Access Control Plan

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>September 20, 2022</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).

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. **Use of data is considered per the following process:**

      1. A need for access or use is recognized by the HSX Board and a workgroup to fulfill that need is created.
      2. The workgroups creates a charter specifying their purpose and designating how the HSX data will be used.
      3. After which, the Governance Process is followed.
B. **Access authorizations are segregated per the following stipulations:**
   1. Access Requests are controlled by the HSX Engagement and Adoption team
   2. Access Approvals follow the HSX Change Management Process
   3. Access Provisioning is controlled by the HSX Support Desk

C. **Default Accounts to HSX Information Systems**
   1. Default accounts are not to be used or left unchanged
      - Default accounts shall either be disabled or changed to meet HSX requirements
      HSX shall validate that default accounts are disabled or revised prior to, or immediately after, promoting the system or application to production

D. **Computer login banners** shall be displayed stating that the computer is private, unauthorized access is prohibited, the conditions and acceptable use of access, and the privacy/security notices. Users shall be required to acknowledge and accept the banner in order to log-in. refer to Attachment 1 – Login Banner for wording and requirement to click Accept before logging in,

E. **The creation of new users follows the following process:**
   - For all users requiring access to the HSX network must first have duo, multi-authentication installed on their mobile device and added to their account. The HSX network is only able to be accessed through HTTPS (which uses SSL encryption). Node Authentication was reviewed but does not work in the HSX environment, instead, all connections are through the internet via SSL.
     1. New Regular User Procedure:
        - For external systems/users:
          - The HSX Engagement and Adoption Team will send a survey (via SurveyMonkey) to the ESA (entity security administrator) as only the ESA is permitted to request (or provision) a new account.
          - The ESA will document the following: name, e-mail, title, which level of access needed (minimum necessary) and verify their identity.
          - The above documentation is submitted to the HSX Support Desk via an HSX Support Ticket.
            - A support ticket or request for a user account needs to be submitted per role/use of HSX services, separated by application. A ticket is submitted per individual to the HSX support desk but accounts may be linked if the user's role necessitates it (as evaluated by the change management team).
            - The documentation submitted is evaluated per the following:
              - Only the minimum access necessary is permitted
              - The Title of individual warrants requested role; the title of the representative matches the level of request.
The role is created by the HSX help desk and the credentials are emailed out securely; an individual account is needed to be created per user role with a unique log in per individual (traceable back to the user).

- For internal systems (e.g. Office 365, project management tool, salesforce accounts, all user accounts are validated and confirmed by HSX Technical Operations.
  - An onboarding meeting is scheduled to identify and validate the user, create the user account, and ensure all instructions for the hardware tokens are received directly by the new user.
  - Each user will have an unique individual account, which is traceable back to the said user.

- The new regular user role is monitored for access on a 90-day schedule by the HSX Security and Operations Team via the HSX single sign-on application system which controls all three separate environments.
  - 90 process to evaluate each account (still necessary to have activated)
  - See Technical Operations Checklist for details of the process. If an account is deemed no longer necessary, a Change Management Ticket is submitted (see Change Management Procedure) and the account deactivated (see removal of access procedure below).
  - If not in use, the user account is deactivated.

2. Administrator User Procedure follows the above regular procedure with the following additions:

- The Technical Operations and Security Team performs a specialized training for the higher privileges
- The Change Management Process is completed.
- If the Change Management ticket is approved, the user receives an account created with two-factor identification (and trained on using the two-factor identification).
- The role is monitored for access on a 30-day basis and evaluated to determine if access is still required.
  - See Technical Operations Checklist for details of the process. If an account is deemed no longer necessary, a Change Management Ticket is submitted (see Change Management Procedure) and the account deactivated (see removal of access procedure below).
  - If not in use, the user account is deactivated.
All privileged account users will download Google Authenticator and/or Microsoft Authenticator from the Apple App store

Systems requiring MFA will provide a scannable QR code to be scanned by the privileged account user using the appropriate authenticator app setup screens

When logging on to a system or application requiring MFA, the user will look up the MFA code from the appropriate Authenticator app and enter it into the MFA field on the login screen.

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

1. After any personnel changes, (promotion, transfer, demotion or termination of employment), the CISO reviews the access rights granted per the ninety (90) and thirty (30) day process detailed above.

2. 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 Support ticket to support@healthshareexchange.org which may only be submitted by an organization’s ESA.
   - Evaluated internally (ninety (90) days depending on audit logs)

3. 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 support ticket for the removal of access is sent to The HSX Support Desk at support@healthshareexchange.org
   - 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.
G. Emergency Access privileges are granted via the following procedure:

1. No regular users will be granted emergency access; thus, only emergency administrator access will be evaluated.
3. If the request is approved, the above procedure
   - Only be evaluated as an administrator (emergency admin access)
   - Have to follow change management policy (emergency change management request)
   - If approved, follow standard procedure for activating admin account (see above).
4. If an emergency account is created, the HSX Support Desk sets the number of days until account automatically deactivates within the HSX single sign on application to "1" or 24 hours.

H. 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 Desk follows the user removal of access procedure detailed above (in Procedure D part 2).
   - Human Resources contacts Ten Penn Center Security to remove physical access rights and, if necessary, to escort and remove the user.

I. A clear statement of the business requirements for controls needed to protect access to data or services is provided to users and service providers via the following procedure:

1. A statement with HSX terms and conditions of access is contained within the initial request of information for access (via SurveyMonkey).
2. A statement with HSX terms and conditions of access is displayed when logging into the HSX query portal. Every time a user logs into the HSX portal, a comment box displaying what the portal is used for and indicates that it should be used as minimum necessary.
3. A statement with HSX terms and conditions of access is displayed when accessing a particular patient's chart and the user must agree and acknowledge that they have the correct permissions to access the privileged information.

J. Upon user registration and de-registration, at a minimum, HSX communicates relevant policies to users and requires signed acknowledgement, through the following process:

1. For external users:
o HSX Members agree to HSX policies and processes through their Participatory agreement and by which all users have acknowledged review of and attest to HSX policies and processes above.

o Following signing the document, the new user administrator training process detailed above will be followed.

2. For internal members (all HSX employees, consultants and interns):
   o All internal members will complete the HSX HIPAA training session (HIPAA) and after which, sign and attest obey by the HSX policies and procedures
   o All internal members therefore attest to understand and cooperate with the training set forth.
   o If any additional access is needed, a Confidentiality Agreement is signed by any employee, intern, and/or contractor prior to being granted access to the information assets.

K. Group, shared or generic accounts and passwords (e.g., for first-time log-on) are not used; unique IDs capable of tracing activities to the responsible individual are created per the above process (part A).

   1. By default, shared accounts are not created nor permitted by the HSX Support Desk.
   2. Exceptions may be pled to the Change Management team and follow the Change Management Procedure. Examples of where this may be permitted are the following:
      o Where there is a clear business benefit
      o Where user functions do not need to be traced and additional accountability controls are implemented.
   3. If the Change Management Ticket is approved, the HSX Support Desk will create the account using the new user process detailed above (in Procedure A of this document).

L. The list of authorized users of any information assets is maintained by the following process:

   1. All user information is maintained through HSX's single sign-on application, which is automatically updated as soon as an account is created/terminated/changed.
   2. Reports from the application are generated to document all user accounts, security roles, and the current status of user.

M. The HSX requires user identification for any transaction that has information security implications and obtains identification through the ESA, who is tasked with the responsibility of ESA to identify and make any requests for any transaction having information security implications.

N. HSX limits the access rights to application functions per the following process:

   1. HSX has developed default security roles based off of the minimum necessary required need /usage.
2. The menus only show sections which are available to the user within application. Any unavailable menus/actions are hidden from the user interface.

O. Outputs from application systems handling covered information are limited to the minimum necessary and sent only to authorized terminals/locations per the following process:
   1. The only role capable of exporting clinical information the provider or administrator of the system.
   2. Providers may export by sending a Direct message which is securely encrypted, directly into the HER system.
   3. Administrators are HSX employees having access and capability of extracting information. All administrators must comply with HSX policies for allowed storage (see Data Handling, Labeling, and Storage Policy and Procedure)
      o Before any export occurs, a Change Management ticket must be submitted and approved (see Change Management Process).

P. All actions and requests require identification and authentication before permission is granted. Access to HSX systems or applications without identification and authentication is expressly prohibited.
   • HSX shall implement a screen timeout after 15 minutes of inactivity that requires authentication to access after such time

Q. Remote administrations sessions are secured via the following process:
   1. Every user is secured through SSL certs for all logins and access rights.
   2. Administrators are required to use two factor identification and authorization.
   3. Remote access to HSX cloud hosted information systems is restricted to whitelisted laptops
   4. Remote access to the HSX office network is blocked at the firewall.

R. The review of access to HSX's network connections uses the following procedure which is completed quarterly at a minimum:
   1. Technical operations review the audit logs for all logins by both actual application (e.g. Mirth) as well as Duo for source identification and geographic location.
   2. If the Technical operations team discovers any suspicious activity, the CISO will be contacted for next actions.
   3. The CISO and HSX Leadership team will evaluate the next steps needed to be taken to address the suspicious activity.
S. Bring Your Own Device (BYOD) and or company owned devices are configured to require an automatic lockout screen, and the requirement is enforced through technical controls by the following procedure:

1. Any device that is either BYOD or company owned that contains, hosts or has any HSX applications, accounts or data on the device is required to either install Com Portal MDM solution by Office 365 or Sophos Security depending on the operating system of the device.
2. The settings are defaulted to ensure that the required lockout screen is applied and can be tracked through the Office 365 or the Sophos Portal if not compliant.

T. Covered or critical information is protected when using internal or external (e.g. USPS) mail services by the following procedure:

1. HSX Administrative staff obtains tracking stickers form the United States Postal Service on an annual basis.
2. All mail that is sent out containing covered information goes through the Administrative Assistant to ensure that the package/letter is labeled with the tracking sticker correctly.
3. The administrative assistant records the tracking label within a spreadsheet used for all tracking purposes.
4. On a daily basis, the Administrative Assistant checks the USPS website using the tracking number to confirm the package/letter status and whereabouts until the package/letter has been delivered.
5. The confirmed delivery is documented within the spreadsheet and archived for seven years.

U. Access to Protected Health Information (PHI)

1. HSX access to PHI shall be limited to HSX workforce members and contracted vendors requiring access to PHI in the performance of their roles and responsibilities.
2. The HSX approved list of its workforce members is defined by job titles requiring access to PHI. Support vendors will only receive physical or logical access for support purposes when necessary, and with management approval.
3. Approved workforce member job titles are Software Engineer, Integration Engineer, Chief Technology Officer, Chief Information Security Officer, Opt-Out Coordinator, Security Analyst, Technical Support Analyst, and contracted vendors with executed Business Associate Agreements.

V. Users who perform privileged functions use separate accounts when performing those privileged functions:

1. For HSX, privileged accounts are defined as the delegation of authority over an HSX system.
2. A privileged account allows a user to perform an action such as the ability to create, read or delete files, accounts, or settings.
3. It has the ability to alter the hardened configuration of a system.
4. In order to obtain a privileged account, it must be granted by the technical operations team and proceed through change management.
5. A separate account than other used is created for privileged actions.
6. Anytime a user applies an action, that action must be approved by the Change Management procedure and should use the designated privileged account.

W. Access rights from an application to other applications are controlled through the following procedure:
1. HSX has a strong Technical Policy that does not allow any occurrence of any single sign on allowable/acceptable business applications.
2. By doing this, authentication to the systems are controlled independently and separate through application portals.
3. In order to access a single system, a support ticket must be submitted to HSX Support Desk.
4. If a request is a privileged or administrative account, this must be submitted to the change management group. If approved, the credential or the account is created only for the application requested. In order to grant access to multiple systems, multiple requests must be made, and require the HSX Support Desk to grant access via multiple portals.
5. HSX does maintain a naming convention for account names and uses randomized passwords but never a single sign on system.

X. HSX monitors for unauthorized connections of mobile devices through the following procedure:
1. The HSX Privacy Officer will monitor the current devices attached to the wifi on a quarterly basis to ensure that a list of all devices on the wifi is created.
2. The Privacy Officer will then check each device on the list to ensure the device is compliant with the Access Control Policy and the Mobile Computing Device Security Policy.

4. Access to HSX Network Equipment
HSX network equipment shall be maintained in a secure environment with limited access controlled by the HSX CISO.
5. Definitions

Within the context of access control, increased risk is defined if there is an elevated likelihood of a large negative impact on HSX Business Operations.

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

6. References

<table>
<thead>
<tr>
<th>Responsible Owner:</th>
<th>Technical Operations</th>
<th>Contact: email</th>
<th>Version #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By:</td>
<td>Brian Wells</td>
<td></td>
<td>1.2</td>
</tr>
<tr>
<td>Current Approval Date:</td>
<td>September 20, 2022</td>
<td>Review Dates::</td>
<td>October 26, 2023</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>December 24, 2022</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>September 20, 2022</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>October 2, 2021</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>October 19, 2020</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>December 30, 2019</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>March 19, 2017</td>
</tr>
<tr>
<td>Date Procedure to go into Effect:</td>
<td>September 20, 2022</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Documents:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Policy</td>
</tr>
<tr>
<td>Create a New User Process</td>
</tr>
<tr>
<td>Change Management Process</td>
</tr>
<tr>
<td>Governance Process</td>
</tr>
<tr>
<td>Glossary</td>
</tr>
<tr>
<td>Mobile Computing Device Security Policy</td>
</tr>
</tbody>
</table>
The HSX computer you are about to log in to is private. Unauthorized access is prohibited.

By logging in, you acknowledge and accept the following terms:

This is a reminder that HSX computers, communication systems, email, Internet access and assigned software are provided to employees for the purpose of conducting HSX business.

While use of the computer, e-mail and Internet is intended for job-related activities, incidental and occasional brief personal use is permitted within reasonable limits, so long as it does not interfere with the employee's work.

Computer, Internet and e-mail usage may be monitored by HSX, including retrieving and reading e-mail messages, texts and any communication used for HSX business. Therefore, e-mail messages and other uses of the company's computers are not confidential. Even though you may be issued a private password or other private access codes or permissions, you should have no expectation of privacy in relation to any HSX systems, networks or equipment.

HSX specifically prohibits the use of computers (including email, Internet access, texts and network permissions) in ways that are disruptive, offensive to others or harmful to morale. Any communication that could be construed as harassment or shows disrespect for others, defames or slanders others, or otherwise harms another person or business is strictly prohibited.

Employees and contractors should immediately notify their supervisor or manager of any violations. Deliberate misuse of any HSX communication networks will be subject to disciplinary action, up to and including termination of employment. Please refer to the End User Computing Device Security policy for additional guidelines and requirements for computing and multimedia equipment.