

UTAH DEPARTMENT OF HEALTH AND HUMAN SERVICES POLICY AND PROCEDURES		
Policy: 07-02	Page 1 of 7	
DATA STEWARDSHIP POLICY		
<p>RATIONALE: This policy describes the authority and procedures for stewardship of data held within DHHS.</p> <p><i>Related Policies:</i> DHHS Sharing Policy 07.04, DHHS Institutional Review Board and Human Research Protections</p>		
Original Effective: July 1, 2022	Revision: May 2, 2022	Next Review Due: May 2, 2025

I. DESCRIPTION

This policy guides how the department shall oversee the stewardship of data held by the department to ensure the safeguarding, management and disclosure of DHHS data resources. This is to assure data is treated as an asset and utilized to the fullest extent allowed by law, federal requirements, or relevant ethical purposes, while also being protected as required by law. Any issues remaining unresolved upon implementation of this policy or questions regarding implementation or interpretation are to be brought to the attention of the director of data, systems and evaluation or the chief privacy and security officer. This policy supersedes any previous policy governing this subject matter.

II. DEFINITIONS

The following terms are defined for this policy as:

- A. **Data:** All records and information created, received, maintained, or transmitted by the department. Data means information about individuals, both identifiable and non-identifiable, within the department’s possession, custody, or control.
- B. **Data stewardship:** The responsibility carried out on behalf of a group, institution, or the public in general to safeguard, protect, and optimize the use of the data resources. Data stewardship relates to the data collected by an organizational unit under the authority of the department. Protecting the department’s data resources includes, and is subject to, all the laws, statutes, administrative rules, contracts or agreements that pertain to the data.

- C. **Data Steward:** A data steward is a department employee who carries out data stewardship responsibilities as defined in this policy.
- D. **DHHS or department:** The Utah Department of Health and Human Services and any operational unit within.
- E. **Disclosure:** The communication of data to any individual or organization outside the department or to operational units within the department that do not routinely have access to the data.
- F. **OU:** Operational units within DHHS, including divisions, offices or standalone operations whose director reports to the executive director, a deputy director, an assistant deputy director, or a division director.

III. POLICY

- A. The department, in its authority to administer the agency, is the owner of the data. OUs shall act as data stewards of these data.
- B. All individuals and contracted partners within the department who oversee, access or use data shall:
 - 1. Treat the department's data as a department-wide asset in support of the department's mission. These data are utilized to determine resource allocation, the effectiveness of programs and systems, and measuring outcomes of individuals served by the department;
 - 2. Ensure the data is properly protected, utilized, and disclosed within the limits of federal and state laws, statutes, administrative rules, memorandums of agreements, grants, and contracts; department policies and relevant ethical principles;
 - 3. Immediately report any suspected violations of information security to the data steward and chief privacy & security officer once they become aware of or suspect a violation, or as soon as practical as outlined within department Security Incident Procedures policy. Incident reporting shall be conducted strictly on a need to-know basis and should not be communicated to individuals not involved with the incident, and
 - 4. Successfully complete the department's privacy and security annual training; or within 30 days of hire, or assignment.
- C. The Director of Data, Systems and Evaluation and the Chief Privacy and Security Officer shall ensure consistency in data stewardship performance.
- D. Each operational unit whose organizational programs collect or hold data shall ensure a data steward is designated for department data resources and ensure defined review and approval procedures for data disclosure are followed per department Data Sharing policy 07-04.
- E. OU directors whose organizational programs collect or hold data shall:
 - 1. Be responsible for the overall handling and stewardship of applicable data resources;

2. Be trained in federal and state laws, statutes, administrative rules, memorandums of agreements, grants and contracts that apply to the data resources under their purview, and
 3. Determine which of its data resources are significant sources of information for surveillance, needs assessment, policy making, and program evaluation.
- F. A data steward does not have the right to conceal or hold protected data for personal benefit, disclose protected data without proper authorization, or arbitrarily limit access to the data.
- G. Data stewards and their designees shall:
1. Be trained in federal and state laws, statutes, administrative rules, memorandums of agreements, grants and contracts that apply to the data resources under their purview;
 2. Successfully complete the DHHS data steward training annually or within 30 days of hire, or assignment.
 3. Oversee the appropriate handling, general safeguarding and optimization of all data under their stewardship which includes:
 - A) Ensuring federal code or regulation, state code or administrative rule, contract, grant, or agreement that pertains to release of the data are followed. If issues related to data use, data sharing, and data security are present they are to seek resolution within the department's chain of command;
 - B) Implementing, maintaining and monitoring data access and security management policies, procedures, processes, and plans for data resources under their purview;
 - C) Assuring that data are modified only in appropriate ways;
 - D) Assuring that data are accessed only by authorized individuals and for authorized purposes;
 - E) Ensuring that human subjects research reviews and ethical reviews are conducted by the department's Institutional Review Board (IRB) or the ethics committee, where warranted;
 - F) Ensuring appropriate disposition of data;
 - G) Ensuring reporting of real or suspected violations of security or a material breach occurs, as outlined within the department Security Incident Procedures policy, for data under their purview, and
 - H) Following the requirements for managing records with the State Archives and supporting the records officer's functions.
- H. IRB Oversight
1. The IRB shall conduct a professional and ethical review of proposed projects and research protocols that involve the use of department data or publication of findings to determine the soundness of scientific protocol, risk to subjects, potential benefit gains, ethical considerations, and risk to the department.

IV. PROCEDURE

- A. The Director of Data, Systems and Evaluation and the Chief Privacy and Security Officer shall:
 1. Conduct reviews of policy and procedures of data stewardship, training, data sharing agreements, and
 2. Provide overall guidance to department data stewards.
- B. Each OU director shall:
 1. Identify and assign a data steward for each data resource under their management and include the assignments and responsibilities in the performance plans of the named individuals.
 2. Maintain the department's data inventory log by:
 - A) Publishing the data steward(s) names and contact information along with the assigned data resource under their purview.
 - B) Review federal or private grants, data sharing provisions, memorandum of agreements or understanding, and data sharing agreements entered into on behalf of the department to ensure appropriate data sharing provisions are included.
- C. Data stewards or their designees shall:
 1. Facilitate access, use and sharing of the data resources, to the extent allowed by federal and state requirements, statutes, administrative rules, department policies, and relevant ethical principles by:
 - A) Familiarizing themselves with the protections, requirements and guidelines associated with the data.
 - B) Seeking advice and direction from a supervisor, the division Assistant Attorney General, or the Chief Privacy & Security Officer, as needed when appropriateness of access, use or sharing is in question.
 - C) Participate in the creation and maintenance of disaster recovery and business continuity plans regarding the data resource by:
 - (1) Completing required training(s), and
 - (2) Participating in meetings or other associated communications.
 2. Ensure data sharing agreements are fully executed, where appropriate by:
 - A) Coordinating with identified department staff tasked with creation of the agreements, and
 - B) Verifying the required procedures and protections, as outlined within the DHHS Data Sharing policy, 07.04 have been followed.
 3. Ensure that IRB reviews occur for uses of data that constitute human subjects research by:
 - A) Working with the requester of the data to verify the request has been submitted to the appropriate IRB Review board, and
 - B) Verifying the IRB's decision for requested use.
 4. Document and maintain adequate records for:

- A) Data management, which outlines management procedures and practices of the data.
- B) Data collection including:
 - (1) Description of the data, and
 - (2) Authorizing law, statute or administrative rule.
- C) Data Disclosure including:
 - (1) If approved:
 - (A) Agreement effective and termination dates;
 - (B) The party, or parties, with whom data is shared;
 - (C) Data elements shared;
 - (D) Intended uses of the data;
 - (E) Data disclosure frequency;
 - (F) Method used to transmit the data;
 - (G) Approved duration of use;
 - (H) Whether IRB approval was required;
 - (I) Data disposition requirements, and
 - (J) Verification of data disposition at termination.
 - (2) If denied:
 - (A) Date of the request;
 - (B) Requestor;
 - (C) Purpose;
 - (D) Data requested;
 - (E) Reason for denial, and
 - (F) Date notification was issued.
- D) IRB reviews including:
 - (1) Title of study;
 - (2) Data source, and
 - (3) Outcome of the review.
- E) Data Destruction/Disposal including:
 - (1) Attestation of disposition of the data using the designated destruction of data certificate template, see Appendix I;
 - (2) Date of destruction/disposal;
 - (3) Person or organization responsible for the disposition;
 - (4) Method of destruction/disposal;
 - (5) Description of the destroyed/disposed record series or medium,
or
 - (6) Document why disposing of the data is not feasible and whether it is indefinite or for a specified period of time.

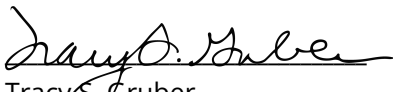
D. Institutional Review Board

- 1. As part of the review process the board shall:
 - A) Ensure data steward(s) are included in a proposed project and have approved the use of the data;

- B) Provide a copy of IRB approved proposals to the data steward(s) of the data;
- C) Notify data steward(s) of requests for continuations or modifications to project or protocol;
- D) Validate data steward approval prior to IRB approval, and
- E) Ensure modification of data sharing agreements occurs, when necessary.

V. EXCEPTIONS

- A. There are no exceptions to this policy.


Tracy S. Gruber

Date **September 19, 2022**

Utah Department of Health and Human Services Executive Director

APPENDIX I: DHHS Certificate of Destruction Template

CERTIFICATE OF DESTRUCTION	
<i>The information described below was destroyed in the normal course of business pursuant to the Departmental retention schedule and destruction policies and procedures.</i>	
Date of Destruction:	Authorized By:
Description of Information Disposed Of/Destroyed:	
Media Type:	
Inclusive Dates Covered:	
METHOD OF DESTRUCTION:	
<input type="checkbox"/> Burning <input type="checkbox"/> Pulping <input type="checkbox"/> Pulverizing	<input type="checkbox"/> Shredding <input type="checkbox"/> Overwriting <input type="checkbox"/> Reformatting
<input type="checkbox"/> Other:	
Records Destroyed By*:	
If On Site, Witnessed By:	
Department Manager:	

*Shall confirm a contract exists if records are destroyed by an outside firm.