UBC REB RETREAT:
A GUIDE TO DATA PRIVACY AND SECURITY

LARRY CARSON, ASSOCIATE DIRECTOR, INFORMATION SECURITY MANAGEMENT
KAITLYN GUTTERIDGE, LEAD PRIVACY, POLICY AND AGREEMENTS, POPULATION DATA BC
PAUL HANCOCK, ACCESS AND PRIVACY MANAGER, OFFICE OF THE UNIVERSITY COUNSEL

populationdata BC
A PLATFORM SUPPORTING RESEARCH ON HUMAN HEALTH, WELL-BEING AND DEVELOPMENT.
UBC

Overview

- Introduction to data privacy and security
- Researcher checklist (data lifecycle)
- Questions

Scope

- Legislation:
  - Freedom of Information and Protection of Privacy Act (FIPPA)
  - Personal Information Protection Act, E-Health Act

- Policies and Procedures:
  - UBC (Privacy Fact Sheets, Policy #104 & Information Security Standards)
  - Affiliated institutions
  - Population Data BC's education and training

Is Big Brother Watching You?

Personal Information: Pizza Delivery

Privacy vs. Security

"**Personal Information"** is **"recorded information** about an **identifiable individual**, not including **contact information"**

Privacy: Rules governing the collection, handling and disclosure of personal information.

Security: Protecting information (especially personal information) from unauthorized access, use, disclosure, modification, or destruction.

What We Want to Avoid …

INFORMATION AND PRIVACY

B.C. Health Ministry alerting thousands about privacy breach of personal data

ANDREA WOO

VANCOUVER — The Globe and Mail

Published M

Last update

Sick Kids doctor loses data on 3,300 patients

Six weeks after Ontario's privacy commissioner ordered the Hospital for Sick Children not to remove electronic health records from the hospital, a doctor lost an external hard drive containing such records at the country's busiest airport.

Medical marijuana privacy breach sparks lawsuit

Envelopes marked 'Marijuana Medical Access Program' sent out to users across Canada

CBC News Posted: Nov 26, 2013 7:47 AM AT | Last Updated: Nov 26, 2013 9:02 PM AT

Minister 'outraged' over stolen laptop holding 620,000 Albertans' health data

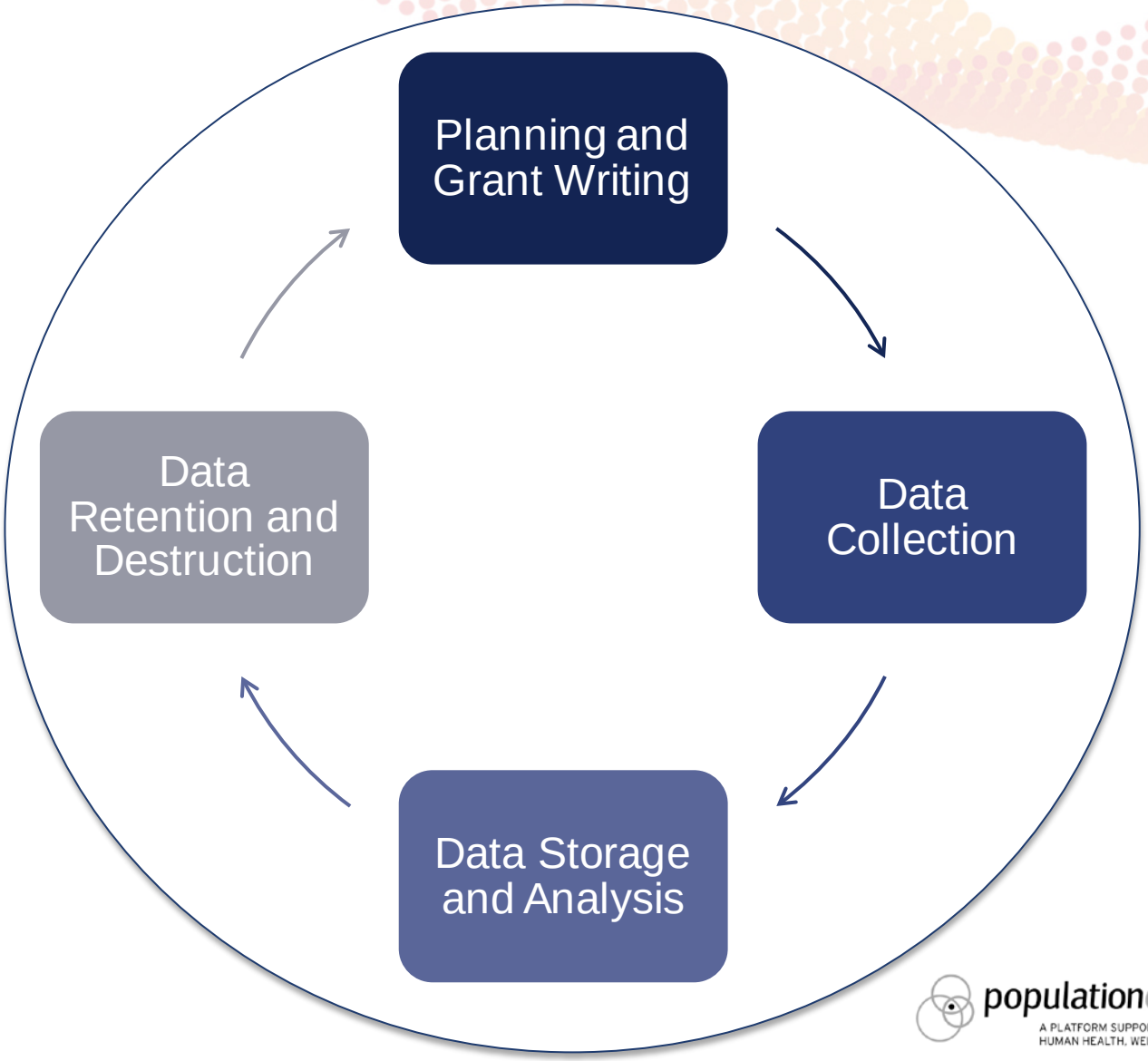
DEAN BENNETT

EDMONTON — The Canadian Press

Published Wednesday, Jan. 22 2014, 7:15 PM EST

Last updated Wednesday, Jan. 22 2014, 10:26 PM EST

Data Lifecycle: The Four Phases



Planning and Grant Writing Phase

- Plan in advance
  - Budget for proper security controls and infrastructure
  - Provide privacy and information security details in your grant proposal and REB application
  - Tri-Council Data Management Plans (Fall 2015)
  - Certification for the creation of databases / registries

- Consider third party requirements
  - Comply with Information Sharing Agreements
  - UBC does not require a Privacy Impact Assessment for research projects, but some Health Authorities do

- Ensure team is trained
  - TCPS2 Course on Research Ethics
  - Confidentiality pledge / project agreement
  - UBC's Privacy Breach procedures
  - Information Security Standards

Data Collection Phase

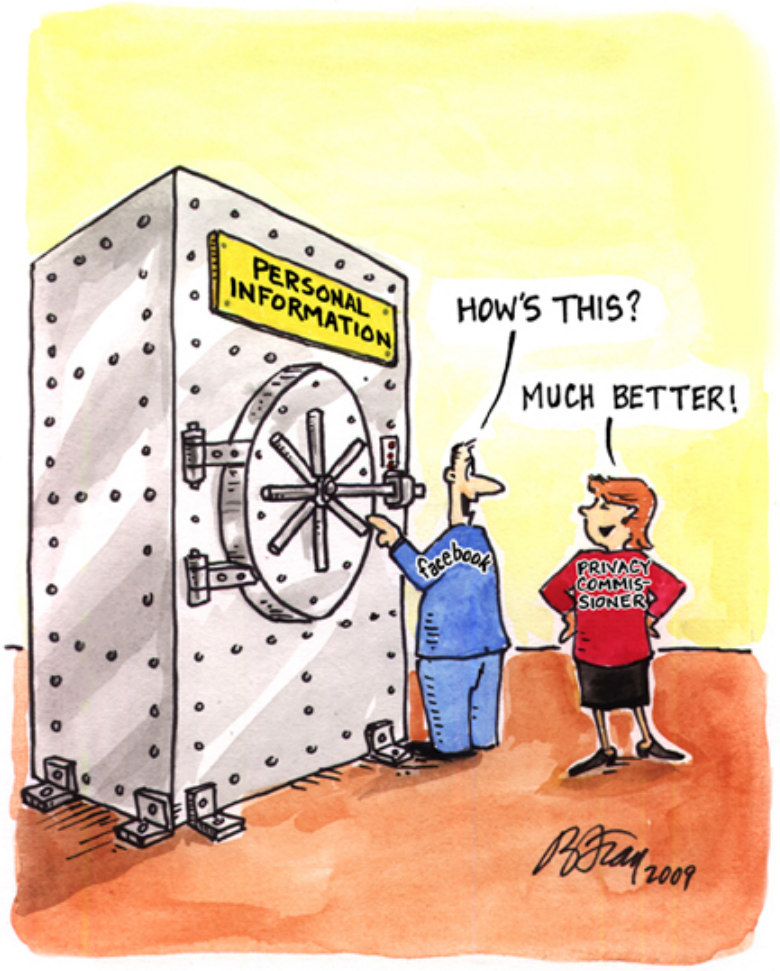
- Consent forms
  - Clearly identify all methods of:
    - Collection, Use, Disclosure, Storage, Linkage
  - Opt-in/out clauses
  - Re-use and permission to contact
- Measurement tools
  - 'Need to know' vs 'nice to know'
  - Hidden collectors such as electronic measurement tools
    - e.g. GPS, Accelerometer, biometric data
- Electronic collection
  - Ensure data is collected through secure encrypted electronic channels

Data Storage and Analysis Phase

- De-identify immediately
  - Segregate personal information from other data
  - Encrypt crosswalk file that correlates study ID to personal information
  - Secure any paper copies with personal information
  - Appoint a privacy guardian for the crosswalk

- Electronic data access
  - Provide access based on roles
  - Restrict user accounts and folder permissions
  - Implement logging function to audit access to data, especially for databases / registries

Data Storage and Analysis Phase



- Use tools such as centralized servers, UBC's Workspace, or PopData's Secure Research Environment
- Cloud storage is less secure and requires consent
- Implement information security controls for your data

Key Data Security Controls

ENCRYPTION	• Reduce data to minimum amount necessary • Word, Excel & Zip files may be encrypted • Devices may also be encrypted (Full Disk Encryption) using strong passwords/passphrases and key escrow
STORAGE ON SERVERS	• Keep data in Canada – say 'no' to the Cloud! • Try to keep data on campus servers and access it remotely (using VPN, VDI or Workspace) • Service providers that store data must have adequate security
STORAGE ON MOBILE MEDIA & DEVICES	• Storing on mobile media (e.g. USB keys, external hard drives) or mobile devices (laptops) is strongly discouraged. • If such storage is necessary, you must encrypt the media/device.
TRANSMISSION	• Explore alternatives to transmission (i.e. remote access) • If you must transmit files by email, encrypt them • When collecting data via servers always use encryption (e.g. HTTPS)
TELECOMMUTING & REMOTE ACCESS	• Remote access via VPN, VDI or Workspace is acceptable • Beware of Certificate Errors

Data Retention and Destruction Stage

- Monitor data retention timelines
- Consider requirements for archiving data
  - Where is the data stored during the 5 – 25 year period post project closure?
- Make appropriate plans for final destruction
  - Electronic information
  - Paper copies
  - External data (collected or transmitted by/to services providers)
- Track and log disposal

So what does this all mean in practice…

Model Answers based off Section 8

8.1. Security of Data During the Course of the Study

1. *How will data be stored?*
2. *How will security of the data be maintained?*
3. *If any data or images are to be kept on the Web, what precautions have been taken to prevent them being copied?*

- When unattended, hardcopy documents and any medical charts are stored in a locked cabinet located in a locked, alarmed room (Address: UBC, School of Population and Public Health, 5467 West Mall Office 123)
- When unattended, electronic data is stored on an encrypted, password protected computer located in a locked, alarmed room, (Address: UBC, School of Population and Public Health, 5467 West Mall Office 123)
- A backup copy of the data is stored on encrypted USB keys located in a locked cabinet in the same room. Some of the data is also stored on two encrypted laptops used by the researchers.

Model Answers based off Section 8

8.1. Security of Data During the Course of the Study

- The computer used to store data is not internet-facing. The laptop computer used to store data is sometimes used to access the internet, but it employs up-to-date firewall and antivirus software.

- Role based access will be initiated; only individuals named in the application with access to the data will be granted access to the data / database; audit and logging mechanisms will be activated and reviewed regularly.

Model Answers based off Section 8

8.2 Access to Data

1. *Who will have access to the data?*
2. *How will all of those who have access to the data be made aware of their responsibilities concerning privacy and confidentiality issues?*

- The following individuals will have access to the data: Jane Doe (PI) and John Smith (research assistant).
- The following individuals will have access to the crosswalk for data linkage purposes: Sarah Milk (programmer)
- These individuals have signed a confidentiality statement. They have also received training on proper security controls as outlined in 8.1 above.

Model Answers based off Section 8

8.3 Protection of Personal Information

1. *Describe how the identity of research participants will be protected both during and after the research study, including how participants will be identified on data collection forms.*

During data collection:

- Paper copies of the survey and information collected from the medical charts will be identified by a Study IDs only. Electronic data will be identified by a Study ID only.
- The Unique Study ID will not derived from or related to the information about the individual, i.e., name, SIN, PHN, hospital number, DOB, address, or unique characteristic.

Model Answers based off Section 8

8.3 Protection of Personal Information

During data analysis:

- Electronic research data will be de-identified by removing names, addresses and any other identifiers and replacing them with a Study ID number. The crosswalk containing the name to Study ID mapping will be stored in two locations: a locked file in John Smith's office, and a separate encrypted electronic file on the computer. Access permission to the folder where the electronic file is stored will be limited to John Smith.
- Medical charts will catalogued only by the participant's Study ID, any names in the documents will be replaced with pseudonyms and all additional identifiers will be removed. The crosswalk containing the names, study ID and pseudonyms will be stored in two locations: a locked file in John Smith's office, and a separate encrypted electronic file on the computer. Access permission to the folder where the electronic file is stored will be limited to John.

Model Answers based off Section 8

8.4 Transfer of Data

1. *Will any data that identify individuals be transferred (available) to persons or agencies outside of the University?*
2. *If **YES**, describe in detail what identifiable information is released, to whom, how the data will be transferred, how and where it will be stored and what safeguards will be used to protect the identity of participants and the privacy of their data.*

- Researcher collected data will be released to the data linkage agency (Sarah Milk: Linkage Central). An electronic copy of the data will be encrypted and uploaded to a secure transfer site maintained by Linkage Central. The website is protected with SSL encryption which ensures that all data transferred between two parties is encrypted in transit. John Smith will provide the encryption password for the files over the telephone upon Central Central's receipt of the files.

Model Answers based off Section 8

8.4 Transfer of Data

- The crosswalk will be transferred separately from the data file using the same method described above. Only PHN will be released for the linkage between the medical charts and researcher collected data.
- A data transfer agreement will be executed between said parties.
- The linkage results will be transferred back to the research team via the same mechanism.
- Upon verification of the files, all data transferred to Linkage Central will be destroyed.

Model Answers based off Section 8

8.5 Retention and Destruction of Data

1. *UBC policy requires that data be kept for at least 5 years **within a UBC facility**. If you intend to destroy the data at the end of the storage period describe how this will be done to ensure confidentiality (e.g., tapes should be demagnetized, paper copies shredded).*

- Data will be stored for a minimum of 5 years at the following address: UBC, School of Population and Public Health, 5467 West Mall Office 123.
- Hardcopy documents will be shredded using a secure shredding service and a data destruction certificate will be kept on file with the PI. Electronic data and backups will be destroyed using a software utility, such as "Secure Erase", to erase or overwrite the data. Logs produced by the data destruction will be kept on file with the PI.
- An attestation from the linkage service will be provided to confirm that the data were destroyed from the programmer's local system/network.
- Any hardcopy documents or electronic data that require further storage and archiving for the purposes of publication or grant requirements, will be stored at the following address: UBC, School of Population and Public Health, 5467 West Mall Office 123).

Questions…