Approved by Chris Urbina, Executive Director and Chief Medical Officer, February 2012

SUMMARY

Colorado Department of Public Health and Environment employees will follow this policy and these procedures for minimizing the sensitive information that is received, collected, amended or maintained to that necessary to accomplish a public health, environmental or administrative objective.

POLICY

Public health analysis, investigations and interventions typically begin with collecting information on individuals that is sensitive in nature. Likewise, information used in employee functions such as medical leave requests or other legal or administrative activities require the collection of sensitive information. Some environmental information also may be of a sensitive nature.

It is department policy that only the minimum information necessary to accomplish the task at hand shall be collected, created, received, amended or maintained. Information requests shall be reviewed and amended if it is found that some part of the information requested is no longer needed.

In addition, the minimum number of people shall be given access to sensitive information, taking into account staff-assigned duties, backup routines and the optimal workflow of the unit.

PROCEDURE

1. Supervisors should note what sensitive information is necessary for a position. See Sensitive Information Inventory Tool.
2. Program managers should ensure information systems are reviewed to eliminate any sensitive information that is not required. Program managers should review the completed Sensitive Information Inventory Tool to identify any sensitive information that can be eliminated.
3. Program managers should consider storing information that is no longer needed for current activities but should be retained for possible future use and to conform to record retention policies.
4. Program managers should review state statutes and Colorado Board of Health rules to identify any that mandate collection of information that is no longer needed. If any such information is identified, the program manager is responsible for developing a plan for revising the rule or statute.

5. All employees should review computer drives and eliminate all unnecessary sensitive information, including old backups, old projects no longer needed, old Word documents, spreadsheets, etc. If a substantial amount of data should be stored, request assistance from the Office of Information Technology staff, if needed, to store in a secure place. Anyone involved in development, enhancement or maintenance of an information system should review and eliminate old files and data sets no longer needed.
6. All employees should review paper files of sensitive information and eliminate those no longer needed. If files are needed to comply with retention policies, but no longer needed for current activities, employees should store the information.
7. All employees should limit requests for information from others to the minimum necessary. When receiving a request for sensitive information, verify that all information requested is needed before releasing. Staff should determine if de-identified information can be used first, and only use information with identifiers if necessary to do so.
8. Any employee not complying with this policy and these procedures may be subject to state personnel system progressive disciplinary action. Other non-employees will be disciplined with appropriate action, up to and including termination.

TOOLS/GUIDANCE/STANDARDS

Sensitive Information Inventory Tool

REFERENCE

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule §164.510 (d) (1), Physical Safeguards, Disposal

HIPAA Privacy Rule §164.502 (b) Minimum Necessary