Mobile Device Protection

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3</td>
<td>September 24, 2021</td>
<td>Chief Information Security Officer</td>
</tr>
</tbody>
</table>

1. Purpose of Procedure

The purpose of this procedure is to develop a process for the protection of mobile computing devices (i.e. laptops and smartphones). Devices are to be protected at all times by access controls, usage restrictions, connection requirements, encryption, virus protections, host-based firewalls, secure configuration, and physical protections.

2. Procedure Scope

All workforce members, including third parties, who may have access or exposure to the HSX’s data must follow this procedure and sign an attestation document acknowledging compliance. All personnel will be trained on the risks, controls implemented, and personal responsibilities by reviewing all HSX policies and procedures upon hire, and before the release of access and/or exposure to HSX data.

3. Procedures

Upon hire, all employees, interns, contractors, members, participants, users, and third parties who may have access or exposure to HSX information assets will be required to have all personal (BYOD) mobile computing devices connected to HSX information assets checked by their HSX Supervisor, or CISO to ensure that the device is compliant.

Laptop encryption is enforced upon device provisioning and monitored centrally by Sophos. Sophos regularly updates mobile code protection, including anti-virus and anti-spyware.

All employees, interns, contractors, members, participants, users, and third parties who may have access or exposure to HSX information assets on a smartphone will be required to

1) Install the InTune Mobile Device Management (MDM) system and associated profile(s) on their smartphone and set up at 6-digit pin and lock screen as authentication before email can be accessed on a mobile device

2) Download the Comp Portal application on smartphones to access HSX approved applications including Outlook, Slack, LastPass, Duo, Jira and SalesForce.

3) The MDM will require full device encryption before HSX applications can be accessed.

4) Install the authorized applications using the InTune Comp Portal application.
In the event of a lost or stolen mobile device, InTune will be used to remote wipe all HSX authorized applications.

Access to HSX systems and servers that support HSX HIE and MarketStreet services shall be restricted to only those HSX authorized devices that are whitelisted by the HSX CISO.

HSX prohibits the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) by the following procedure:

1. On Laptop Devices:
   a. Sophos is installed on every HSX employee’s laptop upon issue date (see New Laptop Setup Procedure). Sophos ensures that security implements controls without a tamper password which may only be obtained through the Technical Operations Team (the administrator).
   b. Any violations of these controls and/or security recommendations sends a warning to the Sophos Software which is monitored by the Technical Operations Team.

2. On Mobile Devices
   a. The MDM will prevent “jail-breaking” or other forms of unauthorized changes. If found, HSX CISO will be notified and appropriate actions will be taken to remediate and address with the mobile device owner.
   b. HSX shall configure Sophos and browsers to restrict / block mobile code from running (ActiveX Controls, postscript, Shockwave movies, Flash animations, etc.)
   c. HSX shall regularly update mobile code protection, including anti-virus and anti-spyware.

Users of authorized mobile and/or BYOD devices are required to conform to HSX privacy and confidentiality policies. In the event of litigation, HSX shall have the right to e-discovery and any legal holds that may be required with respect to mobile devices.

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

5. References

<table>
<thead>
<tr>
<th>Responsible Owner:</th>
<th>Chief Information Security Officer</th>
<th>Contact: email</th>
<th><a href="mailto:Brian.Wells@healthshareexchange.org">Brian.Wells@healthshareexchange.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By:</td>
<td>Brian Wells</td>
<td>Version #</td>
<td>1.3</td>
</tr>
</tbody>
</table>
| Current Approval Date: | September 24, 2022 | Previous Review Dates | October 28, 2023  
|                    |                                  |                | December 21, 2022                
|                    |                                  |                | September 23, 2022               |
| Date Procedure to go into Effect: | October 8, 2021  
October 16, 2020  
March 19, 2019  
April 1, 2017 |
|----------------------------------|------------------|
| Related Documents:              | Audit Logging and Monitoring Policy  
Endpoint Protection Policy  
Glossary  
Incident Management Policy  
Virus and Malware Protection Policy |
|                                 | September 24, 2022 |