Your Health Idaho

Records Retention and Destruction Policy

June 12, 2026

APPROVAL

This policy is adopted as a policy of the Idaho Health Insurance Exchange doing business as Your Health Idaho (YHI) by approval of YHI's board and in accordance with Idaho Code Section 41-6105(1).

APPROVED

_____ DATE:_____

Executive Director
YHI

DATE	DOCUMENT VERSION	REVISION DESCRIPTION	AUTHOR
6/16/2017	V1.0	Board Approved and Policy Implemented	Matt Fuhrman
4/25/2018	V2.0	Updated for Annual Review	Lowell Beaudoin
5/13/2019	V3.0	Updated for Annual Review	John Christensen
4/30/2020	V4.0	Updated for Annual Review	Matt Fuhrman
4/30/2021	V4.01	Updated for Annual Review	Matt Fuhrman
4/30/2022	V4.02	Updated for Annual Review	Matt Fuhrman
4/28/2023	V4.03	Updated for Annual Review	Matt Fuhrman
4/30/2024	V4.04	Updated for Annual Review	Matt Fuhrman
4/30/2025	V4.1	Updated for ARC-AMPE and Annual Review	Matt Fuhrman
4/30/2026	V4.11	Updated for Annual Review	Matt Fuhrman

TABLE OF CONTENTS

1. PURPOSE

The Idaho Health Insurance Exchange doing business as Your Health Idaho (YHI) has legal responsibility for equipment, technology, and data (collectively, the “Information System”). This Policy establishes how YHI will provide guidance with respect to: (i) the retention of records and; (ii) the destruction of records maintained by YHI. YHI Public Records Policy should be referenced along with this policy, when dealing with potential disclosure of public records.

2. BACKGROUND

YHI must maintain the YHI Information Security and Privacy Program that satisfies the requirements for an “Information Security Program” under the Acceptable Risk Controls for ACA, Medicaid, and Partner Entities (ARC-AMPE) established by the Centers for Medicare and Medicaid Services (CMS), United States Department of Health and Human Services. CMS established the ARC-AMPE controls in collaboration with other key stakeholders and based on the National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53).

3. SCOPE

This Policy applies to the Information System and all who connect to the Information System either logically or physically.

4. COORDINATION AMONG ORGANIZATION ENTITIES

4.1. YHI STAFF TRAINING

YHI’s Talent staff will coordinate and support personnel vetting, authorization, and training to implement this Policy.

4.2. VENDOR CONTRACTS

YHI’s agreements with third parties involving the Information System must include compliance with this policy directly or by reference.

4.3. ADAPTATION BY BUSINESS UNITS

Business units within YHI may supplement this Policy by additional policies, procedures, and standards, but this Policy will govern and supersede any policies, procedures, or standards adopted by a YHI business unit.

5. COMPLIANCE

This Record Retention and Destruction policy outlines the main required aspects for the retention and destruction of records maintained by YHI. This Policy and the underlying privacy and security controls govern YHI’s responses to any issues relating to the retention and destruction of records maintained by YHI.

YHI expressly reserves all rights and remedies available to enforce this Policy or address a breach of this Policy. Without limiting YHI's rights and remedies, YHI may limit access to the Information System, use appropriate means to safeguard Information System integrity, and ensure continued delivery of services to users. In support of these objectives, YHI may take actions that include, but are not limited to:

- Monitoring communications across YHI network services
- Monitoring actions on the Information System
- Scanning the Information System for privacy and security vulnerabilities
- Disconnecting any portion of the Information System that YHI deems to have become a privacy and security hazard
- Restricting the Information System from access by people, devices, and other systems and across network resources

5.1. COMPLIANCE MEASUREMENTS

YHI Privacy and Security team will verify compliance to this policy through various methods, including but not limited to: periodic walk-throughs, video monitoring, business tool reports, and internal and external audits.

5.2. EXCEPTIONS

Any exception to the policy must be reviewed by YHI's Privacy and Security Officer (PSO) and approved by the Executive Director (ED) in advance.

5.3. NON-COMPLIANCE

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. ROLES, RESPONSIBILITIES, AND MANAGEMENT COMMITMENT

6.1. YHI EXECUTIVE DIRECTOR

The YHI ED is ultimately responsible for privacy and security within the organization. The ED ensures appropriate oversight and resources are made available to implement and operate the YHI Security and Privacy Program. The ED signs off on privacy and security policies. The ED conducts an annual review of the adequacy and effectiveness of the Security and Privacy Program.

6.2. YHI PRIVACY AND SECURITY OFFICER

The PSO, who is designated by the Chief Information Officer (CIO) and approved by the ED, is responsible to direct the development, implementation, and maintenance of the YHI Security and Privacy Program and for the privacy and security of YHI data and Information Systems. The

PSO will report directly to the CIO with the ability to elevate issues or concerns directly to the ED or Chair of the Board.

The PSO will be the primary advisor to YHI on privacy and security matters and the primary representative for YHI on these matters to external organizations. As such, the PSO is expected to stay informed of evolving regulations, statutes, threats, risks, technology, and recognized best practices and to regularly coordinate with counterparts at CMS, NIST, and other security authorities.

The PSO is responsible for the development, implementation, and maintenance of operational practices consistent with the Security and Privacy Program and its associated implementation documents.

The PSO will review and approve YHI's "Plan of Action and Milestone (POA&M)", as described in the ARC-AMPE standards.

The PSO is a job function that may be incorporated within another job function.

6.3. YHI CHIEF INFORMATION OFFICER

The YHI CIO is responsible for ensuring adequate resources are made available to the YHI Security and Privacy Program. The CIO will periodically review the status of the Security and Privacy Program and the associated performance metrics.

7. POLICY MAINTENANCE

At least once every 365 days, the PSO shall oversee a process by which this Policy is (i) reviewed, (ii) updated to reflect changes in YHI's business, administrative, or technical environments, or applicable federal or state laws and regulations, and (iii) disseminated to all parties who must comply with this Policy. Policies will be reviewed by YHI's Governance Committee, approved by Idaho's Governor appointed Board and signed into effect by YHI's ED.

8. POLICY REQUIREMENTS

8.1. CUSTODIAN RESPONSIBLITIES

The PSO shall designate The Custodian for YHI and its departments. The Custodian shall have the following duties and responsibilities:

- Plan, formulate, and prescribe basic files management and records destruction policies, standards, and procedures, in accordance with this Policy.

- Develop, disseminate, and coordinate Records maintenance, retention and destruction procedures, or computer assisted retrieval programs to meet current and long term needs of YHI.

- Train other personnel in the fundamentals of records management and their roles in the records management program.

- Implement destruction that is required by the Policy.

- Periodically monitor compliance with this Policy and applicable Regulations governing privacy and security of Personally Identifiable Information (PII) and Protected Health Information (PHI).

- Perform audit and reporting duties in accordance with this Policy, including reports to Board of Directors or applicable Committee of the Board of Directors annually regarding the records inventory and immediately upon breach of privacy or security of any PII or PHI.

8.2. RETENTION OF RECORDS

- Inventory of Records. The Custodian shall maintain a log of YHI Records, including the following information:

    - Title of Records: Include category or subject matter of Records or group of Records, as accurately as practicable.

    - Location of Records: Include general location regarding where the Records are stored, and whether the Records are maintained on site or off site.

    - Storage Medium: Include information regarding the media type, including electronic, paper, microfilm, etc., and whether there are multiple copies and mediums for the Record or group of Records.

    - Time Periods Covered: Indicate the period of years covered by the Records.

- Retention Periods: Records shall be maintained in paper or electronic format for a period of ten (10) years. The retention period for Non-Essential Records shall be determined by the Custodian, in consultation with legal counsel as appropriate, based on the following (in descending order of priority):

    - Statutes and regulations: For certain records, federal and state statutes and regulations establish mandatory record retention periods. Applicable statutes and regulations shall be considered for any Record. Importantly, the ARC-AMPE privacy and security controls require certain documents containing PII to be maintained for ten (10) years from the date the document was created or the last effective date, whichever is later. The Regulations require certain Records regarding qualified health plan data to be retained for ten (10) years.

    - Contracts: Third parties and vendors may require that records be retained for certain periods as part of their contracts. The violation of such a contract provision may constitute breach of contract. Any applicable contract shall be considered in determining the retention period for any Record.

    - Statutes of limitations: If the foregoing standards do not require a longer retention period, records should normally be retained for at least the statute of limitations period for claims to which the records may relate. For example, the general

statute of limitations in Idaho is 4 years subject to certain tolling provisions, including Idaho's 6-year tolling limit for minors or incompetents. See Idaho Code §§ 5-224 and -230. For contracts, the general statute of limitations is 5 years. The statute of limitations for most government fraud and abuse claims is generally 6 years.

- Medium for Records: Records may be maintained in paper files or in boxes clearly marked with the contents of the files, in accordance with CMS ARC-AMPE privacy and security controls. Electronic Records may be maintained electronically as further described in Section 8.3 of this Policy. After three years, Non Essential Records shall be electronically scanned and stored in a location with the proper data retention settings for its type of data. Paper copies will be destroyed in accordance with the Media Protection Policy.

- Pending or Threatened Litigation or Investigation: The records retention or destruction policy should be suspended immediately for any Records relevant to any threatened or pending government investigation or litigation. The improper destruction of such Records can result in serious civil and criminal penalties ranging from the loss of evidence necessary to prove or defend against a claim to tort liability for spoliation of evidence to severe federal criminal penalties. The Custodian must approve the destruction of any Records relating to pending, past, or threatened investigations or litigation prior to destruction thereof.

- Historical or Archival Records: If required by state law, Public Records deemed to have historical or archival value may need to be either transferred to the State Archive or retained by the office of record in accord with the standards established by the State Archivist.

8.3. ELECTRONIC RECORDS

- Electronic Records are Records subject to this Policy. Retention and destruction of such Records is governed by the content of the Records, not the form in which the Records are created or stored. Electronic Records shall be maintained in accordance with the retention schedule that covers the content of the Record. The Custodian shall train personnel, officials, including staff, and board members, regarding the retention of Electronic Records to manage Records and comply with applicable, laws, regulations and this Policy.

  YHI shall establish and maintain an electronic Information System to produce, use, and store data files to comply with this Policy. Such system shall:

  - Enable authorized users to retrieve desired documents, through an indexing or text search system;

  - Address disposition of documents in accordance to this Policy and applicable laws, rules, regulations and policies;

  - Maintain sufficient information to allow for identification of each document within a given electronic Information System; and

- Correlate official file copies maintained in electronic recordkeeping systems with related records on paper, microform or other media as appropriate.

Electronic Records shall be associated with descriptive information, known as metadata, which provides evidence about a record's content and the circumstances in which it was created/received and used, which information should be retained until the final disposition of the records. Examples of metadata include: title, date created/received/modified, creator/editor, reference number, record series, access/use restrictions, subject, relationship to other records, and similar data.

Electronic Records shall be archived for the specified period in accordance with CMS ARC-AMPE privacy and security controls (based on the content of the Record). Electronic Records that need to be archived may be attached to an e-mail that may then be sent to an address supplied by the IT department, or printed out and filed depending upon the determination made by the Records Custodian. Records will then be archived for the specified period in the CMS ARC-AMPE privacy and security controls. Upon termination of each Fiscal Year, the Records Custodian shall submit the necessary documentation and direct the IT department to purge Electronic Records which are no longer subject to retention.

Although Electronic Records are generally subject to this Policy, some additional requirements applicable to specific types of Electronic Records are contained herein for guidance on the management specific to Electronic Records.

- E-mail and Portable Storage Media: All YHI officers and staff shall have and use a YHI e-mail address. Members of the Board of Directors who do not have a YHI e-mail address shall copy IdahoHIX@hawleytroxell.com on any e-mails relating to YHI business.

  The following information should be retained for each electronic mail message subject to retention pursuant to CMS ARC-AMPE privacy and security controls: (i) names of the sender and addressees, including those who are cc'd to an e-mail, (ii) the date the message was sent, (iii) message metadata, (iv) any attachment, and (v) any other transmission data necessary for the purpose of providing the context of the record.

  All YHI directors, officers, and staff should ensure that e-mail and other electronic communications are preserved in the appropriate recordkeeping system. If e-mails are Records as defined in this policy (i.e. related to YHI business), they must be maintained in accordance with this Policy, whether or not the e-mail is sent from or received by a personal e-mail account, and whether or not the e-mail is sent from or received by a personal device.

  Subject to such longer retention requirements under the Regulations, general e-mail Records shall be deleted every ninety days. E-mail messages shall be automatically archived when they are received by the YHI e-mail server. Each individual user shall be responsible for determining if any given Records are subject to retention in accordance with CMS ARC-AMPE privacy and security controls, or as otherwise required by this Policy or applicable laws or regulations.

- Website: Records created or posted to the website are subject to the same record requirements as those created or maintained on internal, non web based electronic recordkeeping systems. YHI shall retain and collect data regarding transactions conducted via the website, including submission of application, payments and other on line business.

- Social Media Records: YHI shall retain copies of social media content in accordance with website requirements.

- Desktop Documents: Word processing, spreadsheets, presentations, task lists, calendar and other desktop documents constituting Records (related to YHI business), including such Records accessed, created, received in remote locations or on external devices, such as in the field or home offices, smart phones, portable tablets, notebooks, laptops, personal digital assistants, and portable storage devices shall be retained in accordance with this Policy and for a period of ten years.

8.4. DESTRUCTION OF RECORDS

- Destruction Period: Records shall not be destroyed until the 10 year retention period has expired. Documents not covered under the definition of Records may only be destroyed upon prior approval by the Custodian, with consultation with legal counsel as appropriate. Non Essential Records may be shredded on a daily basis, so long as destruction of such Records does not contradict any retention requirements of the Regulations.

  Records shall be reviewed annually and purged or retained in accordance with the retention periods set forth herein.

- Method of Destruction: Any reasonable method of destruction may be utilized for destruction of Records, including hiring a mobile shredding company to dispose of the data, provided confidentiality of shredded documents that are Records containing PII and PHI must comply with YHI's privacy and security policies and all applicable law. The Custodian shall maintain a log of all Records destroyed, including the type of the record, date destroyed, and method of destruction. Smaller quantities may be shredded internally, so long as inadvertent disclosure is avoided.

9. APPLICABLE LAWS AND/OR REGULATIONS

- The ARC-AMPE suite of documents
- NIST 800-53 series
- The Patient Protection and Affordable Care Act of 2010, as amended
- 45 CFR part 155
- Idaho Code title 41, chapter 61
- IRS Publication 1075