



COLORADO
Department of Public
Health & Environment

December 29, 2023

Staff of the Legislative Council
State Capitol Building
200 East Colfax
Denver, Colorado 80203

Dear Staff of the Legislative Council:

In accordance with Section 24-72-204.5(3), C.R.S., I am pleased to present you with a report outlining the electronic mail (“email”) retention policy of the Colorado Department of Public Health and Environment.

Statute requires reporting to the Staff of the Legislative Council. Specifically:


On or before January 1, 2024, each member of the general assembly, the governor's office and each office of the governor, and each state agency and institution shall submit a report to the staff of the legislative council of the general assembly outlining its respective electronic mail retention policy. The members of the general assembly may submit individual reports or may submit a report that specifies the electronic mail retention policies of multiple members of the general assembly.

The Colorado Department of Public Health and Environment’s *Records, Information, and Email Management* policy is attached.

Sincerely,

Jill Hunsaker Ryan, MPH
Executive Director



	Policy:	Records, Information, and Email Management		
	Number (Part):	2.15	Created:	December 2001
	Supersedes:	<i>Formerly “Records and Information Management”</i>	Revised:	April 2012 January 2016
	Approved By:	Jill Hunsaker Ryan, MPH, Executive Director	Approved:	December 28, 2023

Purpose

This policy sets out a framework wherein employees responsible for managing the department’s records can develop division- and/or program-specific policies and procedures to ensure records are managed and controlled effectively and at best value, commensurate with legal, operational, and informational needs.

This policy relates to all records held in any format by department employees, contractors, subcontractors and grant recipients. The department’s objectives for records management are to ensure the following:

Records are available when needed, from which the department is able to reconstruct activities or events that have taken place.

Records are accessible. Records and the information they hold can be located and displayed in a way consistent with their intended use, and the current version is identified where multiple versions may exist.

Records can be interpreted. The context of the record can be interpreted by the program.

Records can be authenticated. The record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.

Records can be maintained through time. The qualities of availability, accessibility, interpretation and department worthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.

Records are secure from unauthorized or inadvertent alteration or erasure. Access and disclosure are properly controlled, and audit trails track all use and changes to ensure records are held in a robust format that remains readable for as long as records are required.

Records are retained and disposed of appropriately using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value.

Employees are informed and have access to technical assistance and training concerning their responsibilities for recordkeeping and records management.


Roles and Responsibilities

Each division, office, board or commission is responsible for ensuring it meets its legal records management requirements, including the adoption of internal and external governance requirements. Division directors, office directors, or board/commission administrators shall designate one or more staff person(s) to serve as their respective records manager(s) or coordinator(s).

All department employees who create, receive and use department records have records management responsibilities. All employees must ensure they keep appropriate records of their work in the department and manage those records in keeping with this policy and with any guidance subsequently produced.

Records Liaison Officer

The department records liaison officer serves as the liaison to the state archivist; has overall responsibility for records management in the department; and exercises these duties through the development and implementation of department-wide policies and procedures based on law, regulation and guidance. See § 24-80-102.7, C.R.S.

	Policy:	Records, Information, and Email Management		
	Number (Part):	2.15	Created:	December 2001
	Supersedes:	<i>Formerly “Records and Information Management”</i>	Revised:	April 2012 January 2016
	Approved By:	Jill Hunsaker Ryan, MPH, Executive Director	Approved:	December 28, 2023

Records Managers and Coordinators

Records managers and coordinators are responsible for the records generated by their division and/or program activities, i.e., ensuring the records are controlled and managed in a way that meets the objectives of the department’s records and information management policy. Department employees should consult with their division’s records manager for technical assistance and training regarding records management as it pertains to their division. Records managers will consult with the records liaison officer as needed for guidance and technical assistance, or for communicating with the state archivist.

Privacy Officer

The department’s privacy officer has a particular responsibility for the development and implementation of policies and procedures related to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). Some privacy policies and procedures may be applicable to a division’s records and information management program, which may require consultation with the privacy officer.

Contractors, Subcontractors and Grant Recipients

Contractors, subcontractors, and grant recipients are responsible and accountable for department records they create and/or maintain for purposes of the contract or grant. Records disposition shall be in accordance with the contract or grant provisions, federal and state laws, and department policy. When the records retention policy is applicable to a grantor and state or federal law differs from department policy, the grant or legal requirements shall supersede.

Policy

Sensitive or confidential information

Many records subject to record retention requirements contain non-public sensitive or confidential information, such as personally identifiable information. For purposes of this policy, such information shall be referred to as “protected information”. See “Definitions” section of this policy. Such records may be protected by federal and state statutes. See *§ 25-1-1201 et seq., C.R.S.* for a listing of confidential medical records. In addition to statutory requirements, any record that contains sensitive or confidential information should be treated in accordance with the department’s privacy and security policies.

Electronic Mail Messages

Department employees are responsible for managing their email accounts in accordance with the requirements set forth in the “Managing Electronic Mail Messages” section of this policy.


Records Storage

Records fall into two retention categories:

- 1) non-permanent records requiring retention for legal, operational or audit purposes; and
- 2) permanent records (archival).

Records managers and coordinators shall ensure the following principles are incorporated into their division and/or program retention policies and schedules and department employees shall comply with the following:

- All draft records shall be purged upon completion of a final document.

	Policy:	Records, Information, and Email Management		
	Number (Part):	2.15	Created:	December 2001
	Supersedes:	<i>Formerly “Records and Information Management”</i>	Revised:	April 2012 January 2016
	Approved By:	Jill Hunsaker Ryan, MPH, Executive Director	Approved:	December 28, 2023

- All records containing policy deliberations shall be purged once a final policy decision has been made.
- All internal correspondence shall be purged when no longer needed, but no later than the completion of the action being taken (i.e., enforcement action, permit/licensure action, final decision made).
- Records held by employees in their work space shall comply with all provisions of the department and division record retention policies.

Off-site storage

Divisions, offices, boards and commissions may store off-site records using a vendor service as identified in the state price agreement negotiated by the state purchasing office. Records stored at an off-site vendor shall be evaluated regularly for continued storage and retention needs.

Storing business records in personal storage areas such as home basements and garages, private networks or servers, or at off-site vendors not identified in the state price agreement is prohibited.

All communications regarding storing records at the Office of State Archives shall be coordinated through the department’s records liaison officer. Records classified as permanent that are no longer in use by department personnel and have been stored at the department for more than 10 years shall be evaluated for transfer to State Archives. The records manager shall contact the department records liaison officer to schedule a records appraisal and coordinate the transfer.

Electronic and cloud-based storage

The department has experienced tremendous growth in the use of electronically stored information. The ease with which electronically stored information may be created, the number of places where it may be stored, and rules regarding the use of electronically stored information in litigation all require that the department manage its electronically stored information effectively, efficiently and consistent with its legal obligations.


Cloud-based applications store documents in the cloud, sometimes in a proprietary format. These documents are still considered department documents and are subject to all relevant records management laws, rules and policies. Given the limited control that the department has over these applications, an evaluation of each application by the department’s Business Technology Team must occur prior to its use for department purposes. This evaluation must consider technical, records management and privacy concerns. The Business Technology Team will keep a list of approved applications.

The electronic storage of state records in cloud-computing environments designed specifically for records management is prohibited *unless* a contract is in place that complies with federal and state laws, and department regulations and policies, including those of the Office of Information Technology, pertaining to records and information management.

Electronic records are subject to the same retention policies as hard-copy records. Accordingly, all divisions, offices, boards and commissions shall include electronically stored information in the development of their records disposition schedules and policies. Each division and/or program shall develop guidelines or procedure documents to address how electronic records will be maintained by each division, including on individual and shared network access drives.

Inventory of Records Collections

Each division and/or program shall establish and maintain an inventory through which they can account for the records they are maintaining. Records inventories shall be reviewed by the division records manager or coordinator annually.

	Policy:	Records, Information, and Email Management		
	Number (Part):	2.15	Created:	December 2001
	Supersedes:	<i>Formerly “Records and Information Management”</i>	Revised:	April 2012 January 2016
	Approved By:	Jill Hunsaker Ryan, MPH, Executive Director	Approved:	December 28, 2023

Records Disposition Schedules

All department records are retained for a minimum period of time, for legal and operational reasons, either as required by law or policy or determined by the division, office, board or commission-based guidance from the state archivist. The length of time for retaining records will depend on the type of record and its importance to the department’s business functions.

Records managers and coordinators, in consultation with the department records liaison officer, are responsible for establishing record retention periods, which are based upon applicable laws, regulations and guidance and are reflected in each division, board or commission records disposition schedule and rationale.

Each records disposition schedule shall be reviewed every two years and shall be updated when a new business process or category of records has been adopted that necessitates an earlier review/update.

Records Destruction

Records meeting their retention period shall be destroyed according to the applicable schedule. The following requirements apply to the disposition of department records:

- The disposal process and methods shall preserve the confidentiality of documents where applicable through the final point of disposition.
- Paper records containing protected information shall be shredded, not simply thrown out with other classes of records or with miscellaneous trash. It is recommended that confidential destruction services be arranged through the state’s contracted records destruction vendor. Further information may be obtained from the department’s records liaison officer.
- Electronic or machine-readable records containing protected information shall be destroyed in accordance with the department’s device and media control policy.
- Film, audio and videotapes containing protected information also shall be physically destroyed by placing into the electronic media disposal bins available at the CDPHE Main Campus, not simply thrown away. Further information may be obtained from the department’s records liaison officer or privacy officer.

A destruction record is required for the disposition of all department records. A destruction record is an inventory describing and documenting records, in all formats, authorized for destruction, as well as the date, name of authorizing employee, and method of destruction. The destruction record itself shall not contain protected information.


Employees shall work with their division records manager to report records destruction activities no later than annually to the records liaison officer via the department’s records destruction form.

Document Imaging and Scanning

Document imaging may be the most effective and efficient means for retaining certain types of records. Any division or program that is contemplating replacing original records with images of those records shall advise the department records liaison officer prior to implementing such a system.

Divisions, offices, boards or commissions proposing electronic retention systems must be prepared to demonstrate that the following requirements will be met:

- Electronic records shall exhibit a high degree of legibility and readability.

	Policy:	Records, Information, and Email Management		
	Number (Part):	2.15	Created:	December 2001
	Supersedes:	<i>Formerly “Records and Information Management”</i>	Revised:	April 2012 January 2016
	Approved By:	Jill Hunsaker Ryan, MPH, Executive Director	Approved:	December 28, 2023

- Paper copies or electronic records shall be transferred to electronic storage media in an accurate and complete manner.
- Procedures shall be developed to index, store, preserve, retrieve and reproduce all electronically stored records.
- Controls shall be developed to ensure the integrity, accuracy, and reliability of the electronic records.
- Controls shall be developed to prevent and detect the unauthorized creation, alteration, addition, deletion or deterioration of electronically stored records.
- An inspection and quality assurance program shall be developed, which must include regular evaluations of the system and periodic checks of stored records.

Management of Electronic Mail Messages (Email)

The department’s email system will automatically delete electronic mail that is 90 days old from users’ accounts. This includes email in the inbox, sent folder, and other labels. Employees shall preserve any email requiring retention for more than 90 days according to the following guidelines:

- Employees must determine which email messages require retention beyond 90 days for compliance with a retention schedule, and must actively convert those messages into a more permanent form such as a PDF file, then store it with other files being preserved under the same retention category.
- Email messages that do not have a retention requirement outlined in a retention schedule but are of importance to ongoing work or other reporting purposes may be preserved beyond 90 days by applying the DONOTDELETE label to the messages.
- Email messages that are being retained in accordance with a Notice of Litigation Hold or other sensitive holds shall be retained in the electronic mail system by applying the “DONOTDELETE” label while the hold is in effect.
- Email messages that are the subject of a current Colorado Open Records Act request shall be retained for 60 days after the response is complete, pursuant to the department’s Open Records Act policy.


Employees are prohibited from the following practices:

- Downloading or printing emails for the sole purpose of storage.
- Using unapproved software to automate the saving and/or storing of work emails.
- Routinely or automatically forwarding work-related email to personal email accounts for the sole purpose of storing those emails (e.g. no auto-forwarding, filtering, or routine copying of work-related email to a private email account).
- Using a personal peripheral storage device such as a jump drive or other storage devices to save and store work emails.
- Deleting any email the employee knows or reasonably believes is the subject of a CORA request or an active litigation hold.

Employees should routinely manage their state email box in accordance with the standards set forth above and periodically review emails with the “DONOTDELETE” label and remove the label when the email no longer needs to be retained.

Preservation of Records Relevant to Legal Matters

Any record that is relevant to any current, pending or anticipated litigation, claim, audit, agency charge, investigation, or enforcement action shall be retained until final resolution of the matter.

	Policy:	Records, Information, and Email Management		
	Number (Part):	2.15	Created:	December 2001
	Supersedes:	Formerly “Records and Information Management”	Revised:	April 2012 January 2016
	Approved By:	Jill Hunsaker Ryan, MPH, Executive Director	Approved:	December 28, 2023

In these circumstances, the Office of Legal and Regulatory Compliance (OLRC) in conjunction with a representative from the Office of the Attorney General shall notify relevant divisions and Office of Information Technology employees of the need to retain records through the issuance of a Notice of Litigation Hold. This will include a directive that the relevant program’s normal document destruction policies or protocols be temporarily suspended pertaining to relevant records. The OLRC and/or division records manager shall be available to advise employees regarding identifying and preserving any records and other information that could be relevant to the matter.

Employees who become aware that an investigation or legal proceeding has commenced or is anticipated against their division or program shall promptly notify the OLRC so an assessment can be made regarding the issuance of a litigation hold notice to all employees with records with potential relevance to the investigation or legal proceeding.

Records and Information Management Program Inspection

The records liaison officer, in conjunction with division or program records managers and/or coordinators, shall regularly inspect records management practices for compliance with this policy.

The inspection will

- identify areas of operation that are covered by the department, division and program policies and identify which procedures and/or guidance should comply with the policy;
- follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance;
- highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.


Records Management Disaster Plan

A records disaster is a sudden, unexpected event that significantly damages or destroys records or prevents access to the information they contain. A records disaster can deprive employees of the information needed to resume normal operations. To manage records disasters, records managers and coordinators shall develop and implement disaster management plans in accordance with the department’s Continuity of Operations Plan (COOP).

Disclosure of Public Records

Records that are considered *public records* under the Colorado Open Records Act are subject to disclosure upon request, unless specifically exempted pursuant to the act or another federal or state law. The department will take actions as necessary to comply with the legal and professional obligations identified in the following:

- Department Open Records Act policy 2.17;
- Colorado Open Records Act, § 24-72-201 *et seq.*, C.R.S.;
- State Archives and Public Records Act, § 24-80-101 *et seq.*, C.R.S.;
- Uniform Electronic Transactions Act, § 24-71.3-101 *et seq.*, C.R.S.; and
- any new laws affecting records and information management.

	Policy:	Records, Information, and Email Management		
	Number (Part):	2.15	Created:	December 2001
	Supersedes:	<i>Formerly “Records and Information Management”</i>		Revised: April 2012 January 2016
	Approved By:	Jill Hunsaker Ryan, MPH, Executive Director	Approved:	December 28, 2023

Compliance

Any employee not complying with this policy and these procedures may be subject to corrective and/or disciplinary action, up to and including termination. Non-employees who do not comply with this policy and these procedures will be dealt with appropriately.

Definitions

Records management is a discipline that utilizes an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, while at the same time serving the operational needs of the department and preserving an appropriate historical record. The key components of records management are as follows:

- record creation;
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and storage;
- appraisal;
- archiving;
- destruction.


Records life cycle is a term that describes the life of a record through the following phases:

- creation/receipt;
- a period of its “active” use;
- a period of “inactive” retention (such as closed files that still may be referred to occasionally); and
- either disposal or archival preservation.

Records are defined by State archives and public records statutes as “all books, papers, maps, photographs, or other documentary materials, regardless of physical form or characteristics, made or received by any governmental agency in pursuance of law or in connection with the transaction of public business and preserved or appropriate for preservation by the agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the value of the official governmental data contained therein.” Business records created and/or stored outside the department’s information technology server network, e.g. on a personal computer or in the cloud, are also subject to the requirements of this policy.

These statutes further expressly exclude the following from the definition of a record:

- materials preserved or appropriate for preservation because of the value of the data contained therein other than that of an official governmental nature or because of the historical value of the materials themselves
- library books, pamphlets, newspapers or museum material made, acquired or preserved for reference, historical or exhibition purposes
- private papers, manuscripts, letters, diaries, pictures, biographies, books and maps, including materials and collections previously owned by people other than the state or any political subdivision thereof and transferred by them to the state historical society

	Policy:	Records, Information, and Email Management		
	Number (Part):	2.15	Created:	December 2001
	Supersedes:	Formerly “Records and Information Management”	Revised:	April 2012 January 2016
	Approved By:	Jill Hunsaker Ryan, MPH, Executive Director	Approved:	December 28, 2023

- extra copies of publications or duplicated documents preserved for convenience of reference
- stocks of publications
- *electronic mail messages*, regardless of whether such messages are produced or stored using state-owned equipment or software, unless the recipient has previously segregated and stored such messages as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the value of the official governmental data contained therein.

See § 24-80-101(1), C.R.S.

Public records are defined in the Colorado Open Records Act as “all writings made, maintained, or kept by the state, any agency, institution, a nonprofit corporation incorporated pursuant to section 23-5-121(2), C.R.S., or political subdivision of the state, ...for use in the exercise of functions required or authorized by law or administrative rule or involving the receipt or expenditure of public funds.” Notable exemptions from public records include all of the following:


- criminal justice records;
- work products prepared for elected officials;
- information security plan of a public agency; and
- information security incident reports and audit and assessment reports.

Electronic record means a record created, generated, sent, communicated, received or stored by electronic means.

Cloud storage is a model of networked enterprise storage where information is stored in virtualized pools of storage which are generally hosted by third parties.

Protected information is sensitive or confidential information that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization. It is a broad designation, which includes public health information that identifies an individual, personal information for employees, or social security numbers for vendors and licensees. Other sensitive information may include cell phone numbers that are not generally available. Information may be designated as sensitive or confidential on a program-by-program basis at the discretion of the program manager. Examples of protected information include:

- Human Resources Information
 - Human Resources information that includes employee social security numbers or information about any type of employee leave, e.g. KRONOS
- Personal Identifying Information
 - Disease tracking or case-management information that identifies individuals
 - Budgeting and accounting software with social security numbers, including Colorado Operations Resource Engine (CORE), formerly Colorado’s Financial Reporting Systems (COFRS)
 - Facility databases with patient information
 - Registries with individual identifying information
 - Call lists that may include non-published phone numbers or addresses

	Policy:	Records, Information, and Email Management		
	Number (Part):	2.15	Created:	December 2001
	Supersedes:	<i>Formerly “Records and Information Management”</i>		Revised: April 2012 January 2016
	Approved By:	Jill Hunsaker Ryan, MPH, Executive Director	Approved:	December 28, 2023

- Word files, Excel spreadsheets or any other file type with individually identifiable sensitive information
- Medical records reviews or audits that include individual medical information
- Personnel exposure reports on radioactive materials licensees
- Business Information
 - CDPHE computer network diagrams
 - Confidential commercial information about licensees and permittees
- Other Information
 - Privileged information
 - Attorney client privileged communication
 - Deliberative process privileged communication
 - Colorado Open Records Act exempt
 - Information protected due to homeland security concerns

Tools/Guidelines/Standards/References

Colorado Department of Public Health and Environment Open Records Act [Policy 2.17](#)

Colorado Department of Public Health and Environment Privacy and Security [Policies 15.1-15.45](#)

Colorado Department of Public Health and Environment [Continuity of Operations Plan \(COOP\)](#)

Colorado State Archives, [State Records Management Manual](#)

[Colorado Revised Statutes § 24-80-101, et seq.](#) State Archives and Public Records Act

[Colorado Revised Statutes § 24-72-201, et seq.](#) Colorado Open Records Act

[Colorado Revised Statutes § 24-71.3-101, et seq.](#) Uniform Electronic Transactions Act

[Colorado Revised Statutes § 25-1-1201, et seq.](#) Medical Record Confidentiality

Governor’s Office of Information Technology [Information Security Policies & Standards](#)