SPG U-M Standard Practice Guide

Institutional Data Resource Management Policy

601.12

Applies to: All Departments and Units of the University

Search this page

I. PURPOSE

The University of Michigan's *institutional data*[1] resource, by definition, practice, and intent, is a University asset. This SPG establishes policy for the management of University *institutional data* (as defined below) and the responsibilities for the protection of those data. The policy refers to all *institutional data*, whether verbal[2], printed, or electronic, and whether individually controlled, shared, stand alone, or networked.

The policy will serve to:

Ensure establishment, maintenance, and delivery of secure, confidential, trustworthy, stable, reliable, and accessible collections of *institutional data* for shared access by the University community;

Maximize the value received from the data asset by increasing the understanding and use of the data;

Provide an integrated view of the functions of the University;

Improve direct access to data by end-users in accordance with institutional policies and state and federal privacy and security laws and regulations;

Support the University's strategy to incorporate information technology as an integral part of decision-making, competitive positioning, and delivery of services.

II. GOALS

Successful management and protection of information and data is critical to the administrative, clinical, educational, and research functions of the University. Through active planning, organization, and control of these institutional resources, we will:

Manage information as a strategic asset to improve the quality of services to the University and University Healthcare communities;

Implement databases that are consistent, reliable, and accessible to meet institutional requirements;

Provide data management services which result in the highest quality data to all units to help maximize the efficiency and effectiveness of their processes;

Implement and maintain security policies and procedures to protect the data resource.

III. POLICY

The data resource will be safeguarded/protected. As an institutional asset, data will be protected from deliberate, unintentional, or unauthorized alteration, destruction and/or inappropriate disclosure or use in accordance with established institutional policies and practices and federal and state laws.

Data will be shared based on institutional policies, and federal and state laws. *Institutional data*, including *electronic protected health information (ePHI)*, are not owned by a particular individual, unit, department, or system of the University. The data will be made accessible to all authorized users and systems.

Data will be managed as an institutional resource. Data organization and structure will be planned on functional and institutional levels. Data usage and data sources will be managed through the data stewardship principles of administering and controlling data quality and standards in support of institutional goals and objectives.

***Institutional data* will be identified and defined.** Standards will be developed for their representation in the database. Controls will be established to assure the completeness and validity of the data, and to manage redundancy.

Databases will be developed based on needs of University processes. Data architectures will be developed to support our institutional processes. These data architectures will drive physical implementation of databases.

Information quality will be actively managed. Explicit criteria for data validity, availability, accessibility, interpretation, and ease of use will be established and promoted. Action programs for data quality improvement will be implemented.

Contingency plans will be developed and implemented. Disaster Recovery/Business Continuity plans and other methods of responding to an emergency or other *occurrences of damage to systems containing institutional data, including electronic protected health information (ePHI)*, will be developed, implemented, and maintained. These contingency plans shall include, but are not limited to, data backup, disaster recovery, and emergency mode operations procedures. These plans will also address testing of and revision to disaster recovery/business continuity procedures and a criticality analysis.

Access to data will be authorized and managed. User's right of access to *institutional data* will be granted based on authorization provided by University staff who have been designated by the *data steward* as authorized signers for that data. Authorization to access *institutional data*, including *sensitive data*, will be based on appropriateness to the user's role and the intended use. Access will be consistent with applicable requirements of University policies and federal and state laws and will be granted only to those individuals or systems that have been authorized. Authorization and access will be documented, reviewed, modified, and terminated in accordance with University policies, and federal and state laws.

IV. RESPONSIBILITIES FOR IMPLEMENTATION

Every University Dean and Director is responsible for implementing and ensuring compliance with the University of Michigan *Institutional Data* Resource Management Policy and must initiate corrective action with the proper authorities of the University if it is needed. Responsibilities include:

- Applying the University of Michigan Data Administration Guidelines for *institutional data* Resources to the *institutional data* under their stewardship.
- Communicating this policy to employees.
- Establishing specific goals, objectives, and action plans to implement the policy.
- Developing plans that guide information system and database development to satisfy both customers and institutional information needs.
- Actively supporting strong data management through data stewardship.
- Ensuring availability of education and training in data management principles, including security awareness, to workforce members whose jobs require them to access, maintain or use this data.
- Providing an appropriate level of security that corresponds to the sensitivity of the information.

V. DEFINITIONS

DATA STEWARDS are the University Executive Officers having policy-level responsibility for managing a segment of the University’s information resource (see the Data Administration Guidelines for *institutional data* Resources for specific responsibilities).

ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) is a type of sensitive data and refers to information that is created, received, maintained or transmitted electronically that was created or received by a health care provider, health plan,

Attachment	Size

public health authority, employer, life insurer, school or university, or health care clearinghouse; and it relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

INSTITUTIONAL DATA refers to a data element which satisfies one or more of the following criteria:

PRIVATE/CONFIDENTIAL DATA refers to data whose unauthorized disclosure may have moderate adverse effect on the University's reputation, resources, services, or individuals. This is the default classification category and should be assumed when there is no information indicating that data should be classified as public or sensitive.

PUBLIC DATA refers to data whose disclosure to the general public poses little or no risk to the University's reputation, resources, services, or individuals.

SENSITIVE DATA refers to data whose unauthorized disclosure may have serious adverse effect on the University's reputation, resources, services, or individuals. Data protected under federal or state regulations or due to proprietary, ethical, or privacy considerations will typically be classified as sensitive

WORKFORCE MEMBER refers to any faculty, staff, student, volunteer, trainee, or other person whose conduct is under the University's direct control, whether or not the University pays them for their services.

It is relevant to planning, managing, operating, controlling, or auditing administrative functions of an administrative or academic unit of the University;

It is created, received, maintained, or transmitted as a result of educational, clinical, research or patient care activities;

It is generally referenced or required for use by more than one organizational unit;

It is included in an official University administrative report;

It is used to derive an element that meets the criteria above;

It is generated by a University workforce member or agent using any of the above data.

[1] Words that appear in italics are defined in the DEFINITIONS section.

[2] HIPAA http://www.med.umich.edu/u/hipaa/index.htm requires taking reasonable precautions when verbally communicating protected health information. Precautions should also be taken when verbally communicating other sensitive information.

Attachment	Size
Printable PDF of SPG 601.12	37.13 KB

SPG number:
601.12

Date issued:
May 3, 1994

Last updated:
March 6, 2008

Next review date:
January 24, 2009

Applies to:
All Departments and Units of the University

Owner:
Office of the Provost and Executive Vice President for Academic Affairs

Primary contact:
Office of the CIO

Related policies:
Identity Misrepresentation
Information Security Incident Reporting
Information Security Policy
Responsible Use of Information Resources

Related links:
Information Technology Policies and Standards