Policy Number: REG19	**Policy Category:** Information Technology
Policy Title: Remote Network Access	**Effective Date:** 12/15/2011
Sponsor: Melissa Melcher	**Revision Date:** 11/11/2019
Covered Organizations: All Avera owned, leased, sponsored, and managed entities	
Contact: Avera Health Information Security Office – AHISO@avera.org	

1.0 Purpose:

To maintain a secure method of network connectivity between the Avera Network and remote Users connecting through third-party and/or public networks to protect the confidentiality, integrity, and availability of Avera's Information Technology Resources.

2.0 Scope:

This Remote Network Access Policy applies to all Users of Avera Health's Information Technology Resources including all workstations, mobile devices, and other technology, whether Avera-owned or personally owned used for remote network access.

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.

Business Owner (BO) – means an Avera Manager, Director, or higher level executive-titled employee who has detailed first-hand knowledge of the (i) business need/case and objectives of the Avera region, service line, department, etc. consistent with Avera's mission and values; (ii) subject matter of the contract as applicable across Avera or a subset, including the business liability terms of the contract proposed for approval and signature; (iii) potential conflicts of interest, (iv) vendor, third party, or other party to the contract and references; (v) pre-contract involvement and approvals from necessary Avera centralized departments, committees, and councils referenced within but outside of this policy.

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.

Electronic Protected Health Information (ePHI) any PHI that is transmitted or maintained in an electronic media.

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. 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.

Multi-Factor Authentication (aka two-factor or dual-factor authentication) – means a method of authentication in which Users provide two different factors to verify themselves as a second layer of security to protect accounts and systems. Users identify themselves by providing two of the following: (i) something you know (e.g. password or personal identification number (PIN)); (ii) something you have (e.g. cryptographic identification device or a one-time token); or (iii) something you are (e.g. biometrics).

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.

Virtual Private Network (VPN) – means a data network that extends a private connection across a public network to enable Users to securely send and receive data across the public networks through the tunnel between them.

Workforce – means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity or Business Associate, is under the direct control of such Covered Entity or Business Associate, whether or not they are paid by the Covered Entity or Business Associate.

4.0 Policy:

Users are responsible to employ reasonable security measures and remain in compliance with Information Technology policies when utilizing Avera Network remote access. While connected remotely to the Avera Network, Users are responsible for preventing access by non-

authorized individuals to any Avera Information Technology Resources including electronic Confidential Information.

5.0 Procedure:

5.1 General Requirements for Avera Network Remote Access

(1) Remote network access shall only be provided to Users who have a legitimate Avera business need for remote network access to the Avera Network. Access to systems through the remote network access connection shall be only to the minimum amount of information resources necessary to perform the legitimate business need.

(2) Workstations, mobile devices, and other technology, whether Avera-owned or personally-owned, used to gain remote network access must meet Avera Health Information Technology Policies including acceptable use requirements, up-to-date malicious software protection software, additional security measures, and configuration standards. *See* Workstation Acceptable Use Policy (REG31), Mobile Device Acceptable Use Policy (REG33), Workstation and Server Security Policy (REG30), Protection from Malicious Software Policy (REG18), Wireless Network Access Policy (REG29), and additional policies.

(3) Remote network access must be secure and strictly controlled with strong passwords and encryption of both (i) the remote connection through a VPN issued by Avera; and (ii) the mobile device or workstation used to initiate the remote access. Encryption technologies used must meet Avera Health Information Technology Policy standards. *See* Data Encryption (REG09) and Password Management Policy (REG15).

(4) Multi-Factor Authentication is required for all remote network access connections to the Avera Network from a public or third party network.

(5) Generic accounts must not be used for remote network access to the Avera Network.

(6) Users shall not utilize a remote network connection to the Avera Network while being remotely connected through a VPN or other means to a second private network. Connecting Users' workstations or devices to two (2) private networks simultaneously may expose the Avera Network to additional outside environment hostile security risks.

(7) Avera Health Information Technology will periodically audit Users' remote network access sessions for network security monitoring for malicious activity including, but not limited to access from suspicious locations, network scanning, attacks on internal systems, and other activities. Avera Health Information Technology reserves the right to disable any remote network access account without prior notice to the User due to known or reasonably suspected malicious activity.

(8) Avera Health Information Technology will periodically audit Users' workstations, mobile devices, and other technology used to remotely access the Avera Network for

compliance with all Avera Health Information Technology Policies. Users are responsible to periodically review such policies to maintain compliance.

(9) Remote network access Users' accounts will be inactivated if the account hasn't been used within the last six (6) months.

(10) Users shall not circumvent any security procedures, measures, or controls for remote network access to the Avera Network.

(11) Remote network access Users are responsible to prevent unauthorized access to Avera's electronic Confidential Information. Confidential Information through a remote network access connection must be viewed privately. Users must employ reasonable security measures both physical and technical in compliance with Avera Health Information Technology policies to protect the confidentiality, integrity, and availability of Confidential Information.

5.2 Avera Remote Network Access for Workforce Members

(1) Requests for workforce member remote access to the Avera Network shall be submitted to the Avera Health Information Technology Help Desk by the User's direct supervisor through the Avera Health Centralized Ticketing System (AHCS).

(2) Avera Health Information Security Officer may terminate remote network access for Workforce members upon known or reasonably suspected security risks related to a User's remote network access account or workstation, mobile device, or other technology used for such connection.

5.3 Avera Remote Network Access for Third Parties

(1) Avera reserves the right to require a specific application for third party remote network access to the Avera Network.

(2) Business Owners may authorize remote network access for non-Workforce individuals and other third parties subject to (i) a legitimate business need for remote access; (ii) minimum necessary access to electronic Confidential Information for performance of services; and (iii) prior execution of appropriate remote network access and other required agreements (e.g. Business Associate Agreement).

(3) Requests for third-party remote network access to the Avera Network shall be submitted to the Avera Health Information Technology Help Desk by the Business Owner through the Avera Health Centralized Ticketing System (AHCS).

(4) Avera Health Information Security Officer and Chief Compliance Officer may request additional information on the legitimate business need prior to authorizing the third party remote network access. Both reserve the right to deny remote network access upon a lack of a legitimate business need; lack of required executed agreements; or other known or reasonably anticipated security risk to the Avera Network.

(5) Non-Workforce Users and other authorized third parties utilizing remote network access to the Avera Network are required to comply with all applicable Avera Health Information Technology policies related to the technology used for the connection; acceptable use activity of the User or third party while connected; and all security and privacy requirements including, but not limited to, federal and state laws and regulations.

(6) Business Owners are responsible to follow and enforce additional requirements and guidelines for remote network access for third party vendors as provided in Vendor Access Management (REG35) and other applicable policies.

6.0 Reporting:

Users must report known or reasonably suspected violations of any policy to the Avera Health Information Technology Office at AHISO@avera.org or the 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 Reference:

- Access Control: 164.312 (a)(1);
- Access Authorization: 164.308(a)(4)(ii)(B) (Addressable)

National Institute of Standards and Technology (NIST) Special Publication 800-46 R.2, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security", July 2016.

9.0 Related Documents:

Technology Acceptable Use Policy (REG01)
Workstation and Server Security Policy (REG30)
Wireless Network Access Policy (REG29)
Workstation Acceptable Use Policy (REG31)
Password Management Policy (REG15)
Mobile Device Acceptable Use Policy (REG33)
Device Disposal and Reuse of Electronic Storage Media Policy (REG14)
Vendor Access Management (REG35)

10.0 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	Added Token Section	IT Security Team	03/09/2016	03/09/2016	IT Security Team
4	Policy Review	IT Security Team	02/27/2017	02/27/2017	IT Security Council
5	Policy Review	IT Security Team	03/12/2018	03/12/2018	IT Security Council
6	Policy Update	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.