CUA

THE CATHOLIC UNIVERSITY OF AMERICA

Compliance and Ethics Program

http://compliance.cua.edu/

How do I Protect Privacy and Information Security?

Below are quick reference tips for identifying and protecting confidential information. For a definition of confidential data and detailed information and guidance review the University's Information Security and Assurance Policy (http://policies.cua.edu/infotech/infosecurityfull.cfm) **and complete the University's online Privacy and Information Security training** (http://training.cua.edu/infosec/.)

If you have a question about protecting privacy or confidentiality, you should always feel free to contact the Chief Ethics and Compliance Officer/Chief Privacy Officer (tel. 202-319-6170 or CUA-COMPLIANCE@CUA.EDU).

Quick Reference Tips

- **Understand what types of information are confidential and must be protected. For example:**
  - *Student Records/Information* (ex: any document directly related to a student and kept by the University)
  - *Medical or Health Information* (ex: medical histories, test results, reports from health care providers)
  - *Personal Financial Information* (ex: credit/debit card or bank account information, credit reports)
  - *Personally Identifiable Information* (ex: Social Security Number, driver's license number, age, date of birth, sex/gender, race/ethnicity, religion, veteran status)

- **Take affirmative steps to protect confidential data:**
  - Use *physical measures*, such as locking a file cabinet or office door, and keeping mobile devices secured or out of sight.
  - Use *technical measures*, such as strong passwords for computers, computing systems and mobile devices, and locking your computer screen when you walk away.
  - Use *logical measures*, such as not discussing private or confidential information unless necessary.
  - Keep your computer *up to date* with patches and upgrades.
  - *Avoid* e-mailing confidential information. If you must do so, confirm that the recipient is authorized to receive it and send the minimum amount of confidential information necessary for the task.
  - *Do not* access University systems (including e-mail) through "Wi-Fi mobile hot spots."
  - *Shred* confidential data when no longer needed.

- ***Immediately report suspected loss or theft of confidential information*.** Call the Technology Services Information Center at tel. 202-319-4357, Monday – Friday 8:00 a.m. – 9:00 p.m. Eastern, or call the Department of Public Safety at tel. 202-319-5111 at all other times.