HealthShare Exchange
OF SOUTHEASTERN PENNSYLVANIA, INC.

1801 Market Street, Suite 750 Philadelphia PA, 19103 www.healthshareexchange.org

Termination Policy

Version	Approval Date	Owner
1.1	November 8, 2018	Chief Information Security Officer

1. Purpose

To ensure HealthShare Exchange (HSX) owned information assets are retrieved, and logical and physical access is revoked or updated, when an employee's, intern's, contractor's, member's, participant's, user's, or third party's employment, contract, or agreement is terminated, or in certain cases when their roles and/or responsibilities are significantly altered upon a change of employment status (e.g., job transfers, job re-grading, restructuring, etc.).

2. Scope

This policy applies to all employees, interns, contractors, members, participants, users, and third parties regardless of physical location.

The three ways below are the way HSX participants could access the Clinical Data Repository (CDR):

- **Query Portal:** HSX Mirth Results has a Query Portal that users can be given a user account and password. They will be able to access this through https://query.hsxsepa.org
- **Single Sign On (SSO):** HSX has the ability to provide the member a way to login to the query portal by passing credentials (SAML 2.0) by using a secure automatic login for the user who HSX issues user accounts and passwords
- **XCA or XDS Connections:** HSX has the ability to support the IHE standards and connect using the XCA or XDS protocols this provides the deepest integration into the member EHR and provides access to the Clinical Data Repository.

3. Policy

HSX shall develop and implement a termination policy and procedures

- Terminations and changes of job position resulting in changes of roles and responsibilities (e.g., job transfers, job re-grading, restructuring, etc.) shall be communicated to the HSX Chief Information Security Officer (CISO) or designee in a timely manner by Human Resources or the appropriate point of contact of the terminating entity.
- Whenever there is a change in employment status or responsibilities, logical and physical access shall be reviewed and updated or revoked as necessary according to this policy and the *Access Control Policy*.
- Responsibilities for removing or updating logical and physical access shall be clearly defined and assigned.
- All employees, interns, contractors, members, participants, users, and third parties shall return any HSX information assets and property in their possession upon termination of their employment, contract, or agreement.
- It is the responsibility of HSX's CISO or appropriate designee to ensure that all HSX information assets have been purged from terminated resources computer equipment.

Voluntary Termination

- The HSX CISO shall make arrangements to transfer all HSX files and email messages to the HSX network prior to the employee's, contractor's, or third party's departure.
- HSX shall explicitly maintain ownership of confidential data.
- The CISO shall determine whether to close the email account and put an auto responder in place or transfer the email account to another employee or contractor. The CISO will make their decision within 24 hours of the effective date of voluntary termination.
- All other accounts shall be disabled within 24 hours according to the *Access Control Policy*.
- The employee, contractor, member, participant, user, and third parties shall return all HSX property (e.g., information assets, documents, credit cards, access cards, media, removable media, business mobile computing devices, etc.) prior to departure.
- Members shall notify HSX when access is no longer required. Members that do not log in to their HSX account for 90 days shall have their account locked and rendered inactive.

Involuntary Termination

- President and/or direct supervisor will communicate involuntary terminations immediately and where possible in advance of the actual termination event. Human Resources needs to be made aware of the situation.
- HSX shall immediately terminate physical and logical access rights whenever there is increased risk (e.g., in the case of serious misconduct).
- The CISO in concert with Human Resources shall retrieve all HSX property (e.g., information assets, documents, credit cards, access cards, media, removable media, business mobile computing devices, etc.) during the termination process.
    - In the case of death or accident, Human Resources shall make every effort to retrieve HSX property in a timely and compassionate manner.
- The CISO shall immediately secure all files and email messages.
- HSX shall explicitly maintain ownership of confidential data and intellectual property.
- HSX shall preserve all materials of legal significance.
- The CISO shall determine whether to close the email account and put an auto responder in place or transfer the email account to another employee or contractor. The CISO will make their decision prior to, and no later than immediately upon, involuntary termination.
- The CISO shall determine whether to close all other accounts of the involuntarily terminated individual according to the *Access Control Policy* or to transfer the accounts to another employee or contractor temporarily for purposes of preserving forensic investigation results.
- Termination procedures shall allow for immediate escorting off site, if necessary.

Revocation of Access Rights

- The access rights of all employees, contractors, members, participants, users, and third parties shall be removed upon termination of their employment, contract or agreement, or adjusted upon a change of employment (e.g., job transfers, job re-grading, restructuring, etc.) in accordance with this policy and the *Access Control Policy*.
- Upon termination or changes in employment for employees or contractors, physical and logical access rights and associated materials (e.g., passwords, access cards, keys, etc.) are removed or modified to restrict access within 24 hours.
- Changes of employment or other workforce arrangement (e.g., transfers) shall be reflected in removal of all access rights that were not approved for the new employment or workforce arrangement.
- Access changes due to personnel transfer shall be managed effectively. Old accounts shall be disabled after 90 days after non-use for any particular application.

- The access rights that shall be removed or adapted include physical and logical access, keys, identification cards, IT systems and application, subscriptions, and removal from any documentation that identifies them as a current member of the organization.
- Access rights to information assets and facilities shall be reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors including:
    - Whether the termination or change is initiated by the employees, contractors, members, participants, users, and third parties, or instead by management.
    - The underlying reason for the termination.
    - The current responsibilities of the employees, contractors, members, participants, users, and third parties involved.
    - The value of HSX information assets currently accessible to the employees, contractors, members, participants, users, and third parties.

Email Access Revocation

- System administrator will ensure that HSX email accounts are deactivated upon termination of employment, contract, agreement, or other workforce arrangement, or if the email account is no longer sponsored, unless otherwise allowed under this policy.
- On the date of termination, HSX email accounts shall expire unless a temporary extension has been requested by the CISO following an assessment of information security and institutional risks (e.g., legal exposure, reputational, access to HSX enterprise data, etc.) that could potentially result should the account be extended.

4. Enforcement

- The Chief Information Security Officer (CISO) and the Privacy Officer shall be responsible for enforcing compliance with this policy under the direction of the President.
- HSX Member and Participant organizations are responsible for ensuring that when they have terminations their termination process includes revoking logical access to HSX. Also, HSX Member and Participant organizations need to ensure that when there is a change in the responsibilities of a staff member or employee that no longer warrants logical access to HSX that such logical access is revoked.

5. Definitions

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

6. References

Regulatory References:

- HIPAA Regulatory Reference: HIPAA §164.308 (a)(3)(ii)(A), HIPAA §164.308 (a)(3)(ii)(B), HIPAA §164.308 (a)(3)(ii)(C), HIPAA §164.308 (a)(4)(i), HIPAA §164.308 (a)(4)(ii)(B), HIPAA §164.308 (a)(4)(ii)(C), HIPAA §164.308 (a)(5)(ii)(C), HIPAA §164.308(a)(3)(ii)(C), HIPAA §164.308(a)(3)(ii)(C), HIPAA §164.312(a)(2)(i), HIPAA §164.312(a)(2)(ii)
- HITRUST Reference: 02.g Termination or Change Responsibilities, 02.h Return of Assets, 02.i Removal of Access Rights
- PCI Reference: PCI DSS v3 8.1.3

Policy Owner	Security Officer	**Contact**	Daniel.wilt@hsxsepa.org
Approved By	Board HSX Senior Management HSX Privacy and Security Workgroup	**Approval Date**	November 8, 2018
Date Policy In Effect	June 18, 2015	**Version #**	1.1
Original Issue Date	June 18, 2015	**Last Review Date**	November 8, 2018
Related Documents	Access Control Policy Glossary Mobile Device Security Policy Third Party Risk Management Policy		