IT’S PERSONAL

Ask yourself, “how might the work I do affect the person whose data I’m handling?”
Data Security Threats & Risks

It is important to protect the privacy and security of information across UC San Diego. Everyone in the University community has a responsibility to protect data under their jurisdiction or control.

Confidential or restricted data must be protected to prevent theft, compromise, or inappropriate use from unauthorized access or disclosure.

Image source: Symantec Threat Report 2017
DEFINING CONFIDENTIAL AND RESTRICTED INFORMATION

Confidential Information: The term “confidential information” applies broadly to information for which unauthorized access or disclosure could result in an adverse effect. To address this risk, some degree of protection or access restriction may be warranted.

Restricted Information or Data: "Restricted information" is UC's term for the most sensitive confidential information. Restricted information or data is any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.
Examples of PII

Staff and academic personnel records, including but not limited to:

- Employee ID
- Home telephone number and home address
- Name of spouse or other relatives
- Birth date
- Citizenship
- Income tax withholdings
- Information relating to evaluation of performance
- Attendance record

Student records, including but not limited to:

- Student ID
- Transcripts (grades)
- Exam papers
- Test scores
- Evaluations
- Financial aid records
- Loan collection records
- Directory information for students who have requested that information about them not be released as public information

Keep in mind that respecting privacy means protecting info that a person may want to treat privately although it isn’t identified as PII

- e.g. the DNC hack
What Not to Do

- Use Dropbox, or other free or paid non-university service.
- Vendors without signed agreements that include the UC Appendix - Data Security (Appendix DS), and Business Associates Appendix (BAA) if PHI is involved, have not agreed to protect our data and interests in the ways the University requires.
- Once the data is there, you no longer have control over it.
- Ownership may be in question.
- Export control may be an issue if the data isn’t stored in the US.
- Store personally identifiable data on a local or hand-held storage device (e.g. laptop, USB, tablet) that can easily be stolen.
How Do I work with a Word or Excel doc with confidential or restricted data?

- Ensure the collected data is needed for a legitimate business purpose.
- Keep it on centrally managed secure file storage.
- Encrypt the document prior to storing (at rest) and restrict access to it with password protection.
How Do I share it with a unit or authorized person?

• Ensure that sharing the collected data is needed for a legitimate business purpose.
  • Use centrally managed secure file storage (option may depend on unit)
    • network drives
    • Google Drive for Business (G Drive)
    • OneDrive
• If you must share via email, encrypt the file and call with the password.
How Do I securely engage in mobile use on the road?

- VPN

- Never store sensitive data on a mobile device.
- Use centrally managed secure file storage (option may depend on unit)
  - G Drive
  - OneDrive
  - network drives (can be painful)

Image source: Symantec Threat Report 2017
Resources

- cybersecurity.ucsd.edu
- https://its.ucsc.edu/security/restricted.html
- https://its.ucsc.edu/security/pii-training.html
- https://security.ucop.edu/resources/security-awareness/index.html
- https://security.ucop.edu/resources/security-awareness/new-school-year.html
- http://er.educause.edu/blogs/2015/10/youre-an-important-piece-of-the-puzzle