I. Policy

A. Oregon State Hospital (OSH) will govern data as a component of hospital data management.

B. Information assets that require governance must be standardized.

C. The Data Governance Committee (DGC) will be responsible for data governance decisions in accordance with the plan for governing data.

D. The plan for governing data includes:
   1. establishing appropriate responsibility for the management of OSH data as an institutional asset;
   2. addressing the integrity of data by formalizing security, collection, distribution, and retention of data; and
   3. governing the distribution of information assets according to the context for which it was created.

II. Definitions

A. “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.

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

D. “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.

E. “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.

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

G. “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.

H. “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.

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

J. “Staff” for the purposes of this policy means OSH employees, students, interns, contractors, volunteers, and state employees assigned to work at OSH.

K. “Standardization” is a process of applying OSH data guidelines to an information asset. OSH data guidelines are maintained by Technology Services and Data Analysis. These guidelines 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 process for compliance and continuous improvement for hospital data.

III. PROCEDURES

A. Data Collection and Distribution

a. An information asset created by a unit or department and that is never reported, presented, or used by another department has a limited scope. The unit or department may control the context of the information asset’s use within that unit or department.

b. An information asset created by a unit or department and reported or used by a unit or department other than the one that created it has a greater scope of distribution. The information asset must be assessed by DA to determine whether governance is needed.

B. Discovery

1. Data and Analysis will conduct annual assessments of all known information assets used for reporting.

2. 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.

3. Data and Analysis will schedule an assessment when notified of a new information asset.

C. Assessment

1. Information assets will be assessed by DA based upon criteria for sensitivity and scope of distribution. An information asset that exceeds the threshold for either sensitivity or scope of distribution requires governance by the DGC.

   a. The assessment will compare the elements contained in the information asset with the List of Governed Data Elements. An information asset that contains elements listed on the List of Governed Data Elements exceed the threshold for sensitivity.
b. Information that is distributed to an audience beyond the scope of the unit or department that created it exceeds the threshold for scope of distribution.

2. The DGC will maintain the List of Governed Data Elements.
   a. DGC members will submit data elements for consideration to be placed upon or removed from the List of Governed Data Elements.
   b. The decision for placing a data element on the List of Governed Data Elements or removing a data element from the List of Governed Data Elements will be determined by majority vote of the DGC.
   c. The List of Governed Data Elements will be reviewed regularly at DGC meetings.

D. Standardization
   1. An information asset that requires governance will be scheduled for standardization work by staff from Technology Services or Data Analysis.
   2. An information asset that has been processed through the standardization process is governed.
   3. 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. *Information system audit and monitoring policy*, 090-002. Author.

Department of Human Services and Oregon Health Authority Shared Services. Security awareness, training and enforcement, 090-004. Author.


