RUSH COPLEY MEDICAL CENTER

Policy & Procedure

Title: Workstation Use Policy

Author: Dave Moser

Date Initiated: 12/1/19

Next Review Date: 12/1/22

Purpose

To implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

Scope

This policy applies to RCMC in its entirety, including all members of the workforce and all workstations, or other computing devices that connect to the local or wireless network, or to RCMC applications or sensitive information. Additionally, this policy applies to all employee-owned workstations including desktops, laptops, iPads, tablets, and other computing devices, that may regularly or occasionally connect to RCMC in-scope systems, applications, or sensitive information.

Policy

RCMC workstations and other computing devices at RCMC offices are to be used for work related purposes only. Internet access and e-mail use on RCMC workstations is allowed for work related purposes only, and to access remotely-hosted business applications.

RCMC has two wireless networks that are used for different purposes.

- Private:
    - This is used exclusively for access to the RCMC internal network. Access is restricted to RCMC owned equipment.
- Public:
    - This network is offered in most areas. The Public network provides unrestricted Internet access only. Business use of this network is not allowed.

RCMC workstations may not be utilized for any activities that are illegal or in violation of any RCMC policy, procedure, or training. RCMC reserves the right to monitor all activities performed on, or with, RCMC devices and networks. There should be no expectation of privacy by any member of the workforce when utilizing any RCMC computing resources.

RCMC may revoke the access rights of any individual at any time in order to protect or secure the confidentiality, integrity, and availability of sensitive information or to preserve the functionality of electronic information systems.

RCMC will implement reasonable and appropriate measures to secure all computing devices that could be used to access sensitive information. These measures include protection from

malicious software, encryption wherever required or appropriate and beneficial, logging capabilities, theft detection and prevention, positioning, and other measures developed and implemented over time to increase the security of devices and sensitive information.

RCMC will implement enhanced or more restrictive controls on workstations that are typically deployed in the field. These workstations may be audited more often, or may be significantly restricted to prevent usage outside of assigned and approved job duties.

Only RCMC owned mobile devices are allowed direct access to the internal private wireless network. Non-RCMC owned mobile devices are only allowed access to the public wireless network. Non-RCMC owned mobile devices must use Citrix Receiver to access RCMC resources. Citrix receiver can be used on the RCMC public wireless network or through a cellular carrier network. All personal mobile devices that access RCMC resources must be password or PIN protected. Whenever possible mobile devices should enable screen locking and screen timeout functions. PHI must not be stored on any mobile device.

If a personal mobile device is lost or stolen, the incident should be reported to the I.S. Helpdesk. For further guidance on smartphone devices and use, consult the “Smartphone Device Use and Reimbursement” policy

RCMC will attempt to communicate to clients and customers the importance of workstation use and workstation security measures when connecting to RCMC's information systems such as the client portal.

Computing devices not owned by RCMC, but used to access ePHI related to RCMC, must be used in a safe, secure, authorized, and responsible manner while creating, collecting, storing, processing, or transmitting any ePHI, or other sensitive information. When using a device not owned by RCMC, members of the workforce, including consultants, contractors, interns, or other vendors will only store ePHI on RCMC authorized, encrypted, storage devices. Storage of ePHI in any other location on any non-RCMC device, or in any unencrypted manner, is strictly prohibited. For example, ePHI will not be stored on unencrypted laptop hard drives, external hard disk drives, unencrypted non-approved USB drives, CDs, DVDs, compact flash, memory stick, iPod, iPhone, MP3 player, or any other storage device not specifically approved by the Security Officer.

Responsibilities

All members of the workforce are responsible for complying with the requirements of the sanction policy.

Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s)

None

References

Acceptable Use Policy

Smartphone Device Use and Reimbursement Policy

International Standards Organization (ISO 27002) http://www.iso.org

Final HIPAA Omnibus Rule:
https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the

Final HIPAA Security Rule, 45 CFR Parts 160, 162 and 164, Department of Health and Human Services: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
http://www.hhs.gov/ocr/privacy/

Security Management Process 164.308(a)(1)(i) – Standard

American Recovery and Reinvestment Act of 2009:
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf

Contact

Dave Moser
Information Security Officer
2000 Ogden Ave.
Aurora, IL 60504
(630) 978-6200

Policy History

Initial effective date: December 1, 2019

Supersedes: Mobile Computing Devices Policy, Wireless Access Policy