Best Practices for Secure Handling and Storage of Confidential Research Data

Konrad Czechowski & John Sylvestre
Centre for Research on Educational and Community Services
Faculties of Education and Social Sciences

About CRECS

- The Centre for Research on Educational and Community Services (CRECS) collaborates in research, evaluation, and training with organizations in the educational, social service, and health sectors to improve social programs and policies for citizens, especially those facing social exclusion.
- Over 40 Senior Researchers from a variety of Faculties
- A leader in program evaluation and community-based research

About this Work

- Prior CRECS data handling manual written in 2008 did not address issues related to electronic data
- Colleagues expressing uncertainty and confusion regarding how best to handle these data
- No clear uOttawa guidelines regarding the handling of research data
  - Different groups working independently
  - Work funded through our limited budget
- Secure handling of data is critical to protect our participants and to the reputation of our researchers, our centre, and our institution

About The Manual

Manual for Ensuring Privacy, Confidentiality, and Secure Data Storage for the Centre for Research on Educational and Community Services

- Produced recommendations that cover various steps in the research process including data collection, handling, sharing, and storage.
- These guidelines are based on best practices, a review of available literature, and consultation with librarians, REB, data security experts, and researchers.

Method

- Conducted an online search for terms such as "policy data security", "privacy policy" and "data security".
- Reviewed relevant ethical codes both nationally and by discipline.
- Reviewed the websites of Privacy Commissioners of Ontario and Canada.
- Consulted with librarians specializing in data management, the uOttawa data security architect, and research ethics protocol officers.
- Circulated draft to CRECS management committee.
- Presented findings to University and CRECS researchers, students, personnel.

A Multidimensional Approach to Data Handling

A three-dimensional approach was developed to help researchers think about how to handle their confidential data in a secure manner.

1. Extent to which data is directly identifying (TCPS2)
2. Extent to which data carry risk of harm if disclosed
3. Extent to which researcher should secure their data

Levels of Risk and Corresponding Steps to Safely Handling Data

Level of Risk	Steps to Securing Data
4 Information that would cause severe harm if disclosed If disclosed, could create risk of criminal liability, loss of employment, or severe harm to an individual or group.	Field collection: Data should be collected on an encrypted and password protected device. Use of paper material is discouraged, but if used should be handled with extreme care and not left unattended unless in a locked and secure environment. Storage: Data must be stored in a physically locked room (preferably secured by an alarm) on a password protected and encrypted hard drive or computer not connected to university data network. Sharing: Sharing at this level should be limited, data should only be accessed in a secure location. Access: Should be controlled by Principal Investigator (PI), who should keep a list of individuals who have been granted access to data.
3 Information that would likely cause harm if disclosed If disclosed, could create risk of social, psychological, reputational, financial, legal, or other harm to an individual or group.	Field collection: Data should be collected on an encrypted and password protected device. Use of paper material is discouraged, but if used should be handled with extreme care and not left unattended unless in a locked and secure environment. Storage: Data must be encrypted and password protected. Sharing: Data sharing by e-mail discouraged. Files must be encrypted when sharing. Access: Should be controlled by PI, who should keep a list of individuals who have been granted access to data.
2 Sensitive or confidential information If disclosed in its present form, can reasonably be expected to cause some damage to an individual's reputation, or cause embarrassment.	Field collection: Data should be collected on a password protected device. Storage: Data must be password protected, encryption is recommended. Sharing: Files sent via e-mail should be password protected and encrypted. Password must be sent through a different medium.
1 Non-confidential research information Information that in its present form would not cause harm to an individual or group if disclosed but researchers have nevertheless decided to keep it confidential.	Storage: Data must be stored on a password protected computer or drive. Sharing: It is recommended that files sent via e-mail be password protected. Password must be sent through a different medium.

Note. Levels of Risk Adapted from the Harvard Research Data Security Policy

Practical Steps To Secure Data Handling

Step 1: Secure Environment

- Software Up-to-Date
- Malware Scan (Sophos)

Step 2: Password Protect, Encrypt

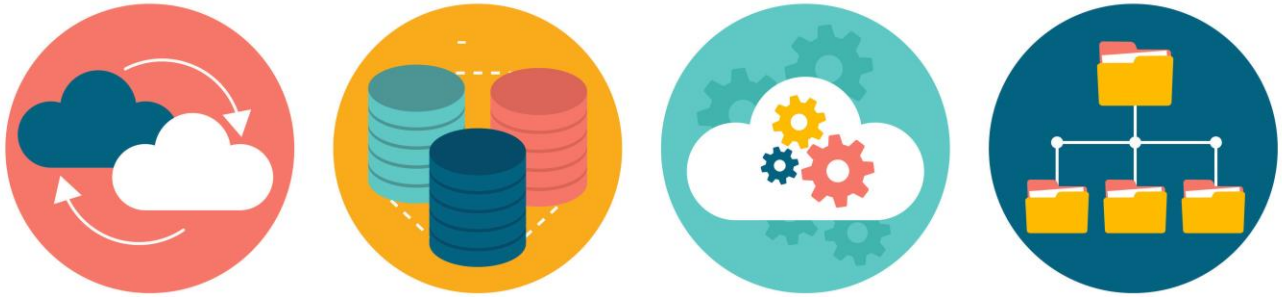
- Password (LastPass)
- Encrypt (Microsoft, VeraCrypt)

Step 3: Permanent File Removal

- "File Shredding" Application

Developing Data Management Plans (DMP)

- Developing a DMP can help address many of the concerns raised in this presentation and implement many of the recommendations outlined.
- We strongly recommended that our researchers develop a DMP prior to beginning a new project.



Recommendations

- Support CRECS in translating work and producing a more accessible document.
- A coordinated uOttawa approach to supporting researchers in secure data handling
- A worksheet/template be developed based on this work that would take the researcher from project planning, to REB submission, to training research staff, to monitoring research implementation
- uOttawa recommended/supported software for encryption, password management, file shredding

Thank you!

Questions, comments?

Konrad Czechowski - kczec041@uottawa.ca

John Sylvestre – john.sylvestre@uottawa.ca