

Division of Disease Prevention (DDP) Security and Confidentiality Policies and Procedures
Verification of Receipt and Assurance of Key Requirements for Non-DDP Personnel¹
(External contractors, service providers and data recipients)

If you handle, use, enter, or analyze DDP's confidential paper or electronic records or data, you must follow these requirements:

- Always protect and maintain security of state property you use (such as paper and electronic records, computers, flash drives, cell phones).
- Do not connect personal storage devices (such as non-state issued cameras, phones, MP3 players, flash drives) to state IT equipment/computers.
- Obtain DDP approval before removing or transporting confidential information from agreed upon locations/offices.
- Transport confidential information in a locked briefcase or similar secure container.
- Use an approved IronKey™ flash drive if you must transport confidential electronic data.
 - Ensure data is encrypted or flash drive is stored under lock and key when not in use,
 - Keep flash drive in a separate location from your computer, and
 - Delete all data immediately after use.
- Store all confidential information in specified, locked filing locations.
- Return all confidential information to locked file locations at end of workday.
- Do not store confidential DDP information on the hard drive of your computer.
- Collect, share, and transport the minimum confidential information necessary to conduct your work.
- Whenever possible, code information to avoid use of disease specific or client identifying information.
- Immediately report any known or suspected confidentiality breach to your immediate supervisor, DDP contract monitor and the DDP director.
- No confidential information should be transmitted via email.
- Send mail in manner that does not allow confidential contents to be revealed.
- Faxes containing confidential information must only be sent to, or received at secure locations.
- Do not disclose confidential information over the telephone without first confirming the recipient is allowed access to the information.
- Make every effort to ensure that confidential data is removed from PCs prior to surplus.
- Avoid photography or video in office locations that involve DDP confidential data, unless it is absolutely necessary for business purposes and approved by your supervisor(s).
- If you are a recipient of data from DDP, you will ensure that all data stewardship activities are handled according to the signed Data Request and Data Recipient Agreement forms.

Your signature below indicates that:

- You have read the Security and Confidentiality Policies and Procedures in its entirety,
- You have read and understand these key requirements, and
- You have discussed any content you do not understand with your supervisor.

Name (*print*): _____ Signature: _____ Date: _____

Supervisor's Signature: _____ Date: _____

If employed external to DDP, identify your employer or affiliation: _____

¹This one-page document summarizes key attributes of the Security and Confidentiality Policies and Procedures. It is not inclusive of all Security and Confidentiality Policies and Procedures requirements.