**Teleworking Procedures**

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>March 19, 2019</td>
<td>Privacy Officer</td>
</tr>
</tbody>
</table>

1. **Purpose**

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

2. **Procedure Scope**

This policy applies to all employees, consultants, interns, and subcontractors of HSX that telework.

3. **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. A unique ID shall be given to each teleworker to access the organization’s network 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 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. HSX SharePoint shall be used for internal file sharing. Jira may be used for technical file sharing related to a ticket.

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

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

K. Additional insurance to address the risks of teleworking 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 teleworking risks among other incidences and exposures.
4. Enforcement

The CISO and Privacy Officer shall be responsible for enforcing compliance with this procedure under the direction of the Executive Director. HSX supervisors shall be responsible for ensuring that their staff comply with this procedure via a one-on-one meeting, or an organizational lunch and learn. Upon training completion, all personnel will be required to sign an attestation document.

5. Definitions

For definitions, please refer to the HSX glossary

6. References

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

<table>
<thead>
<tr>
<th>Responsible Owner:</th>
<th>Privacy Officer</th>
<th>Contact: email</th>
<th><a href="mailto:Don.Reed@healthshareexchange.org">Don.Reed@healthshareexchange.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By:</td>
<td>Board</td>
<td></td>
<td>1.1</td>
</tr>
<tr>
<td></td>
<td>HSX Senior Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current Approval Date:</td>
<td>March 19, 2019</td>
<td>Review Dates:</td>
<td>October 28, 2023</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>December 24, 2022</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>October 21, 2021</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>October 17, 2020</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>March 19, 2019</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>April 1, 2017</td>
</tr>
<tr>
<td>Date Procedure to go into Effect:</td>
<td>April 1, 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Documents:</td>
<td>Glossary</td>
<td>Teleworking Policy</td>
<td></td>
</tr>
</tbody>
</table>
7. Appendix A

Teleworking Home-Inspection Checklist

- All doors and windows have functional locking mechanisms.
- The teleworker has access to a secure container/setting within household with an additional securing mechanism (e.g. lockable desk drawer, safe, etc.)
- The teleworker has access to suitable communication equipment (e.g. work phone, Slack, e-mail account, etc.).
- Teleworker shall use HSX SharePoint for internal file sharing, or Jira as may be required.
- The configuration of wireless network services is encrypted (WPA 2 at a minimum).
- HSX materials and equipment are in a secure place that can be protected from damage and misuse.
- Workspace accommodates workstation, equipment, and related material.
- Desk and chair are at the appropriate height.
- The teleworker will only access HSX Information assets via an HSX managed laptop.
- The teleworker will continue to be subject to all HSX policies and procedures.
- The teleworker’s work location is free from hazards.
- The teleworker will maintain safe working conditions.
- Teleworkers are prohibited from sending or accessing sensitive information over public Wi-Fi.
- Anti-virus protection, operating system and application patching, and host-based firewall requirements are consistent with HSX policies (e.g. passwords, virus protection, and personal firewalls).
- The teleworking area is quiet and private.
- The teleworker will only access the information resources necessary and required to complete job duties.
- The teleworker may not copy any PHI to external media not approved by the company.
- No family member or visitor has access to HSX devices, documentation, or information.

I commit to the following teleworking schedule dedicated to HSX-work hours with the understanding that these are my standard hours and that there will be required additional or different hours based upon my job responsibilities:

<table>
<thead>
<tr>
<th></th>
<th>8:30-12:00 PM</th>
<th>1:00PM-5:00PM</th>
<th>Other (please write in)</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tuesday:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wednesday:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thursday:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friday:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
I, _____________________, verify that all of the above is true and accurate to the full extent of my knowledge. I realize that, if any of the above is proven to be false, teleworking privileges may be revoked and access rights will be received in accordance to the Access Control Policy. Date: ____________

I, _____________________, as HSX CISO confirm receipt of this document. Date: ____________