Policy Number: REG31	**Policy Category:** Information Technology
Policy Title: Workstation Acceptable Use	**Effective Date:** 12/15/2011
Sponsor: Melissa Melcher	**Revision Date:** 11/11/2019
Covered Organizations: All Avera Health owned, leased, sponsored and managed entities.	
Contact: Avera Health IT Security Officer at AHISO@avera.org	

1.0 Purpose:

To specify guidelines for the proper use of a Workstation that accesses Avera's electronic Confidential Information, the manner in which those function are to be performed, and the physical attributes of the surroundings of a specific Workstation or class of Workstation that can access electronic Confidential Information.

2.0 Scope:

This Workstation Acceptable Use Policy applies to all uses and Users of Avera's Information Technology Resources.

3.0 Definitions:

Avera – includes all Avera Health, owned, leased, sponsored, joint venture and managed entities including both patient care and operational entities.

Avera Network – means the information systems and networks (intranet, extranet, internet, and related wide area network (WAN) and local area networks (LANs) supporting the health care and administrative operations of Avera and its managed and independent affiliated entities including, but not limited, to computer equipment, hardware, software, operating systems, storage media, servers, network accounts, data and electronic documents, transmissions and transfers, portable devices, services, and other technology.

Confidential Information – includes, but is not limited to, (i) PHI; (ii) PII; (iii) financial information; (iv) commercial transaction information; (v) corporate strategies; (vi) intellectual property; and (vii) other sensitive information.

Health Information Portability and Accountability Act of 1996, as amended ("HIPAA") – means Public Law 104-191 including the Privacy Rule, Security Rule, Enforcement Rule, HITECH Act, and the Breach Notification Rule. See 45 CFR Part 160, Part 162, and Part 164.

Information Technology Resources – includes, but is not limited to, (i) all Avera owned, licensed, leased, or managed hardware, equipment, devices, and software; (ii) Avera data and information; and (iii) use of the Avera Network regardless of ownership of the computer system or device connected to the network.

Personally Identifiable Information (PII) – Any representation of information that permits the identity of an individual to be reasonably inferred by either direct or indirect means. Further, PII is defined as information (i) that directly identifies an individual (e.g. name, address, social security number or other identifying number or code, telephone number, email address, etc.) or

(ii) by which an agency intends to identify specific individuals in conjunction with other data elements. A common example of PII is employee data.

Protected Health Information (PHI) – as defined by HIPAA, means information including demographic information, which relates to: (i) the individual's past, present, or future physical or mental health or condition; (i) the provision of health care to the individual; or (iii) the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, social security number) when they can be associated with the health information listed above. See 45 C.F.R. §160.103.

User(s) – means all employees, contractors, consultants, volunteers, temporary staff, independent providers and support staff, auditors, researchers, and others using Avera's Information Technology Resources.

Workstations (also referenced as "computer systems") – includes, but is not limited to, personal computers, laptop computers, personal devices, server systems, and any and all other devices that may be connected to the Avera Health network, or which are supplied by Avera Health for business-related purposes without respect to network connectivity and electronic media stored in Avera Health's immediate environment.

4.0 Policy:

Avera will utilize Workstations to assist with patient care services and business operations. Users shall protect electronic Confidential Information and minimize the risk of unauthorized access through Workstations whether working locally on the Avera Network within or remotely from an out of network location. Avera will implement administrative, physical, and technical safeguards for all Workstations on the Avera Network.

5.0 Procedure:

5.1 Workstation Acceptable and Prohibited Use

(1) Users are expected to perform only legitimate business needs based up their role responsibilities on Avera's Workstations in compliance with all Avera Health Information Technology policies.

(2) Users will safeguard electronic Confidential Information created, accessed, used, stored, and transferred on Workstations as referred in the *Data Encryption Policy*.

(3) Users incidental personal use is permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with the User's productivity, does not preempt any business activity, is permitted by the User's management team, and does not cause performance, distress, legal or compliance risk, or morale problems for other Users.

(4) Users may not configure systems that automatically exchange data between Avera's Workstations and personal devices, such as a personal digital assistant (e.g. Alexa, Echo, etc.), smartphone, smart speaker and a personal computer, unless a security risk assessment has been completed and Avera Health Information Technology approves in compliance with all applicable policies. All approved personal devices will be connected to the Avera Health Information Technology device management software for remote removal of electronic Confidential Information and other management capabilities.

(5) Users may not utilize Workstations to identify or browse through Avera's Information Technology Resources including other computer systems or networks outside the scope of their role responsibilities. Browsing through educational materials posted by Avera Health departments on the intranets and SharePoint sites for general use is not a violation of this use restriction.

(6) Users may not access, create, store, transmit, disclose or otherwise manipulate offensive material, including sexist, racist, discriminatory, harassment, violent, or other content, and all material considered being incompatible with the mission and values of Avera Health, the Presentation Sisters, and the Benedictine Sisters.

(7) User may not make unauthorized copies of licensed and copyrighted software, even if for "evaluation" purposes. Reproduction of copyrighted materials is permitted only to the extent legally considered fair use or with the permission of the author or copyright owner. Users may contact the Office of General Counsel for questions on copyright or intellectual property law. Users must assume that software and other materials are copyrighted until directed otherwise by a proper authority.

(8) Users may not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

(9) Users will apply all Avera Health Information Technology acceptable use policies to Workstation use as well.

(10) Users must promptly report all information security alerts, warnings, and suspected vulnerabilities prompted or visible on the Workstations to Avera Health Information Security Office at AHISO@avera.org and Avera Help Desk 605-322-6000. Users must not use Avera computer systems and Workstations to forward such information to others whether the other individuals are internal or external to Avera Health.

5.2 Workstation Configuration Control

(1) *Changes to Application Software*: Avera Health Information Technology maintains a standard list of software packages approved for use on Avera's Workstations. All department purchases of Workstation software must be purchased through Avera Health Information Technology in accordance with other applicable Avera facility policies. Users are not permitted

to install software packages on Workstations without Avera Health Information Technology approval. Users must not permit automatic software installation routines to be run unless these routines have been approved. Avera Health Information Technology may remove unapproved software without advance notice to the involved User.

(2) *Changes to Operating System Configurations*: Users may not change operating system configurations, upgrade existing operating systems, or install new operating systems on computer systems, equipment, and devices owned or managed by Avera Health. If such operating system changes are required, Avera Health Information Technology will update accordingly in person or with remote system maintenance software.

(3) *Changes to Hardware:* Workstations must not be altered in any way without the prior knowledge of and authorization from appropriate personnel within Avera Health Information Technology.

(4) All above changes to applications, operating systems, or hardware accessing, storing, transferring, using, or otherwise disclosing electronic Confidential Information require a technology security risk assessment prior to implementing the changes.

(5) *Rights To Programs Developed*: All computer programs and documentation generated by, or provided by users for the benefit of Avera are the property of Avera Health unless otherwise directed in writing between the applicable parties. All other material developed by Avera Health Users using computer systems is considered the property of Avera Health. This material includes patents, copyrights, and trademarks.

5.3 Workstation Backups

(1) *Archival Copies*: The original distribution media for all Workstation software must be stored in the Avera Health Information Technology office, or in such other safe and secure location as may be designated by Avera Health Information Technology. License documentation for all software will be retained for verification of the rights granted by the software manufacturer to use the software.

(2) *Periodic Backup*: All sensitive, valuable, or critical information stored on Avera Health Workstations must be periodically backed up based on data criticality. Unless automatic backup systems are configured, Users are responsible for making at least one current backup copy of sensitive, critical, or valuable files. These separate backup copies should be made each time that a significant number of changes are saved. User-generated backups must be periodically stored off-site in an Avera approved secure location. Selected files from backups must be periodically restored to demonstrate the effectiveness of every backup process. Department managers must verify that proper backups are being made on all computer systems used for production business activities.

5.4 Workstation Physical Security

(1) *Equipment Theft*: Avera computer systems and Workstations must be marked with identification information that clearly indicates it is Avera Health property. Workstations that

access or store electronic Confidential Information must be specifically identified in Avera's asset management system. Periodic physical inventories will be completed by Avera Health Information Technology to track the movement of computer systems and related equipment. Users must immediately report reasonable suspicion or knowledge of equipment theft as defined in the *Device Disposal and Reuse of Electronic Storage and Media* policy.

(2) *Donation or Sale of Equipment*: Before an Avera Workstation is provided to any third party, the equipment or media must be physically inspected by Avera Health Information Technology to determine that all electronic Confidential Information has been removed in compliance with *Device Disposal and Reuse of Electronic Storage and Media* policy.

(3) *Lending Computer Systems To Others*: Users must never lend an Avera owned or managed Workstation to another individual unless that other individual is an authorized User and prior authorization was given by Avera Health Information Technology.

(4) *Custodians for Equipment*: The primary User of a Workstation is considered the custodian for the equipment. If the equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, the custodian must promptly inform his/her department manager or the Avera Health Information Technology Help Desk at 605-322-6000. With the exception of portable machines, Avera's computer systems may not be moved or relocated without the knowledge and approval of Avera Health Information Technology.

(5) *Use of Personal Equipment*: Users may not take their personally-owned computers, computer peripherals, or computer software into Avera Health owned or managed facilities for use on the Avera Network without prior authorization from Avera Health Information Technology and full compliance with all applicable policies. Users may not use their own computer systems for Avera business unless these systems have been evaluated and approved by Avera Health Information Technology. Users may not connect their personally-owned mobile devices including smartphones and smart speakers into Avera's Workstations.

(6) *Positioning Display Screens*: The display screens for all computer systems used to handle electronic Confidential Information must be positioned such that the information cannot be readily viewed through a window, by persons walking in a hallway, by persons waiting in reception, offices, and related areas or other unauthorized individuals. Position keyboards so that unauthorized persons cannot readily see Users enter passwords, encryption keys, and other security-related parameters. Users may request privacy screens from Avera Health Information Technology to assist with security measures.

(7) *Locking Sensitive Information*: When not being used by authorized Users, or when the Workstation is not clearly visible in an area where authorized Users are working, all removable storage media and portable devices containing electronic Confidential Information must be locked in secure enclosures.

6.0 Reporting:

Users must report known or reasonably suspected violations of any policy to Avera Health's Information Security Office at AHISO@avera.org or Corporate Compliance Hotline at 888-881-8395.

7.0 Violations of Policy:

Violations of any policy may expose Avera to unacceptable risk in patient care, business operations, and legal liability. Violation of this policy subjects the User to disciplinary action, up to and including loss of privileges to use Avera's Information Technology Resources and termination of employment or other relationship with Avera as well as potential for criminal and civil legal liability. *See also Avera's Administrative Policy No. 736 "Corrective Action."*

8.0 References:

HIPAA Physical Safeguards - Standard: Workstation Use: 164.310(b) (Required)

9.0 Related Documents:

Data Encryption Policy (REG09)
Device Disposal and Reuse of Electronic Storage and Media (REG14)
Technology Acceptable Use Policy (REG01)
Email Acceptable Use Policy (REG08)
Mobile Device Acceptable Use Policy (REG33)
Remote Access Policy (REG19)
Security Risk Analysis Policy (REG20)
Wireless Access Policy (REG29)
Workstation and Server Security Policy (REG30)

10. Revision History:

Rev #	Revision Summary	Submitted By	Submission Date	Approval Date	Approved By
1	New	IT Security Council	07/01/2012		
2	Updated Format	IT Security Council	05/09/2013		
3	Policy Review	IT Security Team	02/27/2017	02/27/2017	IT Security Council
4	Policy Review	IT Security Team	03/12/2018	03/12/2018	IT Security Council
5	Policy Revision	IT Security Team	11/11/2019	11/11/2019	IT Security Council

The official policy in effect is located on SharePoint under *IT Support Services – IT Policies & Training Resources*. Downloading any policy with the intent to modify the content without prior authorization from the Avera Health Information Security Officer is prohibited.

This policy was developed as a guide and is not intended to define any employment standard and does not suggest or provide contractual rights of employment. This policy should be used as a guide, however, unless prevented by law. Avera leaders may deviate from this guide to respond to individualized circumstances.