

Main Line Health, Inc. and Main Line Health, Inc. Subsidiaries		
Working Together to Serve the Community		
This policy applicable to:	<input checked="" type="checkbox"/> All Subsidiaries <input checked="" type="checkbox"/> All Hospitals <input checked="" type="checkbox"/> All Acute Care Hospitals	<input checked="" type="checkbox"/> BMRH <input checked="" type="checkbox"/> MLHC <input checked="" type="checkbox"/> Mirmont Treatment Center

HUMAN RESOURCES STANDARD PRACTICES AND PROCEDURES

Policy Name: Confidentiality Policy

Policy Purpose: To establish a policy and procedure for protecting the confidentiality of any and all privileged information.

Policy Statement: It is the policy of Main Line Health System that all employees (including contracted service employees) are required to maintain the confidentiality of all privileged information. Privileged information consists of, but is not limited to, data that can be communicated verbally, electronically, or in hard copy regarding the following:

- A. Patient information (e.g. diagnosis, content of medical records)
- B. Information regarding family members of patients
- C. Employee information (e.g. salary, demographics)
- D. Financial reports
- E. Non-public information regarding the financial, clinical or operational status of the System

I. Procedure:

- A. The Human Resources Department is responsible for:
 - A. Ensuring the employee e-signs the “Confidentiality Statement” during onboarding through the ATS, Taleo.
 - B. Ensuring appropriate Performance Management in a Just Culture is followed for employees who do not comply with Main Line Confidentiality and Health IS Security Policies and Procedures
- B. The manager is responsible for:
 - A. Explaining how the confidentiality of privileged information relates to the employee’s position, department, and the organization during departmental orientation
 - B. Reviewing the Confidentiality Policy and practice as it relates to each employee on an annual basis in accordance with CBT requirements
 - C. Educating and enforcing the Confidentiality and IS Security Policies and Procedures with their employees.
- C. The employee is responsible for:
 - A. Understanding how the confidentiality of privileged information relates to his/her position, department, and the organization
 - B. E-Signing the “Confidentiality Statement” as part of their onboarding.
 - C. Complying with all applicable IS Security Policies and Procedures

Reference: HIPAA

Related Policies: Administrative IS Security Policies and Procedures

Origination Date: January 1, 1990

Revision Date: June, 2017; March, 2015; December 2004, June 1, 2003, February 2001;

Review Date: March, 2018; March, 2017; March, 2016; March, 2015; April, 2010; July, 2009; July 2008; March 2007; December, 2004

NOTE: A copy of the “Confidentiality Statement” follows this policy.

CONFIDENTIALITY STATEMENT

I understand and agree that:

- A. As an employee, volunteer or contractor of the Main Line Health System, I may have access to privileged information of a highly confidential nature.
- B. Privileged information consists of, but is not limited to, data regarding the following:
 - 1. Employees: Salary and demographic information, social security number, medical information including all computerized information.
 - 2. Patients: Diagnosis and procedures, content of medical records and any personal information.
 - 3. Family members of patients: Any and all personal information.
 - 4. Financial: Any and all reports.
 - 5. System: Any and all information in draft or preliminary forms.
- C. Law protects the confidentiality of privileged information, and as an employee of the Main Line Health System, it is my responsibility to preserve and protect this confidentiality.
- D. I am also responsible for maintaining strictest confidentiality regarding computer system access and information. This prohibits sharing of sign on ID/password information and/or providing physical access to a terminal in "active" status. I will only access information on patients/employees about whom I have a business need to know. Likewise, I will discuss information only with employees who have a business need to know. I will not attempt to gain access to areas of the system(s) that are not necessary for the performance of my job.
- E. I am solely and fully accountable for any information entered into the system(s) under my password. I will notify my manager immediately if I suspect someone has gained unauthorized access to my password.
- F. I am responsible for completely exiting from the system(s) when I am finished working on the terminal or when leaving my work area for any extended period of time.
- G. Any unauthorized access to, use of or disclosure of privileged information or any other confidential information concerning a current or past patient or employee of the Main Line Health System will be subject to Performance Management and may result in immediate discharge from employment with the System, and possible legal action against me.
- H. I am responsible for maintaining confidential information after no longer employed.

DATE: _____ SIGNATURE: _____

PRINT NAME (CLEARLY): _____

Document Information

Document Title

Confidentiality Policy

Document Description

N/A

Approval Information

Approved On: 01/23/2019

Approved By: Human Resources [Christina Batot (BatotC)]

Approval Expires: 04/30/2019

Approval Type: Process

Document Location: / Human Resources

Keywords: N/A

Printed By: Guest User

Standard References: N/A

Note: This copy will expire in 24 hours