HealthShare Exchange

190 N. Independence Mall West | Suite 701 | Philadelphia PA 19106 | 215.391.4905 | www.healthshareexchange.org

Remote Work Policy and Procedures

Version	Approval Date	Owner
1.2	October 13, 2021	Chief Information Security Officer

1. Purpose

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

This remote work policy is in effect due to public health guidelines recommending work from home when feasible. There is no specified period of time for remote work arrangements for the entire HSX team. HSX will continue to monitor guidance from health officials along with the need and feasibility for continued remote work.

2. Scope

This policy applies to all employees, consultants, interns and subcontractors of HSX who work remotely.

3. Policy

Remote Work Policy:

- HSX is allowing employees, interns co-ops, fellows and consultants to work remotely.
- HSX shall implement remote work operational plans, procedures and guidelines, and continually update to maintain compliance with the industry standards.
- Additional insurance to address the risks of remote work 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 remote work risks among other incidences and exposures.

Remote Work Activities:

- Remote work activities shall only be authorized if appropriate security arrangements and controls are in place, and if they comply with HSX's policies.
- All HSX employees, interns, co-ops, fellows and consultants shall receive training on security awareness, privacy and their responsibilities concerning remote work.
- HSX shall provide information assets for remote work that shall only be used for HSX purposes by authorized employees, interns/co-ops and contractors.
- 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.
- All remote workers 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.
- All products for remote work shall be backed up within the appropriate HSX approved file storage application.
- Upon termination of remote work activities, access rights shall be reviewed in accordance with the *Access Control Policy*.
- Upon termination of remote work activities, all HSX information assets related to remote work shall be returned to HSX as soon as practical in accordance with the *Termination Policy*.
- Suitable protection of the remote work site shall be in place to protect against the theft of information assets and the unauthorized disclosure of confidential data.
- Remote access shall comply with the *Remote Access Policy*.
- The Remote Work Home Inspection Checklist has been completed and approved by HSX management which includes stipulations regarding the suitable protection of the remote work environment in order to protect against the theft of information assets and the unauthorized disclosure of confidential data.
- Remote worker 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 remote worker will only access the information resources necessary and required to complete job duties.
- Remote worker shall take care to avoid the risk of exposing information to unauthorized persons especially when working with any sensitive information.
- If there has been a breach or a possible breach in security, both the Chief Information Security Officer and the Privacy Officer must be notified as soon as possible.
- Remote worker will notify their manager if unable to work for any reason. Failure to do so will result in disciplinary action.

- Remote worker is responsible for expenses incurred at home related to work area.
- Remote Worker is responsible for any injuries or incidents that occur in the Remote Work area.

Remote Work- Availability:

- All remote workers must be available to work during HSX business hours- 8:30AM - 5:00PM Eastern Standard Time unless alternate arrangements have been formalized with their supervisor. This applies to employees residing in different time zones.
- Remote workers must be consistently available for internal team meetings, updates with their supervisor, meetings with external stakeholders (members, vendors, etc.) and to individual team members.
- Remote workers are responsible for ensuring that their communication is timely and professional.

Remote Work Location- Time Zones/Travel:

- Approval must be obtained from the supervisor prior to travel if there are plans to work during this time.
- If working while away from the primary remote work site, remote worker must ensure that appropriate security arrangements and controls are in place along with full compliance with HSX policies.
- Remote work outside of the United States is prohibited.

4. Procedures

A. Remote Work 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 remote worker responsibilities prior to commencing remote work activities.

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

C. Unique IDs shall be given to each remote worker to access the organization's networks and systems via a remote connection, which will be secured via an encrypted channel.

D. The use of personally owned equipment that is not under the control of HSX to conduct remote work 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 remote worker.

E. The configuration of wireless network services shall be encrypted (WPA2 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 remote worker is not present and will be stored in a secure area when not in use.

H. Remote Work Site Inspection Procedure:

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

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

J. Additional insurance to address the risks of remote work is provided through the following procedure:

1. On an annual basis, the HSX Leadership Team purchases and provides cyber security for the year, ensuring HSX protection in the event of any disclosures which includes addressing any remote work risks among other incidences and exposures.

5. Enforcement

Both the CISO and the Privacy Officer shall be responsible for enforcing compliance with this procedure under the direction of the President & CEO.

HSX supervisors shall be responsible for ensuring that their staff comply with this procedure via a one-on-one meeting, or an organizational Lunch & Learn. Upon completion of training, all personnel will be required to sign an attestation document.

6. Definitions

For definitions, please refer to the HSX glossary

7. References

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

Responsible Owner:	Chief Information Security Officer	**Contact: email**	Brian.wells@healthshareexchange.org
Approved By:	HSX Leadership	**Version #**	1.2
Current Approval Date:	October 13 , 2021	**Review Dates:**	October 13, 2021 October 17, 2020 March 19, 2019 April 1, 2017
Date Procedure to go into Effect:	April 1, 2017		
Related Documents:	Glossary		