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

Data Retention and Archiving Policy

Version	Approval Date	Owner
1.1	December 13, 2018	Chief Information Security Officer

1. Purpose

This policy addresses the retention and destruction of documents and other records, both in hard copy and electronic media ("documents").

Purposes include (a) retention and maintenance of documents necessary for the proper functioning of the organization as well as to comply with applicable legal requirements; (b) destruction of documents which no longer need to be retained; and (c) guidance for the Board of Trustees, officers, and HealthShare Exchange (HSX) employees with respect to their responsibilities concerning document retention and destruction.

2. Scope

This policy covers the responsibilities of HSX Board members, employees, interns, contractors, members, participants, users, and third parties with respect to maintaining and documenting the storage and destruction of the organization's documents. The President shall ensure that there is a report to the Board of Trustees regarding the Data protections covered under this policy, as the Board of Trustees maintain the ultimate direction of management.

3. Policy

The Chief Information Security Officer (CISO) shall be responsible for documenting the actions taken to maintain and/or destroy organization documents and retaining such documentation.

The CISO may also modify the Document Retention Schedule from time to time as necessary to comply with law and/or to include additional or revised document categories as may be appropriate to reflect organizational policies and procedures.

HSX employees, interns, contractors, members, participants, users, and third parties shall be familiar with this policy, shall act in accordance therewith, and shall assist the President and CISO, as requested, in implementing it.

HSX employees, interns, and contractors, shall be responsible to produce specifically identified documents upon request of management, if the person still retains such documents. In that regard, after each project in which an HSX employee, intern or contractor has been involve it shall be the responsibility of the CISO to confirm whatever types of documents the individual retained and to request any such documents which the President and/or the CISO feels will be necessary for retention by the organization.

In particular instances, the Administrator may require that the contract with a consultant and/or third party specify the particular responsibilities of the consultant and/or third party with respect to this Policy.

Suspension of Document Destruction; Compliance:

HSX has a duty to preserve (or halt the destruction of) documents once litigation, an audit or a government investigation is reasonably anticipated. Therefore, if the President becomes aware that litigation, a governmental audit or a government investigation has been instituted, or is reasonably anticipated or contemplated, the President shall immediately order a halt to all document destruction under this Policy, communicating the order to all Board members, employees, interns, contractors, members, participants, users, and third parties affected in writing. The President may thereafter amend or rescind the order only after conferring with legal counsel. If any Board member or staff member becomes aware that litigation, a governmental audit or a government investigation has been instituted, or is reasonably anticipated or contemplated, with respect to the organization, and they are not sure whether the President is aware of it, they shall make the President aware of it.

Failure to comply with this Policy, including, particularly, disobeying any destruction halt order, could result in possible civil or criminal sanctions. In addition, for employees it could lead to disciplinary action including possible termination under the Sanctions and Termination policies.

Electronic Documents; Document Integrity:

Documents in electronic format shall be maintained just as hard copy or paper documents are, in accordance with the Document Retention Schedule. Due to the fact that the integrity of electronic documents, whether with respect to the ease of alteration or deletion, or otherwise, may come into question, the CISO shall attempt to establish standards for document integrity, including guidelines for handling electronic files, backup procedures, archiving of documents, and regular checkups of the reliability of the system; provided, that such standards shall only be implemented to the extent that they are reasonably attainable considering the resources and other priorities of the organization.

Privacy:

It shall be the responsibility of the Privacy Officer under the direction of the President and , in consultation with legal counsel, to determine how privacy laws will apply to the organization's documents from and with respect to employees, interns, contractors, members, participants, users, and third parties ; to establish reasonable procedures for compliance with such privacy laws; and to allow for their audit and review on a regular basis.

Emergency Planning:

Documents shall be stored in a safe and accessible manner. Documents which are necessary for the continued operation of the organization in the case of an emergency shall be regularly duplicated or backed up and maintained in an off-site location. The CISO under their direction of the President shall develop reasonable procedures for document retention in the case of an emergency.

Document Creation and Generation:

The Administrator shall discuss with staff the ways in which documents are created or generated. With respect to each employee or organizational function, the Administrator shall attempt to determine whether documents are created which can be easily segregated from others, so that, when it comes time to destroy (or retain) those documents, they can be easily culled from the others for disposition. For example, on an employee-by-employee basis, are e-mails and other documents of a significantly non-sensitive nature so that they might be deleted, even in the face of a litigation hold with respect to other, more sensitive, documents? This dialogue may help in achieving a major purpose of the Policy -- to conserve resources -- by identifying document streams in a way that will allow the Policy to routinely provide for destruction of documents. Ideally, the organization will create and archive documents in a way that can readily identify and destroy documents with similar expirations.

Document Retention Schedule:

Periods are suggested but are not necessarily a substitute for counsel's own research and determination as to appropriate periods.

Accounting and Finance

Document Type	Retention Period
Accounts Payable	Seven (7) Years

Document Type	Retention Period
Accounts Receivable	Seven (7) Years
Annual Financial Statements and Audit Reports	Permanent
Bank Statements, Reconciliations and Deposit Slips	Seven (7) Years
Canceled Checks – Routine	Seven (7) Years
Canceled Checks – Special **Such as loan repayment**	Permanent
Credit Card Receipts	Three (3) Years
Employee Business Expense Reports Documents	Seven (7) Years
General Ledger	Permanent
Interim Financial Statements	Seven (7) Years

Contributions Gifts Grants

Document Type	Retention Period
Contribution Records	Permanent
Documents Evidencing Terms of Gifts	Permanent
Grant Records	Seven (7) Years After End of Grant Period

Corporate and Exemption

Document Type	Retention Period
Articles of Incorporation and Amendments	Permanent
Bylaws and Amendments	Permanent

Document Type	Retention Period
Minute Books - Including Board and Committee Minutes	Permanent
Annual Reports to Attorney General and Secretary of State	Permanent
Other Corporate Filings	Permanent
IRS Exemption Application (Form 1023 or 1024)	Permanent
IRS Exemption Determination Letter	Permanent
State Exemption Application (if applicable)	Permanent
State Exemption Determination Letter (if applicable)	Permanent
Licenses and Permits	Permanent
Employer Identification (EIN) Designation	Permanent

Correspondence and Internal Memoranda

Hard copy correspondence and internal memoranda relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document to which they relate.

Document Type	Retention Period
Hard copy correspondence and internal memoranda relating to routine matters with no lasting significance	Two (2) Years
Correspondence and internal memoranda important to the organization or having lasting significance	Permanent Subject to Review

Electronic Mail (Email) to or from the organization

Electronic mail (emails) relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document to which they relate but may be retained in hard copy form with the document to which they relate.

Document Type	Retention Period
E-mails considered important to the organization or of lasting significance should be printed and stored in a central repository.	Permanent Subject to Review
E-mails not included in either of the above categories	Twelve (12) Months

Electronically Stored Documents

Electronically stored documents (e.g., in pdf, text or other electronic format) comprising or relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document which they comprise or to which they relate but may be retained in hard copy form (unless the electronic aspect is of significance).

Document Type	Retention Period
Electronically stored documents considered important to the organization or of lasting significance should be printed and stored in a central repository (unless the electronic aspect is of significance).	Permanent Subject to Review
Electronically stored documents not included in either of the above categories	Two (2) Years

Employment, Personnel and Pension

Document Type	Retention Period
Personnel Records	Ten (10) Years After Employment Ends
Employee Contracts	Ten (10) Years After Termination
Retirement and Pension Records	Permanent

Insurance

Document Type	Retention Period
Property, D&O, Workers' Compensation and General Liability Insurance Policies	Permanent
Insurance Claims Records	Permanent

Legal and Contracts

Document Type	Retention Period
Contracts, Related Correspondence and Other Supporting Documentation	Ten (10) Years After Termination
Legal correspondence	Permanent

Management and Miscellaneous

Document Type	Retention Period
Strategic Plans	Seven (7) Years After Expiration

Document Type	Retention Period
Disaster Recovery Plan	Seven (7) Years After Replacement
Policies and Procedures Manual	Permanent

Property – Real, Personal and Intellectual

Document Type	Retention Period
Property deeds and purchase/sale agreements	Permanent
Property Tax	Permanent
Real Property Leases	Permanent
Personal Property Leases	Ten (10) Years After Termination
Trademarks, Copyrights and Patents	Permanent

Tax

Document Type	Retention Period
Tax Exemption Documents and Correspondance	Permanent
IRS Rulings	Permanent
Annual Information Returns – Federal and State	Permanent
Tax Returns	Permanent

4. Procedures

None

5. Enforcement

- This policy will be enforced by the Chief Information Security Officer (CISO) under the direction of the President. The CISO shall supervise and coordinate the retention and destruction of documents pursuant to this Policy and particularly compliance with the Document Retention Schedule.

6. Definitions

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

7. References

Policy Owner	Security Officer	**Contact**	Daniel.wilt@healthshareexchange.org
Approved By	HSX Board HSX Leadership	**Approval Date**	December 13, 2018
Date Policy In Effect	January 17, 2014	**Version #**	1.1
Original Issue Date	January 17, 2014	**Last Review Date**	December 13, 2018
Related Documents	Glossary		