Removal of Access Procedures

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>3/19/2019</td>
<td>Chief Information Security Officer</td>
</tr>
</tbody>
</table>

1. Purpose of Procedure

To establish HealthShare Exchange (HSX) requirements for managing and controlling access to information assets and information services in support of compliance with legal regulations (e.g., HIPAA) and to protect and lower risk to business operations.

To ensure that HSX’s information assets and information services are properly protected against unauthorized access, while meeting the access requirements for all authorized users.

To ensure that only appropriate and specifically-authorized Members and Participants gain access to the HSX Health Information Exchange (HIE).

To establish the procedures for employee termination and removal of access.

2. Procedure Scope

All employees, interns, contractors, members, participants, users, and third parties who may have access or exposure to HSX information assets are required to comply with this process.

This process covers access to all enterprise data regardless of whether that data is stored on or provided via HSX information assets or on a third-party-hosted service or equipment.

This process is restricted to the HSX definition of “acceptable use” meaning solely for care coordination and treatment based upon the HSX Participatory Agreement (PAR). HSX issued hardware must only be used per previous definition by HSX employees, interns, contractors, members, participants, users, and third parties.

3. Procedures

A. Changes and removal of access privileges are completed via the following procedure:

1. Changes to Access
   - After any personnel changes, (promotion, transfer, demotion or termination of employment), the CISO reviews the access rights granted.
   - System Administrators are notified by an HSX Senior Manager when an individual’s access rights change (e.g. termination or change in a position)
Information Technology makes the necessary changes within 24 hours of being notified.

A change to access privileges is completed via a Change Management Ticket which may only be submitted by an organization's ESA.

Evaluated internally (90 days depending on audit logs)

2. **Removal of Access**

If a temporary account was created, the HSX Support Desk will place time stamp on how long until account expires within the HSX single sign on application which will not exceed 365 days and will reflect the duration needed for functionality.

A Change Management ticket for the removal of access is created

The HSX Support Desk adheres to the following procedure to remove a user:

- Log in to the environment that the user has an account (development, test, and/or production)
- Log into the Mirth single sign on
- Look user up by e-mail address
- Click into user account
- Set status to "deactivate."
- A confirmation e-mail sent to ESA and the ESA confirms that the user has been removed.

**B. If an HSX Employee has been terminated, the following procedures will be followed:**

1. If an HSX employee is scheduled to be terminated, HSX Senior Management makes a request via e-mail to the Technical Operations Team and detail the appropriate timeline for the following events (to be completed within a maximum of 24 hours of the decision):
   
   - The HSX Senior Management would notify the HSX Support Desk and Human Resources, copying the CISO.
   - The HSX Support team follows the user removal of access procedure detailed above.
   - Human Resources contacts building security to remove physical access rights and, if necessary, to escort and remove the user if necessary.

2. During the termination process, HSX Senior Management shall ensure the return of all HSX assets, including but not limited to equipment, all corporate documents, manuals, information stored on electronic media, credit cards, and any other assets known to have been provided to the employee or contractor,

**C. When company property is returned, the following procedure is completed to deleting data from hard-drives prior to property transfer, exchange, or disposal/surplus.**

1. All files contained on the company property are reviewed and, if deemed essential, documented within OneDrive or the appropriate application.

2. The company property is returned to the CISO.
3. The CISO removes all files.
4. If the device is being retired, the CISO physically damages the hardrives beyond repair.

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>1.1</td>
</tr>
<tr>
<td>Current Approval</td>
<td>March 19, 2019</td>
<td>Previous</td>
<td>October 28, 2023</td>
</tr>
<tr>
<td>Date:</td>
<td></td>
<td>Approval/Review Date:</td>
<td>December 18, 2022</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Date:</td>
<td>October 9, 2021</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>October 20, 2020</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>January 19, 2017</td>
</tr>
<tr>
<td></td>
<td>Date Procedure to go into Effect:</td>
<td>January 19, 2017</td>
<td></td>
</tr>
<tr>
<td>Related Documents:</td>
<td>Access Control Policy</td>
<td>Create a New User Process</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change Management Process</td>
<td>Governance Process</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>