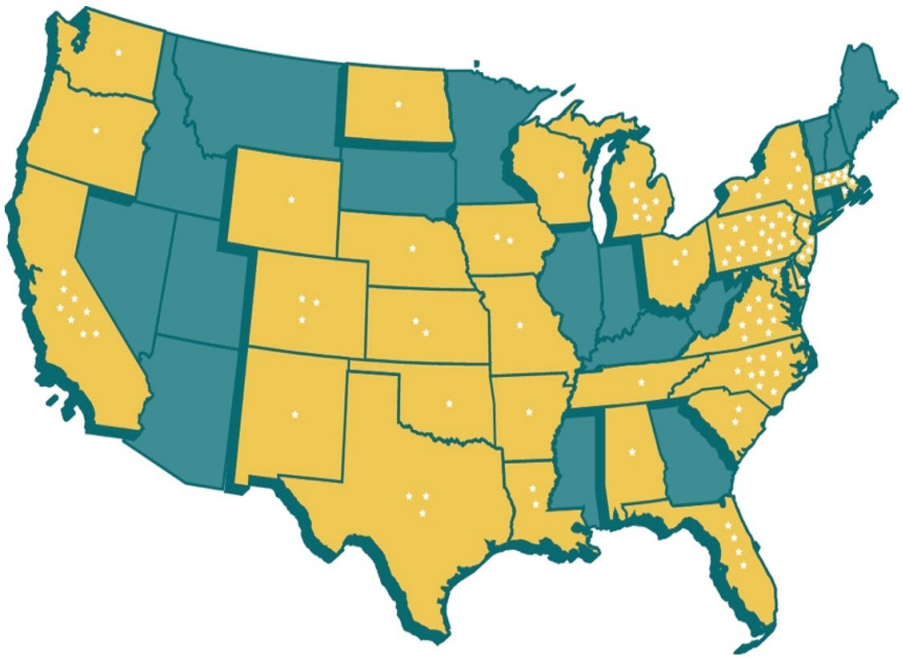
The Program of All-inclusive Care for the Elderly (PACE) is administered by MassHealth and Medicare to provide a wide range of medical, social, recreational, and wellness services to eligible participants. The goal of PACE is to allow participants to live safely in their homes instead of in nursing homes.

You do not need to be on MassHealth to enroll in PACE. However, if you meet the income and asset guidelines, you may be eligible for MassHealth and MassHealth may pay your PACE premium. Individuals may also self pay.

To enroll in PACE you must:

- Be 55 or older
- Live in the service area of a PACE organization;
- Be certified by the state as eligible for nursing home care;
- Live in the community (not a nursing home);
- Be able to live safely in the community;
- Agree to receive health services exclusively through the PACE organization; and
- Meet the Social Security Act Title XVI disability standards, if 55 through 64 years of age.

There are 124 PACE programs operating in 31 states (yellow states):



PACE services include but are not limited to the following:

- Physical Therapy
- Primary Care
- Adult Day Care
- Hospital Care
- Meals
- Recreational Therapy
- Social Services
- Prescription & OTC Drugs
- Nutritional Counseling
- Social Work Counseling
- Occupational Therapy
- Medical Specialty Services
- Dentistry
- Transportation
- Home Care
- Nursing Home Care
- Lab/X-ray Services
- Emergency Services

PACE organizations, support your family members & other caregivers with training, support groups, and respite care

All potential enrollees must be evaluated by a nurse to assess nursing home eligibility requirements.

The PACE Benefit

Once enrolled, a participant's care is coordinated by the Interdisciplinary Team (IDT). With PACE, the focus is on preventive services, functional maintenance as well as on-going medical care. Periodic assessment by the IDT assures that the needs of the participant are being met as he or she ages in place.

The PACE Interdisciplinary Team (IDT):

- Primary Care Provider
- Registered Nurse
- Social Worker
- Activity Coordinator
- Personal Care Attendant
- Registered Dietician
- Home Care Coordinator
- Physical Therapist
- Occupational Therapist
- Transportation Coordinator
- PACE Center Manager

Participant Rights:

- The right to be treated with respect.
- The right to protection against discrimination.
- The right to information and assistance.
- The right to a choice of providers.
- The right to access emergency services.
- The right to participate in treatment decisions.
- The right to have your health information kept private.
- The right to file a complaint.
- The right to leave the program

- Summit ElderCare is Fallon Health's PACE program
- Service Hampden County, Hampshire County, Middlesex County and Worcester County
- Physicians at Summit ElderCare specialize in Geriatrics
- Mission is to maximize the dignity and respect of older adults and enable them to remain in their homes and communities for as long as is medically possible.

Element Care Contacts
Administrative Offices: 781-715-6608
Referrals: 877-803-5564
Compliance Hotline: 781-715-6618

- Non-profit healthcare organization
- PACE Program that serves Essex County and Middlesex County
- Mission is to coordinate and provide health and social services to individuals in their service area, to enable them to remain in their own homes and communities with dignity, safety and as much independence as possible.

Contracted Service Provider Overview

As a contracted service provider for the PACE program administered by Element Care, you are our partner in providing quality care and services to frail elders in the community. Element Care has developed this overview sheet to address frequently asked questions and provide pertinent information about communication between the Element Care PACE program and our contracted vendors.

Vision: To provide the best quality health care and social services to individuals living in our service area.

Mission Statement: Our mission is to coordinate and provide health and social services to individuals in our service area, to enable them to remain in their own homes and communities with dignity, safety and as much independence as possible.

Communication

Element Care believes that communication with our contracted providers is crucial to the well being of our participants. To that end, our contracted partners should feel free to contact any of our Element Care adult day health centers with questions or concerns about participant care at any time. The contact information for all of our sites can be found in this welcome materials packet.

Element Care Incident Reporting

Contracted providers should be mindful to identify and communicate all reportable incidents through established channels. Examples of reportable incidents include but are not limited to the following: (i) any injury sustained by an Element Care participant, (ii) medication losses or errors, (iii) breaches of confidentiality, and (iv) adverse care outcomes. Reportable incidents occurring after normal business hours should be reported through the On-Call system.

Element Care On-Call

It is the policy of Element Care to maintain a 24-hour emergency coverage system for all of its participants. The coverage is provided by Element Care clinical staff on a rotating basis. During business hours, Monday-Friday 8:00am to 4:00pm, participants and contracted vendors are instructed to call the appropriate Element Care site directly in the event of any illness, question or call services. Element Care maintains three systems for provision of on-call services.

Direct lines to the on-call system are as follows:

- **Lynn Sites:** Market, Buffum, School and Friend participants call 877-845-8442
- **North Shore Sites**: Cummings and Emerson participants call 978-837-9479
- **Merrimack Valley Sites**: Nevins and Lowell participants call 855-857-7349

Grievances

A grievance is a complaint, concern, issue or problem, either written or oral, expressing dissatisfaction with the services provided or the quality of Participant care. A participant, family member or representative may register a verbal or written grievance with any Element Care staff member or contracted provider at any time. The staff member receiving the grievance will document the issue and see to it that it is addressed through proper channels within Element Care.

NH Healthy Families

Overview of NH Healthy Families

- Is a Managed Care Organization (MCO)
- Is a wholly owned subsidiary of Centene Corporation, a national Medicaid coverage provider in 22 states
- Is underwritten by Granite State Health Plan Inc.
- Serves the medical and behavioral health needs of our NH members from the NH Healthy Families in the Bedford, NH headquarters
- Providing Medicaid benefit coverage in all 10 counties in NH
- Currently serving Medicaid, Granite Advantage and Exchange Program populations
- Membership exceeds 93,000

Specialty Companies

- National Imaging Associates (NIA): 1-800-635-2873
- Envolve Vision: 1-800-334-3937
- CTS for non-emergent transportation: 1-866-769-3085
- Envolve Pharmacy Solutions: 1-866-769-3085
- AcariaHealth (Specialty Drugs): 1-855-535-1815

Provider Relations Services

- Primary liaison between NH Healthy Families and the provider network
- Provides education
- Facilitates inquiries related to policies, procedures and operational issues
- Reviews payment and clinical policies
- Patient Panel questions
- Assist in Provider Portal registration

Website and Provider Secure Portal Tools

- Public site at www.NHhealthyfamilies.com & www.ambetter.nhhealthyfamilies.com

Member Eligibility

- Standard Medicaid
- Health Protection Program
- Ambetter
- Ambetter – FFM
- Eligibility verified through the secure portal, provider service call center and the NH MMIS Health Enterprise Portal

Access & Availability

- Each PCP is responsible for maintaining sufficient facilities and personal to provide covered physician service 24 hours a day, 365 days a year
- Coverage must consist of one of the following means
    - Answering service

    - Call forwarding to covering physician
    - After-hours, on-call coverage
- Independent Urgent Care Centers
    - ClearChoice MD – https://ccmdcenters.com/
    - ConvenientMD – https://convenientmd.com/

Medical Management

- Care Management Programs: 1-866-0769-3085
- Start Smart for Your Baby
- The CentAccount (Medicaid) & My health Pay Programs (Ambetter)
    - Promotes appropriate utilization of preventative services by rewarding members for practicing health behavior
    - Rewards can be used at the following locations:
        - CVS, Family Dollar, Dollar General, Rite Aid & Walmart on baby care, healthy groceries, over the counter meds & personal care items.

Prior Authorization

- Refer to the Provider Resources page at www.NHhealthyfamilies.com & www.ambetter.nhhealthyfamilies.com

Claims Submission - Claims may be submitted in 3 ways

- Secure web portal
- Electronic clearinghouse
- Original paper and corrected claims

Member Grievances, Appeals, & State Fair Hearing

- Grievances can be filed orally over the phone, in writing via mail or fax, or in person
- Appeals can be filed orally or in writing by the member or the member's authorized representative

Cultural Competency Plan & Disability Sensitivity

- Enables NH Healthy Families to meet the diverse cultural and linguistic needs of members
- NH Healthy Families complies with the Americans with Disabilities Act (ADA)

WRITTEN INFORMATION SECURITY PLAN (WISP)

Table of Contents

Comprehensive Written Information Security Program for 201 CMR 17.00

bb. Use of Electronic Main (E-mail) in Communication of Restricted Information #4013
cc. Alternative Communication of PHI #4013
dd. Security, Safeguarding and Staff Access to M/R Information #4014
ee. Access to PHI in an Emergency Event #4015
ff. Confidential Paper Disposal #4016
gg. Destruction of Patient Records #4017
hh. Electronic Signature, Attestation and Authorship in Electronic Medical Record (EMR) #1009
ii. Vendor Confidentiality #1011
jj. Passwords for Information Systems #1034
kk. Information Security, Responsibility for #1052
ll. HIPAA Privacy – Reporting of Data Breaches #1064
mm. Virtual Private Network (VPN) Remote Access #1065
nn. TMCAH Breach Tool

Comprehensive Written Information Security Program for 201 CMR 17.00

201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth is the regulation that implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information (*PI*) about a resident of the Commonwealth of Massachusetts. As a part of the requirements of this regulation, Home Health Foundation and its subsidies is creating, implementing and training employees on this written information security program (*WISP*).

The information contained herein is a part of the Corporate Compliance Program at Home Health Foundation.

I. OBJECTIVE

TMCAH has developed this to create effective administrative, technical and physical safeguards for the protection of personal information for the residents of the Commonwealth of Massachusetts, as well as our employees, and to comply with our obligations under 201 CMR 17.00.

The WISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of residents of the Commonwealth of Massachusetts.

For purposes of this WISP, "personal information" is as defined in the regulations: a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:

a. Social Security number;
b. Driver's license number or state-issued identification card number; or
c. Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit

access to a resident's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

II. PURPOSE

The purpose of the WISP is to promote achievement of the following:

1. Ensure the security and confidentiality of personal information;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE

In formulating and implementing the WISP, TMCAH has addressed and incorporated the following protocols:

1. Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;
2. Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
3. Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
4. Designed and implemented a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00; and
5. Implemented regular monitoring of the effectiveness of those safeguards.

IV. RESPONSIBILITY FOR INFORMATION SECURITY – Security Manager

TMCAH has designated the V.P. of Quality, Compliance and Risk to implement, supervise, delegate authority and maintain the WISP. The V.P. of Quality, Compliance and Risk has delegated information security responsibility to the Director of Information Technology (Security) and to the Health Information and Compliance Coordinator (Health Information Privacy). These designated employees (the "Data Security Coordinators") will be responsible for the following:

1. Implementation of the WISP including all provisions outlined in Section VI;
2. Daily operation protocols;
3. Training of all employees;
4. Regular testing of the WISP's safeguards;
5. Evaluating the ability of any of our third-party service providers to implement and maintain appropriate security measures for the personal information to which we have

permitted them access, and requiring such third-party service providers by contract to implement and maintain appropriate security measures;
6. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information;
7. Reviewing and revising any and all sections of this WISP as appropriate, as a result of an investigation of a data breach of personal information; and
8. Conducting training sessions for all managers, employees and independent contractors, including temporary and contract employees who have access to personal information on the elements of the WISP.

V. INTERNAL RISKS – MITIGATION/SAFEGUARDS

The following areas have been identified as reasonably foreseeable internal and external risks and have been assessed, considering the safeguards which are implemented as part of this WISP as noted:

1. **Personal information is used during the quoting of prospective accounts and the servicing and remarketing of existing clients' accounts.**
   - Some of this PI is found on paper records and files that are maintained at employees' desks for the period of time that the corresponding accounts are being worked.
   - Upon completion of the tasks and work corresponding to the paper records and files for these documents are then placed in a shred bin on the Agency floor until a third-party service provider, a shredding company, is called to come and dispose of these papers via shredding. A receipt and certificate of destruction is provided once the papers have been shredded.
   - PI is also found in an electronic format in the agency management system and in a separate document management system (that contains both client and employee information). All Agency employees have a unique used id and password for both systems that contain PI, and security permissions are set to restrict access to employee data to management only.

2. **All Agency employees have physical access to the few filing cabinets that are maintained at the Agency that contain PI. All Agency employees are deemed to have a true, business-related need, to have access to said information.**

3. **PI is also transmitted via email during the course of normal Agency operations. Most often this information is regarding start of care and is via (documents) attached to the emails. Internal email within our systems is encrypted.**

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are employed:

1. We will only collect personal information of patients, customers or employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal, state or local regulations.
2. Access to records containing personal information shall be limited to those employees whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose.
3. Written and electronic records containing personal information shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.
4. Our frequent business records associated retention and secure destruction periods are included in Destruction of PHI #7033.
5. A copy of the WISP/PHI Considerations is to be distributed to employees at new employee orientation. It shall be the employee's responsibility for acknowledging in writing, by signing the acknowledgement sheet, that he/she has received a copy of the WISP and will abide by its provisions. Employees are encouraged and invited to advise the WISP Data Security Coordinators of any activities or operations which appear to pose risks to the security of personal information. If the Data Security Coordinators is him or herself involved with these risks, employees are encouraged and invited to advise any other manager or supervisor or business owner.
6. All employment contracts, where applicable, will be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of personal data as defined by the WISP.
7. Terminated employees must return all records containing personal data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any device owned directly by the terminated employee
8. A terminated employee's physical and electronic access to records containing personal information shall be restricted at the time of termination. This shall include remote electronic access to personal records, voicemail, internet, and email access. All keys, keycards, access devices, badges, company IDs, business cards, and the like shall be surrendered at the time of termination.
9. Disciplinary action will be applicable to violations of the WISP, irrespective of whether personal data was actually accessed or used without authorization. All security measures including the WISP shall be reviewed at least annually to ensure that the policies contained in the WISP are adequate meet all applicable federal and state regulations.
10. Should operation practices change in a way that impacts the collection, storage, and/or transportation of records containing personal information the WISP will be reviewed to ensure that the policies contained in the WISP are adequate meet all applicable federal and state regulations.
11. The Data Security Coordinator(s) or designee shall be responsible for all review and modifications of the WISP and shall fully consult and apprise V.P. of Quality, Compliance and Risk of all reviews including any recommendations for improves security arising from the review.
12. The Executive Administrative Assistant to the CEO, or designee shall maintain a secured and confidential master list of all lock combinations, passwords, and keys. The list will identify which employees possess keys, keycards, or other access devices and that only approved employees have been provided access credentials.

13. The Data Security Coordinators or his/her designee shall ensure that access to personal information in restricted to approved and active user accounts.
14. Current employees' user ID's and passwords shall conform to accepted security standards. All passwords shall be changed at least every 90 days, more often as needed.
15. Employees are required to report suspicious or unauthorized use of personal information to a supervisor, Data Security Coordinators or V.P. Of Quality, Compliance and Risk.
16. Whenever there is an incident that requires notification pursuant to the Security Breach Notifications of Massachusetts General Law Chapter 93H: "Security Breaches", the V.P. of Quality, Compliance and Risk or designee shall conduct root cause and post-incident review of events and actions taken, if any, in order to determine how to alter security practices to better safeguard personal information.

VI. EXTERNAL RISKS – MITIGATION/SAFEGUARDS

To guard against external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are employed:

1. Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes personal information.
2. Personal information shall not be removed from the business premises in electronic or written form absent legitimate business need and use of reasonable security measures, as described in this policy.
3. All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any computer that stores or processes personal information.
4. There shall be secure user authentication protocols in place that:
    a. Control user ID and other identifiers;
    b. Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies;
    c. Control passwords to ensure that password information is secure.

VII. DAILY OPERATION and RECORD KEEPING PROTOCOLS

This section of our WISP outlines our daily efforts to minimize security risks to any computer system that processes or stores personal information, ensures that physical files containing personal information are reasonable secured and develops daily employee practices designed to minimize access and security risks to personal information of our clients and/or customers and employees.

Daily Operation Protocols shall be reviewed and modified as deemed necessary. Any modifications to the Daily Operation Protocols shall be published in an updated version of the WISP.

Recordkeeping Protocols: We will only collect personal information of clients and customers and employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal and state and local laws.

The Daily Operation Protocols and the Recordkeeping Protocols are made up of the following features:

1. Any personal information stored shall be disposed of when no longer needed for business purposes or required by law for storage. Disposal methods must be consistent with those prescribed by the WISP.
2. Any paper files containing personal information of patients or employees shall be stored in a locked filing cabinet. The V.P. of each company will determine a limited list of employees who will maintain the keys to the secured data location and the Data Security Coordinators will be assigned keys to filing cabinets to only those individuals are allowed access to the paper files.
3. Individual files may be assigned to employees on an as-needed basis by the department supervisor.
4. All employees are prohibited from keeping unsecured paper files containing personal information in their work area when they are not present (e.g. lunch breaks).
5. At the end of the day, all files containing personal information are to be returned to the locked filing cabinet by all employees. Department heads, managers or coordinators are responsible for assuring adherence.
6. The Compliance Department or IT Department will conduct periodic, unannounced work space audits to assess for the existence of unsecured personal information.
7. Paper or electronically stored records containing personal information shall be disposed of in a manner that complies with M.G.L. c. 93I sec. 2 (See Attachment D: Standards for disposal of records containing personal information; disposal by third party; enforcement) and as follows:
    a. Paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;
    b. Electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.
    c. Electronic records containing personal information shall not be stored or transported on any portable electronic device, sent or transmitted electronically to any portable device, or sent or transported electronically to any computer, portable or not, without being encrypted. The only exception shall be where there is no reasonable risk of unauthorized access to the personal information or it is technologically not feasible to encrypt the data as and where transmitted.
    d. If necessary for the functioning of individual departments, the department head, in consultation with the Data Security Coordinators or V.P. of Quality, Compliance and Risk, may develop departmental rules that ensure reasonable restrictions upon access and handling of files containing personal information and must comply with all WISP standards. Departmental rules are to be published as an addendum to the WISP and be added to the Information Security Plan.

Access Control Protocols

TMCAH shall control access to personal information based upon employee role. We shall also apply the standard of minimum necessary and limit data sets to those required to successfully complete required job tasks. We shall employ the following:

1. All our computers shall restrict user access to those employees having an authorized and unique log-in ID assigned by the Information Technology Department.
2. All computers that have been inactive for 5 or more minutes shall require relog- in.
3. After 5 unsuccessful log-in attempts by any user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by the Data Security Coordinators or his/her designee.
4. Access to electronically stored records containing personal information shall be electronically limited to those employees having an authorized and unique login ID assigned by the Data Security Coordinators.
5. Where practical, all visitors who are expected to access areas other than the lobby space at all work locations or are granted access to office space containing personal information should be required to sign-in with a Photo ID at a designated reception area where they will be assigned a visitor's ID or guest badge. Visitors are required to wear said visitor ID in a plainly visible location on their body, unless escorted at all times.
6. Where practical, all visitors are restricted from areas where files containing personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing personal information are stored.
7. Cleaning personnel (or others on site after normal business hours and not also authorized to have access to personal information) are not to have access to areas where files containing personal information are stored.
8. All computers with an internet connection or any computer that stores or processes personal information must have a reasonably up-to-date version of software providing virus, anti-spyware and anti-malware protection installed and active at all times.
9. An inventory of all company computers and handhelds authorized for personal information storage is contained in HIPAA/HITECH Risk Assessment Year End 2018, which shall be made known only to the Data Security Coordinators and other managers on a "need to know" basis.

Third Party Service Provider Protocols

Any service provider or individual that receives, stores, maintains, processes, or otherwise is permitted access to any file containing personal information ("Third Party Service Provider") shall be required to meet the following standards as well as any and all standards of 201 CMR 17.00. (Examples include third parties who provide off-site backup storage copies of all our electronic data; paper record copying or storage service providers; contractors or vendors working with our customers and having authorized access to our records):

1. Any contract with a Third-Party Service Provider signed on or after March 1, 2010 shall require the Service Provider to implement security standards consistent with 201 CMR 17.00.

2. It shall be the responsibility of the V.P. of Quality, Compliance and Risk or designee to obtain reasonable confirmation that any Third-Party Service Provider is capable of meeting security standards consistent with 201 CMR 17.00.
3. Any existing contracts with Third Party Service shall be reviewed by the V.P. of Quality, Compliance and Risk or designee. These Service Providers shall meet the security standards consistent with 201 CMR 17.00 by March 1, 2012 or other Service Providers will be selected, when feasible to do so.
4. A list of currently known third party service providers is contained in Attachment B: Third Party Service Providers

VIII. Breach of PI Data Security Protocol

Should any employee know of a security breach at any of our facilities, or that any unencrypted personal information has been lost or stolen or accessed without authorization, or that encrypted personal information along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the following protocol is to be followed:

1. Employees are to notify the V.P. of Quality, Compliance and Risk and/or Data Security Coordinators in the event of a known or suspected security breach or unauthorized use of personal information.
2. The V.P. of Quality, Compliance and Risk shall be responsible for drafting a security breach notification to be provided to the Massachusetts Office of Consumer Affairs and Business Regulation and the Massachusetts Attorney General's office. The security breach notification shall include the following (also see Appendix).:
    a. A detailed description of the nature and circumstances of the security breach or unauthorized acquisition or use of personal information;
    b. The number of Massachusetts residents affected at the time the notification is submitted;
    c. The steps already taken relative to the incident;
    d. Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and
    e. Information regarding whether law enforcement officials are engaged in investing the incident
3. The notice to the Attorney General and the Director of Consumer Affairs and Business Regulation will also require to certify that credit monitoring services comply with Section 3A.
4. TMCAH shall provide notice as soon as practicable and without unreasonable delay (a) when it knows or has reason to know of a PI security breach, or (b) knows or has reason to know that PI was acquired or used by an unauthorized person or used for an unauthorized purpose (see Appendix).
5. The V.P. of Quality, Compliance and Risk shall be responsible for drafting a security breach notification to be provided to the Massachusetts Residents impacted. The security breach notification shall include the following (also see Appendix):
    a. the consumer's right to obtain a police report;
    b. how a consumer requests a security freeze;
    c. the necessary information to be provided when requesting the security freeze; and

d. that there shall be no charge for a security freeze; provided however, that the notification shall **not** include:
e. the nature of the breach or unauthorized acquisition or use; or
f. the number of Massachusetts residents affected by the security breach or the unauthorized access or use.

6. Per April 2019 Amendment, "A notice [to the Massachusetts Residents impacted] provided pursuant to this section shall not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case, and where otherwise necessary to update or correct the information required, a person or agency shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information."
7. Whenever there is a PI security breach or unauthorized use of PI, there shall be an immediate mandatory post-incident review of events and actions taken, if any, to determine whether any changes to TMCAH's security practices and the WISP are required to improve the security of PI for which TMCAH is responsible.

Appendix
Requirements for Security Breach Notifications under Chapter 93H
Pursuant to M.G.L. c. 93H, s. 3(b), if you own or license data that includes personal information of a Massachusetts resident, you are required to provide written notice **as soon as practicable and without unreasonable delay** to:

1. The Attorney General (AGO);
2. The Director of the Office of Consumer Affairs and Business Regulation (OCABR); and
3. The affected Massachusetts resident

When you know or have reason to know (a) of a breach of security; **or** (b) that personal information of a Massachusetts resident was acquired by or used by an unauthorized person or used for an unauthorized purpose.

Credit Monitoring Changes
Eighteen (18) months of credit monitoring services are now required per April 2019 Amendment.

Notice to the AGO and OCABR

The notice to the Attorney General and the Director of Consumer Affairs and Business Regulation shall include, but not be limited to:

1. the nature of the breach of security or the unauthorized acquisition or use;
2. the number of Massachusetts residents affected by such incident at the time of notification; the name and address of the person or agency that experienced the breach of security;
3. the name and title of the person or agency reporting the breach of security, and their relationship to the person or agency that experienced the breach of security;
4. the type of person or agency reporting the breach of security;
5. the person responsible for the breach of security, if known;

6. the type of personal information compromised, including but not limited to, social security number, driver's license number, financial account number, credit or debit card number or other data;
7. whether the person or agency maintains a written information security program; and
8. any steps the person or agency has taken or plans to take relating to the incident, including updating the WISP.

The notice to the Attorney General and the Director of Consumer Affairs and Business Regulation will also require that they certify that credit monitoring services comply with Section 3A.

See Attorney General Template below.

Notice to Affected Massachusetts Residents

A person or agency that has experienced a breach of security or the unauthorized acquisition or use of personal information of Massachusetts residents must also provide notice to those affected Massachusetts residents. This notice shall include, but not be limited to:

1) the consumer's right to obtain a police report;
2) how a consumer requests a security freeze;
3) the necessary information to be provided when requesting the security freeze; and
4) that there shall be no charge for a security freeze; provided however, that the notification shall **not** include:

a) the nature of the breach or unauthorized acquisition or use; or

b) the number of Massachusetts residents affected by the security breach or the unauthorized access or use.

Per April 2019 Amendment, "A notice provided pursuant to this section shall not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case, and where otherwise necessary to update or correct the information required, a person or agency shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information."

ATTORNEY GENERAL NOTIFICATION TEMPLATE LETTER

Attorney General Maura Healey
Office of the Attorney General
One Ashburton Place, 20th Floor
Boston, MA 02108

Dear Attorney General Healey:

Pursuant to M.G.L., c. 93H, we are writing to notify you of a (a breach of security/an unauthorized access to use of personal information) involving (number) Massachusetts resident (s).

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OF ACCESS
(Incident description)

NUMBER OF MASSACHUSETTS RESIDENTS AFFECTED
(This paragraph should specify the number of affected individuals residing in Massachusetts whose personal information was the subject of the incident. This paragraph should also indicate that these Massachusetts residents have received or will shortly receive notice pursuant to M.G.L. c. 93H, s. 3(b) and should specify the manner in which Massachusetts residents have or will receive such notice. Also include a copy of the notice to affected Massachusetts residents in your notification to the Attorney General).

STEPS TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT
(outline the steps taken or plan to take relating to the incident including without limitation, what was discovered during the incident, reported the incident to law enforcement; evidence of personal information has been used for fraudulent purposes; whether credit monitoring was offered to consumers; and what measures you have taken to ensure that similar incidents do not occur in the future.)

OTHER NOTIFICATION AND CONTACT INFORAMTION
(Indicate whether we provided similar notification to the Director of Consumer Affairs and Business Regulation. Include the name and contact information for the person whom the Office of the Attorney General may contact if there are any additional questions)

TEMPLATE LETTER TO AFFECTED MASSACHUSETTS RESIDENTS

Date

Consumer Name
Address
City, MA

Dear _____:

We are writing to notify you that a [breach of security/unauthorized acquisition or use] of your personal information occurred on [date(s)].

YOUR NOTICE MUST INCLUDE THE FOLLOWING INFORMATION:

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;

8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

[**NOTE: Although not required by M.G.L. c. 93H, you should also consider providing the affected Massachusetts residents with additional information to protect themselves against identity theft or other fraud including, but not limited to: the placement of fraud alerts on their credit file; the need to review their credit reports for unexplained activity; and the need to review credit card or other financial accounts for any suspicious and/or unauthorized activity. Many companies provide affected Massachusetts residents with free credit monitoring services. If you are providing credit monitoring services for affected Massachusetts residents, you should provide them with information concerning how they may enroll for such credit monitoring services as well as any telephone numbers or websites that you have set up to answer any questions they may have concerning the incident. Please note that any additional advice provided to affected Massachusetts residents may vary on a case-by-case basis and these information suggestions are not a complete list of all the information that you may want to provide affected Massachusetts residents to better protect themselves against identity theft or fraud].**

If you should have any further questions, please contact [provide contact information].

Sincerely,