HealthShare Exchange
OF SOUTHEASTERN PENNSYLVANIA, INC.

1801 Market Street, Suite 750 Philadelphia PA, 19103 www.hsxsepa.org

Remote Access Policy

Version	Approval Date	Owner
1.0	November 11, 2019	Chief Information Security Officer

1. Purpose

To establish how HealthShare Exchange (HSX) ensures the security of remote access to the network in order to protect confidential data and information assets.

2. Scope

This policy is applicable to all employees, interns, contractors, members, participants, users, and third parties who work outside of HSX's environment, and who connect to HSX's network, systems, applications, and data, including but not limited to applications that contain HSX confidential data such as protected health information (PHI), from a remote location.

3. Policy

Remote Access Policy

- HSX shall manage and control access to its internal and external networks. Users shall only be provided with access to internal and external networks that they have been specifically authorized to use. Appropriate authentication methods shall be used to control access by remote users.
- All users who connect to HSX's networks from a remote location shall use only HSX approved and managed secure remote access technologies, as determined by the Chief Information Security Officer (CISO).
- All remote access shall use multi-factor authentication mechanisms. Any exceptions shall be documented and approved by the CISO.
- Remote access users shall be categorized into one of the following groups:
    - **Category 1**: Employees and contractors with permanent Remote Access. These individuals require 24-hour system availability and are called upon

to work remotely or who travel frequently. Category 1 access offers the same level of file, folder and application access as on-site access.

- **Category 2**: Employees and contractors with temporary Remote Access. These individuals require temporary remote access due to an extended period of time away from the office. Category 2 access is restricted to only the period of time necessary.
- **Category 3**: Third Parties offering product support and other Business Associates with access to PHI. These users require varied access to PHI depending on the application or system supported and/or accessed. A Business Associate Agreement (BAA) must be on file prior to granting Category 3 access, and all such access must be audited at least annually.

- Each user's remote access category assignment shall be documented and maintained.
- Remote access users are responsible for adhering to all of HSX's policies, not engaging in illegal activities, and not using remote access for interests other than those of HSX.
- Remote access accounts to HSX information assets by HSX vendors and business partners shall be disabled until such time as services are required and approved by HSX management. Access must be disabled once approved services are completed.
- Violation of this policy by remote access users may result in corrective disciplinary action, up to and including termination of employment and/or removal of access to HSX information assets according to the *Sanctions Policy*.
- Violation of this policy by others, including providers, providers' offices, Business Associates, and partners may result in termination of the relationship and/or associated privileges.
- Violation of this policy may also result in civil and criminal penalties as determined by federal and state laws and regulations.

Requesting Remote Access

- Remote access shall be strictly controlled and shall only be granted to employees and contractors with a defined business need, and with approval by the CISO.
- Employees and contractors shall register for a multi-factor authentication mechanism (e.g., token).
- Business Associates and other third parties (e.g. contractors, vendors) shall be granted remote access provided they have a contract or BAA with HSX which clearly defines the type of remote access permitted (e.g., stand-alone host, network server, etc.) as well as other conditions which may be required, such as virus protection software. Such contractual provisions must be reviewed and approved by the CISO before remote access shall be permitted.

- Remote access is strictly controlled and shall be made available only to Business Associates and other third parties with a defined business need, at the discretion of and approval by the CISO.
- All employees and contractors granted remote access privileges must have signed and comply with the Confidentiality Agreement kept on file with Human Resources as determined by HSX.
- Remote access accounts that have shown no activity for 90 days shall automatically be disabled. The CISO is responsible for ensuring this occurs.

Remote Security

- Connectivity from a user's remote location to HSX's network is a "user managed" service. This means that the user shall be responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees necessary for enabling their connectivity from the remote location.
- All computing devices that remotely connect to the HSX network must apply the most up-to-date anti-malware software and security patches. This shall include personally-owned computing devices (e.g., laptops, home computers, tablets, smartphones, etc.). For computing devices using a Microsoft Operating System, all HSX-endorsed Microsoft security patches must be applied and kept current.
- Remote users shall ensure that remote worksites meet security and configuration standards established by HSX. This shall include configuration of personal routers and wireless networks.
- Remote users that connect to the HSX network must configure the equipment to comply with HSX's policies.
- Malware updates and security patching must be allowed to complete, i.e., remote users may not stop the update process on HSX's computer devices or on personal computing devices.
- A host-based firewall shall be used on all computing devices connecting remotely to the HSX network and may not be disabled for any reason.
- HSX shall maintain logs of all activities performed by remote access users while connected remotely to HSX's network according to the *Audit, Logging, and Monitoring Policy*.
- System Administrators shall review remote access logs and shall use automated Intrusion Detection Systems (IDS) to detect suspicious activity.

Remote Privacy

- Only authorized users shall be permitted remote access to any of HSX's computer systems, computer networks, and/or information, and must adhere to all of HSX's policies.

- Remote users, including Business Associates and other third parties, shall log-off and disconnect from HSX's network when access is no longer required to perform job responsibilities.
- Remote users shall lock the workstation and/or system(s) when unattended so that no other individual is able to access any ePHI or other confidential data.
- Remote access users shall automatically be disconnected from the HSX network when there is no recognized activity for 15 minutes.
- Remote access users shall ensure that unauthorized individuals do not access the HSX network. At no time shall any remote access user provide their username or password to anyone, nor shall they configure their remote access device to remember or automatically enter their username and password.
- Remote access users must take necessary precautions to secure all of HSX's information assets and confidential data in their possession.
- Copying of confidential data (e.g., PHI, SSNs, PII, HSX confidential records, etc.) to removable media (e.g., hard drive, USB, CD, etc.) shall be strictly prohibited, unless HSX has granted prior approval in writing.

4. Enforcement

- HSX supervisors shall be responsible for ensuring that their staff comply with this policy.
- Each member, participant and third party shall be responsible for ensuring that their respective physicians, care managers and other staff follow this policy.
- The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the Executive Director.

5. Definitions

For a complete list of definitions, refer to the *Glossary*.

6. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA § 164.312(e)(1)

Policy Owner	Security Officer	**Contact**	Daniel.wilt@healthshareexchange.org

Approved By	Brian Wells	**Approval Date**	November 11, 2019
Date Policy In Effect	November 29, 2018	**Version #**	1.0
Original Issue Date	November 29, 2018	**Last Review Date**	November 11, 2019 September 15, 2019
Related Documents	Audit, Logging, and Monitoring Policy Business Associate Agreement (BAA) Template Confidentiality Agreement Glossary Sanctions Policy System Access Request Form		