

# Utah Department of Health

## Bureau of Emergency Medical Services and Preparedness

### Data Release Policy

The Utah Department of Health, Bureau of Emergency Medical Services and Preparedness, data release policy is based on Utah Code and the Department of Health Data Stewardship Policy.

#### Purpose

The purpose of this policy as outlined in the Utah Department of Health Data Stewardship Policy is to,

- A. *Assure data are treated as an asset and utilized to the fullest extent;*
- B. *Assure wide access to and use of data within the limits of existing statutes, rules, federal requirements, Department policies, and relevant ethical principals;*
- C. *Assure coordinated collection of data and requests for data;*
- D. *Provide guidance for data sharing practices;*
- E. *Assure that data are managed to protect confidentiality;*
- F. *Assure that the data are used in the proper context;*
- G. *Establish roles and responsibilities associated with the implementation of this policy.*

#### Definitions

The following definitions from Utah Code Title 26 Chapter 3 are included in this policy:

- (1) *“Disclosure” or “disclose” means the communication of health data to any individual or organization outside the department.*
- (2) *“Health data” means any information, except vital records as defined in Section 26-2-2, relating to the health status of individuals, the availability of health resources and services, and the use and cost of these resources and services.*
- (3) *“Identifiable health data” means any item, collection, or grouping of health data which makes the individual supplying it or described in it identifiable.*
- (4) *“Individual” means a natural person.*
- (5) *“Organization” means any corporation, association, partnership, agency, department, unit, or other legally constituted institution or entity, or part of any of these.*
- (6) *“Research and statistical purposes” means the performance of activities relating to health data, including:*
  - (a) *describing the group characteristics of individuals or organizations;*
  - (b) *analyzing the interrelationships among the various characteristics of individuals or organizations;*
  - (c) *the conduct of statistical procedures or studies to improve the quality of health data;*

- (d) the design of sample surveys and the selection of samples of individuals or organizations;*
- (e) the preparation and publication of reports describing these matters; and*
- (f) other related functions.*

The following definitions from Utah Code Title 63G Chapter 2 (Government Records Access and Management Act) are included in this policy:

*(1) The following records are private:*

- (a) records concerning an individual's eligibility for unemployment insurance benefits, social services, welfare benefits, or the determination of benefit levels;*
- (b) records containing data on individuals describing medical history, diagnosis, condition, treatment, evaluation, or similar medical data...*

A record is controlled if:

- (1) the record contains medical, psychiatric, or psychological data about an individual;*
- (2) the governmental entity reasonably believes that:
  - (a) releasing the information in the record to the subject of the record would be detrimental to the subject's mental health or to the safety of any individual; or*
  - (b) releasing the information would constitute a violation of normal professional practice and medical ethics; and**
- (3) the governmental entity has properly classified the record...*

The following records are protected if properly classified by a governmental entity...

- (10) records the disclosure of which would jeopardize the life or safety of an individual...*

The Utah Department of Health Data Stewardship Policy provides further definitions for this policy:

- 1. Data stewardship – The responsibility carried out on behalf of a larger group, institution, or the public in general to safeguard, protect, and optimize the use of the data resources. Data stewardship in the Utah Department of Health 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 statutes and rules that pertain to the data. A data steward does not have the right to conceal or hold protected health data for personal benefit, disclose protected health data without proper authorization, or arbitrarily limit access to the data.*
- 2. Health data – Any data relating to the health status of people, living or dead; all forms of data relating to health including data on the extent and nature of the illness, disability and other aspects of well being; environmental, social and other health hazards; determinants of health.*
- 3. Identifiable health data – [Title 26-3-1 Definition] "Identifiable health data" means any item, collection, or grouping of health data which makes the individual supplying it or described in it identifiable.  
With regard to individuals, the term means any item, collection or grouping of data which contains the name of the individual or any identifying number, symbol,*

*other identifying characteristics, or any unique grouping of data, which, when combined with other available data, makes the individual recognizable. With regard to organizations that have received an assurance of non-disclosure from the Department, the term means, any item, collection or grouping of data, which makes the organization as recognizable as if a name had been affixed. Identifiable health data encompasses health data that identifies individuals by name, unique identifier, or other identifying characteristics. The definition also encompasses health data identifying organizations that have received an assurance of nondisclosure by the Department.*

4. *Disclosure – [Title 26-3-1 Definition] “Disclosure” or “disclose” means the communication of health data to any individual or organization outside the department.*
5. *Institutional Review Board (IRB) – An official Department body whose mission is to review for approval research projects involving human subjects. Certain statutes and rules define bona fide research approved by an IRB as one criterion for release of identifiable health data. Thus, IRB review and approval is required for certain uses of health data.*

## Data Release per Utah Code

The following sections from Utah Code Title 26 Chapter 3 are included in this policy:

*26-3-7.1. Disclosure of health data -- Limitations.*

*The department may not disclose any identifiable health data unless:*

- (1) one of the following persons has consented to the disclosure:*
  - (a) the individual;*
  - (b) the next-of-kin if the individual is deceased;*
  - (c) the parent or legal guardian if the individual is a minor or mentally incompetent; or*
  - (d) a person holding a power of attorney covering such matters on behalf of the individual;*
- (2) the disclosure is to a governmental entity in this or another state or the federal government, provided that:*
  - (a) the data will be used for a purpose for which they were collected by the department; and*
  - (b) the recipient enters into a written agreement satisfactory to the department agreeing to protect such data in accordance with the requirements of this chapter and department rule and not permit further disclosure without prior approval of the department;*
- (3) the disclosure is to an individual or organization, for a specified period, solely for bona fide research and statistical purposes, determined in accordance with department rules, and the department determines that the data are required for the research and statistical purposes proposed and the requesting individual or organization enters into a written agreement satisfactory to the department to protect the data in accordance with this chapter and department rule and not permit further disclosure without prior approval of the department;*

- (4) *the disclosure is to a governmental entity for the purpose of conducting an audit, evaluation, or investigation of the department and such governmental entity agrees not to use those data for making any determination affecting the rights, benefits, or entitlements of any individual to whom the health data relates;*
- (5) *the disclosure is of specific medical or epidemiological information to authorized personnel within the department, local health departments, official health agencies in other states, the United States Public Health Service, the Centers for Disease Control and Prevention (CDC), or agencies responsible to enforce quarantine, when necessary to continue patient services or to undertake public health efforts to control communicable, infectious, acute, chronic, or any other disease or health hazard that the department considers to be dangerous or important or that may affect the public health;*
- (6) *the disclosure is of specific medical or epidemiological information to a "health care provider" as defined in Section 78-14-3, health care personnel, or public health personnel who has a legitimate need to have access to the information in order to assist the patient or to protect the health of others closely associated with the patient. This Subsection (6) does not create a duty to warn third parties;*
- (7) *the disclosure is necessary to obtain payment from an insurer or other third-party payer in order for the department to obtain payment or to coordinate benefits for a patient; or*
- (8) *the disclosure is to the subject of the identifiable health data.*

26-3-8. *Disclosure of health data -- Discretion of department.*

*Any disclosure provided for in Section 26-3-7 shall be made at the discretion of the department, except that the disclosure provided for in Subsection 26-3-7(4) must be made when the requirements of that paragraph have been met.*

26-3-9. *Health data not subject to subpoena or compulsory process -- Exception. Identifiable health data obtained in the course of activities undertaken or supported under this chapter may not be subject to discovery, subpoena, or similar compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this chapter be compelled to testify with regard to such health data, except that data pertaining to a party in litigation may be subject to subpoena or similar compulsory process in an action brought by or on behalf of such individual to enforce any liability arising under this chapter.*

26-3-10. *Department measures to protect security of health data.*

*The department shall protect the security of identifiable health data by use of the following measures and any other measures adopted by rule:*

- (1) *limit access to identifiable health data to authorized individuals who have received training in the handling of such data;*
- (2) *designate a person to be responsible for physical security;*
- (3) *develop and implement a system for monitoring security; and*
- (4) *review periodically all identifiable health data to determine whether identifying characteristics should be removed from the data.*

The following sections from Utah Code Title 63G Chapter 2 (Government Records Access and Management Act) are included in this policy:

*63G-2-202. Access to private, controlled, and protected documents.*

- (1) Upon request, a governmental entity shall disclose a private record to:*
  - (a) the subject of the record;*
  - (b) the parent or legal guardian of an unemancipated minor who is the subject of the record;*
  - (c) the legal guardian of a legally incapacitated individual who is the subject of the record;*
  - (d) any other individual who:*
    - (i) has a power of attorney from the subject of the record;*
    - (ii) submits a notarized release from the subject of the record or his legal representative dated no more than 90 days before the date the request is made; or*
    - (iii) if the record is a medical record described in Subsection **63G-2-302(1)(b)**, is a health care provider, as defined in Section **26-33a-102**, if releasing the record or information in the record is consistent with normal professional practice and medical ethics; or*
  - (e) any person to whom the record must be provided pursuant to:*
    - (i) court order as provided in Subsection (7); or*
    - (ii) a legislative subpoena as provided in Title 36, Chapter 14.*
- (2) (a) Upon request, a governmental entity shall disclose a controlled record to:*
  - (i) a physician, psychologist, certified social worker, insurance provider or producer, or a government public health agency upon submission of:*
    - (A) a release from the subject of the record that is dated no more than 90 days prior to the date the request is made; and*
    - (B) a signed acknowledgment of the terms of disclosure of controlled information as provided by Subsection (2)(b); and*
  - (ii) any person to whom the record must be disclosed pursuant to:*
    - (A) a court order as provided in Subsection (7); or*
    - (B) a legislative subpoena as provided in Title 36, Chapter 14.*
- (b) A person who receives a record from a governmental entity in accordance with Subsection (2)(a)(i) may not disclose controlled information from that record to any person, including the subject of the record.*
- (3) If there is more than one subject of a private or controlled record, the portion of the record that pertains to another subject shall be segregated from the portion that the requester is entitled to inspect.*
- (4) Upon request, a governmental entity shall disclose a protected record to:*
  - (a) the person who submitted the record;*
  - (b) any other individual who:*
    - (i) has a power of attorney from all persons, governmental entities, or political subdivisions whose interests were sought to be protected by the protected classification; or*
    - (ii) submits a notarized release from all persons, governmental entities, or political subdivisions whose interests were sought to be protected by*

- the protected classification or from their legal representatives dated no more than 90 days prior to the date the request is made;*
- (c) *any person to whom the record must be provided pursuant to:*
    - (i) *a court order as provided in Subsection (7); or*
    - (ii) *a legislative subpoena as provided in Title 36, Chapter 14; or*
  - (d) *the owner of a mobile home park, subject to the conditions of Subsection 41-1a-116(5).*
- (5) *A governmental entity may disclose a private, controlled, or protected record to another governmental entity, political subdivision, another state, the United States, or a foreign government only as provided by Section 63G-2-206.*
- (6) *Before releasing a private, controlled, or protected record, the governmental entity shall obtain evidence of the requester's identity.*
- (7) *A governmental entity shall disclose a record pursuant to the terms of a court order signed by a judge from a court of competent jurisdiction, provided that:*
- (a) *the record deals with a matter in controversy over which the court has jurisdiction;*
  - (b) *the court has considered the merits of the request for access to the record; and*
  - (c) *the court has considered and, where appropriate, limited the requester's use and further disclosure of the record in order to protect:*
    - (i) *privacy interests in the case of private or controlled records;*
    - (ii) *business confidentiality interests in the case of records protected under Subsection 63G-2-304(1), (2), (40)(a)(ii), or (40)(a)(vi); and*
    - (iii) *privacy interests or the public interest in the case of other protected records;*
  - (d) *to the extent the record is properly classified private, controlled, or protected, the interests favoring access, considering limitations thereon, outweigh the interests favoring restriction of access; and*
  - (e) *where access is restricted by a rule, statute, or regulation referred to in Subsection 63G-2-201(3)(b), the court has authority independent of this chapter to order disclosure.*
- (8) (a) *A governmental entity may disclose or authorize disclosure of private or controlled records for research purposes if the governmental entity:*
- (i) *determines that the research purpose cannot reasonably be accomplished without use or disclosure of the information to the researcher in individually identifiable form;*
  - (ii) *determines that:*
    - (A) *the proposed research is bona fide; and*
    - (B) *the value of the research outweighs the infringement upon personal privacy;*
  - (iii)(A) *requires the researcher to assure the integrity, confidentiality, and security of the records; and*
  - (B) *requires the removal or destruction of the individual identifiers associated with the records as soon as the purpose of the research project has been accomplished;*
  - (iv) *prohibits the researcher from:*

- (A) *disclosing the record in individually identifiable form, except as provided in Subsection (8)(b); or*
- (B) *using the record for purposes other than the research approved by the governmental entity; and*
- (v) *secures from the researcher a written statement of the researcher's understanding of and agreement to the conditions of this Subsection (8) and the researcher's understanding that violation of the terms of this Subsection (8) may subject the researcher to criminal prosecution under Section 63G-2-801.*
- (b) *A researcher may disclose a record in individually identifiable form if the record is disclosed for the purpose of auditing or evaluating the research program and no subsequent use or disclosure of the record in individually identifiable form will be made by the auditor or evaluator except as provided by this section.*
- (c) *A governmental entity may require indemnification as a condition of permitting research under this Subsection (8).*
- (9) (a) *Under Subsections 63G-2-201(5)(b) and 63G-2-401(6), a governmental entity may disclose to persons other than those specified in this section records that are:*
  - (i) *private under Section 63G-2-302; or*
  - (ii) *protected under Section 63G-2-304 subject to Section 63G-2-308 if a claim for business confidentiality has been made under Section 63G-2-308.*
- (b) *Under Subsection 63G-2-403(11)(b), the records committee may require the disclosure to persons other than those specified in this section of records that are:*
  - (i) *private under Section 63G-2-302;*
  - (ii) *controlled under Section 63G-2-303; or*
  - (iii) *protected under Section 63G-2-304 subject to Section 63G-2-308 if a claim for business confidentiality has been made under Section 63G-2-308.*
- (c) *Under Subsection 63G-2-404(8), the court may require the disclosure of records that are private under Section 63G-2-302, controlled under Section 63G-2-303, or protected under Section 63G-2-304 to persons other than those specified in this section.*

Non-routine data requests and data requests subject to Utah Code Title 63G Chapter 2 (Government Records Access and Management Act) shall be forwarded to Department legal counsel for approval.

## Data Release per Department of Health

The following sections of Utah Department of Health Data Stewardship Policy are included in this policy:

...[E]ach data steward shall, for all data under stewardship:

- (a) *Update and maintain the relevant portions of the Department's Data Inventory on DOHnet;*

- (b) *Facilitate access to the data to the extent allowed by statutes, rules, federal requirements, Department policies, and relevant ethical principles;*
- (c) *Create and maintain data access, security and management plans;*
- (d) *Establish access policies and procedures that assure appropriate protection of both individual confidentiality/privacy and of the public trust under which those data are collected;*
- (e) *Create and maintain an adequate record of data collection and management procedures and practices (data management log);*
- (f) *Create and maintain disaster recovery and business continuity plans;*
- (g) *Assure that data are modified only in appropriate ways [using documented procedures];*
- (h) *Follow state and federal legal requirements regarding release of data;*
- (i) *Comply with the terms of applicable legal agreements and contracts;*
- (j) *Assure that data are accessed only by authorized individuals and for authorized purposes;*
- (k) *Comply with requirements for registration of data records with the state archivist and fulfilling functions of the records officer;*
- (l) *Implement data sharing agreements where appropriate;*
- (m) *Seek advice and direction from supervisor for unusual data use and data sharing situations;*
- (n) *Assure that IRB reviews occur for uses of data that constitute human subjects research and that ethical reviews are conducted, where warranted, for non-research uses of data.*

*IV. Procedures for Sharing Data Among Department Programs:*

*Data sharing among Department's organizational units and their programs and systems is both supported and encouraged. The data requester for both one-time and ongoing sharing of data shall negotiate with the appropriate data steward. The source data steward(s) shall document the data sharing decisions in an informal data sharing agreement, by tracking the:*

- A. Party, or parties, with whom data are shared;*
- B. Nature/type of the data shared;*
- C. Intended uses of the data;*
- D. Frequency of the exchange of data.*

*Formal data sharing agreements are not required but may be developed by the data stewards. Documented policies, procedures, and protocols that clarify appropriate uses of data are encouraged.*

*V. Procedures for Release of Identifiable Health Data to Parties Outside the Department for Research:*

- A. All requests for access to non-publicly available identifiable health data, made for research purposes by any outside organization or individual, shall be directed to the appropriate data steward. Requests must be in writing and must include:*
  - 1. Nature/type of the data requested;*
  - 2. Purposes for which the data will be used;*
  - 3. Allowable uses of the data;*

4. Assurance that the confidentiality and security of the data will be maintained;
  5. Provisions for data storage, retention, and disposal.
- B. Before deciding to release individually identifiable health data, the data steward(s) shall consider the following prior to releasing the data:
1. *Need for the Requested Data – Does there exist a compelling need or absolute necessity for the requested data; can the data be replaced with non-identifiable data; is this the minimum data to meet the need; does the need for this data justify the risk of disclosure; or can test data be used?*
  2. *Use of the Data – Will the data be used for legitimate purposes; will data use be restricted to the stated purposes?*
  3. *Confidentiality/Security of the Data – Will the data be safeguarded and protected; does there exist a potential for violation of the confidentiality of the data or actual physical theft or loss; will the data be disclosed or re-released to anyone at any time under any circumstances; and will the data be properly disposed?*
- C. *If uncertain if release is allowable, the data stewards shall obtain advice and direction from their immediate supervisor who will take the issue up the chain of command. If the proposed uses of the data constitute human subjects research or if statutes, rules, federal requirements, and Department policies require it, the data steward shall assure that human subjects review and approval by an appropriate IRB is obtained.*
- D. *Data sharing agreements are required for all external sharing of identifiable health data.*
- E. *The data steward will evaluate the feasibility and difficulty to produce the data and may request that an appropriate charge be paid to recover costs and applicable fees.*

#### *VI. Procedures for Release of De-identified Health Data to Parties Outside the Department:*

*Requests for de-identified health data by any outside organization or individual must be directed to the appropriate data steward.*

- A. *If the data are available publicly, the data steward shall direct the requestor to the appropriate source location.*
- B. *If the data are not publicly or generally available, the data steward will evaluate the feasibility and difficulty to produce the de-identified data and may request that an appropriate charge be paid to recover costs and applicable fees.*

#### *VII. Data Sharing Agreements*

- A. *Data sharing agreements shall be used with parties outside of the Department:*
  1. *When sharing identifiable health data;*
  2. *When sharing health data that has been de-identified by removing fewer than all of the data elements specified in the safe harbor provisions of the HIPAA privacy regulation.*

- B. *Data sharing agreements are not required to share data that has been de-identified by removing all or more of the data elements specified in the safe harbor provisions of the HIPAA privacy regulation, unless those data still could meet the definition of identifiable data included at the end of this document.*
- C. *Data sharing agreements may be required to share data among Department programs depending on the applicable statutes and regulations.*
- D. *Upon agreement from the data steward, or from the appropriate level of management, approval to access the data can be granted, with the following assurances given by the data requestor and recorded in a formal data sharing agreement:*
- *Party, or parties with whom data will be shared;*
  - *Time period of the agreement;*
  - *Nature/type of the data requested;*
  - *Intended uses of the data;*
  - *Frequency of the exchange of data;*
  - *Requirement that the requestor will protect completely the confidentiality of the data provided;*
  - *Requirement that the requestor will not disclose or release the identifiable health data without specific written permission from the Department;*
  - *Requirement that the requestor will report immediately the loss or theft of any identifiable data or related confidential materials to the appropriate Data Steward;*
  - *How the requestor will maintain the confidentiality and the security of the data;*
  - *A statement that the Department is either the owner or has rights to control the use and dissemination of the data;*
  - *Provision describing and how the data will be disposed of at the conclusion of the agreement;*
  - *Assurances that the requestor will obey all state and federal laws regarding the use of the data;*
  - *Specification of rights for audit of data use practices;*
  - *Provisions regarding secondary release of the data;*
  - *A provision that the recipient will hold the Department harmless from all liability arising from the recipient's use or disclosure of the data; and*
  - *Consequences of violation of the agreement.*

## Policy Implementation

This policy is to be implemented according the Bureau of Emergency Medical Services and Preparedness Data Release Procedures.

## Unresolved Issues

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, Bureau of Emergency Medical Services and Preparedness.