Data Privacy

Overview

- What is data privacy?
- What are some of the best practices in data privacy?
- What are some things we should be aware of when handling research data?

What is data privacy?

What is data privacy?

X

What is data privacy?

X X

What is data privacy?

Privacy: has a number of meanings and aspects:

= the right to be free from intrusion or interference by others

= control over the collection, use, and disclosure of your information

= regulatory compliance

What is data privacy?

Privacy: has a number of meanings and aspects:

= the right to be free from intrusion or interference by others

= control over the collection, use, and disclosure of your information

= regulatory compliance

Security ≠ Privacy

What is data privacy?

Privacy: has a number of meanings and aspects:

= the right to be free from intrusion or interference by others

= control over the collection, use, and disclosure of your information

= regulatory compliance

Security ≠ Privacy
Ethics ≠ Privacy

What is data privacy?

Privacy: has a number of meanings and aspects:

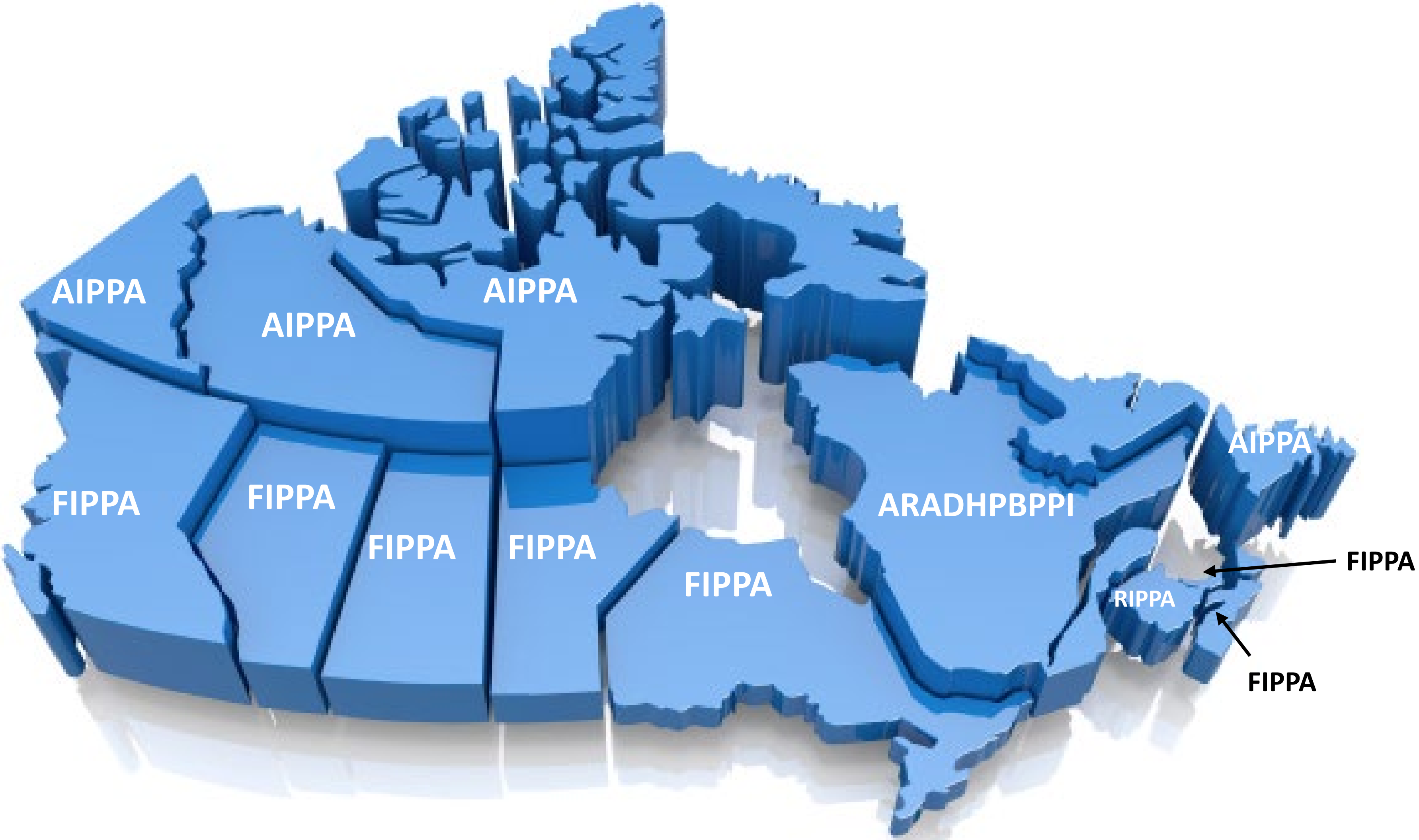
= the right to be free from intrusion or interference by others

= control over the **collection, use, and disclosure** of your information

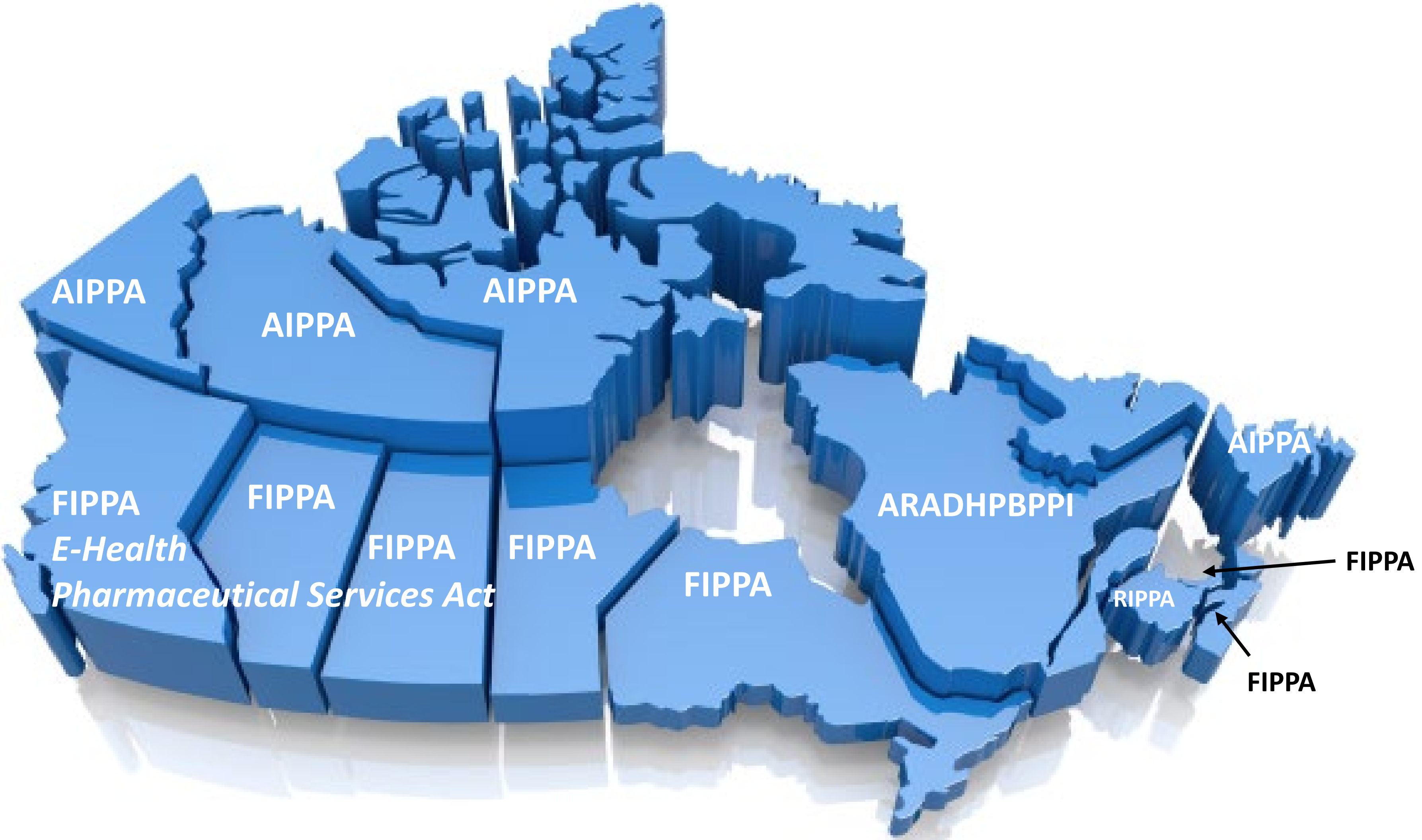
= regulatory compliance

Security ≠ Privacy
Ethics ≠ Privacy

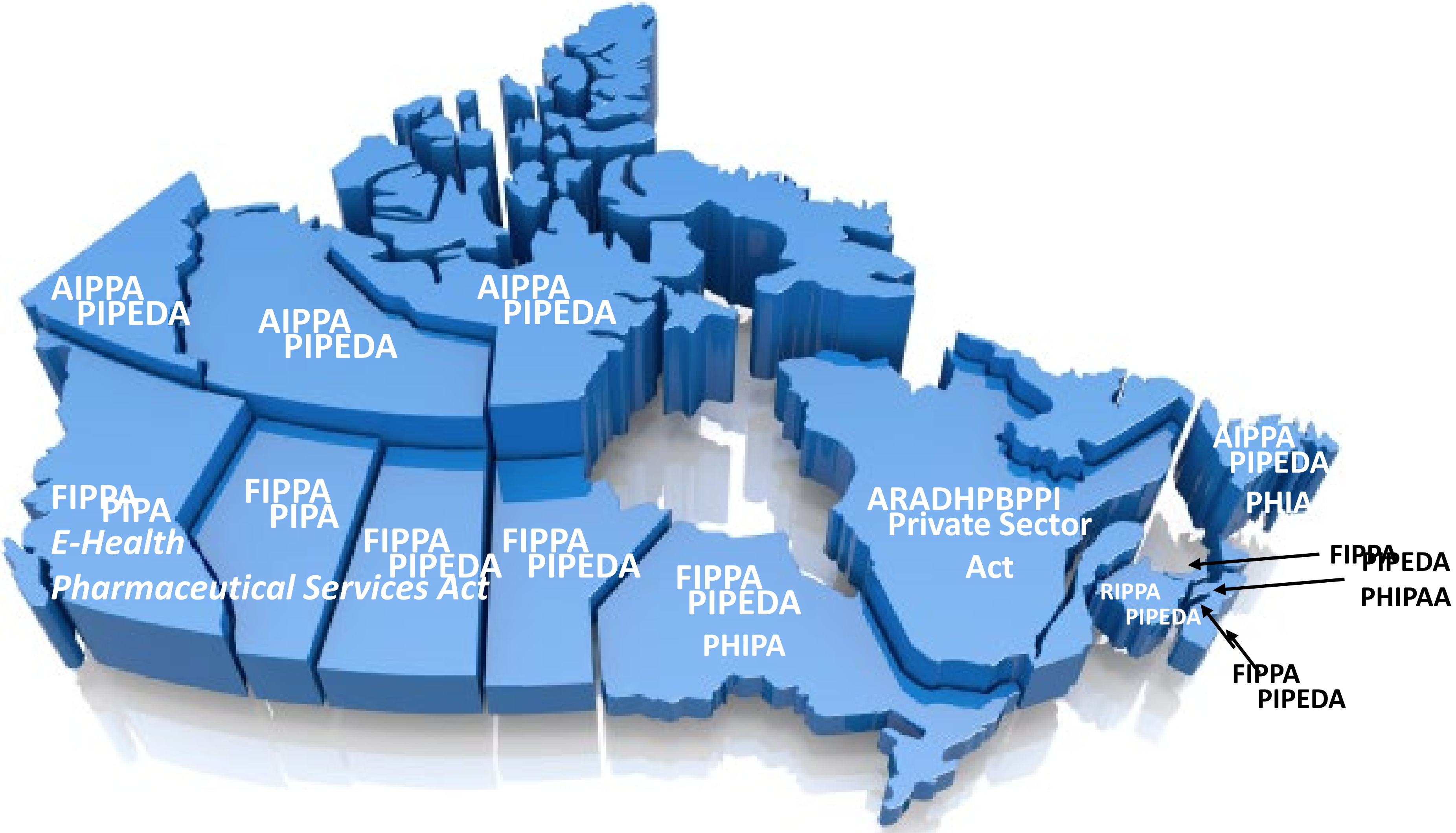
Provincial Legislation – Public Sector



Provincial Legislation – Public Sector



Provincial Legislation – Public + Private Sector



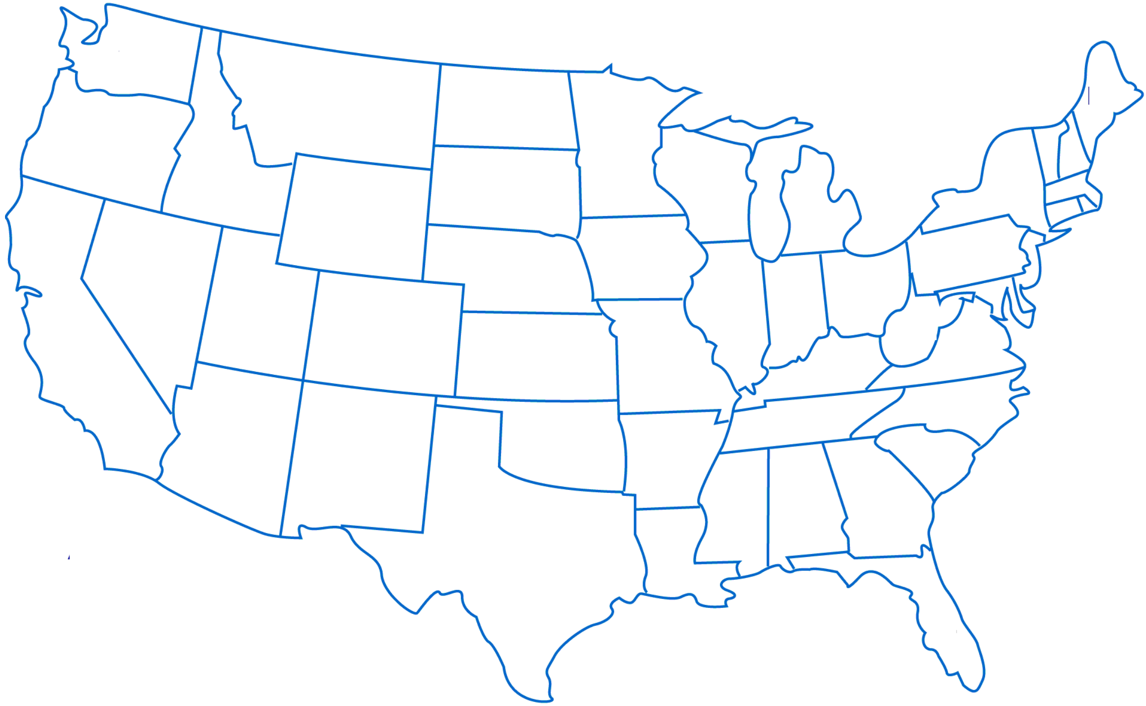
And More!

And More!

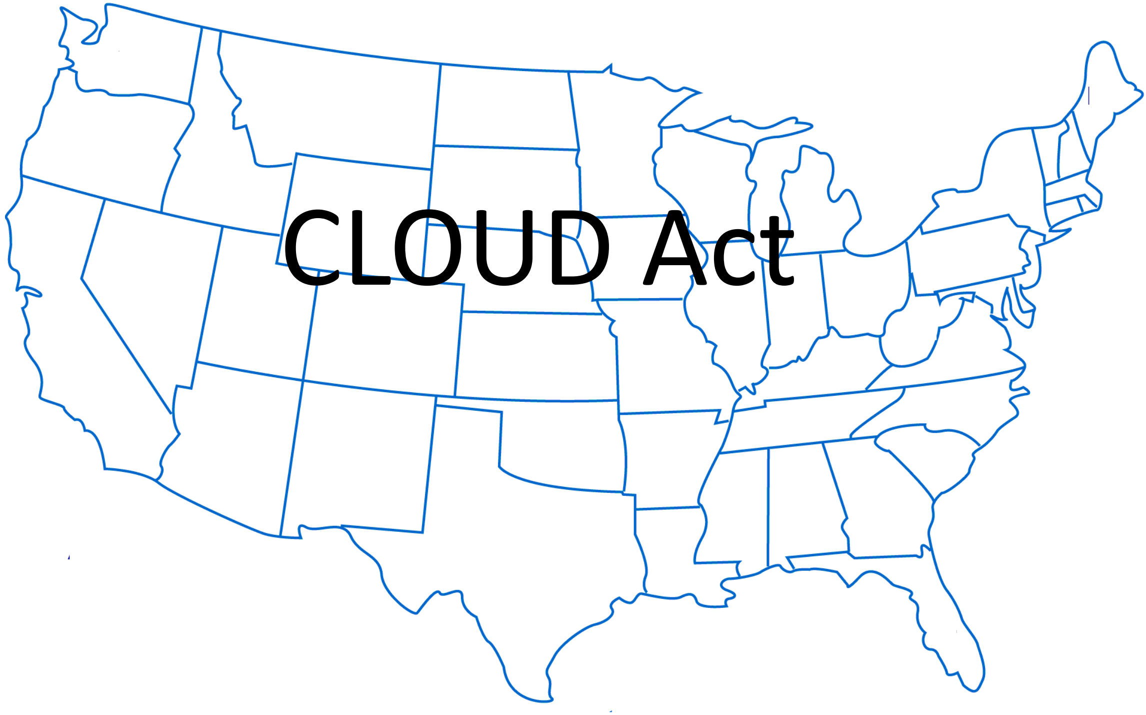
GDPR
25 MAY 2018

And More!

And More!

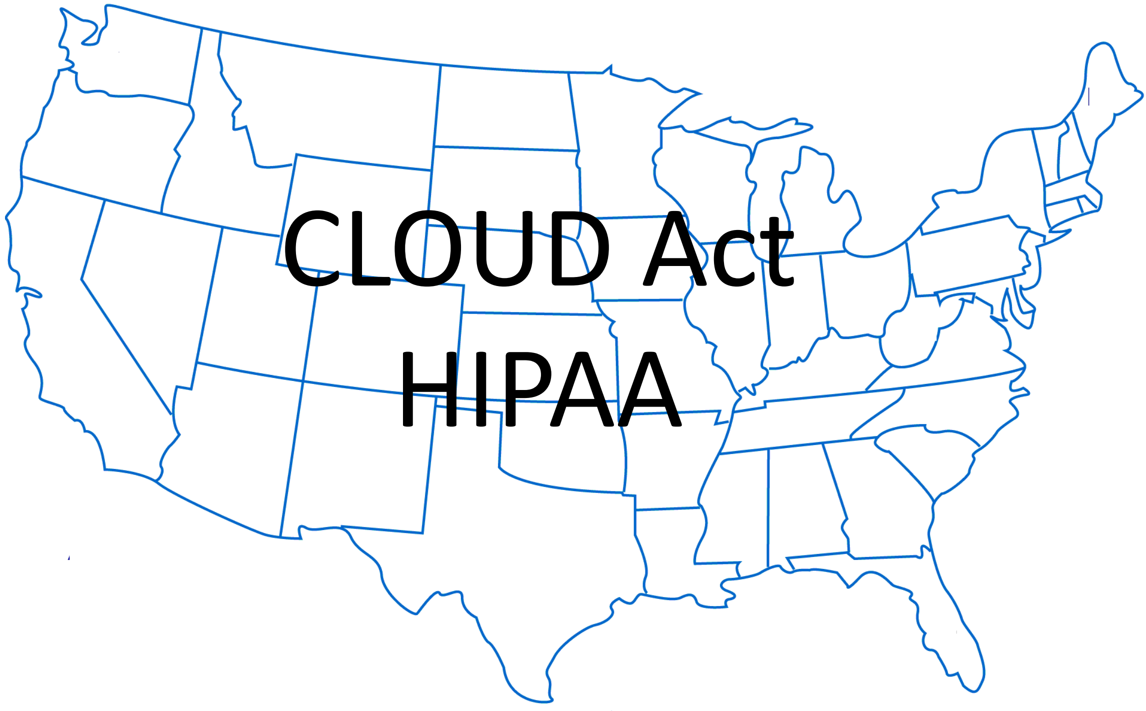


And More!



CLOUD Act

And More!

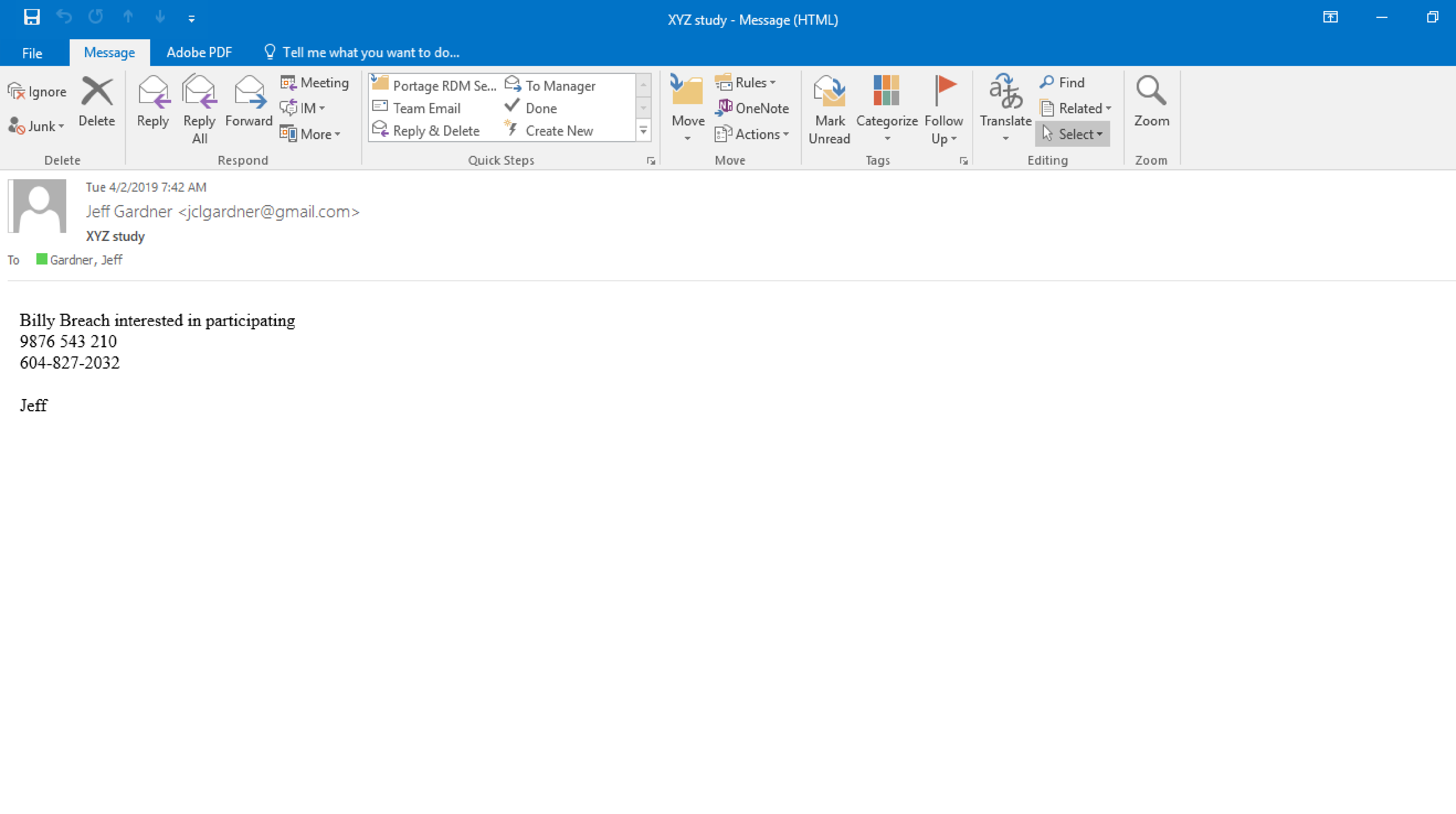


CLOUD Act

HIPAA

Role of privacy in research

- Education / Outreach



Tue 4/2/2019 7:42 AM

Jeff Gardner <jclgardner@gmail.com>

XYZ study

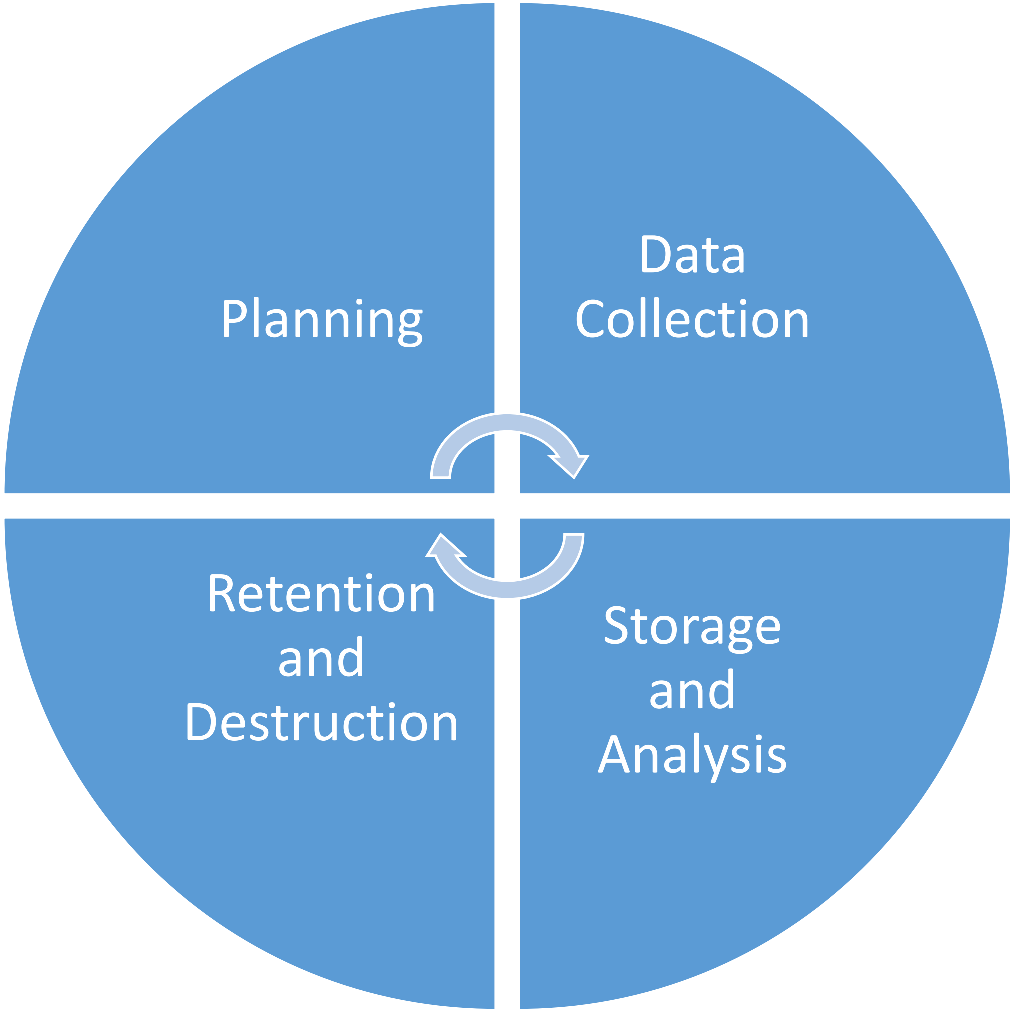
To 🟩 Gardner, Jeff

Billy Breach interested in participating
9876 543 210
604-827-2032

Jeff

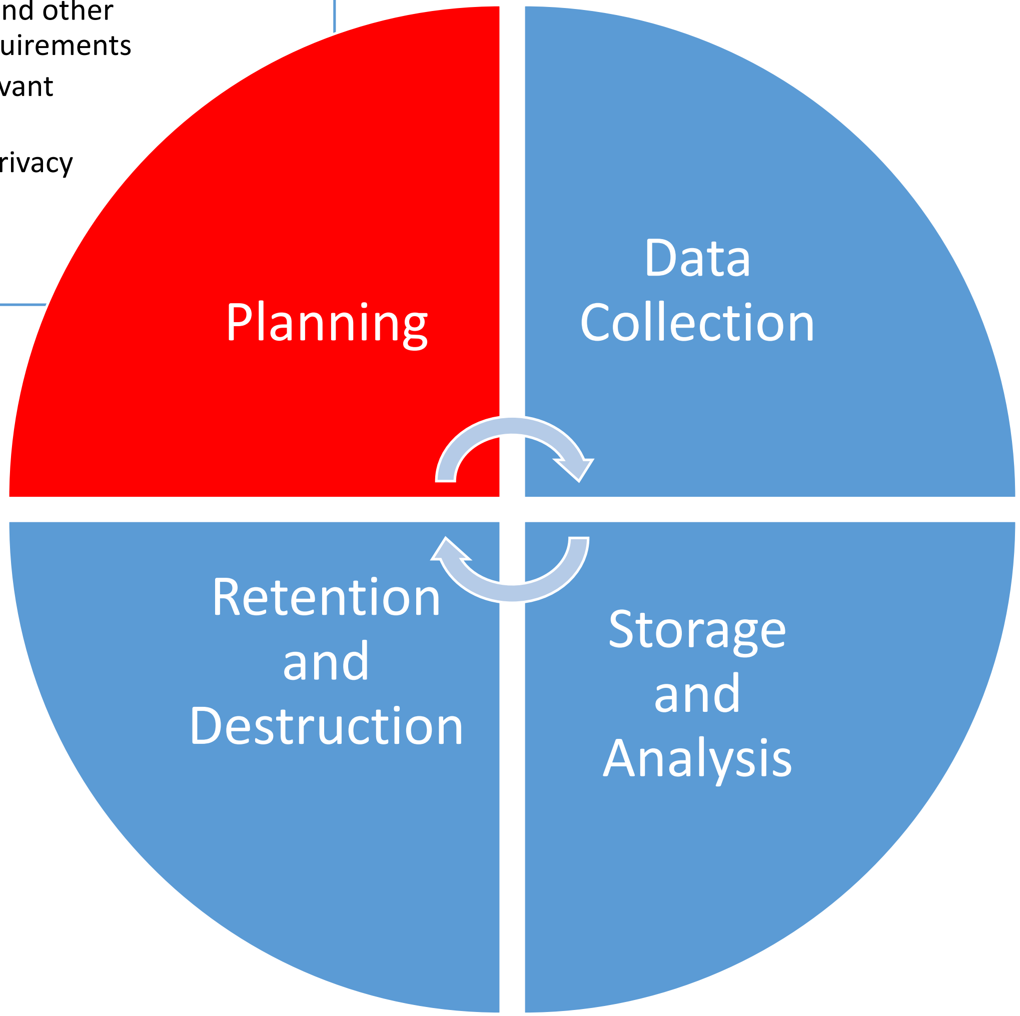
Research Data Lifecycle

Research Data Lifecycle



Research Data Lifecycle

- Understand legislative, institutional, and other regulatory requirements
- Complete relevant training
- Engage your privacy person!
- DMP



Planning

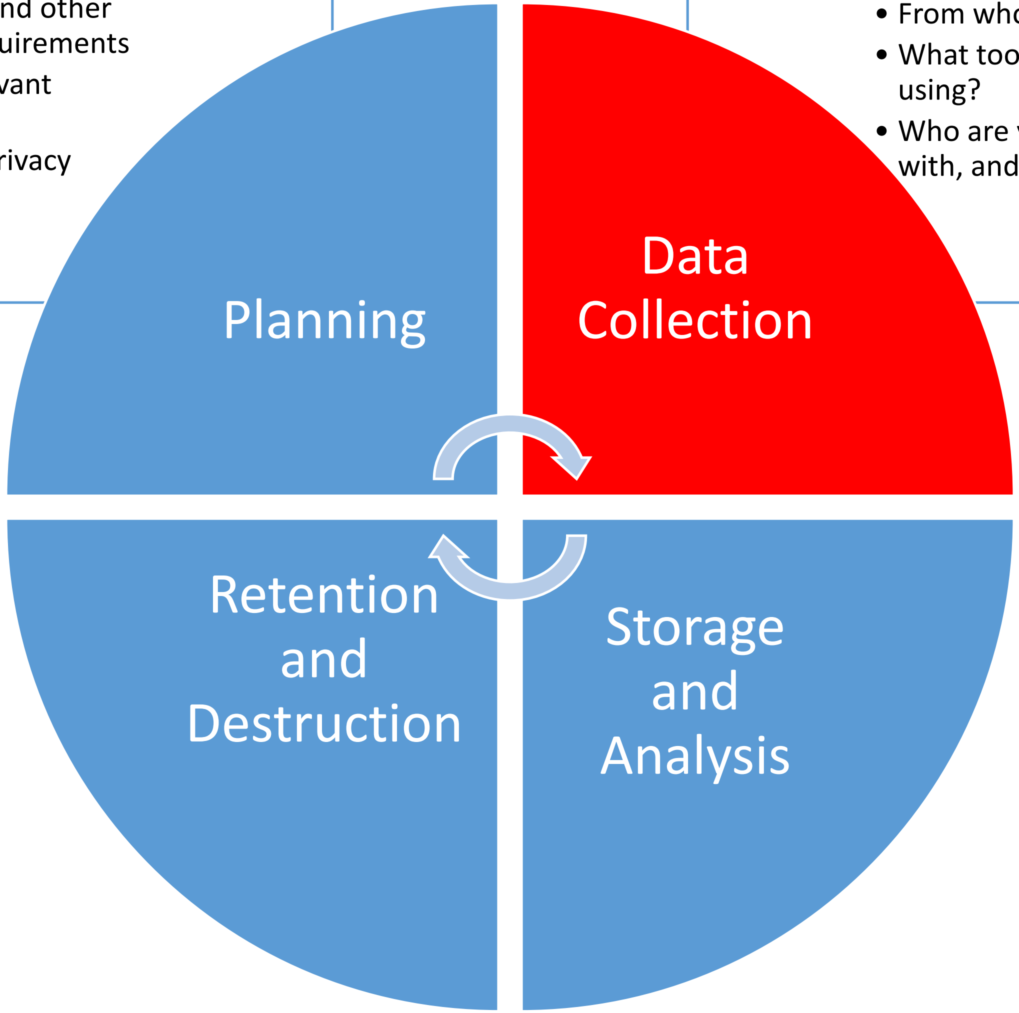
Data Collection

Storage and Analysis

Retention and Destruction

Research Data Lifecycle

- Understand legislative, institutional, and other regulatory requirements
- Complete relevant training
- Engage your privacy person!
- DMP



Planning

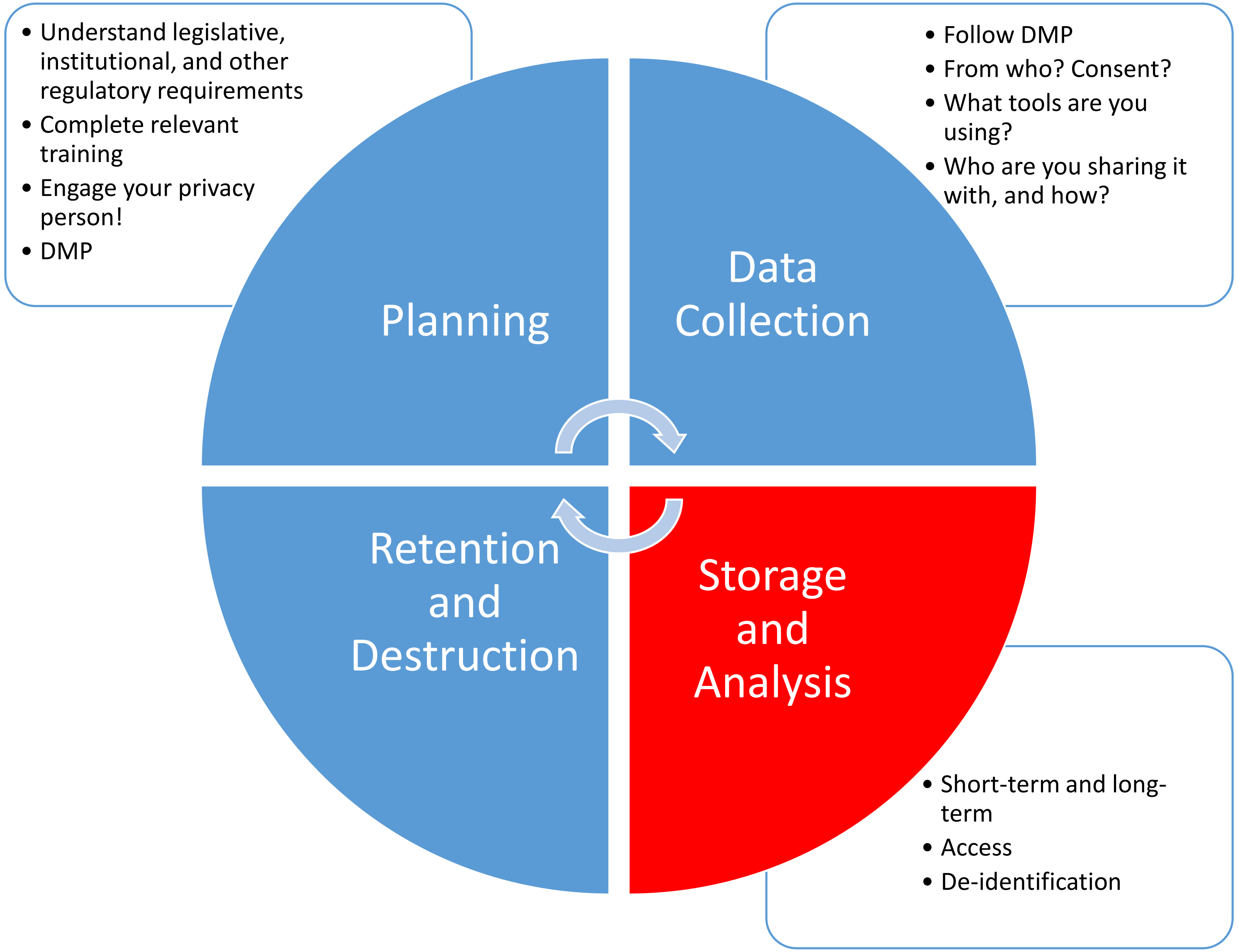
Data Collection

Storage and Analysis

Retention and Destruction

- Follow DMP
- From who? Consent?
- What tools are you using?
- Who are you sharing it with, and how?

Research Data Lifecycle



- Understand legislative, institutional, and other regulatory requirements
- Complete relevant training
- Engage your privacy person!
- DMP

Planning

Data Collection

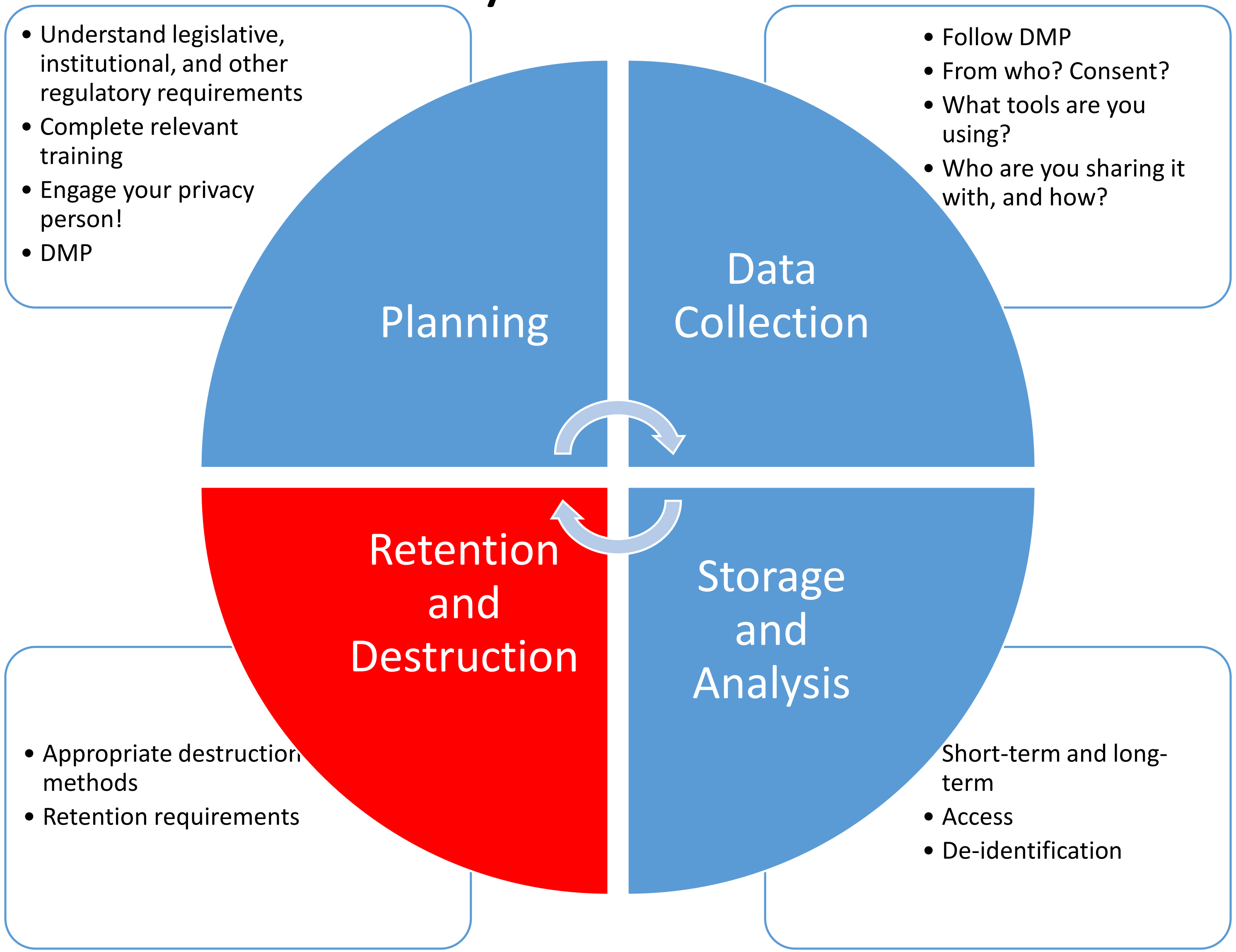
- Follow DMP
- From who? Consent?
- What tools are you using?
- Who are you sharing it with, and how?

Storage and Analysis

- Short-term and long-term
- Access
- De-identification

Retention and Destruction

Research Data Lifecycle



Planning

- Understand legislative, institutional, and other regulatory requirements
- Complete relevant training
- Engage your privacy person!
- DMP

Data Collection

- Follow DMP
- From who? Consent?
- What tools are you using?
- Who are you sharing it with, and how?

Storage and Analysis

- Short-term and long-term
- Access
- De-identification

Retention and Destruction

- Appropriate destruction methods
- Retention requirements

Data Management Plan

Data Management Plan

- Who are you collecting information about?
- Who are you sharing the data with?
- Who will have access to the data?

Data Management Plan

- What information are you storing?
- Are their any personal information or proprietary information?

Data Management Plan

- Where will you be storing the data at the different stages of your project?
- Where will you be keeping the data for analysis
- Where will you be keeping the data for retention

Data Management Plan

portage

Shared stewardship of research data

DMP Assistant is a bilingual tool for preparing data management plans (DMPs). The tool follows best practices in data stewardship and walks researchers step-by-step through key questions about data management.

https://assistant.portagenetwork.ca/

FIPPA is not the problem – but…

- Can personal information be disclosed outside of Canada?

- Can I store personal information outside of Canada?

- Can I use the cloud…like, AWS, or Azure?

FIPPA is not the problem – but…

- Can personal information be disclosed outside of Canada? **– yep!**

- Can I store personal information outside of Canada?

- Can I use the cloud…like, AWS, or Azure?

FIPPA is not the problem – but…

- Can personal information be disclosed outside of Canada? **– yep!**

  33.1 (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

  (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable;

  (s) in accordance with section 35 [disclosure for research or statistical purposes];

- Can I store personal information outside of Canada?

- Can I use the cloud…like, AWS, or Azure?

FIPPA is not the problem – but…

- Can personal information be disclosed outside of Canada? **– yep!**

  33.1 (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

  (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable;

  (s) in accordance with section 35 [disclosure for research or statistical purposes];

- Can I store personal information outside of Canada? **– yep!**

- Can I use the cloud…like, AWS, or Azure?

FIPPA is not the problem – but…

- Can personal information be disclosed outside of Canada? **– yep!**

  33.1 (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

  (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable;

  (s) in accordance with section 35 [disclosure for research or statistical purposes];

- Can I store personal information outside of Canada? **– yep!**

  30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:

  (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;

- Can I use the cloud…like, AWS, or Azure?

FIPPA is not the problem – but…

- Can personal information be disclosed outside of Canada? **– yep!**

  33.1 (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

  (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable;

  (s) in accordance with section 35 [disclosure for research or statistical purposes];

- Can I store personal information outside of Canada? **– yep!**

  30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:

  (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;

- Can I use the cloud…like, AWS, or Azure? **– yep!**

FIPPA is not the problem – but…

- Can personal information be disclosed outside of Canada? **– yep!**

  33.1 (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

  (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable;

  (s) in accordance with section 35 [disclosure for research or statistical purposes];

- Can I store personal information outside of Canada? **– yep!**

  30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:

  (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;

- Can I use the cloud…like, AWS, or Azure? **– yep!**

  It depends…see above to start. (Remember, the above applies to personal information).

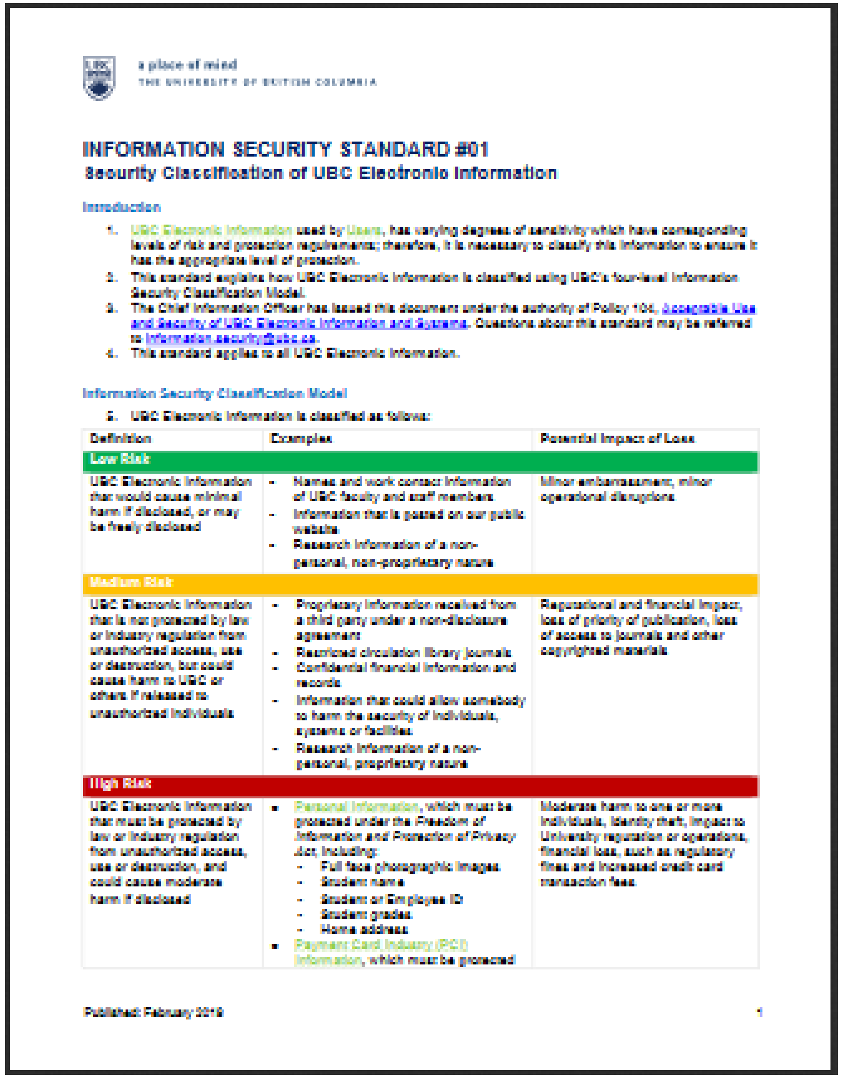
FIPPA/institutional standards – drop (mention in next few slides)

- What do researchers care about?
- Store information / share information
- Section 11 – may be changing to allow Compute Canada – clarification – they are not personal accounts but also not institutional account; therefore do not need to store a copy on UBC systems
- “Non-personal” “non-institutional”
- But not for high risk; very high risk information (personal information) – require STRA but likely no

Institutional Standards

UBC Security Standard #01: Security Classification

- 4 level classification: Low, Medium, High, Very High risk
  - Research information of a non-personal, **non-proprietary** nature is considered Low Risk
  - Research information of a non-personal, **proprietary** nature is considered Medium Risk
  - Personal information and Personal Health Information considered High and Very High risk



a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #01
Security Classification of UBC Electronic Information

Introduction

1. UBC Electronic Information used by Users, has varying degrees of sensitivity which have corresponding levels of risk and protection requirements; therefore, it is necessary to classify this information to ensure it has the appropriate level of protection.
2. This standard explains how UBC Electronic Information is classified using UBC's four-level Information Security Classification Model.
3. The Chief Information Officer has issued this document under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.
4. This standard applies to all UBC Electronic Information.

Information Security Classification Model

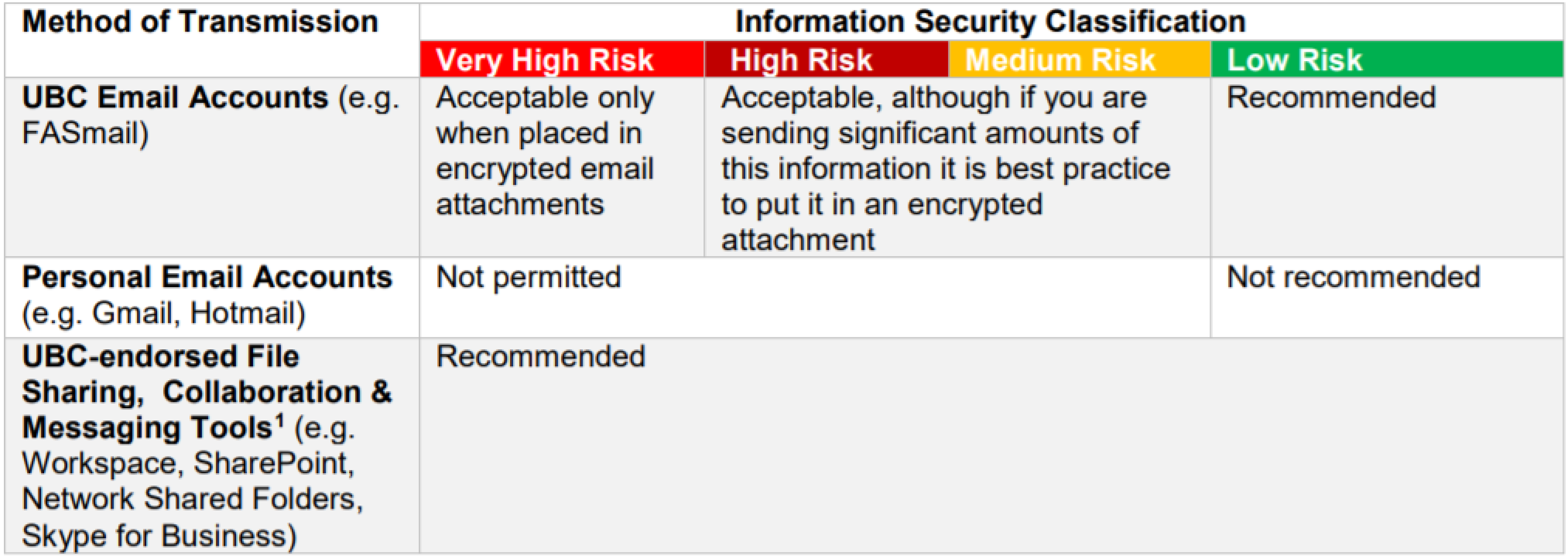
5. UBC Electronic Information is classified as follows:

Definition	Examples	Potential Impact of Loss
Low Risk		
UBC Electronic Information that would cause minimal harm if disclosed, or may be freely disclosed	- Names and work contact information of UBC faculty and staff members - Information that is posted on our public website - Research information of a non-personal, non-proprietary nature	Minor embarrassment, minor operational disruptions
Medium Risk		
UBC Electronic Information that is not protected by law or industry regulation from unauthorized access, use or destruction, but could cause harm to UBC or others if released to unauthorized individuals	- Proprietary information received from a third party under a non-disclosure agreement - Restricted circulation library journals - Confidential financial information and records - Information that could allow somebody to harm the security of individuals, systems or facilities - Research information of a non-personal, proprietary nature	Reputational and financial impact, loss of priority of publication, loss of access to journals and other copyrighted materials
High Risk		
UBC Electronic Information that must be protected by law or industry regulation from unauthorized access, use or destruction, and could cause moderate harm if disclosed	▪ Personal Information, which must be protected under the Freedom of Information and Protection of Privacy Act, including: - Full face photographic images - Student name - Student or Employee ID - Student grades - Home address ▪ Payment Card Industry (PCI) Information, which must be protected	Moderate harm to one or more individuals, identity theft, impact to University reputation or operations, financial loss, such as regulatory fines and increased credit card transaction fees

Published: February 2018

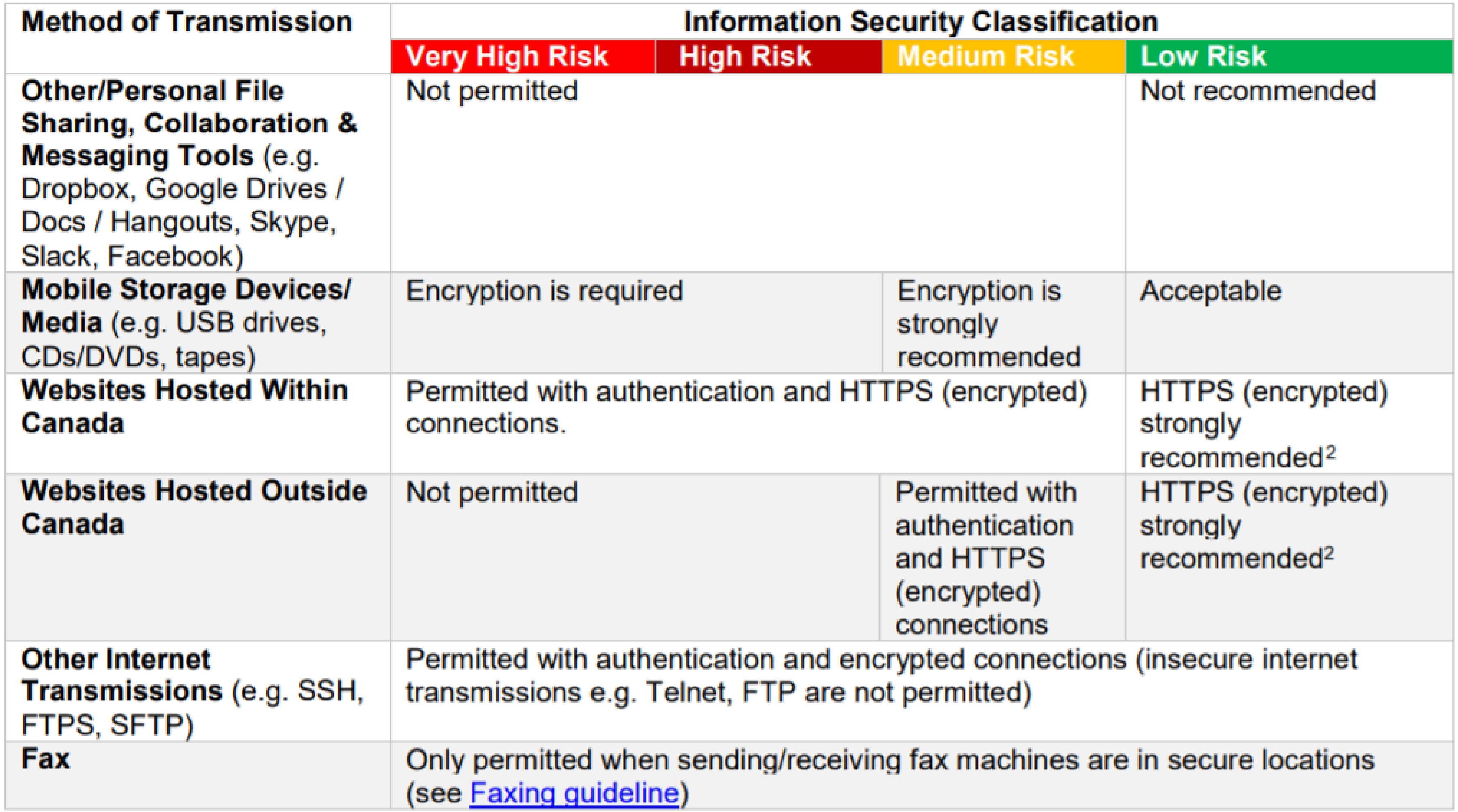
1

UBC Security Standard #03: Transmission and Sharing of UBC Electronic Information



Method of Transmission	**Information Security Classification**			
	Very High Risk	**High Risk**	**Medium Risk**	**Low Risk**
UBC Email Accounts (e.g. FASmail)	Acceptable only when placed in encrypted email attachments	Acceptable, although if you are sending significant amounts of this information it is best practice to put it in an encrypted attachment		Recommended
Personal Email Accounts (e.g. Gmail, Hotmail)	Not permitted			Not recommended
UBC-endorsed File Sharing, Collaboration & Messaging Tools[1] (e.g. Workspace, SharePoint, Network Shared Folders, Skype for Business)	Recommended			

UBC Security Standard #03: Transmission and Sharing of UBC Electronic Information

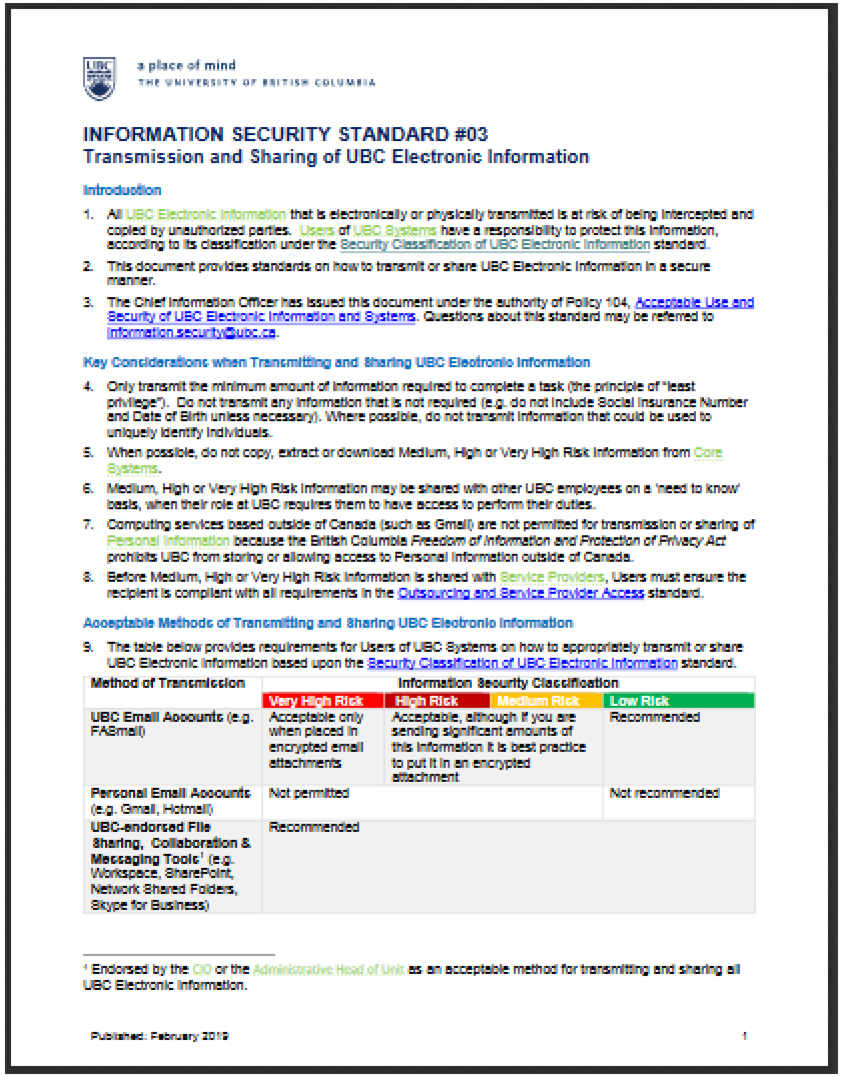


Method of Transmission	**Information Security Classification**			
	Very High Risk	**High Risk**	**Medium Risk**	**Low Risk**
Other/Personal File Sharing, Collaboration & Messaging Tools (e.g. Dropbox, Google Drives / Docs / Hangouts, Skype, Slack, Facebook)	Not permitted			Not recommended
Mobile Storage Devices/ Media (e.g. USB drives, CDs/DVDs, tapes)	Encryption is required		Encryption is strongly recommended	Acceptable
Websites Hosted Within Canada	Permitted with authentication and HTTPS (encrypted) connections.			HTTPS (encrypted) strongly recommended[2]
Websites Hosted Outside Canada	Not permitted		Permitted with authentication and HTTPS (encrypted) connections	HTTPS (encrypted) strongly recommended[2]
Other Internet Transmissions (e.g. SSH, FTPS, SFTP)	Permitted with authentication and encrypted connections (insecure internet transmissions e.g. Telnet, FTP are not permitted)			
Fax	Only permitted when sending/receiving fax machines are in secure locations (see Faxing guideline)			

UBC Security Standard #03: Transmission and Sharing of UBC Electronic Information

11. Subject to section 9, If the User is using personal accounts or other information sharing tools to share UBC Electronic Information, they are responsible for ensuring that a copy of this information is stored on UBC Systems at all times

*(UBC Electronic Information: Is information needed to conduct activities in support of the administrative, academic, and research mandates of the University.)



a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #03
Transmission and Sharing of UBC Electronic Information

Introduction

1. All UBC Electronic Information that is electronically or physically transmitted is at risk of being intercepted and copied by unauthorized parties. Users of UBC Systems have a responsibility to protect this information, according to its classification under the Security Classification of UBC Electronic Information standard.
2. This document provides standards on how to transmit or share UBC Electronic Information in a secure manner.
3. The Chief Information Officer has issued this document under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

Key Considerations when Transmitting and Sharing UBC Electronic Information

4. Only transmit the minimum amount of information required to complete a task (the principle of "least privilege"). Do not transmit any information that is not required (e.g. do not include Social Insurance Number and Date of Birth unless necessary). Where possible, do not transmit information that could be used to uniquely identify individuals.
5. When possible, do not copy, extract or download Medium, High or Very High Risk Information from Core Systems.
6. Medium, High or Very High Risk Information may be shared with other UBC employees on a 'need to know' basis, when their role at UBC requires them to have access to perform their duties.
7. Computing services based outside of Canada (such as Gmail) are not permitted for transmission or sharing of Personal Information because the British Columbia *Freedom of Information and Protection of Privacy Act* prohibits UBC from storing or allowing access to Personal Information outside of Canada.
8. Before Medium, High or Very High Risk Information is shared with Service Providers, Users must ensure the recipient is compliant with all requirements in the Outsourcing and Service Provider Access standard.

Acceptable Methods of Transmitting and Sharing UBC Electronic Information

9. The table below provides requirements for Users of UBC Systems on how to appropriately transmit or share UBC Electronic Information based upon the Security Classification of UBC Electronic Information standard.

Method of Transmission	Information Security Classification			
	Very High Risk	High Risk	Medium Risk	Low Risk
UBC Email Accounts (e.g. FASmail)	Acceptable only when placed in encrypted email attachments	Acceptable, although if you are sending significant amounts of this information it is best practice to put it in an encrypted attachment		Recommended
Personal Email Accounts (e.g. Gmail, Hotmail)	Not permitted			Not recommended
UBC-endorsed File Sharing, Collaboration & Messaging Tools[1] (e.g. Workspace, SharePoint, Network Shared Folders, Skype for Business)	Recommended			

[1] Endorsed by the CIO or the Administrative Head of Unit as an acceptable method for transmitting and sharing all UBC Electronic Information.

Published: February 2019 1

Compliance

Compliance

Compliance

Compliance

Compliance

Compliance

aws

Dropbox

Google Drive

Azure

iCloud

Compliance

aws
Dropbox
REDCap™
Research Electronic Data Capture
Google Drive
Azure
iCloud

Questions?

Questions?

jeff.gardner@ubc.ca

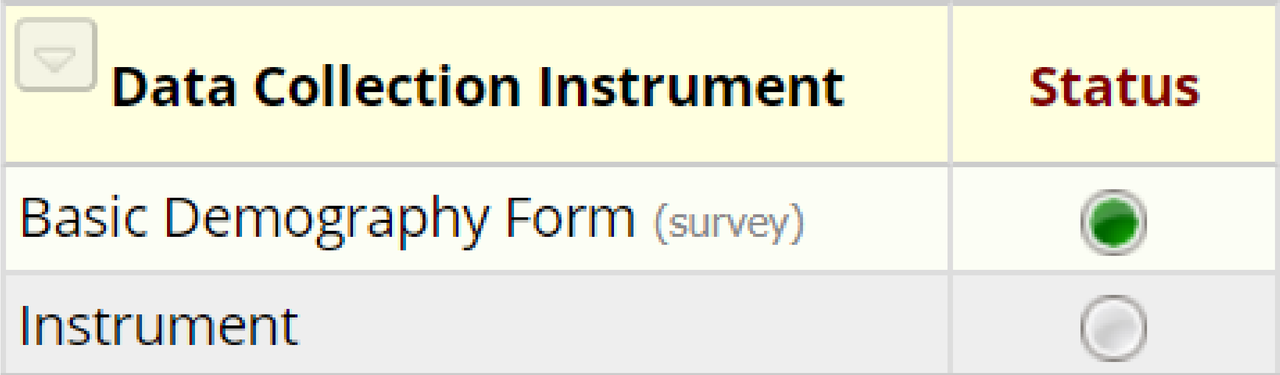
REDCap

What is REDCap?

- Data capture web tool
- Data can be captured via surveys and/or data entry
- It is one of those tools that is seen as the silver bullet or the solution to all data capture needs

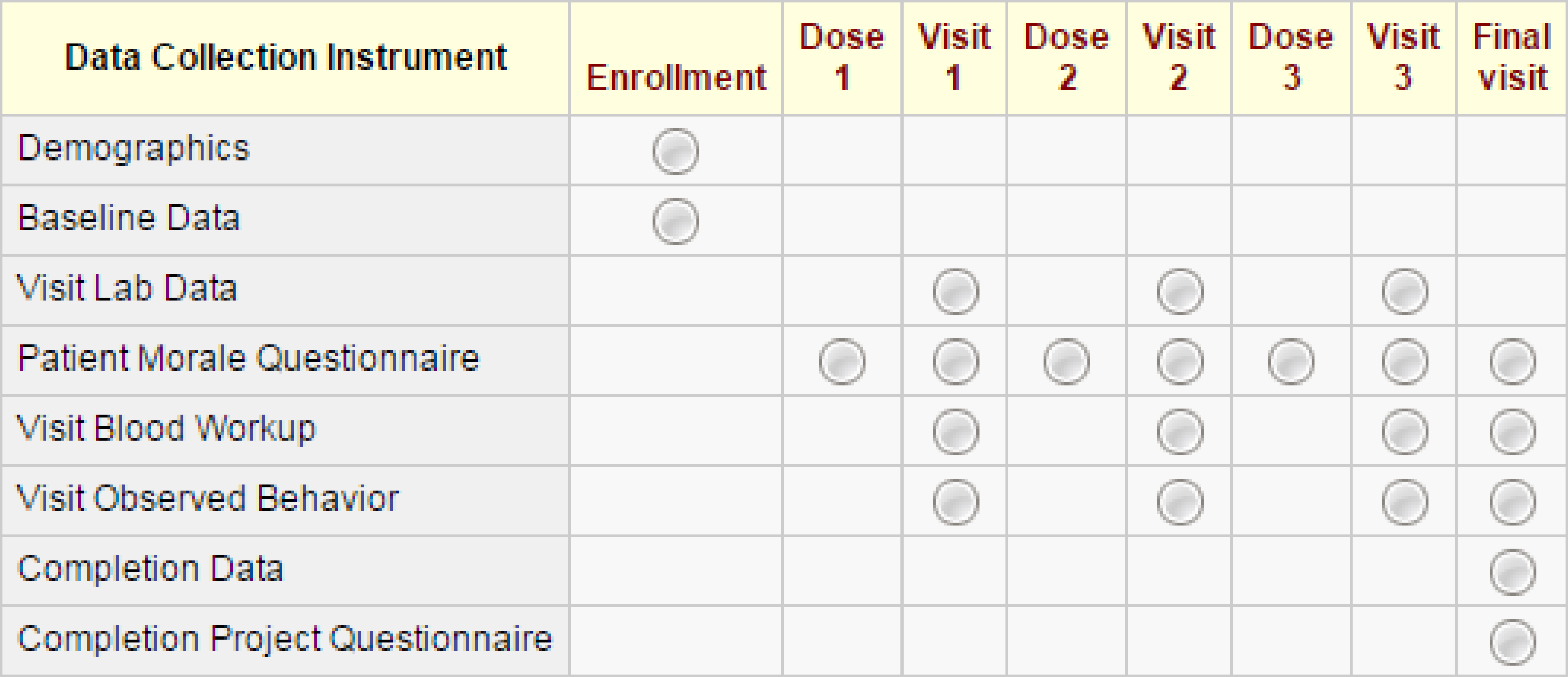
Classic project vs longitudinal study

Study ID **2**



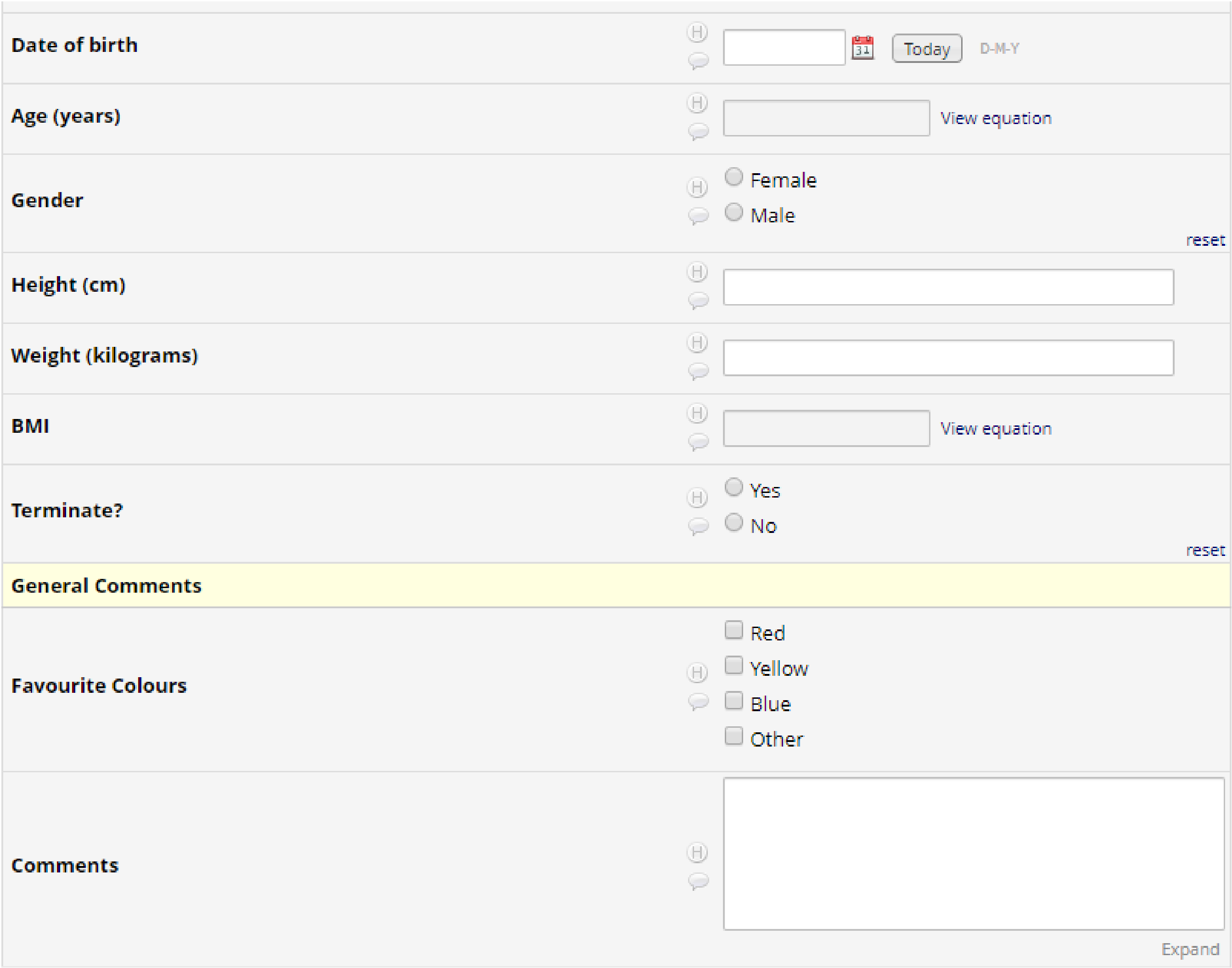
Data Collection Instrument	Status
Basic Demography Form (survey)	●
Instrument	○

Classic project vs longitudinal study



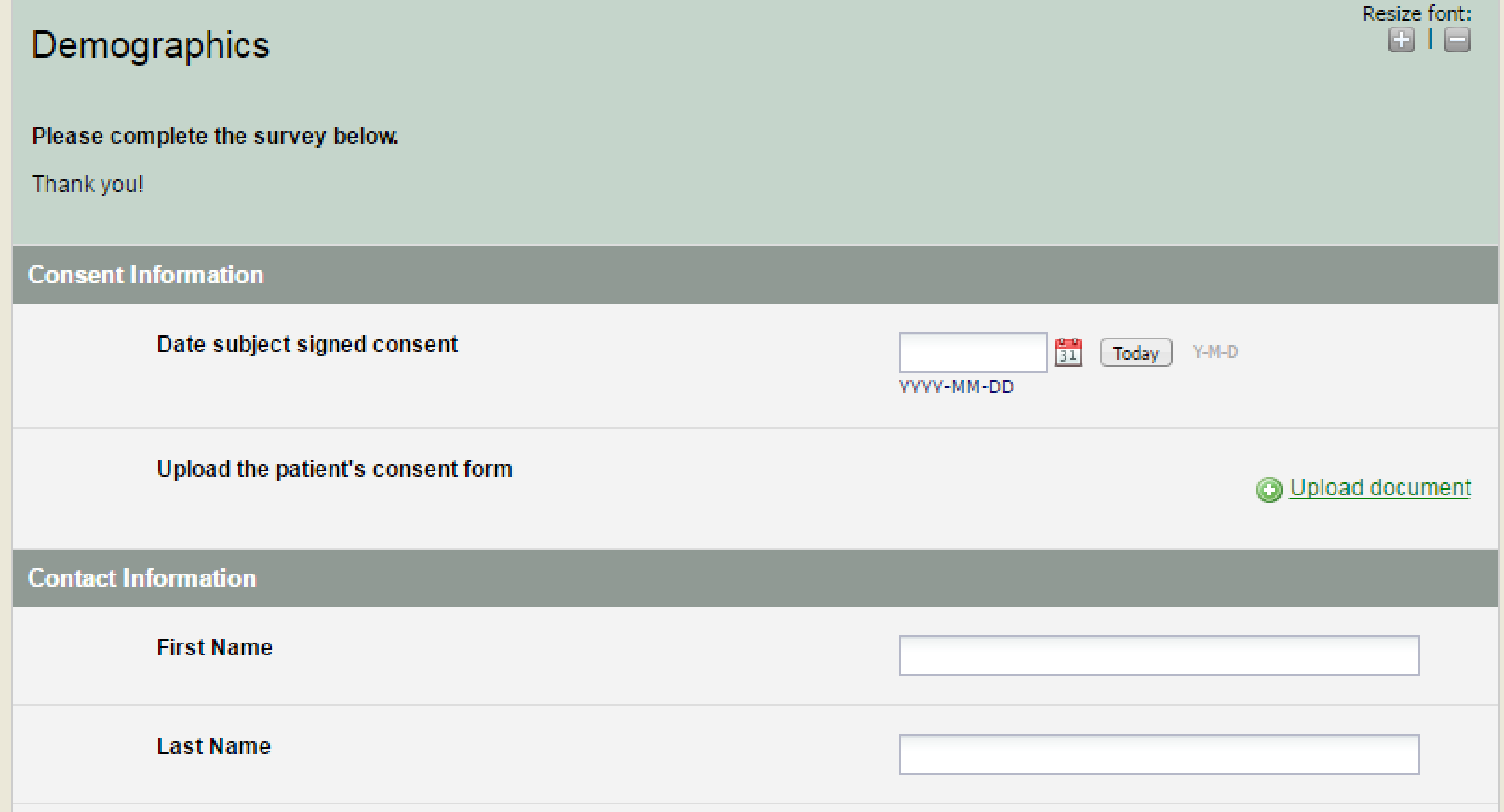
Data Collection Instrument	Enrollment	Dose 1	Visit 1	Dose 2	Visit 2	Dose 3	Visit 3	Final visit
Demographics	○							
Baseline Data	○							
Visit Lab Data			○		○		○	
Patient Morale Questionnaire		○	○	○	○	○	○	○
Visit Blood Workup			○		○		○	○
Visit Observed Behavior			○		○		○	○
Completion Data								○
Completion Project Questionnaire								○

Data Entry Forms



Date of birth	Today D-M-Y
Age (years)	View equation
Gender	○ Female ○ Male reset
Height (cm)	
Weight (kilograms)	
BMI	View equation
Terminate?	○ Yes ○ No reset
General Comments	
Favourite Colours	□ Red □ Yellow □ Blue □ Other
Comments	Expand

Surveys



Demographics

Please complete the survey below.

Thank you!

Consent Information

Date subject signed consent [ ] Today Y-M-D
YYYY-MM-DD

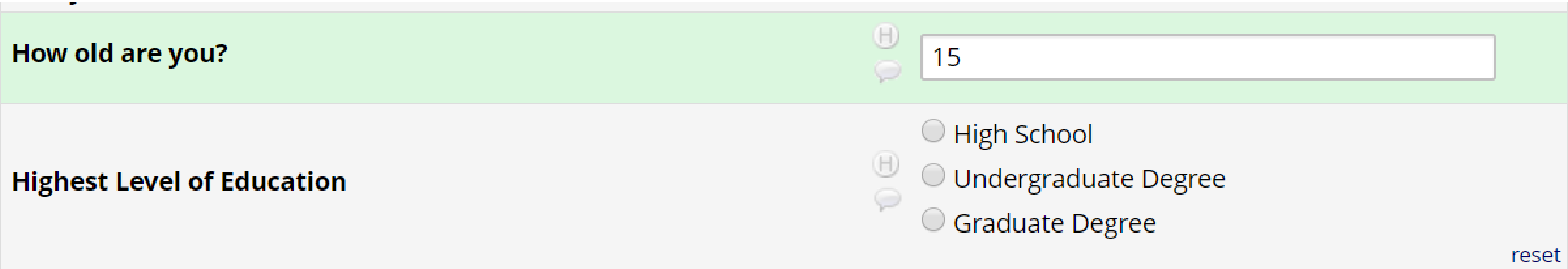
Upload the patient's consent form Upload document

Contact Information

First Name [ ]

Last Name [ ]

Branching Logic

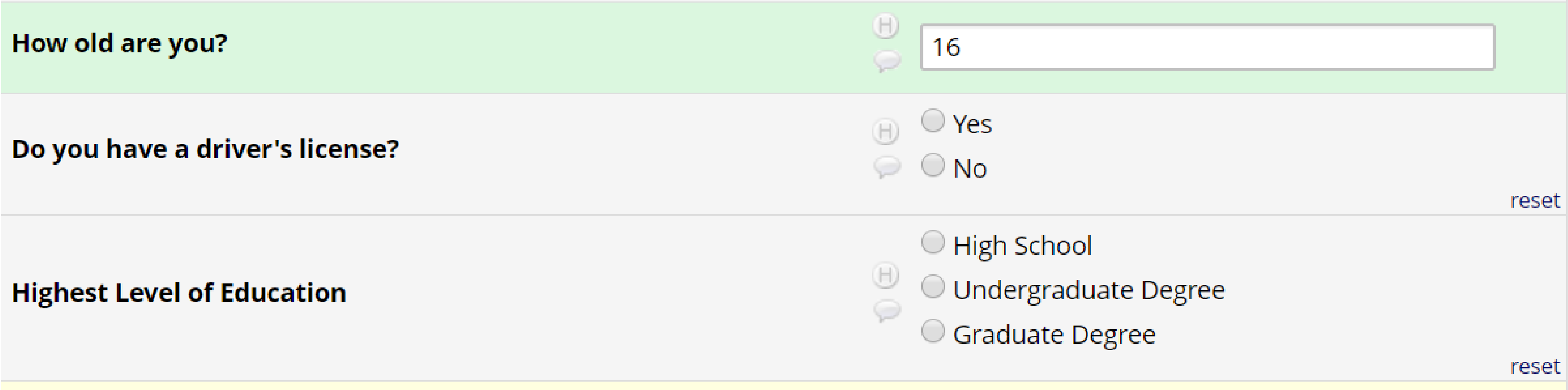


How old are you? 15

Highest Level of Education

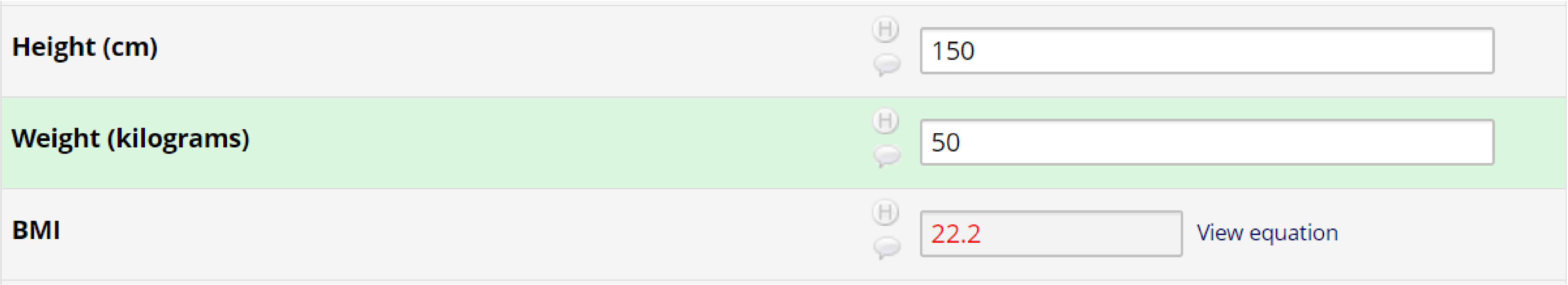
○ High School
○ Undergraduate Degree
○ Graduate Degree

Branching Logic



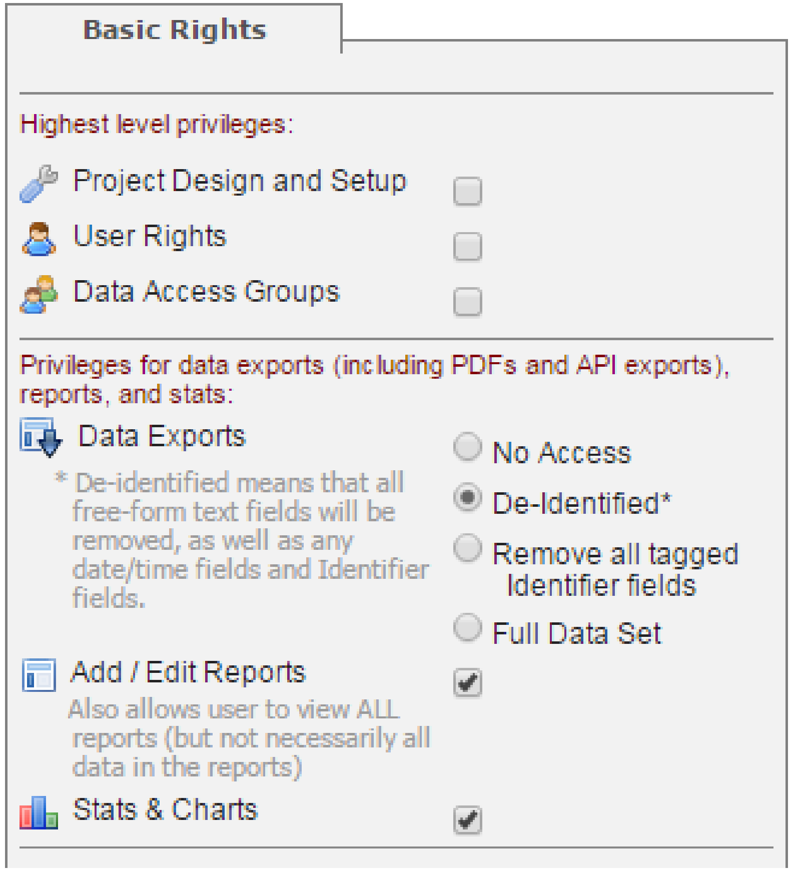
How old are you?	16
Do you have a driver's license?	○ Yes ○ No reset
Highest Level of Education	○ High School ○ Undergraduate Degree ○ Graduate Degree reset

Calculations



Height (cm)	150	
Weight (kilograms)	50	
BMI	22.2	View equation

Granular Permissions



Basic Rights

Highest level privileges:

- Project Design and Setup ☐
- User Rights ☐
- Data Access Groups ☐

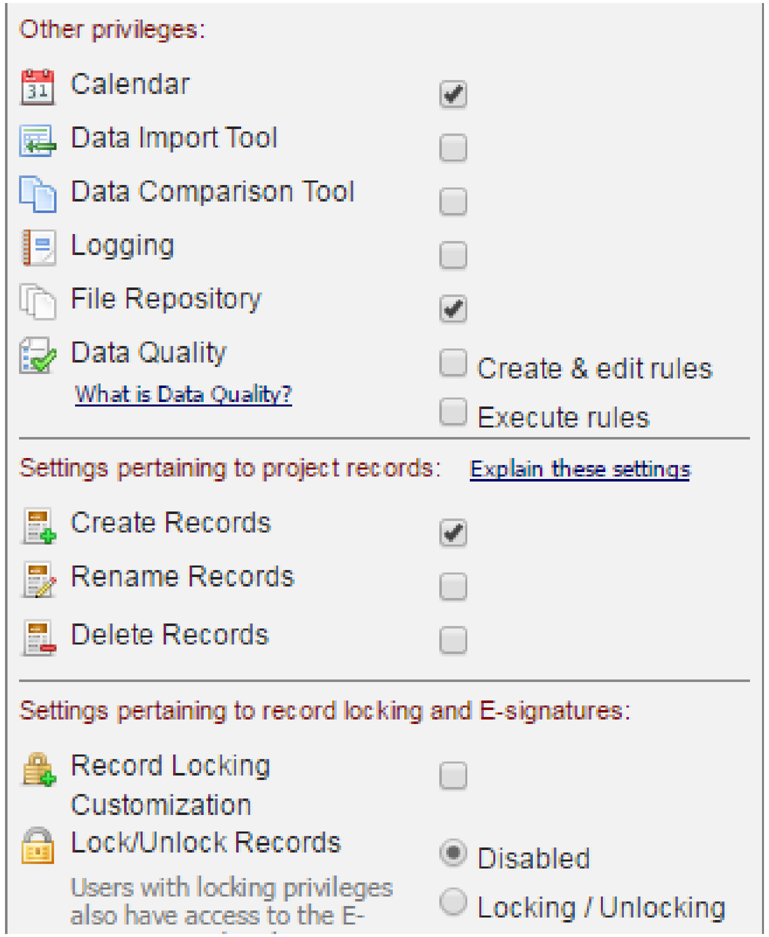
Privileges for data exports (including PDFs and API exports), reports, and stats:

Data Exports
○ No Access
● De-Identified*
○ Remove all tagged Identifier fields
○ Full Data Set

* De-identified means that all free-form text fields will be removed, as well as any date/time fields and Identifier fields.

Add / Edit Reports ☑
Also allows user to view ALL reports (but not necessarily all data in the reports)

Stats & Charts ☑



Other privileges:

- Calendar ☑
- Data Import Tool ☐
- Data Comparison Tool ☐
- Logging ☐
- File Repository ☑
- Data Quality ☐ Create & edit rules ☐ Execute rules

What is Data Quality?

Settings pertaining to project records: Explain these settings

- Create Records ☑
- Rename Records ☐
- Delete Records ☐

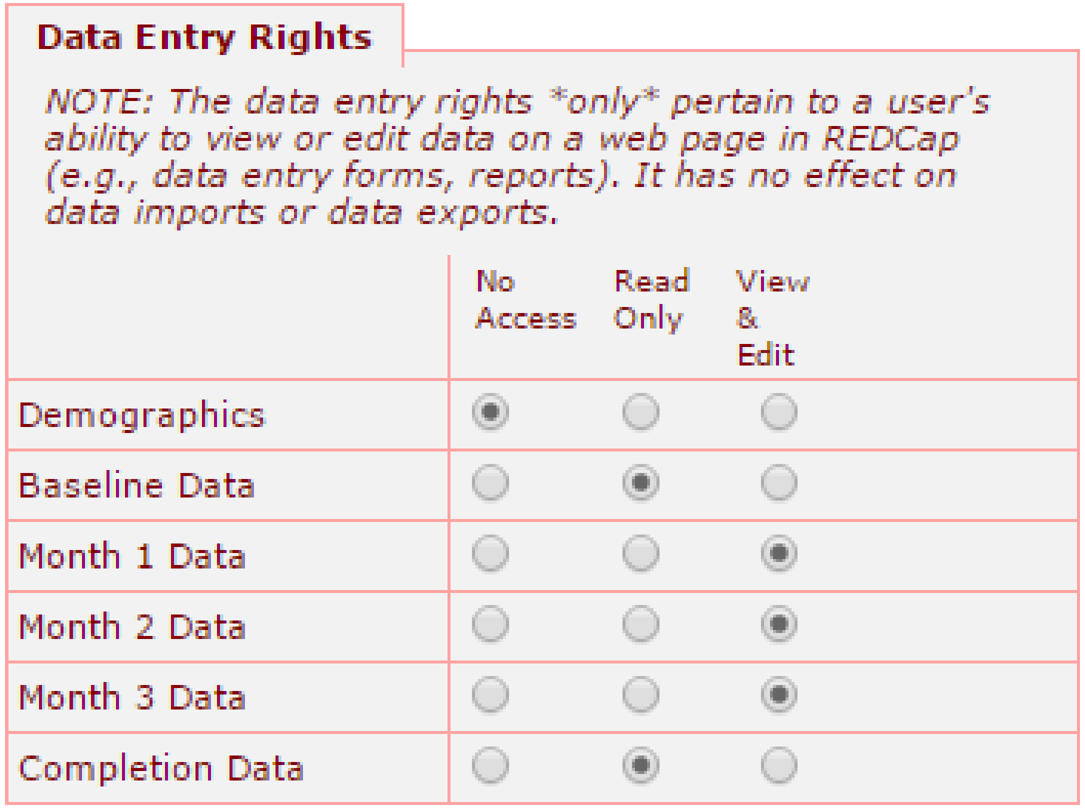
Settings pertaining to record locking and E-signatures:

Record Locking Customization ☐

Lock/Unlock Records
● Disabled
○ Locking / Unlocking

Users with locking privileges also have access to the E-

Granular Permissions

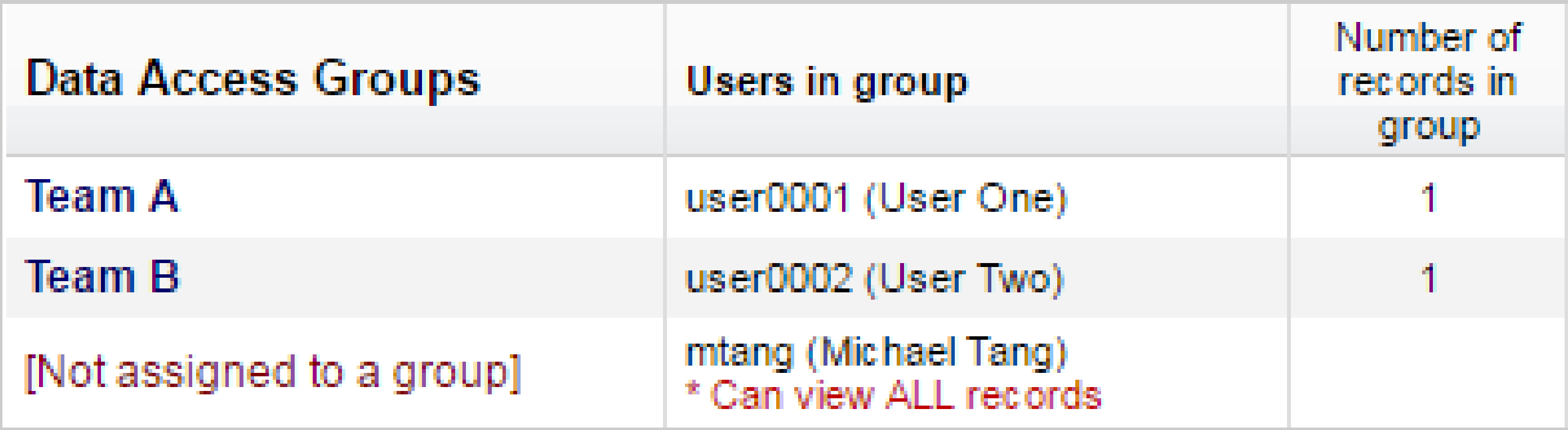


Data Entry Rights

*NOTE: The data entry rights *only* pertain to a user's ability to view or edit data on a web page in REDCap (e.g., data entry forms, reports). It has no effect on data imports or data exports.*

	No Access	Read Only	View & Edit
Demographics	●	○	○
Baseline Data	○	●	○
Month 1 Data	○	○	●
Month 2 Data	○	○	●
Month 3 Data	○	○	●
Completion Data	○	●	○

Granular Permissions



Data Access Groups	Users in group	Number of records in group
Team A	user0001 (User One)	1
Team B	user0002 (User Two)	1
[Not assigned to a group]	mtang (Michael Tang) * Can view ALL records	

Example

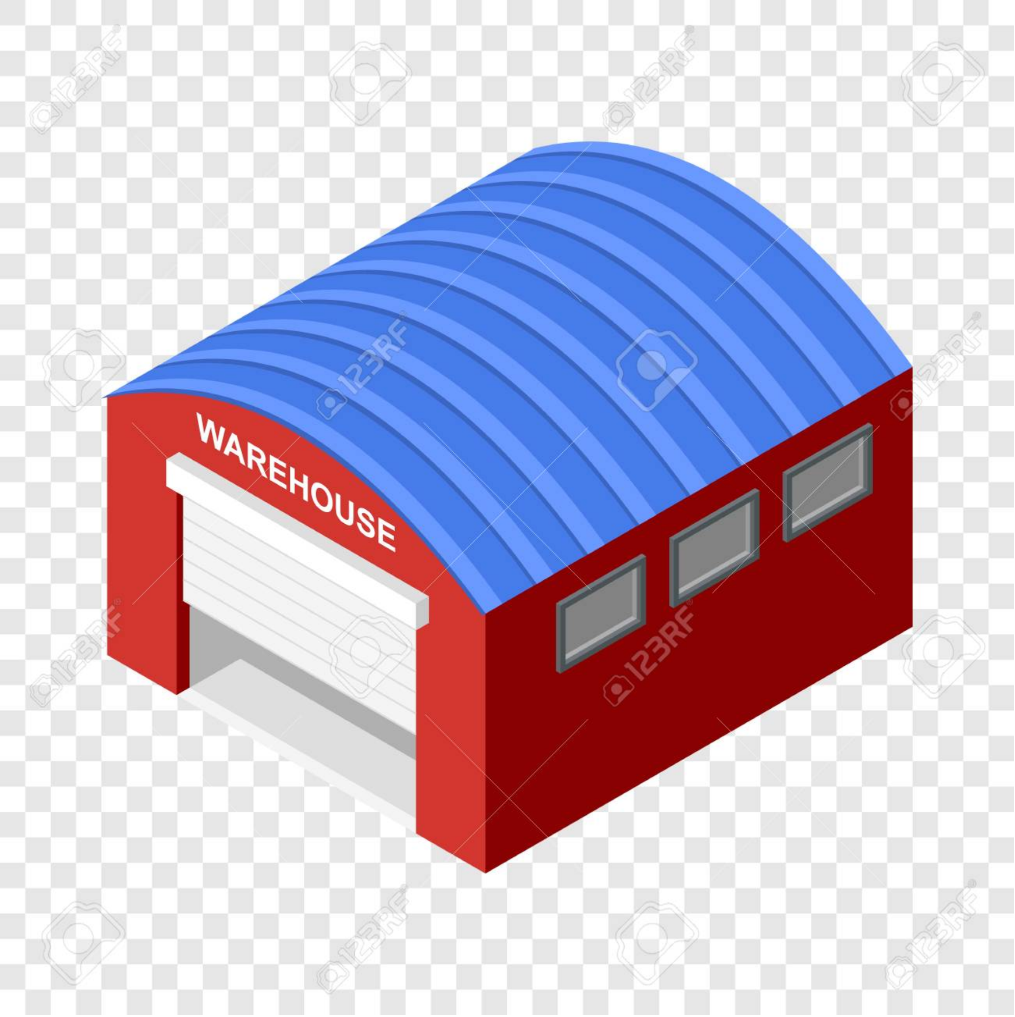
Project 1: Screening Log **(All Referred Patients)** **(Kept till end of recruitment period)**	**Project 2: Enrolled Identifying Info Log** **(Only Enrolled Patients)** **(Kept till end of project period)**	**Project 3: Research Data Log** **(Only Enrolled Patients)** **(Kept till end of project period)**

Example

Project 2: Enrolled Identifying Info Log
(Only Enrolled Patients)
(Kept till end of project period)

Project 3: Research Data Log
(Only Enrolled Patients)
(Kept till end of project period)

Upcoming Data Warehouse



End
Demo
£

Questions?

Contact

jeff.gardner@ubc.ca
michael.tang@ubc.ca
redcap.support@ubc.ca