Transmission Security and Encryption Policy

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>January 16, 2019</td>
<td>Chief Information Security Officer</td>
</tr>
</tbody>
</table>

1. Purpose
The transmission of PHI using secure and encrypted means is required for HealthShare Exchange (HSX) to ensure we protect the information being shared.

2. Scope
This applies to all employees, contractors, members, participants, users, vendors, and third parties that transmit PHI with HSX.

3. Policy
- HSX strives to contract with appropriate vendors to protect against unauthorized access to PHI that is being transmitted over an electronic communication network through implementation of “reasonable and appropriate” security measures to ensure that electronically transmitted ePHI is not improperly modified without deletion until disposed of.
- HSX shall require its contracted vendors to implement encryption, on a routine basis for any and all PHI accessed or transmitted through the exchange, including but not limited to PHI transmitted through email.
- HSX shall ensure that the confidentiality and integrity of electronic commerce are maintained.
- HSX shall ensure electronic commerce and online transactions are checked to determine if they contain covered information.
4. Procedures

1. The Security Officer together with the respective departments and management shall be responsible on an ongoing basis for identifying, evaluating, implementing, monitoring and updating cyber security mechanisms as necessary and appropriate to reasonably safeguard the confidentiality, integrity and availability of all IT and data from cyber security threats and vulnerabilities and minimize the impact of such threats and vulnerabilities on business operations. The Security Officer shall identify all key personnel responsible for implementation of cyber security controls. The Security Officer, along with key personnel, shall assess, identify and implement additional security mechanisms in the following areas [specify in greater detail the current activity controls in place and being put in place]:

2. If it is not “reasonable and appropriate” to implement encryption, HSX shall document the reasons why and a reasonable alternative here:
   - It is not “reasonable and appropriate” to implement such procedures because: (insert description here)
   - The reasonable alternative that will be used to implement such procedures is: (insert description here)
   - The reasonable alternative that will be used to implement such procedures is: (insert description here)

5. Enforcement

   - The CISO shall be responsible for enforcing compliance with this policy under the direction of the President.

6. Definitions

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

7. References

   Regulatory References:
   - None
<table>
<thead>
<tr>
<th><strong>Policy Owner</strong></th>
<th>Chief Information Security Officer</th>
<th><strong>Contact</strong></th>
<th><a href="mailto:Brian.wells@healthshareexchange.org">Brian.wells@healthshareexchange.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approved By</strong></td>
<td>Board HSX Management Team</td>
<td><strong>Approval Date</strong></td>
<td>January 16, 2019</td>
</tr>
<tr>
<td><strong>Date Policy In Effect</strong></td>
<td>December 24, 2013</td>
<td><strong>Version #</strong></td>
<td>1.2</td>
</tr>
</tbody>
</table>
| **Original Issue Date** | December 24, 2013 | **Last Review Date** | January 16, 2019 
September 15, 2019 |
| **Related Documents** | Glossary                            |             |                                    |