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

Teleworking Policy

Version	Approval Date	Owner
2.0	September 12, 2019	CISO

1. Purpose

To support the security of HealthShare Exchange (HSX) by limiting teleworking activities to explicitly approved processes and circumstances.

2. Scope

This policy applies to all HSX employees and interns, co-ops and fellows.

3. Policy

Teleworking Policy:

- HSX shall allow employees, interns co-ops and fellows to telework if the employing department determines that teleworking will allow work to be performed effectively and productively.
- HSX shall implement teleworking, operational plans, procedures, and guidelines and continually update the previous to be in accordance to the industry standards.
- Teleworking is a privilege, not a benefit or a right. HSX shall have the right to terminate a teleworking arrangement at any time.
- Participation in teleworking is voluntary. Employees and interns/co-ops shall have the right to decline teleworking unless the Business Continuity Plan (BCP) has been activated, in which case HSX shall determine if teleworking from an alternate site shall be mandatory for the duration of time that the BCP is active.
- Additional insurance to address the risks of teleworking is provided through the following procedure: On an annual basis, the HSX Leadership team purchases and provides cyber security insurance for the year, ensuring HSX protection in the event of any disclosures which includes addressing any teleworking risks among other incidences and exposures.

Teleworking Activities:

- HSX shall develop and implement a teleworking policy, operational plans, procedures, a review process for teleworking requests, a teleworking agreement and teleworking security guidelines.

- Teleworking activities shall only be authorized if a schedule is submitted and approved by HSX management, if appropriate security arrangements and controls are in place, and if they comply with HSX's policies.
- Teleworkers shall receive training on security awareness, privacy, and their additional responsibilities while teleworking.
- HSX shall provide information assets for teleworking that shall only be used for HSX purposes by authorized employees, interns/co-ops and contractors. Contractors not authorized to access PHI or HSX confidential information may, upon approval by HSX CISO, may not be issued an HSX laptop for those non-confidential services.
- The use of HSX information assets by other persons (e.g., family, friends, etc.) shall be strictly prohibited. Only HSX personnel are permitted to access HSX information on devices used for HSX business.
- The teleworker must have access to suitable communication equipment to contact technical support, and technical support shall be available for assistance should any issues arise via HSX approved communications applications.
- The use of personally-owned equipment that is not under the control of HSX to conduct telework involving HSX confidential data shall be strictly prohibited except for what is allowed under the *Remote Access Policy*.
- All products of teleworking shall be backed-up within the appropriate HSX approved file storage application.
- Upon termination of teleworking activities, access rights shall be reviewed in accordance with the *Access Control Policy*.
- Upon termination of teleworking activities, all HSX information assets related to the telework shall be returned to as soon as practicable in accordance with the *Termination Policy*.
- Suitable protection of the teleworking site shall be in place to protect against the theft of information assets and the unauthorized disclosure of confidential data.
- Remote access for teleworkers shall comply with the *Remote Access Policy*.
- The Teleworking Home-Inspection Checklist has been completed and approved by HSX management which includes stipulations regarding the suitable protection of the teleworking environment in order to protect against the theft of information assets and the unauthorized disclosure of confidential data.
- Teleworker is authorized to complete all tasks and work assigned regularly with the expectation of an additional level of risk awareness to adjust working conditions and/or work products to ensure appropriate security mechanisms are in place when working remotely. In doing so, the teleworker will only access the information resources necessary and required to complete job duties.
- The teleworker shall take care to avoid the risk of overlooking by unauthorized persons especially when working with any sensitive information.
- If there has been a breach or a possible breach in security, the Chief Information Security Officer and Privacy Officer must be notified as soon as possible.

4. Procedure

Teleworking Procedures:

A. Teleworking activities shall only be authorized if appropriate security arrangements and controls are in place, and if they comply with HSX's Policies. An HSX administrator shall complete training on security awareness, privacy and teleworker responsibilities prior to commencing teleworking activities.

B. Teleworking activities are only authorized if security arrangements and controls that comply with relevant security policies and organizational requirements are in place.

C. IP addresses for authorized teleworker requiring access to AWS servers shall be whitelisted.

D. There shall be no remote access by teleworkers to HSX office network. Access to HSX AWS servers will be secured via an encrypted channel.

E. The use of personally-owned equipment that is not under the control of HSX to conduct telework involving HSX confidential data shall be strictly prohibited except for what is allowed under the Remote Access Policy. HSX retains ownership over any assets used by the teleworker.

E. The configuration of wireless network services shall be encrypted (WPA 2 at a minimum).

F. Anti-virus protection, Operating System and application patching, and host-based firewall requirements shall be consistent with HSX policies.

G. All HSX devices, documentation, and information shall not be left in public settings when the teleworker is not present and will be stored in a secure area when not in use.

H. Teleworking Site Inspection Procedure:

1. Teleworking in a home-setting:
   - Complete home inspection check-list (see Teleworking Agreement), return to HSX manager, and receive approval before teleworking commencement.
2. Teleworking in a public setting:
   - Teleworking has been authorized by HSX management.
   - The teleworker has submitted and received approval for a teleworking schedule to his/her HSX manager.
   - The teleworking area shall be quiet and private.
   - The teleworker shall keep all HSX devices, documentation and information in his/her possession at all times
   - The teleworker shall take care to avoid the risk of overlooking by unauthorized persons especially when working with any sensitive information.
   - The teleworker will only access the information resources necessary and required to complete job duties.
   - The teleworker has access to suitable communication equipment (e.g. work phone, Slack, e-mail account, etc.).

I. Teleworking activities will be audited annually by HSX supervisors and management.

Encrypted, VPN solutions (or private lines) are implemented for employee, intern/co-op, contractor or third party (e.g., vendor) remote access to the organization's network, and their access is logged.

5. Enforcement

- HSX supervisors shall be responsible for ensuring that their staff comply with this policy.
- The CISO and Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the President.

- HSX Supervisors shall be responsible for ensuring that their staff comply with teleworking requirements using one-on-one meetings, organizational lunch and learns and a signed Teleworking Agreement and security checklist.

6. Definitions

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

7. Reference

Regulatory References:

- HIPAA Regulatory Reference: HIPAA §164.310(a)(2)(i), HIPAA §164.310 (b)
- HITRUST Reference: 01.y Teleworking

Policy Owner	CISO	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	Board HSX Senior Management	**Approval Date**	September 12, 2019
Date Policy In Effect	February 23, 2016	**Version #**	2.0
Original Issue Date	June 23, 2015	**Last Review Date**	September 12, 2019
Related Documents	Access Control Policy Business Continuity Management Policy Glossary Remote Access Policy Termination Policy Teleworking Agreement, Guidelines and Checklist		