

OREGON STATE HOSPITAL

POLICIES AND PROCEDURES

SECTION 1: Administration

POLICY: 1.014

SUBJECT: Data Governance

**POINT
PERSON:** DATA AND ANALYSIS MANAGER

APPROVED: DOLORES MATTEUCCI
SUPERINTENDENT

DATE: DECEMBER 12, 2019

I. POLICY

- A. Oregon State Hospital (OSH) will govern data as a component of hospital data management.
- B. The Data Governance Committee (DGC) will make data governance decisions, including:
 1. establishing appropriate responsibility for managing OSH data as an institutional asset;
 2. addressing data integrity by formalizing data security, collection, distribution, and retention; and
 3. governing information asset distribution according to the context for which it was created.
- C. DGC will govern an information asset that exceeds established thresholds for sensitivity or scope of distribution.
 1. A unit or department may control an information asset which is created by that unit or department and which is never reported, presented, or used by another department.
 2. An information asset created by a unit or department and which is reported or used by a unit or department other than the one that created it must be assessed by the Data and Analysis Department (DA) to determine whether governance is needed.
- D. Information assets that require governance will be standardized as delineated in this policy.
- E. This policy applies to all staff including employees, volunteers, trainees, interns, contractors, vendors, and other state employees assigned to work at OSH.
- F. OSH follows all applicable regulations, including federal and state statutes and

rules; Oregon Department of Administrative Services, Shared Services, and Oregon Health Authority policies; and relevant accreditation standards. Such regulations supersede the provisions of this policy unless this policy is more restrictive.

- G. Staff who fails to comply with this policy or related procedures may be subject to disciplinary action, up to and including dismissal.

II. DEFINITIONS

“Assessment” for the purposes of this policy refers to analyzing an information asset to determine if the data contained within exceeds the established thresholds for either sensitivity or scope of distribution.

“Data” for the purposes of this policy refers to the most basic component of electronic information stored on OSH’s networks in the form of words, numbers, diagrams, and images. Data refers to the value of numbers, definition of words, or images.

“Data elements” refers to a unit of data defined by type (e.g., alphanumeric, true/false, text, date); and name (i.e., “field name”, “tag”, or “caption”) or other identifier. Some data elements have additional attributes such as size (e.g., number of characters or digits of precision) and permissible values. Examples of data elements are: patient identification number, patient name, phone number, county, diagnosis, or date of birth.

“Data governance” means strategic planning and decision making on data-related issues. Data governance activities include, but are not limited to: addressing policies and strategic initiatives on data-related topics; establishing data standards and protocols for collection, displaying and storing data; and addressing data integrity issues by verifying that data is reported and presented within the appropriate context for which it was intended.

“Data sensitivity” refers to data or information which requires controls on disclosure. OSH-defined sensitive data elements are in the List of Governed Data Elements. Examples of sensitive data include, but are not limited to: patient identification number, patient name, admit date, diagnosis, or legal status.

“Discovery” refers to a continuous communication cycle of data governance at OSH that includes DA scheduling annual assessments of known information assets and directors and department managers notifying DA when a new information asset is created.

“Information asset” refers to a compilation of data where context can be applied and includes, but is not limited to: reports, spreadsheets, databases, directories, repositories of images, the electronic health record, or any combination of the above.

“List of Governed Data Elements” refers to a list of data elements maintained by the DGC. Data elements on this list contain data that exceed the threshold established for either data sensitivity or scope of distribution. Examples of data elements on the list include: patient identification number, social security number, or diagnosis.

“Scope of distribution” is a threshold established by the DGC that refers to the intended audience and distribution of information.

“Standardization” is a process of applying OSH data guidelines to an information asset. OSH data guidelines are maintained by DA and Technology Services and include, but are not limited to:

- a. formalizing policies, rules, procedures, and protocols for the collection, display, transmission, security, and retention of data;
- b. requiring the use of uniform procedures for collection, validation, display and distribution for information assets that exceed the thresholds established for data sensitivity and scope of distribution;
- c. establishing safeguards and controls to guard data against accidental loss, damage, unauthorized alteration, unintentional change, and accidental destruction; and
- d. monitoring the compliance and continuous improvement process for hospital data.

III. PROCEDURES

- A. DA will assess information assets according to established data element criteria for sensitivity and scope of distribution.
- B. DA will conduct annual discovery assessments of all known information assets used for reporting.
 1. A manager must notify DA when a new information asset is created with the intent to be distributed beyond the manager’s unit or department.
 2. DA will schedule an assessment when notified of a new information asset.
- C. The DGC will maintain a List of Governed Data Elements.
 1. DGC members will propose data element actions for the List of Governed Data Elements.
 2. Changes to the List of Governed Data Elements will be determined by majority vote of the DGC.
 3. The List of Governed Data Elements will be reviewed regularly at DGC meetings.
- D. Technology Service or DA will schedule standardization work for information assets that require governance.

- E. A request for an exception to formalized standardization can be made to the DGC. The requestor must submit the request in writing detailing the reasoning for the exception.

IV. REFERENCES

Department of Human Services and Oregon Health Authority Shared Services. *General security policy*, 090-001. Author.

Department of Human Services and Oregon Health Authority Shared Services. *Information system audit and monitoring policy*, 090-002. Author.

Department of Human Services and Oregon Health Authority Shared Services. *Information security and privacy awareness and training*, 090-004. Author.

Joint Commission Resources, Inc. (2019). *The joint commission comprehensive accreditation manual for hospitals*, IM.02.01.03 EP2. Oakbrook Terrace, IL: Author.

Joint Commission Resources, Inc. (2019). *The joint commission comprehensive accreditation manual for hospitals*, IM.02.02.03 EP1. Oakbrook Terrace, IL: Author.

Office of Information Services (2016, February). *General privacy*, 100-001. Author.

Oregon State Hospital Policy and Procedure Manual. *Electronic health record access*, 2.013. Author.

Oregon State Hospital Policy and Procedure Manual. *Records retention and destruction*, 2.006. Author.

Oregon State Hospital Policy and Procedure Manual. *Privacy and security of patient information*, 2.008. Author.