

IDAHO HEALTH INSURANCE EXCHANGE

RECORD RETENTION AND DESTRUCTION POLICY

I. Purpose

This statement of policy is intended to provide guidance to the staff of the Idaho Health Insurance Exchange (“**Exchange**”) with respect to the retention and destruction of records maintained by the Exchange and other matters. The Exchange Public Records Policy should be referenced along with this policy, when dealing with potential disclosure of public records.

This Record Retention and Destruction Policy aids the efficient and economical management of maintenance, retention, preservation and disposal of Exchange records. Effective record management requires that records are kept only so long as they have some administrative, fiscal, or legal value. When records no longer fulfill the value for which they were created, they should be destroyed, absent legal requirements to retain the records, or some historic or other significance requiring permanent retention.

II. Definitions. Any terms used herein but not defined shall have the meanings ascribed to such terms in the Public Records Policy. For purposes of this policy, the following terms shall have the following meanings:

- A. “**Appeal Records**” means records relating to any appeals filed with the Exchange, including appeals relating to exemptions, eligibility determinations, or other matters within the purview of the Exchange’s duties, and including the appeal, the appeal decision, all papers and requests filed in an appeal proceeding, and a transcript or recording of any hearing testimony or official report containing the substance of what happened at the hearing and any exhibits introduced at the hearing.
- B. “**Application Materials**” means application forms and instructions provided to users of the Exchange, and completed applications and related materials provided by users of the Exchange.
- C. “**Copy**” means transcribing by handwriting, photocopying, duplicating machine and reproducing by any other means so long as the record is not altered or damaged.
- D. “**Custodian**” means the person having personal custody and control of the records in question. If no such designation is made by the Exchange, then custodian means any public official or Exchange employee having custody of, control of, or authorized access to records and includes all delegates of such officials, employees or representatives. Initially, the Finance Director is the Custodian, or such other person as the Finance Director may designate in writing.

- E. **“Electronic Records”** means electronic records, including email, word-processing documents, spreadsheets, databases, websites, images, video, audio, multimedia, interactive documents, scanned/digitized documents, etc. and includes records created, sent, or received by employees, appointees, or elected officials, as well as contractors working with the Exchange.
- F. **“Eligibility, Enrollment, Coverage Records”** means eligibility determinations, redeterminations, notices relating to determinations and redeterminations, terminations of coverage and notices regarding terminations, and related materials, designations of authorized representatives regarding eligibility determinations and applications.
- G. **“Federal Tax Information”** means “return information” as defined in Internal Revenue Code Section 6103(b).
- H. **“General Marketplace Records”** means information disclosures, enrollee surveys and data, call center logs, Exchange website pages, outreach and education materials, and other records created or maintained by the Exchange.
- I. **“Grant Materials”** means applications for federal or state grants and related materials, including notices of awards, grant agreements, documentations and reports required to be retained pursuant to grant agreements, and all related records.
- J. **“HIPAA”** means the Health Insurance Portability and Accountability Act.
- K. **“Marketplace Contracts”** means Exchange contracts entered into with third parties for the purpose of fulfilling the obligations of the Exchange relating to eligibility determinations, enrollment, the application process and related contracts, and agreements with Medicaid, Chip, or other providers.
- L. **“Marketplace Records”** means Appeal Records, Application Materials, Eligibility, Enrollment, Coverage Records, Plan Information, Navigator Program Records, Marketplace Reports and General Marketplace Records.
- M. **“Marketplace Reports”** means evaluations, reports and transmissions to the Department of Health and Human Services or other state or federal governmental body required by federal or state laws and regulations relating to enrollment, eligibility, tax credits, premium payments, and financial data of the Exchange.
- N. **“Navigator Program Records”** means records pertaining to the consumer assistance program including standards, procedures, licensing, certifications, and agreements with agents, brokers, navigators, application counselors or in-person assisters.
- O. **“Non-essential Records”** means records not usually within the definition of public records, such as unofficial copies of documents kept only for convenience

or reference, working papers, appointment logs, duplicate copies of records, records not directly related to the conduct or administration of Exchange business.

- P.** “**Personally Identifiable Information**” means information that can be used on its own or with other information to identify, contact or locate a single person, or identify an individual in context, including personally identifiable information created or collected by the Exchange for purposes of determining eligibility for enrollment in a qualified health plan, determining eligibility for insurance affordability programs, or determining eligibility for exemptions, which may only be used or disclosed to the extent necessary to carry out functions described in the Regulations. Personally Identifiable Information includes (but is not necessarily limited to) a person’s date of birth, social security number, mother’s maiden name, and other similar data. Personally Identifiable Information includes Federal Tax Information.
- Q.** “**Plan Information**” means information on insurance plans, including enrollee satisfaction surveys, provider directories, assessments and ratings data, enrollment data and documentation provided to qualified health plans, determinations of qualified health plans, including certification, recertification, and decertification.
- R.** “**Protected Health Information**” shall have the meaning ascribed to such term in HIPAA.
- S.** “**Public Record**” or “**Record**” includes, but is not limited to, any Writing containing information relating to the conduct or administration of the public’s business prepared, owned, used or retained by the Exchange regardless of physical form and characteristics. The terms “Public Record” and “Record” include Electronic Records such as e-mail correspondence relating to the conduct or administration of Exchange business.
- T.** “**Regulations**” shall mean Part 155 of Title 45 of the Code of Federal Regulations or other applicable federal laws and regulations relating to the Exchange.
- U.** “**Writing**” includes, but is not limited to, handwriting, typewriting, printing, photostating, photographing and every means of recording, including letters, words, video, pictures, sounds or symbols or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, magnetic or punched cards, discs, drums or other storage media.

III. Custodian’s Responsibilities. The Custodian shall have the following duties and responsibilities:

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

2. Develop, disseminate, and coordinate Records maintenance, retention and destruction procedures, or computer assisted retrieval programs to meet current and long-term needs of the Exchange.
3. Train other personnel in the fundamentals of records management and their roles in the records management program.
4. Review retention schedule, appended hereto as Schedule A, annually and update or amend as needed and maintain an inventory of records, as described in the Policy.
5. Implement destruction that is required by the Policy
6. Periodically monitor compliance with this Policy and applicable Regulations governing security of Personally Identifiable Information and Protected Health Information.
7. 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 security of any Personally Identifiable Information or Protected Health Information.

IV. Retention of Records

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

1. **Title of Records.** Include category or subject matter of Records or group of Records, as accurately as practicable.
2. **Location of Records.** Include general location regarding the location for the Records stored, and whether the Records are maintained on-site or off-site.
3. **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.
4. **Time Periods Covered.** Indicate the period of years covered by the Records.

B. Retention Periods. The Custodian shall maintain and update Schedule A with record retention periods for all Exchange Records. Records shall be maintained in paper or electronic format for the periods set forth in Schedule A attached hereto. The retention period for records not covered in Schedule A shall be determined by the Custodian, in consultation with legal counsel as appropriate, based on the following (in descending order of priority):

1. **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 HIPAA privacy and security rules require certain documents, containing Protected Health Information, to be maintained for 6 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 years.

2. **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.

3. **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 I.C. §§ 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.

C. 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.

D. Historical or Archival Records. Idaho Code Section 67-5751A and 67-4126 requires that all public records designated as having historical or archival value must be either transferred to the State Archive or retained by the office of record in accord with the standards established by the State Archivist. All Exchange records that are considered old or of some historical significance will be stored in acid free file folders and boxes. All metal items that could rust will be removed, such as paper clips, staples, and prong fasteners. Each box will contain a contents list and will be labeled as, "HISTORICAL-DO NOT DESTROY."

E. Personally Identifiable Information and Protected Health Information. The Exchange shall ensure that records containing Personally Identifiable Information or Protected Health Information are retained and protected in accordance with the Regulations, HIPAA, or other applicable law. Such information may only be created, collected, used, or disclosed in accordance with the Regulations.

1. **Privacy and Security of Personally Identifiable Information and Protected Health Information**

The Exchange shall identify Records containing Personally Identifiable Information or Protected Health Information as Records containing Personally Identifiable Information or

Protected Health Information and shall ensure adequate safeguards are in place to maintain confidentiality of such records, permit only restricted access to such Records and to prevent inadvertent disclosure thereof. The Exchange has developed and utilizes secure electronic interfaces when sharing Personally Identifiable Information or Protected Health Information electronically. Records containing Personally Identifiable Information or Protected Health Information shall only be created, retained, accessed and used to the extent necessary to accomplish the specific permitted purpose for which such information is required and Personally Identifiable Information or Protected Health Information may not be used to discriminate against any individual to which such information relates. Records containing Personally Identifiable Information or Protected Health Information shall not be disclosed to anyone other than personnel necessary to accomplish the specific permitted purpose for which such information is required or to the individual to whom such information relates upon written request therefor. Any Records containing Personally Identifiable Information or Protected Health Information must be destroyed at the end of the applicable retention period in a secure manner, either through shredding, incineration, or through another method which ensures confidentiality and non-disclosure of Personally Identifiable Information or Protected Health Information.

2. Access to Personally Identifiable Information or Protected Health Information by the Individual

An individual may request access to the Personally Identifiable Information or Protected Health Information about such individual by providing a written request to the Exchange. The Exchange shall provide access to such information within a reasonable time frame and in a readable format. Individuals may dispute the accuracy or integrity of such Personally Identifiable Information or Protected Health Information and request correction of erroneous information by filing a written request to the Exchange setting forth the inaccuracy and providing evidence of the correct information. Such request shall be reviewed and responded to in writing within a reasonable timeframe. In the event the request is denied, the individual may appeal through the standard appeal process and record of the request, denial and appeal shall be retained by the Exchange in accordance with Schedule A.

3. Breach of Security of Personally Identifiable Information or Protected Health Information

Breaches of the security of Personally Identifiable Information or Protected Health Information shall be immediately reported to the Custodian and the Committee responsible for oversight of this Policy. The Exchange shall ensure notification to the affected parties and others, as may be required by applicable law or regulation or any contract applicable to the data that has been breached, as soon as practicable following discovery of the breach, and in any event within the timeframes required by applicable law, which are set forth on Schedule B hereto.

In the event of a breach, the Policy shall be reviewed to determine whether amendment is necessary to ensure appropriate treatment and safeguarding of Personally Identifiable Information or Protected Health Information and remedial action shall be taken as necessary.

4. **Contracts with Vendors, Contractors, and Third Parties.**

All contracts between the Exchange and its contractors or vendors shall provide obligations on the part of such vendors or contractors to comply with federal and state laws, including laws and regulations regarding privacy and security of Personally Identifiable Information and Protected Health Information as set forth in this Policy or other applicable Exchange policies and procedures. Such contracts shall contain provisions permitted the Exchange or its designee to audit the records of such third party to ensure compliance with Exchange policies, procedures, and applicable federal and state law and regulations.

F. 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.

The Exchange shall establish and maintain an electronic information system to produce, use, and store data files to comply with this Policy. Such system shall:

- (a) enable authorized users to retrieve desired documents, through an indexing or text search system;
- (b) provide appropriate security to ensure integrity of the documents and restrict accessibility where necessary to protect Personally Identifiable Information or Protected Health Information;
- (c) ensure that a standard interchange format is provided, when necessary, to permit the exchange of documents on electronic media between agency computers using different software/operating systems and the conversion or migration of documents on electronic media from one system to another;
- (d) address disposition of documents in accordance to this Policy and applicable laws, rules, regulations and policies;
- (e) maintain sufficient information to allow for identification of each document within a given electronic information system; and
- (f) 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 Schedule A (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 Schedule A. 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.

1. **E-mail and Portable Storage Media**

All personnel, officers, or others associated with the Exchange shall be required to have an use an Exchange e-mail address. Members of the Board of Directors shall be required to copy the Health Exchange account on any e-mails relating to Exchange business. Departing officials shall return or destroy, as appropriate, all portable storage media or other device capable of storing data in the individuals' possession containing Electronic Records of the Exchange. Personnel, officers, and others associated with the Exchange may not copy or transfer Electronic Records to another device without prior approval of the Custodian.

The following information should be retained for each electronic mail message subject to retention pursuant to Schedule A: (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.

Messages sent or received using an external electronic mail system should ensure that the records are preserved in the appropriate recordkeeping system - if they are Records as defined in this policy (i.e. related to Exchange business), they must be maintained in accordance with this Policy, whether or not the e-mail used is the exchange email, and whether or not computer is a personal computer.

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

2. **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 system. The Exchange shall retain and collect data regarding transactions conducted via the website, including submission of application, payments and other on-line business.

3. **Social Media Records**

The Exchange shall retain copies of social media content in accordance with website requirements.

4. **Desktop Documents**

Word-processing, spreadsheets, presentations, task lists, calendar and other desktop documents constituting Records (related to Exchange business), including such Records accessed, created, received in remote locations or on external devices, such as in the field or home offices, portable tablets, notebooks, laptops, personal digital assistants and portable storage devices shall be retained in accordance with this Policy and for the period specified in Schedule A (based on the content of the Record).

5. **Security of Electronic Records**

The Exchange shall ensure only authorized personnel have access to Electronic Records, back-up and recovery to protect against information loss, personnel and contractors/vendors are trained or otherwise required to safeguard confidential information (including Personally Identifiable Information and Protected Health Information), minimize risk of unauthorized disclosure or alteration of records, and ensure security is included in computer systems security plans.

V. Medium for Records

Records may be maintained in paper files, in boxes clearly marked with the contents of the files and the disposal date, in accordance with Schedule A's retention schedule. Electronic Records may be maintained electronically. After three years, non-essential Records shall be relocated off-site, with an index on-site logging the locations and contents of boxes stored off-site.

VI. Destruction of Records

A. Destruction Period. Records shall be destroyed at the end of the retention period provided on Schedule A for the relevant Record. Documents not listed on Schedule A 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 listed in Schedule A.

Records shall be reviewed annually and purged or retained in accordance with the retention periods set forth on Schedule A, or as otherwise prudent, in accordance with this Policy.

Computer information shall be backed up on a daily basis. At the end of each day, the previous night's backup will be stored off-site. Week-end backups will be held for a period of three weeks. Month-end backups shall be held on a permanent basis, with every other month's backup being stored off-site.

B. 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 Personally Identifiable Information and Protected Health Information must be assured. 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.

Records containing confidential information, including Personally Identifiable Information and Protected Health Information, shall be destroyed in a method that ensures destruction of the Records, protects against disclosure, and preserves the confidentiality of such information (i.e. shredding or incinerating).

VII. Third-Party Vendors. To the extent that the Exchange utilizes an outside entity to assist with records retention or destruction, the Exchange shall ensure that it has a HIPAA-compliant contract with the entity to the extent such Records may contain Protected Health Information subject to HIPAA. The HIPAA privacy and security rules require that covered entities take appropriate administrative, physical, and technical safeguards to protect health information. Covered entities must enter business associate contracts with entities that retain or destroy documents on behalf of the covered entity. The documents must be destroyed in a manner that will protect against improper disclosure. The Exchange shall apply equivalent standards for destruction of Records containing Personally Identifiable Information.

VIII. Annual Review

The Custodian shall conduct an annual review of this Policy. The annual review process shall include (i) an inventory of records, (ii) review and update of the retention schedule, and (iii) report to the Board of Directors or applicable committee of the Exchange. In addition, the Custodian shall review annually the Exchange's electronic information systems for conformance with procedures, standards, policies.

A. Inventory

The Custodian shall create and maintain a log of Records, which shall be reviewed and updated annually. The log is essential to developing an updated Records Retention Schedule (see Schedule A). The log should contain the following information:

- (1) **Record Series.** The title of each series of Records. A "series" is a group of similar records arranged under a single filing system or kept together as a unit, which deal with a particular subject (i.e. budget, personnel, etc.), result from the same activity, or have a special form. The title of each record series should be as accurate as possible.
- (2) **Media.** Determine the media for each Record series (paper, microfilm, etc.). Note whether the same record exists in several medium.
- (3) **Time Period Covered.** Determine the period of years covered by each series.

(4) Activity Level. The amount of activity determines where the record should be stored, active records need to be readily available inactive records may be warehoused in low cost storage.

(5) Volume. Note the volume of each record series by the cubic feet of space they occupy.

Once the log is updated, it can be used to review and update the Records Retention Schedule.

B. Retention Schedule and Policy Update

Once the inventory is conducted and the log is updated, it can be used to review and update the Records Retention Schedule. Schedule A shall be updated to reflect records currently maintained by the Exchange. In addition, this Policy should be amended as necessary to ensure that all Records are dealt with in this Policy.

C. Annual Records Report

At the end of each fiscal year, the Custodian shall prepare a report to the Board including the updated Policy and Retention Schedule and submitting necessary amendments for approval. The Report shall also contain detailed information relating to any breaches of this Policy that have occurred during the fiscal year, the responses to any breaches, and remedial actions taken to ensure the breach is not repeated. The Report shall include a log of all records to be destroyed in accordance with this Policy for approval. Finally, the Report shall including an assessment of whether data is being properly retained and destroyed in accordance with this Policy.

**SCHEDULE A
RETENTION PERIODS**

RECORD SERIES	GENERAL DESCRIPTION	RETENTION RECOMMENDATIONS
Administration		
Organizational/ Governance [Board meeting recordings]	Articles of incorporation, Bylaws, Board meeting minutes, Committee meeting minutes, Committee Charters, Board resolutions, Annual reports	Permanent
Policies and Procedures	Board, administrative, or committee policies and procedures and any delegation orders	Active period + 6 years
Internal Reports	Reports from staff, departments, and/or committees	3 years except that reports that implicate fraud and abuse issues should be retained for at least 6 years. Daily and non-annual reports may be destroyed after year-end statistics are compiled in an annual report
Property records	Deeds, titles, licenses, permits, appraisals	Permanent
Construction records	Contracts, work orders, certificates, etc.	Permanent
Contracts, Leases, RFPs	All contracts and leases, including construction contracts, vendor contracts, equipment and property leases, etc.	Active Period + 6 years, including any warranty period.
Litigation Case Files	All files relating to litigation involving the Exchange	Permanent
Feasibility Studies	Any studies conducted before installation and implementation of technology, equipment, process, or procedure, including studies of systems analysis for the initial establishment and major changes of these systems	Permanent
Executive Correspondence	Correspondence that documents how the office is organized and functions, pattern of action, its policies, procedures and achievements	Active Period + 6 years
General Correspondence	Routine correspondence not duplicated elsewhere, which does not include policy decisions or directives, how the office is organized, how it functions, its pattern of action, procedures, achievements. Records that are general in nature and do not relate directly to primary responsibilities of an office or agency. Letters of appreciation, congratulations, charity fund, parking assignments, records of a general nature which could be created in the course of administering agency programs, could include office organization, staffing, procedures, and internal communications.	Maintain significant correspondence for at least 6 years, routine or less significant correspondence for active period plus 2 years
Working Papers and Technical Reference Files	Records which have a short-term use and comprise background records, such as preliminary studies, drafts, analyses, notes, interim reports, and financial performance audits, drawings, periodicals, books, clippings, extra copies, brochures, catalogs, vendor price lists, publications	Active period and destroy if no longer administratively valuable

	Daily Activity Schedules	Records containing substantive information re official activities, not otherwise incorporated into official files, such as calendar, schedules, appointment books, logs, diaries, documenting meetings, telephone calls, trips, visits, other activities of employees, etc.	Active period + 1 year
Business and Finance Records			
	General financial records	-Accounts payable/receivable -Financial reports -Financial audits -Bank records (statements, checks, etc.) -Budgets	10 years
Compliance Records			
	Compliance documentation	Employee training, auditing and monitoring; reports of problems; investigations; correspondence with regulators; self-disclosures	10 years
	HIPAA records	Notice of Privacy Practices, if any, authorizations, privacy officer designation, disclosure log, business associate contracts, employee training, employee sanctions, policies and procedures, complaints, security assessment, security standards documentation	6 years from later of the date created or last effective date
	Federal Tax Information	Logs of receipt, use, disclosure, etc.	5 years (audit records related to a security breach must be retained for 7 years)
Marketplace Records			
	Information Disclosures	Disclosures provided to Exchange users	Active period +10 years
	Enrollee Surveys and Data	Survey and Data conducted by or retained by Exchange or third party on behalf of the Exchange	Active period +10 years
	Call Center Logs	Data collected regarding call centers utilized by Exchange users	Active period + 10 years
	Outreach and Education Materials	Materials created and provided to Exchange users or the general public for educational or informational purposes	Active period + 10 years
	Appeal Records	Records relating to any appeals filed with the Exchange, including appeals relating to exemptions, eligibility determinations, or other matters within the purview of the Exchange's duties, and including the appeal, the appeal decision, all papers and requests filed in an appeal proceeding, and a transcript or recording of any hearing testimony or official report containing the substance of what happened at the hearing and any exhibits introduced at the hearing	Active period + 10 years
	Application Materials	Application forms and instructions provided to users of the Exchange, and completed applications and related materials provided by users of the Exchange	Active period + 10 years
	Eligibility, Enrollment, Coverage Records	Eligibility determinations, redeterminations, notices relating to determinations and redeterminations, terminations of coverage and notices regarding terminations, and related materials, designations of authorized representatives regarding eligibility determinations and applications	Active period +10 years

	Plan Information	Analyses and summaries of insurance plans, including enrollee satisfaction surveys, provider directories, assessments and ratings data, enrollment data and documentation provided to qualified health plans, determinations of qualified health plans, including certification, recertification, and decertification	Active period +10 years
	Navigator Program Records	Records pertaining to the navigator program including standards, procedures, licensing, certifications, and agreements with agents, brokers, navigators, counselors	Active period +10 years or other period required by Exchange policy
	Marketplace Reports	Evaluations, reports and transmissions to the Department of Health and Human Services required by federal laws and regulations relating to enrollment, eligibility, tax credits, premium payments, and financial data of the Exchange	Active period +10 years
	Marketplace Contracts	Exchange contracts entered into with third parties for the purpose of fulfilling the obligations of the Exchange relating to eligibility determinations, enrollment, the application process and related contracts, and agreements with Medicaid, Chip, or other providers	Active period +10 years
	Grant Materials	Applications for federal or state grants and related materials, including notices of awards, grant agreements, documentations and reports required to be retained pursuant to grant agreements, and all related records	Active period + 10 years (or other period required by Grant Agreement)
Human Resources/Personnel			
	Employment info (FLSA)	Payroll, job descriptions, wages, job evaluations, employment contracts, time cards, wage rate schedule, W-2s, W-4s	7 years from date of last employment
	Employment actions	Hiring, promotion, demotion, transfer, termination, layoff, pay rates or compensation terms	7 years from date of last employment
	Employment and social security taxes		7 years after taxes due (or paid, if paid after due date) or claim filed.
	ERISA benefit plan records	Records required to be filed pursuant to ERISA	Date of filing plus 6 years
	Medical and exposure records pertaining to employee exposure to toxic substances or harmful physical agents (OSHA)	Employment questionnaires or -histories; employment medical exams; first aid records; medical opinions or diagnoses; descriptions of treatments and prescriptions; medical complaints	30 years from date of last employment
Marketing and Public Relations			
	Marketing materials	Marketing/Public Relations	6 years from last effective date
	Contributor records	Public Relations	Permanent
	Publications	Marketing Publications	Permanent
Risk Management			
	Accident/incident reports		Up to 11 years
	Liability Policies		For occurrence-based policies, 20 years after expiration. For claims-made policies, 6 years after expiration.

	Property and casualty insurance policies		6 years after expiration
Assets			
	Computer Systems	Hardware Documentation (operational manuals, hardware configurations, control systems)	Life of Asset + 5 years
	Other assets		Life of Asset + 5 years

**SCHEDULE B
BREACH NOTIFICATION REQUIREMENTS**

<u>Applicable Law/Regulation/Contract Provision</u>	<u>Notification Requirement</u>
Idaho Code § 28-51-105	<p>As soon as possible to affected Idaho resident.</p> <p>Attorney General’s Office within 24-hours following discovery.</p>
HIPAA	<p>Must be provided without unreasonable delay and in no case later than 60 days following discovery of a breach, to the following parties:</p> <p><i>Individual notice.</i> Provide notice in written form by first-class mail or e-mail (if the individual has agreed to receive notices electronically). May provide publication notice in certain circumstances. Must include a description of the breach, description of types of information involved, steps affected individuals should take to protect themselves from harm, and prevent further breaches.</p> <p><i>Media notice.</i> For breach affecting more than 500 residents of a State or jurisdiction, must provide notice to prominent media outlets serving the State or jurisdiction. Must include a description of the breach, description of types of information involved, steps affected individuals should take to protect themselves from harm, and prevent further breaches.</p> <p><i>Notice to the Secretary.</i> Notify the Secretary of HHS via website and filing out electronic breach report form. If the breach affects less than 500 individuals, may inform the Secretary annually rather than within 60 days.</p> <p><i>Covered Entity.</i> If the breach is at or by a business associate, the business associate must notify the covered entity without unreasonable delay and no later than 60 days.</p>
CMS data sharing agreements	Within one-hour after discovery to HHS. [confirm]