

STATE OF COLORADO

John W. Hickenlooper, Governor
Christopher E. Urbina, MD, MPH
Executive Director and Chief Medical Officer

Dedicated to protecting and improving the health and environment of the people of Colorado

4300 Cherry Creek Dr. S. Laboratory Services Division
Denver, Colorado 80246-1530 8100 Lowry Blvd.
Phone (303) 692-2000 Denver, Colorado 80230-6928
Located in Glendale, Colorado (303) 692-3090

<http://www.cdphe.state.co.us>



Colorado Department
of Public Health
and Environment

Privacy and Security Compliance Statement of Understanding

I, _____ understand that I am required to abide by the Colorado Department of Public Health and Environment's privacy and security policies and procedures contained in parts 11 and 15 of the department Policy Manual, which are referred to in the list below. I agree to fully adhere to department policies and procedures.

I understand that the department is the sole owner of its information technology resources and may monitor employees' system use and access to computer files. The department may record any network activity or systems use transmitted or received. These archives may be provided to law enforcement agencies for investigation.

I acknowledge that violation of department privacy and security policies could lead to employment termination or criminal prosecution as part of the department's [Sanctions for Violations](#) policy.

Employee Responsibilities

Appropriate Use of State Systems	
	Related policy
Use information systems only for state business, which includes computers, networks, internet, e-mail, and data.	11.3 , 15.10
Communicate professionally in e-mail messages.	11.3 , 15.10
Adhere to copyright restrictions.	15.10
Do not let others use your user accounts.	11.2 , 15.10
Register all software (including downloads) with ITS.	15.10 , 15.18
Contact IT staff to scan disks for viruses before loading files on computers.	15.10 , 15.18

Minimize Access to Sensitive Information	
	Related policy
Minimize information collected and stored to what is needed to complete assigned duties.	15.9
Release sensitive information (e.g., personal health information, financial or employee data with social security numbers) only in compliance with state and federal laws.	15.26
Provide sensitive information only to people who sign data use agreements.	15.27
Verify identity of recipient before providing sensitive information.	15.14

Protect Sensitive Information	
	Related policy
Use strong passwords and protect them from disclosure to others.	15.12
Use password protected screen savers.	15.13
Ensure that sensitive information is not exposed through inappropriate viewing of computer monitors, printers and copiers.	15.22 , 15.24
Encrypt all sensitive information stored on local drives or removable media (e.g., CDs, flash drives).	15.18
Transmit sensitive information through secure channels (not unsecured e-mail) and only to those authorized to receive it.	15.10 , 15.15 , 15.20
Ensure physical access to workspace, faxes or files is limited to authorized individuals.	15.19
Dispose of sensitive information on paper documents in locked recycle bins.	15.23
Dispose of removable media in a secure media disposal bin or through the ITS Help Desk.	15.21
Transfer or dispose of all computers, PDAs or other devices through ITS.	11.3 , 15.21
Employ home safeguards equivalent to department safeguards (e.g., firewalls, virus protection).	15.18
Report privacy and security incidents to your supervisor and the Help Desk (e.g., viruses).	15.6

Training	
	Related policy
Complete the state's Cyber Security training annually.	15.8
Complete of the department's HIPAA training if working with health-related data.	15.8
Read and sign this Statement of Understanding to meet the department's obligation for reviewing the applicable Privacy and Security and Information Technology policy requirements.	15.1

Accepted by:

(Signature) (Date)

Approved by Program Manager:

(Signature) (Date)

Program/Division: _____

Sent to Human Resources: _____
(Date)