

University of Colorado at Denver and Health Sciences Center

Protect Your Data

Employees of UCDHSC have access to, and are responsible for protecting, a wide variety of sensitive information. Faculty, in particular, has access to information that affects people's lives, such as medical information, credit card and social security numbers, and student's academic records. Failure to take care of this information places people at risk of identity theft, misuse of personal funds, or unauthorized modification of information. We therefore have a responsibility to educate ourselves on how best to protect the information we store electronically.

UCDHSC has administrative, technical, and physical safeguards in place, as well as policies and procedures, to ensure adequate protection of information we store from potential risks such as loss or modification. It is your responsibility to be aware of and understand these policies and procedures.

What is Electronic Media?

Electronic media can be an electronic computing device such as a laptop or desktop computer, PDA, or other devices that you might use to store sensitive information like diskettes, compact disks (CDs), DVDs, tapes, memory sticks, or any of the types of removable storage devices.

Security Tip

When possible, access to the sensitive information should be limited only to individuals who require access and only to the extent necessary to fulfill that person's work obligations.

What Can I Do?

This pamphlet presents ways that you should secure the information you use. If you have questions, please contact the IT Services Department or Regulatory Compliance Office for answers and additional help.

- It is best to store sensitive information on servers rather than desktop computers. Those can either be servers maintained by your organizational unit or provided by the IT Services Department. Unfortunately, you can't always trust that your information is safe on a desktop or laptop computer.
- If you think you might have sensitive information on a desktop computer, contact the IT Services Department to have them help you move your information to a secure server.
- If for some reason you can't store your sensitive information on a server, ensure that the data is encrypted and backed up. If you are unsure how to do this, the IT Services Department can help you.
- Use your campus account and password to login to the network; never share your account or password with others.
- Whenever feasible, use complex passwords, on any system storing sensitive information.
- Always enable your screen saver to lock your computer during inactivity and require it to be password protected.
- Always have current anti-virus software installed and keep your security patches up to date.
- Always ensure sensitive information sent or received via email or at a web site is encrypted.
- Always destroy electronic media containing sensitive information prior to its decommission.
- Always securely remove all sensitive information from electronic media before re-using it.
- Make an inventory of the sensitive information your department uses or stores.
- Look into ways to de-identify data used in daily tasks such as keeping grades.
- Obtain departmental permission to remove sensitive information from the office.
- Limit the amount of information stored on mobile devices and workstations to the minimum necessary needed to do your job.

But What If I Have a Laptop?

How Should I Store Devices?

Physically securing your mobile device is critical! Treat mobile storage devices as if they contained your personal information. Don't allow staff to leave devices in unattended vehicles, unlocked offices, or unsupervised in common areas.

- If at all possible, don't store data on it.
- If information must be stored on it, regularly copy the data to a secure server that is backed up frequently, preferably nightly.
- Password protect the laptop, using the UCDHSC password standards.
- Encrypt any sensitive information.
- Always use virtual private network (VPN) software and personal firewall software appropriately configured when making a remote connection to the campus network.
- When not in use, secure portable electronic media such as removable drives, CDs, or other portable computing devices containing sensitive information

What Do I Do If Electronic Media Is Lost Or Stolen?

If on campus:

- Inform your supervisor
- Contact campus police (Fitzsimons - 303-724-4444; DDC - 303-556-5000)
- Contact the UCDHSC Regulatory Compliance Office at - 303-724-1435 or the UCDHSC IT Security Principal through the IT Services Help Desk at (HSC) 303-724-4357 or (DDC) 303-315-3457.

If off campus:

- Contact the police department in the appropriate jurisdiction.
- If the computer or device contained sensitive University information, follow the steps above, including contacting the campus police.