Encrypting and Securing Devices Procedure

1. Purpose of Procedure
To support the security of HealthShare Exchange (HSX) by encrypting sensitive data and controlling physical security.

2. Procedure Scope
This policy applies to all employees, consultants, interns, and subcontractors of HSX that work in the HSX office or deal with ePHI and sensitive business information.

3. Procedure
Encrypting the startup disk for a Mac OS:

1. Choose Apple menu ( ) > System Preferences, then click Security & Privacy.
2. Click the FileVault tab.
3. Click the Lock button, then enter an administrator name and password.
4. Click “Turn On FileVault”.

<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>Chief Information Security Officer</td>
</tr>
</tbody>
</table>
If other users have accounts on the Mac, each user must type in their password before they will be able to unlock the disk. For each user, click the “Enable User” button and enter the user's password.
Encrypting and Securing Devices Procedure

The User accounts that added after turning on FileVault are automatically enabled.

**Encrypting a USB flash drive in MacOS:**
1. Insert USB drive into computer
2. Open Finder and locate the USB drive on the left side of the window
3. Right click on the USB drive and click “Encrypt”
4. When prompted, select a password for the USB drive
5. Select a password hint that will aid in retrieving the password
6. Ensure that the MacBook is connected to a charger and begin encryption
7. Give encrypted USB drive to designated HSX staff who will place the drive in a secure location

**Encrypting a Windows OS:**
1. Sign in to Windows with an administrator account.
2. Go to Start, enter encryption, and select Change device encryption settings from the list of results.
3. Select Manage BitLocker, select Turn on BitLocker, and then follow the instructions.

**Encrypting an iPhone:**
Apple automatically encrypts their devices since iOS 8 (2014) with the implementation of a security code or fingerprint. To add one (or both) of the two:

1. Head to Settings
2. Select Touch ID & Passcode (or Passcode for older devices without a fingerprint sensor)
3. Click on the Turn Passcode On option
4. Enter a strong passcode or password

**Encrypting an Android Device:**
Google’s Nexus phones and tablets and most devices with Android 6.0 Marshmallow (Galaxy S7 and Galaxy S7 Edge) are encrypted by default with the addition of a security code or fingerprint. To add one (or both) of the two:

1. Head to **Settings**
2. Click **Security**
3. Select **Screen Lock**
4. Create a security code

**Encrypting an older Android device (Galaxy S6, Moto X Pure):**

The user must manually encrypt an older device such as the Galaxy S6 or the Moto X Pure. The steps to do so are as follows:

1. Ensure the phone is plugged in (the process could take up to an hour to complete).
2. To create a passcode:
   a. Head to **Settings**
   b. Click **Security**
   c. Select **Screen Lock**
   d. Create a security code
3. Head to **Settings**
4. Select **Security**
   a. On a Galaxy S6:
      i. Select **Lock Screen and Security**
      ii. Select **Other Security Settings**
5. Click on **Encrypt phone**

**Encrypting an Android device’s internal SD card:**

1. Head to Settings
2. Select Security
3. Encrypt External SD card
4. Click Enable
Physical Security:

1. Note: This is required for any mobile device storing encrypted or unencrypted ePHI or one with access to sensitive information that does not first require HITRUST compliant authentication (multifactor authentication over an approved secure and encrypted protocol without local storage).

2. Before beginning, please view the procedure called “Procedure: Sensitive Media Protection Outside Controlled Areas” if this device ever leaves the office.

3. The device must be retrieved from safe storage in the office. Ask the Technical Operations Lead or the CISO to retrieve it. They will keep track of this request and however long the device is in your possession.

4. Note the date and time of retrieval for your own records.

5. Always keep this device on your person or in secure, locked storage. An extreme level of caution and vigilance should be used if the device is explicitly approved by the CISO to be unencrypted.

6. When you are ready to return the device, give it to the Technical Operations Lead or the CISO so they can store it and note its return. Update your own records.

4. Enforcement

- HSX supervisors shall be responsible for ensuring that their staff comply with security measures in this process.
- The CISO and Privacy Officer shall be responsible for enforcing compliance with this process under the direction of the Executive Director.

5. Definitions

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

6. References

Regulatory References:

- HITRUST References: 01.x Mobile Computing and Communications, 09.o Management of Removable Media, 09.q Information Handling Procedures
### Encrypting and Securing Devices Procedure

<table>
<thead>
<tr>
<th>Process Owner</th>
<th>Technical Operations</th>
<th>Contact</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>Approval Date</td>
<td>March 19, 2019</td>
</tr>
<tr>
<td>Date Process in Effect</td>
<td>May 8, 2017</td>
<td>Version #</td>
<td>1.1</td>
</tr>
<tr>
<td>Original Issue Date</td>
<td>May 8, 2017</td>
<td>Last Review Date</td>
<td>October 27, 2023</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>December 10, 2022</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>October 5, 2021</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>October 18, 2020</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>March 19, 2019</td>
</tr>
<tr>
<td>Related Documents</td>
<td>Access Control Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Media Protection Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sensitive Media Outside Controlled Areas Procedure</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>