Workstation Security for HIPAA Policy

Effective:
September 2, 2016

Purpose

The standards for protecting health information are prescribed in the federal law known as the Health Insurance Portability and Accountability Act (HIPAA). HIPAA and Montreat College's HIPAA policies apply to individually identifiable information on past, present, and future health care or payment for health care, which HIPAA calls Protected Health Information (PHI). PHI stored electronically is called ePHI. This policy is designed to ensure the appropriate privacy and security of all PHI and ePHI across the college. The purpose of this policy is to provide guidance for security of information on the workstation and information to which the workstation may have access. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

Scope

This policy applies to all Montreat College employees, contractors, workforce members, vendors, and agents with a college-owned or personal workstation connected to the Montreat College network and accessing ePHI.

Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity, and availability of sensitive information, including protected health information (PHI), and that access to sensitive information is restricted to authorized users. The following physical and technical safeguards for all workstations accessing electronic protected health information (ePHI) must be implemented:

- Physical access to workstations must be restricted only to authorized personnel.
- Workstations must be secured by either screen lock or logout prior to leaving the workstation area.
- A password-protected screen saver with a 10-minute timeout period must be implemented to ensure that workstations left unsecured will be protected. The password must comply with Montreat College's Password Policy.
- Workstations must be used for authorized purposes only.
- No unauthorized software may be installed on workstations accessing ePHI.
- All sensitive information, including ePHI must be stored on network servers.
- Laptops and mobile devices containing sensitive information must be secured by using cable locks or by locking them in drawers or cabinets.

- Laptops must comply with the Portable Workstation Encryption Policy.
- Privacy screen filters must be installed or other physical barriers used to prevent exposing data.
- Workstations must be kept updated with the latest operating system security updates.
- Running applications must be exited and open documents must be closed when not in use.
- All workstations must use a surge protector or UPS (Uninterruptible Power Supply).
- If wireless network access is used, the workstation must be connected to the proper Montreat College wireless network.

Policy Compliance

Compliance Measurement

Campus Technology will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by Campus Technology in advance.

Non-Compliance

The responses for violation of this policy will include, but are not limited to, the following:

- Notification: alerting a user to what appears to be an inadvertent violation of this policy in order to educate the user to avoid subsequent violations.
- Warning: alerting a user to the violation, with the understanding that any additional violation will result in a greater penalty.
- Loss of computer privileges: limitation or removal of computer privileges, either permanently or for a specified period of time.
- Restitution for damages: requiring reimbursement for the costs of repairs to or replacement of computer related material, equipment, hardware, software, data, and/or facilities, which reimbursement shall include, but not be limited to, the cost of additional time spent by college employees due to the violation.

In addition to the aforementioned, violators may be subject to disciplinary action – which may include termination – as may be prescribed by other rules, regulations, handbooks, procedures, or policies applicable to the violator. Furthermore, the violator may be subject to civil suits or ordinances, laws, statues, or regulations of the applicable local government, the State of North Carolina, or the United States of America.

Definitions of Terms

Sensitive Data: Data such as social security numbers, personal health information (PHI), personal identity information (PII), financial data, proprietary data, graded papers, etc. that must be handled with the utmost care, stored securely, and be protected to the greatest possible extent.

HIPAA 164.210

http://www.hipaasurvivalguide.com/hipaa-regulations/164-310.php

About HIPAA

http://abouthipaa.com/about-hipaa/hipaa-hitech-resources/hipaa-security-final-rule/164-308a1i-administrative-safeguards-standard-security-management-process-5-3-2-2/

Contact Information

Campus Technology
Phone: 828-669-8012 Ext. 3663
Email: support@montreat.edu

Revision History

Initial Draft: 08/05/2016
Revised: 08/18/2016
Revised: 09/02/2016