Data Security

Tom Conway, Eric Folk and Joey Martinelli

Have you ever downloaded or stored sensitive information onto a computer or mobile/storage device?

Congratulations YOU are Officially a Data Custodian!!

- Anyone who downloads or stores sensitive information on a computer or storage device **becomes a data custodian through that act.**
- Add new title to your **C.V. !**

As a great Data Custodian, you are…

- Responsible for implementing and administering controls over the resources according to University policies and parameter.
- Responsible for the technical safeguarding of sensitive information, including ensuring security transmission and providing approved access control systems.

Be an AWESOME Data Custodian!!

- Data custodians are the managers and/or administrators of systems or media on which sensitive data resides,
- Personal computers, laptop computers, PDAs, smartphones, storage systems, USB drives, paper files and any other removable or portable devices.

Why is Data Security Important?

- Responsibilities and Obligations to **Participants** (IRB)
- Responsibilities and Obligations to the **University** (Policy)
- Responsibilities and Obligations to **Partners** (Good Will)
- **VERY BAD STUFF** can happen if things go wrong

What Kind of Data Are We Talking About?

Sensitive Information

- Sensitive information is subject to privacy considerations or has been classified as confidential

Examples of Sensitive Information

- **Student records,** grades, IEPs, assessments, etc. (Family Educational Rights & Privacy Act -FERPA)
- **Health information**, -Health Insurance Portability & Accountability Act (HIPAA)
- **Personal financial information**
- **Job applicant records** (names, transcripts, etc.)
- **Social Security Numbers**
- **Dates of birth**
- **Private home addresses and phone numbers**

Examples of Sensitive Information

- Driver license numbers and State ID Card numbers
- Access codes, passwords & PINs for online systems
- Answers to "security questions”
- **Confidential information**
- Detailed information about security systems
- Confidential salary information

Good Data Security Practices

- Know UH and Partner Agency data policies!
- Do an honest evaluation of current data practices
- Quickly correct any oversights
- Have a plan for if/when things go wrong
- Commit Yourself to ensuring the privacy of your partners and participants

Evaluate Your Data Use:

- How do we **use** sensitive information?
- Where and how do we **store** this information in physical and digital worlds?
- Do we **REALLY** need to have access to this data where it is?
- What are the **commitments** you made to your participants, partners, and others concerning data privacy and confidentiality?

Evaluate Your Data Use:

- What is the **worst-case scenario** if a mean/evil/desperate person had access to all of this information?
- How have the people who can access this information been **trained** to use this information?
- What do we do if **something goes wrong**?
- What are the specific steps we are going to take to **insure sustainable and consistent compliance** with data use and storage policies?

What Can Go Wrong?

- Online data could be attacked.
- Computers and devices could be stolen/lost.
- Identity theft
- People could suffer very bad outcomes if their privacy is violated
- Partners & funders could lose trust in CDS.

Some Things You Should KNOW

- Sensitive Information should not be stored in file sharing systems (Dropbox, Google Drive, Box etc.)
- Computers and devices should be password protected and encrypted
- There are ways to securely share sensitive information when necessary

How to Protect Information

- Know where information is stored
- Safeguard it with physical security
- Encrypt it
- Redact it
- Delete it

Best Practices…some of which are required!

- Redact anything going digital
- Passwords and Encryption
- Investigate the COE approved “OwnCloud” file sharing system
- Keep Sensitive Information on a separate secure system
- Use erase/remove software on all devices

OwnCloud

- University approved online file sharing system
- Computers will be encrypted
- Data stored on university-controlled servers
- Currently in trial will roll out next semester
- Contact COE Tech for more information

What to do if stuff goes bad!

- Notification
- Determine exposure
- UH Human Studies Program (IRB)
- IRB "Unanticipated Problem Report"
- IRB Corrective Action Plan
- IRB WILL contact your Funder's Project Officer

Get Started with UH Policy

EXECUTIVE POLICY: on Security & Protection of Sensitive Information

http://www.hawaii.edu/apis/ep/e2/e2214.pdf

Review UH Infosec Resources that are available here:

http://www.hawaii.edu/infosec/policies.html

Take UH INFOSEC Training here:

http://www.hawaii.edu/infosec/training.html

Thank You!

For more info contact Tom or Joey

In partial fulfillment of IRB corrective action plan proposed by the Dual Enrollment with Individualized Supports Project