PRIVACY AND CONFIDENTIALITY

Generally. In accordance with § 24-72-502, C.R.S., it is departmental policy to protect individual privacy in the collection, storage, transfer, and use of personally identifiable information, regardless of the source or medium. To the extent the Department must use personally identifiable information to complete particular transactions, collection must be minimized to the least amount of information that is required to process the transaction.

Information Protected. "Personally identifiable information" means information about any individual, including employees, that could reasonably be used to identify such individual, including, but not limited to, first and last name, residence or other physical address, electronic mail address, telephone number, birth date, credit card information, and social security number. Medical information, disability and accommodation requests, time and attendance records, leave requests, financial information including salary history, and earning statements are also protected. Various federal and state laws may require additional protection of certain personal information. However, "personally identifiable information" does not include information collected as part of any regulatory, investigative, or criminal justice purpose, information collected as part of litigation in which the State is a party, or information that is required to be collected pursuant to any state or federal statute or regulation.

Limited Access and Disclosure. Employees shall not access nor disclose personally identifiable information unless it is necessary to discharge their job responsibilities. Employees shall not seek or access protected information out of curiosity, out of malice, for personal gain, or for any other impermissible purpose, even if they are otherwise authorized in the ordinary course of business. Employees shall hold in confidence and refrain from disclosing protected information to any person, including employees of federal, state, or local governments, unless the requestor has a demonstrated official business reason for the information, or the person to whom the information pertains has authorized its release. Requests from persons outside of state government must be handled in accordance with the departmental Open Records Act policy. All personally identifiable information is governed by the Open Records Act, §§ 24-72-201, *et. seq*., C.R.S. including the protection of personnel files and other confidential information in § 24-72-204(3)(a), C.R.S., the Department's Open Records Act policy, and the Department's Records Retention policy.

Precautions. Employees have the responsibility to ensure that all information is properly protected and secured. Materials containing personally identifiable information should not be left unattended or in plain view. E-mail addresses and fax numbers should be verified, and authorized persons should be available to receive faxes containing personally identifiable information. If an employee receives an e-mail or fax in error, he or she should promptly notify the sender.

Although it is natural for employees to ask about a co-worker's illness, laws such as the Family and Medical Leave Act, and the Health Insurance Portability and Accountability Act, impose strict confidentiality requirements. Supervisors and affected employees need to communicate and agree on what co-workers may be told. Medical information, including leave requests and approvals, must be secured and only those with a business need should have access.