190 N. Independence Mall West | Suite 701 | Philadelphia PA 19106 | 215.391.4905 |
www.healthshareexchange.org

Data Retention and Archiving Policy and Procedure

Version	Approval Date	Owner
1.3	December 13, 2019	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, including data stored in the Health Information Exchange Systems ("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. The retention periods within the tables below shall meet or exceed the retention periods found in Appendix A – Federal Records Retention Guidelines - of this policy.

Accounting and Finance

Document Type	Retention Period
Accounts Payable	Seven (7) Years
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

Document Type	Retention Period
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
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) is not to be utilized to store important documents or confidential HSX information. Such documents and information from those emails shall be stored either in an appropriate folder on OneDrive or printed and stored in a central locked repository. Those documents shall then be retained in accordance with the related retention schedules identified within this policy.

Document Type	Retention Period
Email retention configuration is set to:	2 years and then move to Archive

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
Access Rights and Responsibilities Documentation	Minimum of Six (6) Years after Termination of Access
Strategic Plans	Seven (7) Years After Expiration
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

Personal Health Information

HIPAA requirement is to retain required documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. HIPAA requirements preempt State laws if they require shorter periods. Your State may require a longer retention period. The HIPAA requirements are available at 45 CFR 164.316(b)(2). However, the Commnwealth of Pennsylvania has more stringent retention requirements and, therefore, preempt HIPAA retention requirements. The current PA code 28 Pa. Code § 115.23 through Register Vol. 50, No. 6, February 8, 2020 Section 115.23 - Preservation of medical records**(a)** Medical records, whether original, reproductions or microfilm, shall be kept on file for a minimum of 7 years following the discharge of a patient.**(b)** If the patient is a minor, records shall be kept on file until his majority, and then for 7 years or as long as the records of adult patients are maintained.

HITRUST requirements go even further than any state or federal requirements as noted in the table below.

Document Type	Retention Period
Accounting of Disclosures Documentation	Permanent
Records of disclosures for treatment, payment, and healthcare operations	Permanent

Document Type	Retention Period
Personal Health Information	Minimum of fifty (50) years following the death of the individual

4. Procedures

- The CISO shall supervise and coordinate the retention and destruction of documents pursuant to this Policy and particularly compliance with the Document Retention Schedule.
- The CISO shall supervise and coordinate the retention and archiving or destruction of electronically stored information pursuant this Policy and particularly compliance with the Document Retention Schedule.
- The CISO shall monitor for any revisions to regulatory requirement and maintain the Document Retention Schedule in accordance with such changing regulatory requirements
- Any requested exceptions to this policy shall be submitted in writing via the HSX Policy Exception Form to the CISO.
    - The CISO will review such request and evaluate its appropriateness and alignment with company and regulatory requirements and document the decision on the form.
    - The CISO shall communicate the decision to the requestor and senior HSX management and, if approved, open a change management ticket with the Policy Exception Form attached. The CISO shall also monitor the execution.
    - All Policy Exception Forms shall be retained by the CISO.

5. Enforcement

- This policy will be enforced by the Chief Information Security Officer (CISO) under the direction of the President.

6. Definitions

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

7. References

Policy Owner	Chief Information Security Officer	**Contact**	Brian.Wells@healthshareexchange.org
Approved By	HSX Board HSX Leadership	**Approval Date**	December 13, 2019
Date Policy In Effect	January 17, 2014	**Version #**	1.2
Original Issue Date	January 17, 2014	**Last Review Date**	December 6, 2022 October 5, 2021 October 17, 2020 September 15, 2019 December 13, 2019
Related Documents	Glossary		

190 N. Independence Mall West | Suite 701 | Philadelphia PA 19106 | 215.391.4905 |
www.healthshareexchange.org

Appendix A – Federal Record Retention Guidelines

Federal Record Retention Guidelines

g·Neil

Record	Period of Retention	Applicable Law	Suggested Form/Folder
Age Discrimination in Employment Act (ADEA)			
Job Posting Job Advertisements	1 year	29 CFR 1627.3(b)(1)(vi)	Store in Job-File Folder
Job Applications	1 year (includes seasonal and temporary workers)	29 CFR 1627.3(b)(1)(i)	Application for Employment Long Application for Employment Short
Solicited Resumés (including records pertaining to the failure or refusal to hire any individual)	1 year	29 CFR 1627.3(b)(1)(i)	Store in Job-File Folder
Unsolicited Resumés	Not required to be kept, but recommended as good business practice.		
Screening Tests	1 year for employers with 100 or fewer employees. Employers with over 100 employees: though regulations do not specify time, it is safe to say at least 1 year	29 CFR 1627.3(b)(1)(iv) 29 CFR 1607.15 (A)(1)	HR Assessments – employment test
Drug Test Results for General Industry	1 year after action taken	29 CFR 1627.3(b)(1)(v)	Store in Confidential Employee Medical Records Folder
Result of Physical Exams	1 year	29 CFR 1627.3(b)(2)(v)	Store in Confidential Employee Medical Records Folder
Hiring, promotion, demotion, transfer, selection for training, layoff, recall, or discharge of any employee	1 year after action taken	29 CFR 1627.3(b)(1)(ii)	Job Application, Performance Review, Payroll Status Change, Separation Notice, Exit Interview, Separation Agreement
Payroll Records	4 years for tips and total wages	29 CFR 1627.3(a)	Store in Payroll Records Folder. W-4, W-2, 1099
Employee Records including name, address, date of birth, occupation, rate of pay, compensation per week	3 years (4 years under FICA)	29 CFR 1627.3(a)	Document on and Store in Confidential Employee Record Folder
Records or Charges of Discrimination and any personnel records relevant to a pending charge	Until final disposition	29 CFR 1627.3(b)(3)	Confidential Employee Records folder
Benefit Plans	at least 1 year after termination of plan	29 CFR 1627.3(6)	
Job orders submitted to employment agency	1 year	29 CFR 1627.4(a)(1)(iii)	Job File/Folder
Department of Transportation (DOT)			
Drug Test Results for Transportation Industry	1-5 years after action taken	49 CFR 382.401	Store in Confidential Employee Medical Records Folder
Equal Employment Opportunity Commission (EEOC)			
Request for Reasonable Accommodations	1 year after the record made or 1 year after the action taken, whichever is later.	29 CFR 1602.14	Request for Reasonable Accommodations
Hiring, promotion, demotion, transfer, selection for training, layoff, recall, or discharge of any employee	1 year after record made or 1 year after action taken, whichever is later.	29 CFR 1602.14	Job Application, I-9, Performance Review, Payroll Status Change, Separation Notice, Exit Interview, Warning Notice, Separation Agreement
EEO-1	Most recent year report kept on file	29 CFR 1602.7	EEO-1 Summary Report
Termination Records	1 year from termination date	29 CFR 1602.14	Payroll Status Change, Separation Agreement, Exit interview

Federal Record Retention Guidelines

g·Neil

Record	Period of Retention	Applicable Law	Suggested Form/Folder
Employee Polygraph Protection Act (EPPA)			
Polygraph Test	3 years from the date the polygraph test is conducted	2 USCA § 1314 3 USCA § 414 29 USCA § 2002	Confidential Employee Record Folder
Employee Retirement Income Security Act (ERISA)			
Benefit Plans	6 years	29 USC 1027	
Federal Insurance Contribution Act (FICA)			
Payroll Records	4 years (3 years under ADEA) for occupation, rate of pay, compensation earned by each employee.	FICA Reg § 316001-1(e)(2)	Store in Payroll Records Folder or Confidential Employee Record Folder
Fair Labor Standards Act (FLSA)			
Child Labor – verification of age for minors	3 years	29 CFR 516.2, 516.5	Store in Confidential Employee Record Folder
Employment Contracts	3 years	29 CFR 516.5(b)(4)	Store in Confidential Employee Record Folder
Payroll Records	4 years – payroll records, certificates, collective bargaining agreements, contracts, plans, trusts.	29 CFR 516.5	Store in Payroll Records Folder, W-4, W-2, 1099
Employee evaluations, seniority systems, wage rates, merit systems, collective bargaining agreements	3 years	29 CFR 516	Performance Review
Family and Medical Leave Act (FMLA)			
FMLA Documentation	3 years after leave ends	29 CFR 825.500(b)	Request for FMLA Leave, Company Response, Physician Certification, Payroll Status Change, Absence Report, FMLA Tracker, Store in Employee FMLA Folder
Federal Unemployment Tax Act (FUTA)			
Unemployment Tax	4 years from the tax due date or tax payment whichever is greater	26 CFR 31.6001-1(e)(2)	
Immigration Reform and Control Act (IRCA)			
I-9 Forms and additional verification information	Employers with more than 10 employees at any time during the last calendar year: 3 years following the end of the year to which they relate.	8 USC 1324(b)(3)(A)(B)	I-9 Form or I-9 Compliance Kit
Occupational Safety and Health Act (OSHA)			
OSHA Forms related to injuries and illnesses	Employers with 10 or more employees: 5 years following the end of the year to which they relate.	29 CFR 1904.33	Accident Illness Report, OSHA 300A, OSHA Form 300
Medical exams and records related to or indicating employee exposure to toxic substances or otherwise harmful physical agents	30 years after termination of employment	29 CFR 1910.1020(I)	Store in Confidencial Employee Medical Records Folder
Record concerning measurement of employee noise exposure	2 years	29 CFR 1910.95(m) (3)(i)	Confidential Employee Record Folder

For more information regarding any of the suggested forms, contact G.Neil at 800.999.9111 or shop online at www.gneil.com

g·Neil LABOR LAW