

ODH Directive 24A DATA STEWARDSHIP

Subject: **Data Stewardship**

1. Purpose. The purpose of this policy is to:

- A. Assure data are treated as an asset and utilized to the fullest extent within the limits of existing statutes, rules, federal requirements, Department policies, and relevant ethical principles;
- B. Assure a consistent process for handling requests for data access and release;
- C. Provide guidance for data access and release;
- D. Assure that data are managed to protect confidentiality and security;
- E. Assure that data resources include sufficient documentation to allow appropriate use and interpretation; and
- F. Establish roles and responsibilities associated with the implementation of this policy.

This directive supersedes any past practice, previously issued directive or previously issued policy and will remain in effect until canceled or superseded. The Office of the General Counsel is responsible for this directive.

2. Discussion. Data are essential to the mission and purpose of the Ohio Department of Health (Department). Data collected by organizational units or individuals within the Department are collected under the authority of the Department. The stewardship and use of those data are ultimately the responsibility of the Department. All Department employees and contracted individuals working for an organizational unit within the Department must protect the confidentiality of the data and are subject to ODH Directive 7: Use and Security of Agency IT Resources.

The missions and purposes of organizational units within the Department often complement each other and sharing data helps the Department to accomplish its overall mission. In order to help the programs meet their goals, the Department supports data sharing between its organizational units whenever that sharing supports legitimate public health purposes.

Organizational units and their data stewards are responsible to ensure the best and proper use of data under their stewardship. They should facilitate and

promote the sharing of data as an asset to support legitimate public health purposes. For data sharing within the Department, written policies, protocols, and agreements are encouraged for tracking purposes and for clarifying appropriate uses of data. Data sharing agreements or a memorandum of understanding are generally needed when sharing data with state agencies or other governmental or non-governmental parties outside the Department. ODH Institutional Review Board approval is generally needed when sharing data with entities external to the Department.

Data stewards may limit access to data when necessary to exercise appropriate stewardship of those data (e.g., preventing inappropriate disclosure of confidential data). However, the exercise of data stewardship includes the support of internal data sharing and does not include arbitrarily restricting access to data resources.

3. Definitions. Several terms are explained for the purpose of creating a common understanding of the issues covered by this policy.

A. 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 Ohio 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.

B. 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.

C. Disclosure: Definition: "Disclosure" or "disclose" means the communication of health data to any individual or organization outside the department.

D. 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.

E. Protected Health Information: Information, in any form, including oral, written, electronic, visual, pictorial, or physical that describes an individual's past, present, or future physical or mental health status or condition, receipt of

treatment or care, or purchase of health products, if either of the following applies:

- (1) The information reveals the identity of the individual who is the subject of the information; or
- (2) The information could be used to reveal the identity of the individual who is the subject of the information, either by using the information alone or with other information that is available to predictable recipients of the information.

4. Responsibilities.

A. General Responsibilities. All individuals in the Department must adhere to ODH Directive 7: Use and Security of Agency IT Resources. All individuals in the Department who use health data have responsibilities that include:

- (1) Protecting the confidentiality of data within the limits of existing statutes, rules, federal requirements, Department policies, and relevant ethical principals; and
- (2) Referring requests for data to the appropriate data steward.

B. Data Steward Responsibilities. In addition to the general responsibilities of employees described under paragraph 3.A above, each data steward shall, for all data under stewardship:

- (1) Work with the Office of the General Counsel and the Institutional Review Board to determine whether data are public or non-public and to develop data access and release policies and procedures for sharing of non-public individual level and tabulated health data among Departmental Programs and to Parties Outside the Department to include the development of Data Sharing Agreements;
- (2) Develop a schedule with the Office of the General Counsel for regular and routine review of the policies and procedures adopted;
- (3) Facilitate access to data to the extent allowed by existing statutes, rules, federal requirements, Department policies, and relevant ethical principles; comply with the terms of applicable legal agreements and contracts regarding release of data; and implement data sharing agreements where appropriate;
- (4) Maintain a log of all data requests and releases;

- (5) Assure that Institutional Review Board review occurs as appropriate for access and release of all individual level data;
- (6) Assure that all data requests, particularly denials of public record requests, are coordinated with the Office of the General Counsel in accordance with the procedures developed pursuant to this policy;
- (7) Update and maintain relevant portions of the Department's Guide to Selected ODH Databases on ODHNet, including contact information for the data steward;
- (8) Work with the Office of Management Information Systems (OMIS) to create and maintain data access, security and management plans for electronic data sets that are accessed only by authorized individuals and for authorized purposes;
- (9) Perform an annual review with supervisors and OMIS to insure appropriate user's data access rights;
- (10) Tracking of searches of any of the Department's databases is required and shall be tracked pursuant to Ohio Revised Code sections 1347.99, 121347.15, 5703.211, and 1347.15; and
- (11) Respond to requests for data only as allowed by this policy, other Department policy, or state or federal law.

C. Division/Office Responsibilities. Each Division / Office Chief whose organizational units / programs collect or hold data shall:

- (1) Assure that a data steward is assigned to each data resource in their respective Divisional Office;
- (2) Assure that data steward assignments and responsibilities are incorporated into job descriptions for named individuals;
- (3) Assure that supervisors of data stewards support the functions and responsibilities of named individuals;
- (4) Assure the development of data access and release policies and procedures for data resources in their respective Division / Office;
- (5) Seek resolution from the Office of the General Counsel for non-routine requests for data access and release; and
- (6) Assure timely response to requests for data access and release.

D. Office of the General Counsel Responsibilities. To bring consistency in data stewardship performance, the Office of the General Counsel shall:

- (1) Advise on the development of access policies and procedures that assure appropriate protection of both confidentiality / privacy and the public trust under which those data are collected;
- (2) Approve access policies and procedures prior to implementation by data steward;
- (3) Review non-routine data sharing requests and provide advice to the appropriate data steward;
- (4) Document opinions and advice, where appropriate; and
- (5) Orient and update data stewards on new state laws that may impact data confidentiality and release.

E. Institutional Review Board Responsibilities. The ODH IRB will approve, in conjunction with the ODH Office of General Counsel, access policies and procedures prior to implementation by a data steward. In addition, an ODH IRB review must occur as a requirement for access and release of individual level data sets. Before recommending release of individual level health data sets, the IRB shall be satisfied of the following:

- (1) There exists a compelling need or absolute necessity for the requested data set;
- (2) The data set need cannot be met with public individual level data;
- (3) The data set is the minimum appropriate to meet the data need;
- (4) The need for this data set justifies the risk of disclosure;
- (5) The data set will be used for legitimate purposes;
- (6) The data set will be restricted for the stated purposes it is requested;
- (7) The data will be safeguarded and protected; and
- (8) The data set will be properly disposed of at the end of the study period.

All requests for Individual Level Data Sets shall be reviewed on a regular schedule.

F. Office of Management Information Systems. OMIS shall assure the creation and maintenance of data access, security and management plans for electronic data sets available through the Department's secure warehouse including measures to assure that electronic data sets available through the Department's secure warehouse are accessed only by authorized individuals.

5. Procedures for Individual Level Health Data. The following procedures shall be followed for the sharing or release of individual level health data:

A. Sharing Between Department Programs. Data sharing between the Departments organizational units and their programs and systems is both supported and encouraged. The source data steward(s) shall document the data sharing decisions in a data sharing log that includes the party or parties, with whom data are shared; the nature type of the data shared; the intended uses of the data; and the frequency of the exchange of data. Documented policies, procedures, and protocols that clarify appropriate uses of data are required.

B. Release to Parties Outside the Department. All requests for access to individual level health data, made by any outside organization or individual, shall be directed to the appropriate data steward. Requests must be in writing and must include a completed ODH Institutional Review Board Application. The Bureau or Division Chief whose organizational unit / program collects or holds the requested data must acknowledge such requests prior to IRB review. Data sharing agreements are required whenever personal health information is shared.

6. Data Sharing Agreements. Data sharing agreements must be used when releasing personal health information data to parties outside the Department, and may be required, when sharing personal health information data to parties inside the Department. Data sharing agreements must be developed in coordination with the Office of the General Counsel and the Institutional Review Board. The data sharing agreement must include at a minimum:

- A. Party, or parties with whom data will be shared;
- B. Time period of the agreement;
- C. Nature/type of the data requested;
- D. Intended uses of the data, including linkages with other data;
- E. Frequency of the exchange of data;
- F. Requirement that the requestor will protect completely the confidentiality of the data provided;

- G. Requirement that the requestor will not disclose or release the identifiable health data without specific written permission from the Department;
- H. Requirement that the requestor will report immediately the loss or theft of any identifiable data or related confidential materials to the appropriate Data Steward;
- I. How the requestor will maintain the confidentiality and the security of the data;
- J. A statement that the Department is either the owner or has rights to control the use and dissemination of the data;
- K. Provision describing how the data will be disposed of at the conclusion of the agreement;
- L. Assurances that the requestor will obey all state and federal laws regarding the use of the data;
- M. Specification of rights for audit of data use practices;
- N. Provisions regarding secondary release of the data;
- O. A provision that the recipient will hold the Department harmless from all liability arising from the recipients use or disclosure of the data; and
- P. Consequences of violation of the agreement.

Data sharing agreements may change through time and may be modified to meet specific needs.

7. Disclosure of Non-Identifying Individual Level Data. the Ohio Department of Health ("ODH") will routinely provide summary, statistical, or aggregate information that does not reasonably identify an individual. When in the best interest of the public's health, ODH may disclose non-identifying individual level data to the public according to law and as set out in this policy. Recognizing that an informed population is more likely to protect itself against health threats, ODH seeks to balance this interest with a fundamental respect for the privacy of individuals in determining the time, place, manner, and type of information ODH will disclose. Accordingly, ODH will utilize the following guidelines:

- A. When disclosure of individual level data is in the best interest of the public's health, ODH will disclose only the age, gender, and county of residence.

- B. ODH will not disclose additional information unless disclosing the information would have strong public health significance such as may be necessary to prevent, mitigate, or abate a public health threat.
- C. To the extent practical and where it is appropriate, ODH will consult with its staff, its public health partners, and/or the individual or the individual's family prior to any disclosure.
- D. The current or present condition or prognosis of the individual does not affect nor diminish the privacy concerns and rights of the individual. The privacy of this information is supported by Ohio law and by the United States Health Insurance Portability and Accountability.

8. Unresolved Issues/Policy Implementation. Any issues remaining unresolved upon implementations of this policy or questions regarding implementation or interpretation are to be brought to the attention of the Office of the General Counsel.

9. Applicability. This policy applies to all ODH employees. The policy pertains to datasets and to tabulations of datasets that do not meet the Department's disclosure limitation standard for public release.

10. Authority. This directive is promulgated by the Director of Health pursuant to Ohio Revised Code sections 121.02, 121.07, 124.134, 3701.03 and 3701.04 which authorize the Director to create, promulgate and enforce rules for the safe, efficient, economic and proper operation of the agency.

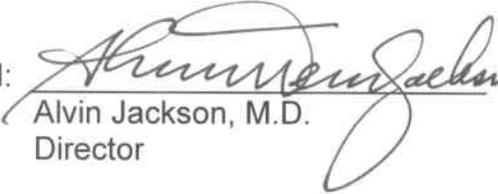
Approved:  Date: 6-30-2009
Alvin Jackson, M.D.
Director

Table of Effective Changes

Version	Effective Date	Superseded/Modified	Significant Changes
24	11/30/2007	NA	First issuance
24A	06/30/2009	Directive 601 Directive 1202 24	Consolidation of similar policies and revisions in accordance with new O.R.C. (predominately 1347), OIT and ODH policy updates