Policy Number: REG01	**Policy Category:** Information Technology
Policy Title: Technology Acceptable Use	**Effective Date:** 07/01/2012
Sponsor: Melissa Melcher	**Revision Date:** 11/11/2019
Covered Organizations: All Avera Health owned, sponsored, leased, and managed entities.	
Contact: Avera Health Information Security Office – AHISO@avera.org	

1.0 Purpose:

To establish rules for the acceptable use of Information Technology Resources within the Avera Network, either locally, remotely, or disconnected, as well as the use of personally-owned resources when connected to the Avera Network or accessing Avera's data while disconnected from the Avera Network. The rules are implemented to protect Avera's patients, employees, and entity operations.

2.0 Scope:

This Technology 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. 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.

4.0 Policy:

Avera's Information Technology Resources will be used appropriately to support our mission and values in compliance with this policy. Inappropriate use increases Avera's exposure to security risks including intrusion attacks, compromise of data or systems, interruptions of patient care and operations, and unauthorized access or use of electronic Confidential Information. Personally-owned computers and devices connected at a facility to the Avera Network, remotely accessing the Avera Network, or using Avera's Confidential Information while disconnected are subject to all Avera Health Information Technology policies.

5.0 Procedure:

5.1 General Rules for Acceptable Use:

(1) Users shall not use only authorized devices, systems, services, and networks when accessing Avera's Information Technology Resources. All Avera mobile and computing devices must be approved and managed through Avera Health Information Technology Department. Personally-owned mobile and computing devices must meet minimum security standards and be authorized by Avera Health Information Technology.

(2) Users shall have no expectation of privacy regarding your use of Information Technology Resources or information created, modified, downloaded, or otherwise stored therefrom such use. Avera authorized employees may monitor equipment, systems, and network traffic at any time.

(3) Users shall not access Confidential Information without permission or need to know due to your designated responsibilities. You may access or use such information only to the extent authorized and minimum necessary to fulfill your assigned duties.

(4) Users shall not use equipment, hardware, devices, software, services, or information to interfere with the proper operation of Avera's Information Technology Resources.

(5) Users are responsible for the security of your passwords and accounts. Do not share accounts, user names, and/or passwords with other individuals. Do not use someone else's account and password.

(6) Data, documents, and other electronic Confidential Information stored on Avera's Information Technology Resources or personal devices remains the property of Avera.

(7) Users must use extreme caution when opening e-mail attachments received from unknown senders which may contain security risks. DO NOT attempt to circumvent the security protections by opening the item on another device.

(8) Users are responsible for exercising good judgment regarding the reasonableness of personal use in accordance with Avera policies. In the absence of policy direction or for any uncertainty/question you may have, consult your supervisor, Avera Health's Information Security Officer, or Avera Health's Privacy Officer.

(9) Users should take all reasonably necessary steps to safeguard Confidential Information and prevent unauthorized access, disclosure or other use thereof.

(10) Users are responsible for using the Information Technology Resources in compliance with other Avera policies as well as federal, state, and local laws. You should review our policies and ask the Avera Health Information Security Officer if you have any questions.

(11) Users must promptly report suspicious information technology uses or messages to the Avera Health Information Security Office at AHISO@avera.org or the Corporate Compliance Hotline at 888-881-8395.

5.2 Security and Proprietary Information- Avera implements safeguards and actively monitors the Avera Network to protect the confidentiality, integrity, and availability of our Information Technology Resources. Users should be aware, however, that Avera cannot guarantee complete security.

(1) Avera, or an authorized agent on its behalf, may monitor and/or audit users' use of Avera's Information Technology Resources and the Avera Network at any time.

(2) All information should be presumed Confidential Information unless directed otherwise by authorized Avera employees.

(3) System level passwords will be changed in accordance with Avera's Password Management Policy in compliance with best practices and applicable regulations.

(4) Mobile devices are especially vulnerable to security risks to the Avera Network. Mobile devices must be encrypted prior to use with Confidential Information.

(5) All systems, computers, and devices connected to the Avera Network shall maintain up-to-date approved intrusion detection software.

5.3 Unacceptable Use Examples- Unacceptable use includes, but is not limited to, the examples provided below. The following non-exclusive list of activities are strictly prohibited:

(1) Engage in any activity that is unethical or illegal under local, state, federal or international law.

(2) Violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Avera.

(3) Copy without authorization copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Avera or the end user does not have an active license.

(4) Download or install any unauthorized software, including shareware and freeware.

(5) Intentionally introduce or attempt to introduce malicious code or programs into a device, computer, server, network, or other Information Technology Resource.

(6) Share user account password(s) with others or allow others to use any of your system accounts. This prohibition includes coworkers, leaders, family, friends, and visitors.

(7) Download, create, distribute, or transmit material or information that is in violation of discrimination, sexual harassment, hostile workplace, or other harassment or offensive conduct laws.

(8) Make fraudulent offers of products, items, or services originating from any Avera account.

(9) Intentionally contribute to, attempt to, or cause security incidents or disruptions of network communication. Security incidents include, but are not limited to, accessing data of which the User is not authorized to access or logging into a server or account that the User is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

(10) Conduct port scanning or security scanning unless prior authorization is received from Avera Health Information Technology.

(11) Execute any form of network monitoring that will intercept data not intended for the User's system unless this activity is authorized as part of the User's assigned duties.

(12) Circumvent User authentication or security of any system, network or account.

(13) Disclose Avera's electronic Confidential Information to third parties without prior approval from Avera Health's Information Security Office or Avera Health's Office of General Counsel. *See also Avera's Administration Policy No. 734, "Evaluation of Alleged Inappropriate Discloser-Policy Number"*

(14) Use Avera's Information Technology Resources in any activity that would jeopardize Avera's Internal Revenue Service (IRS) tax-exempt status for applicable entities.

(15) Violate any other policy applicable to use of Information Technology Resources.

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:

9.0 Related Documents:

Email Acceptable Use (REG08)
Internet Acceptable Use (REG13)
Workstation Acceptable Use (REG31)
Mobile Device Acceptable Use (REG33)

10.0 Revision History

Rev #	Revision Summary	Submitted By	Submission Date	Approval Date	Approved By
1	Updated Format	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 Avera Health's 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.