Securely Managing and Publishing Sensitive Data

Isaac Pratt, PhD

February 8, 2023

Research Data Management Services
McMaster University

Lewis & Ruth
Sherman Centre
for Digital Scholarship
scds.ca

McMaster University | Library

McMaster University is located on the traditional Territories of the Mississauga and Haudenosaunee Nations, and within the lands protected by the “Dish With One Spoon” wampum agreement.

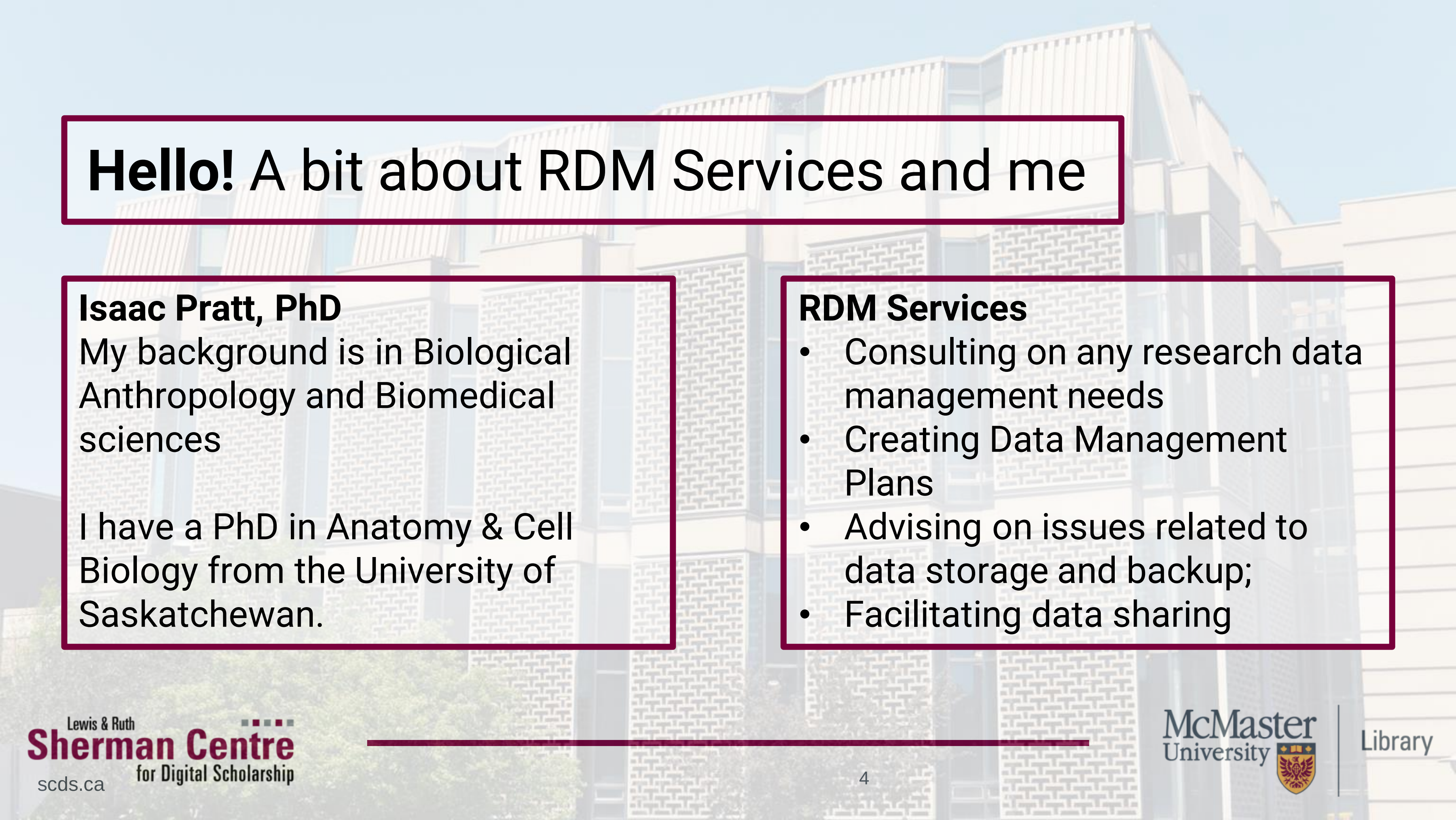
Laslovarga, “Webster Falls in Winter, Waterdown, Hamilton, Ontario, Canada - Spencer Gorge / Webster's Falls Conservation Area,” 23 January 2011, Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Waterdawn_Webster_Falls_in_Winter8.jpg

Certificate Program

The Sherman Centre offers a Certificate of Completion that rewards synchronous participation at 7 workshops. We also offer concentrations in Data Analysis and Visualization, Digital Scholarship, and Research Data Management.

Learn more about the Certificate Program: https://scds.ca/certificate-program
If you would like to be considered for the certificate, verify your participation in this form: https://u.mcmaster.ca/verification

At an unspecified point during the workshop, a code will be read aloud. This is the answer to the third question of the form.



Hello! A bit about RDM Services and me

Isaac Pratt, PhD

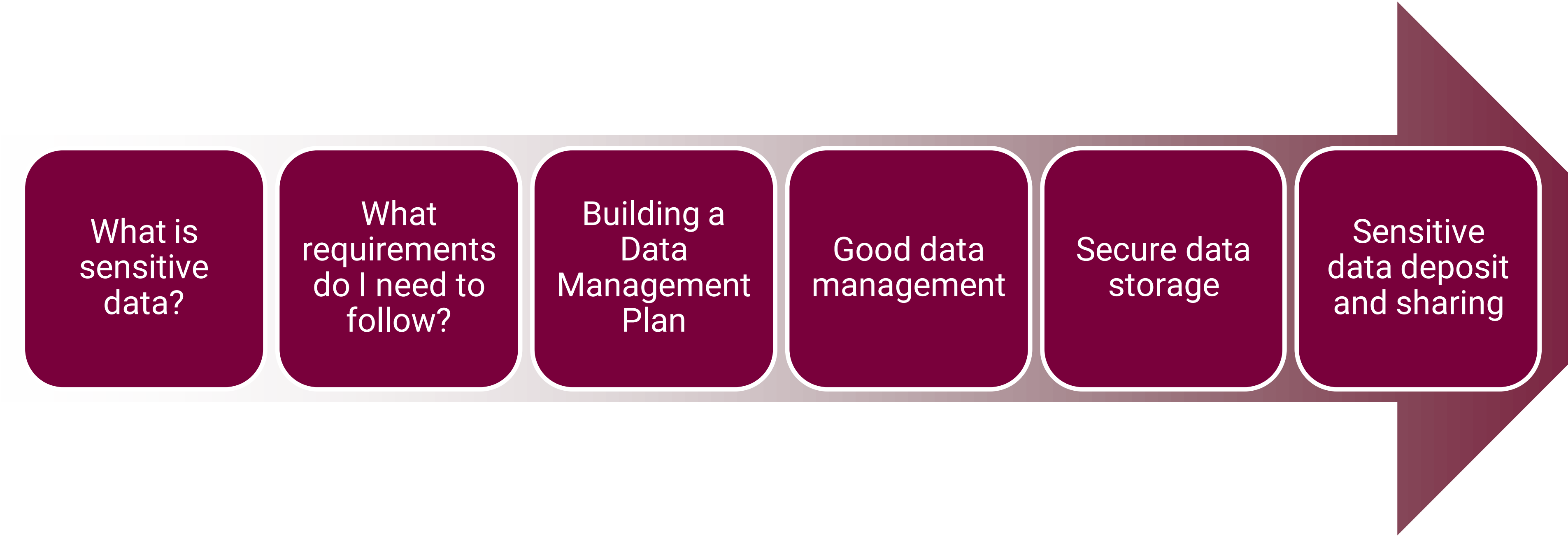
My background is in Biological Anthropology and Biomedical sciences

I have a PhD in Anatomy & Cell Biology from the University of Saskatchewan.

RDM Services

- Consulting on any research data management needs
- Creating Data Management Plans
- Advising on issues related to data storage and backup;
- Facilitating data sharing

Outline



What is sensitive data?

What requirements do I need to follow?

Building a Data Management Plan

Good data management

Secure data storage

Sensitive data deposit and sharing

⚠ What is sensitive data:

Sensitive data is any data that would cause harm if released openly.

- Research data containing personal identifying information or personal health information
- Commercially sensitive data, including data generated under a commercial research funding agreement
- Data relating to rare or endangered species
- Data likely to harm an individual or community or have a significant negative public impact if released

What requirements do I need to be aware of?

Ethics

- Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2022)
- MREB, HiREB

Funders

- Tri-Agency Research Data Management Policy
- NIH Data Management & Sharing Policy

Data sources

- Data sharing/transfer agreements – MILO Sample Agreements

Journals

- Data availability statements and data sharing policies - Frontiers Materials and data policies

Privacy legislation

- EU General Data Protection Regulation (GDPR)
- in Canada based on the National Standard Model Code for the Protection of Personal Information

Privacy principles

There are 10 privacy principles that underpin the Canadian Model Code, including:

1) Accountability
2) Identifying purposes
3) Consent
4) Limiting collection
5) Limiting use, disclosure and retention
6) Accuracy
7) Safeguards
8) Openness
9) Individual access
10) Challenging compliance

Canadian Ethics principles - TCPS2

- **Respect for Persons:**
  - **Informed consent**, voluntary participation, limiting undue influence, assent process, deception and debrief, etc.
- **Concern for Welfare**
  - Holistic view of welfare, identify risks, minimize and mitigate risks, procedures in place to address likely harms, **data security**, etc.
- **Justice**:
  - Sharing burdens and benefits of research, just exclusion/inclusion, **disseminating results**, etc.
- **Ethical Duty of Confidentiality**
  - Researchers shall safeguard information entrusted to them and not misuse or wrongfully disclose it

Funder Requirements

Home > Interagency research funding > Policies and Guidelines > Research Data Management

Research Data Management

Tri-Agency Statement of Principles on Digital Data Management

Tri-Agency Research Data Management Policy

Tri-Agency RDM Policy – CIHR:

- CIHR currently requires researchers to deposit bioinformatics, atomic, and molecular coordinate data into the appropriate public database.

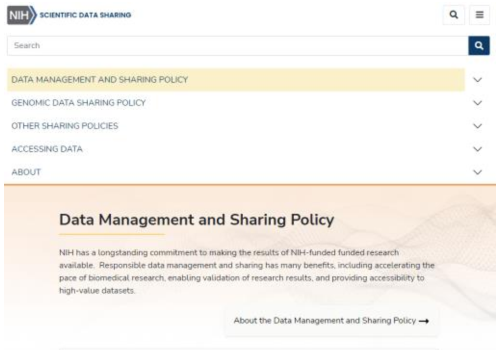
Data Management Plans (in pilot phase)

- Grants will require data management plans (DMPs) to be submitted at the time of application.

Data Deposit (launch tbd)

- Grant recipients will be required to deposit into a digital repository research data that supports journal publications and pre-prints from funded research
- Grant recipients are not required to share their data
- First Nations, Métis and Inuit communities
- “researchers should only make data accessible if doing so is ethical, legal, and is in consonance with any commercial or other agreements the researcher has entered into”

Funder Requirements


NIH SCIENTIFIC DATA SHARING
Search
DATA MANAGEMENT AND SHARING POLICY
GENOMIC DATA SHARING POLICY
OTHER SHARING POLICIES
ACCESSING DATA
ABOUT

Data Management and Sharing Policy

NIH has a longstanding commitment to making the results of NIH-funded funded research available. Responsible data management and sharing has many benefits, including accelerating the pace of biomedical research, enabling validation of research results, and providing accessibility to high-value datasets.

About the Data Management and Sharing Policy →

National Institutes of Health (NIH) *Data Management and Sharing Policy*

Data Management Plans:

- NIH requires all applicants planning to generate scientific data to prepare a DMS Plan that describes how the scientific data will be managed and shared.

Data Sharing:

- “Scientific data should be made accessible as soon as possible.”
- *“certain factors (i.e., ethical, legal, or technical) may necessitate limiting sharing to some extent. Foreseeable limitations should be described in DMS Plans”*
- *“Consider whether access to shared scientific data derived from humans should be controlled”*

Journal Requirements

Journals have increasing requirements for data sharing:

Social Science and Medicine

- “This journal **requires and enables you to share data** that supports your research publication where appropriate”
- “If you have made your research data available in a data repository, you can link your article directly to the dataset”
- “we require you to state the availability of your data in your submission if your data is unavailable to access or unsuitable to post”

Indigenous Data Sovereignty

When researchers are working with Indigenous communities, they should abide by principles of indigenous data sovereignty like the CARE principles. For Canadian First Nations, the OCAP principles are recommended:

- **Ownership**: a community or group owns information collectively in the same way that an individual owns his or her personal information.
- **Control**: First Nations, their communities, and representative bodies are within their rights to seek control over all aspects of research and information management processes that impact them.
- **Access**: First Nations must have access to information and data about themselves and their communities regardless of where it is held.
- **Possession** is the mechanism by which ownership can be asserted and protected, through direct physical control of data.

1. **Plan:** Create a Data Management Plan

- A **Data Management Plan (DMP)** is your plan for how you will create, store, organize, document, secure, preserve, and share your research data.
- A living document which speaks to the management of data both **during** the active phases of your research and **after** the completion of the research project.

DMP

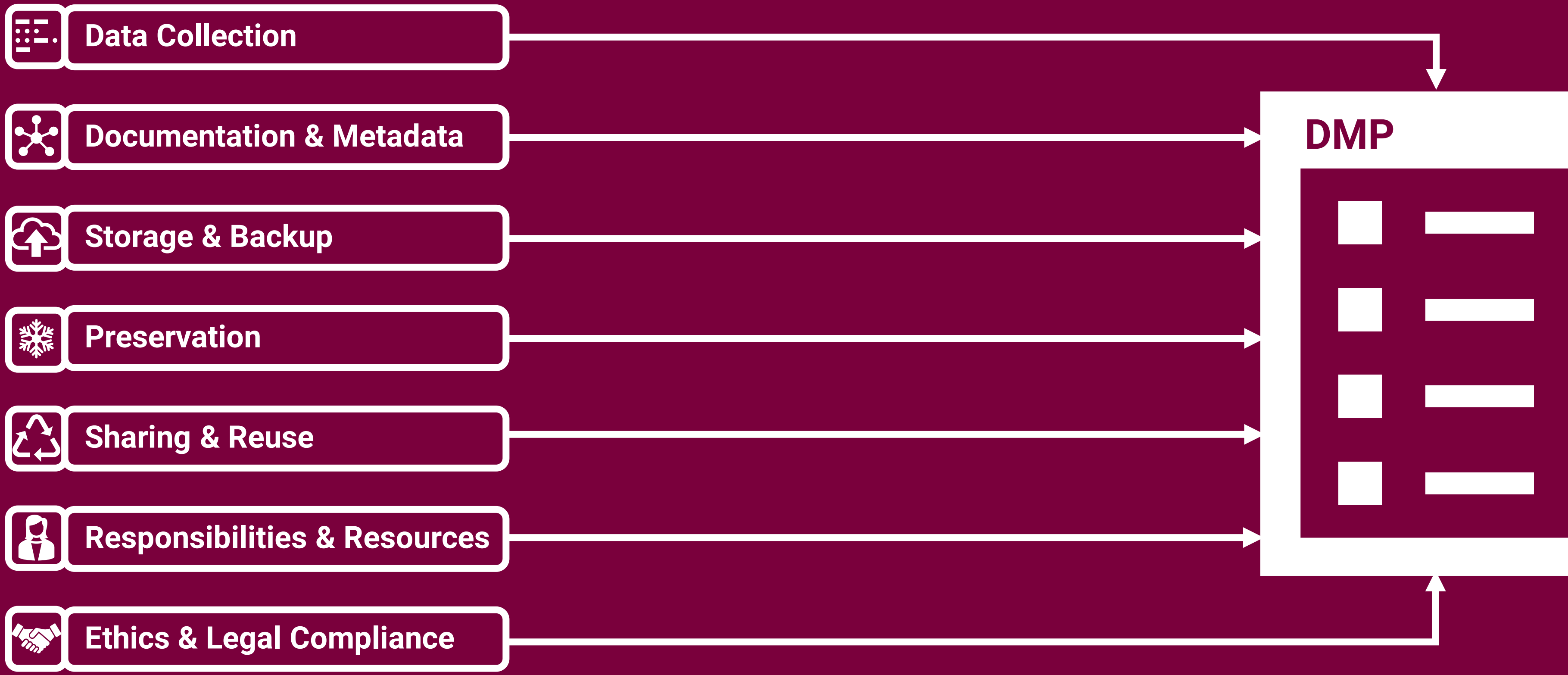
Photo by Hanna Morris on Unsplash.

Why create a DMP?

- A blueprint for how you will be working with your data during your project
- Avoid potential pitfalls and problems before they occur
- Prepare for future stages of research including potential data sharing
- Many research funders require grant applicants to submit a DMP – including the Tri-Agencies (NSERC, CIHR, SSHRC – started 2022) and NIH

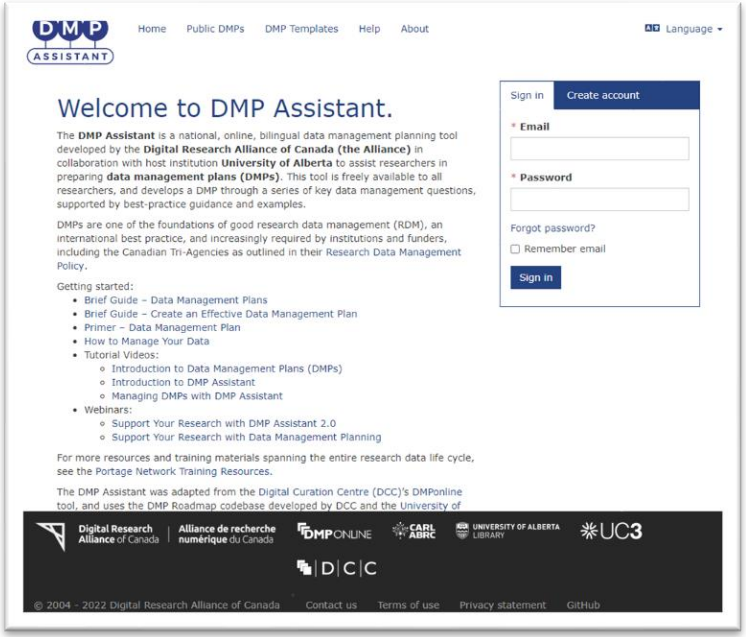
McMaster University | Library

What goes in a Data Management Plan?



- Data Collection
- Documentation & Metadata
- Storage & Backup
- Preservation
- Sharing & Reuse
- Responsibilities & Resources
- Ethics & Legal Compliance

DMP



Welcome to DMP Assistant.

The **DMP Assistant** is a national, online, bilingual data management planning tool developed by the **Digital Research Alliance of Canada (the Alliance)** in collaboration with host institution **University of Alberta** to assist researchers in preparing **data management plans (DMPs)**. This tool is freely available to all researchers, and develops a DMP through a series of key data management questions, supported by best-practice guidance and examples.

DMPs are one of the foundations of good research data management (RDM), an international best practice, and increasingly required by institutions and funders, including the Canadian Tri-Agencies as outlined in their Research Data Management Policy.

Getting started:

- Brief Guide – Data Management Plans
- Brief Guide – Create an Effective Data Management Plan
- Primer – Data Management Plan
- How to Manage Your Data
- Tutorial Videos:
  - Introduction to Data Management Plans (DMPs)
  - Introduction to DMP Assistant
  - Managing DMPs with DMP Assistant
- Webinars:
  - Support Your Research with DMP Assistant 2.0
  - Support Your Research with Data Management Planning

For more resources and training materials spanning the entire research data life cycle, see the Portage Network Training Resources.

The DMP Assistant was adapted from the Digital Curation Centre (DCC)'s DMPonline tool, and uses the DMP Roadmap codebase developed by DCC and the University of

© 2004 - 2022 Digital Research Alliance of Canada

A web-based, bilingual data management planning tool

Available to all researchers in Canada

A guided creation process

Exportable data management plans

assistant.portagenetwork.ca/

Data Management Practices

Good data management

Research project management

De-identification

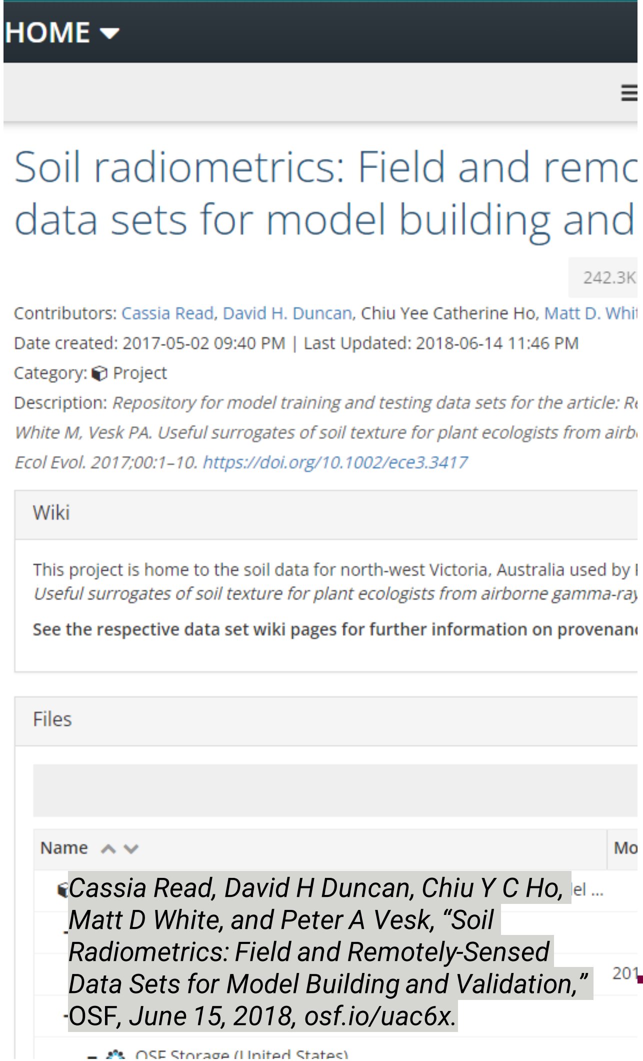
Secure data storage

Data storage practices and controls

3rd party tools and services

Cybersecurity practices

Encryption



Soil radiometrics: Field and remc
data sets for model building and

242.3K

Contributors: Cassia Read, David H. Duncan, Chiu Yee Catherine Ho, Matt D. Whi

Date created: 2017-05-02 09:40 PM | Last Updated: 2018-06-14 11:46 PM

Category: Project

Description: *Repository for model training and testing data sets for the article: R*
White M, Vesk PA. Useful surrogates of soil texture for plant ecologists from airb
Ecol Evol. 2017;00:1–10. https://doi.org/10.1002/ece3.3417

Wiki

This project is home to the soil data for north-west Victoria, Australia used by
Useful surrogates of soil texture for plant ecologists from airborne gamma-ray

See the respective data set wiki pages for further information on provenan

Files

Cassia Read, David H Duncan, Chiu Y C Ho, Matt D White, and Peter A Vesk, "Soil Radiometrics: Field and Remotely-Sensed Data Sets for Model Building and Validation," OSF, June 15, 2018, osf.io/uac6x.

Research Project Management

- **Collaboration**: Microsoft teams let you control your team and share and work on documents together in real-time, avoiding multiple versions and copies sent by email.
- **Reference Management**: Zotero or Endnote support collaboration through shared citation libraries.
- **Notetaking software**: Obsidian, OneNote, Notion, or an Electronic Lab Notebook allow you to create organized, linked notes that you can use to document your research practices
- **REDCap:** REDCap is a powerful web tool for collecting and organizing longitudinal data.

Learn more at **rdm.mcmaster.ca/organize**

De-identification definitions

From the TCPS2:

- **Coded information** – direct identifiers are removed from the information and replaced with a code. With access to the code it is possible to re-identify specific participants.
- **Anonymized information** – the information is irrevocably stripped of direct identifiers, a code is not kept, and risk of re-identification of individuals from remaining indirect identifiers is low or very low.
- **Anonymous information** – the information never had identifiers associated with it (e.g., anonymous surveys) and risk of re-identification is low or very low.
    - De-identification is not a 'guarantee' of privacy and risks of re-identification can often remain.

De-identifying data

Pseudonymization

Generalization: grouping specific values into categorized ranges.

- For example, grouping specific ages into age ranges or merging categories into larger groups.

Suppression: deleting individual cases or responses.

- For example, if there is only one individual in a particular age range of a specific ethnicity, the ethnicity response for that individual could be deleted to preserve the ethnicity category as a whole.

The ‘small cell’ problem

K anonymity

k-anonymity is a mathematical approach to ensuring a dataset is anonymous.

A dataset has k-anonymity when a particular individual in the dataset cannot be distinguished from k other individuals in the dataset.

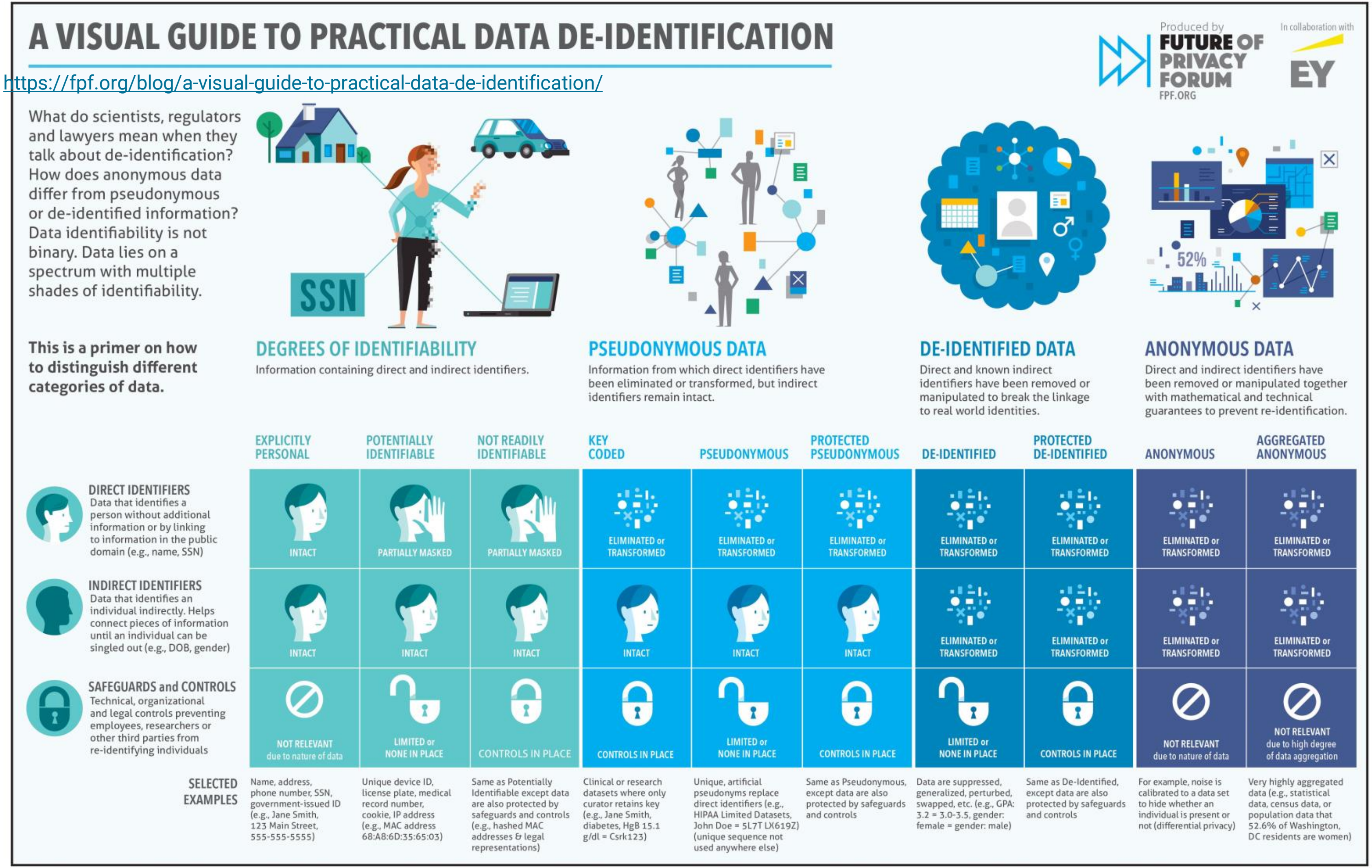
‘k’ is a number set by the researcher - most commonly set to 5. This means it should not possible to isolate a group of fewer than 5 identical individuals.

Amnesia https://amnesia.openaire.eu/

sdcMicro https://cran.r-project.org/web/packages/sdcMicro/index.html

For a more comprehensive overview see the Portage Network’s Reducing Risk Webinar and slides

https://fpf.org/blog/a-visual-guide-to-practical-data-de-identification/



A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION

Produced by FUTURE OF PRIVACY FORUM FPF.ORG

In collaboration with EY

What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.

This is a primer on how to distinguish different categories of data.

DEGREES OF IDENTIFIABILITY

Information containing direct and indirect identifiers.

PSEUDONYMOUS DATA

Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.

DE-IDENTIFIED DATA

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.

ANONYMOUS DATA

Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	AGGREGATED ANONYMOUS
DIRECT IDENTIFIERS Data that identifies a person without additional information or by linking to information in the public domain (e.g., name, SSN)	INTACT	PARTIALLY MASKED	PARTIALLY MASKED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
INDIRECT IDENTIFIERS Data that identifies an individual indirectly. Helps connect pieces of information until an individual can be singled out (e.g., DOB, gender)	INTACT	INTACT	INTACT	INTACT	INTACT	INTACT	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
SAFEGUARDS and CONTROLS Technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals	NOT RELEVANT due to nature of data	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	NOT RELEVANT due to nature of data	NOT RELEVANT due to high degree of data aggregation
SELECTED EXAMPLES	Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)	Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68:A8:6D:35:65:03)	Same as Potentially Identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses & legal representations)	Clinical or research datasets where only curator retains key (e.g., Jane Smith, diabetes, HgB 15.1 g/dl = Csrk123)	Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets, John Doe = 5L7T LX619Z) (unique sequence not used anywhere else)	Same as Pseudonymous, except data are also protected by safeguards and controls	Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPA: 3.2 = 3.0-3.5, gender: female = gender: male)	Same as De-Identified, except data are also protected by safeguards and controls	For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)	Very highly aggregated data (e.g., statistical data, census data, or population data that 52.6% of Washington, DC residents are women)

Linking file/key

- You may need or want to keep a file linking the participant names and IDs or pseudonyms. Keep in mind your data is not anonymous if a linking file exists
- Linking files should be encrypted and stored on separate devices or systems than the data.
- Linking files and the included personal information should be destroyed/deleted when no longer required to increase privacy.

De-identification

Recordings and transcripts

- Video and audio recordings are inherently more identifiable than transcripts
- Researchers should transcribe recordings and limit access and may delete original recordings if they are no longer needed.
- Direct identifiers in transcripts should be pseudonymized or generalized where possible – not just name but also locations, ages, genders, etc

Data storage administrative controls

- Don’t collect identifiers that aren’t relevant to the research
- Data should be de-identified as soon as possible, with pseudonyms replacing names
- Researchers should work from de-identified data and not from identifiable data where possible
- Linking files/keys should be stored separately from de-identified data
- Data should only be made accessible to team members who need access

Data storage technological controls

- Store data on password protected devices
- Data stored on internet-connected devices needs to be encrypted
- Data should be stored in a secured environment or server rather than on individual computers or devices
- Back up devices need to follow the same requirements
- Data must be encrypted and password protected when shared – email should not be used for high risk data

Cloud storage

- Public cloud services (Google Drive, Dropbox) cannot be used for medium/high risk data but are fine for low risk data
- Institutional services such as MacDrive or OneDrive accessed through McMaster may be used in combination with encryption
- OneDrive is less flexible when working with outside collaborators but Teams
- MacDrive can create a shared folder that collaborators can access and can create encrypted folders
- Researchers using cloud storage should be careful about who they share files with and should enable security features like MFA

Evaluating 3rd party services

- High risk data should stay on campus and with the researchers, not on 3rd party platforms.
- Terms of use should be examined closely to see what platforms are doing with data – this may not align with regulatory requirements
- Data storage location should be in Canada, ideally in Ontario
- Data should be shared in a de-identified form when possible
- Individual contractors should sign confidentiality agreements

Backup Strategies (3-2-1)

A good data storage plan needs to balance accessibility and convenience against security and reliability.

3 Copies of your data (at least!)

Example:
1 copy stored locally on **hard drive** for analysis
1 copy stored on **cloud storage** platform
1 copy stored in a **secure campus drive**

2 Copies are on-hand (easily accessible) on different systems (internal hard drive, cloud storage, etc.)

- a "**production**" (working) copy
- a "**production backup**" copy

1 Copy is in another location ("off-site") from the others with a ***trusted*** service provider

Long term/archival storage

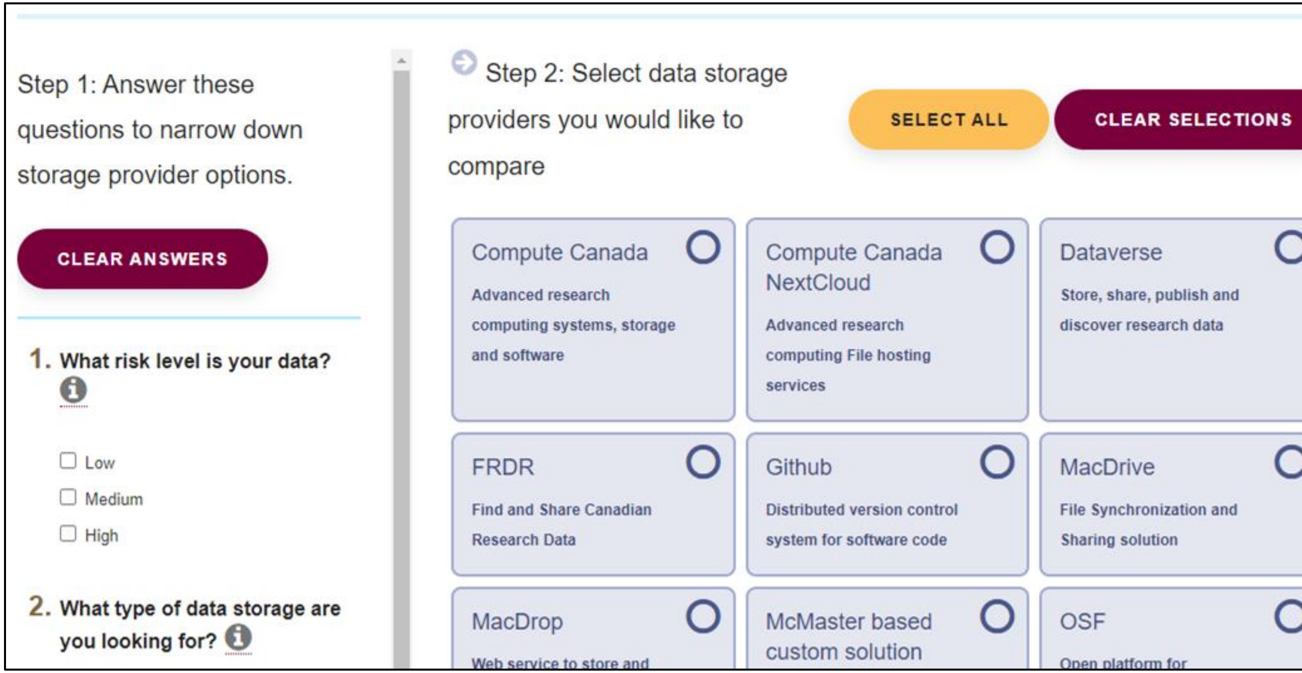
- Researchers should consider how they will preserve data over the long term. Many research funders require data to be retained for a set period.
- Storing data on campus servers (department/faculty/RHPCS) is preferable to storing data on an external drive
- Keeping data on your laptop isn't a good preservation plan
- Publishing/depositing data to an online data repository is a good option for researchers who are comfortable making data open

Research Data Storage Finder Tool

http://u.mcmaster.ca/storagefinder

McMaster RDM Services has a **Data Storage Finder**, an interactive tool to help you find a vetted storage provider depending on risk, volume, and other needs.

This tool also allows you to compare feature sets of selected options.



Step 1: Answer these questions to narrow down storage provider options.

1. What risk level is your data? ℹ

☐ Low
☐ Medium
☐ High

2. What type of data storage are you looking for? ℹ

Step 2: Select data storage providers you would like to compare

Compute Canada ○
Advanced research computing systems, storage and software

Compute Canada NextCloud ○
Advanced research computing File hosting services

Dataverse ○
Store, share, publish and discover research data

FRDR ○
Find and Share Canadian Research Data

Github ○
Distributed version control system for software code

MacDrive ○
File Synchronization and Sharing solution

MacDrop ○
Web service to store and

McMaster based custom solution ○

OSF ○
Open platform for

Encryption

Encrypt **individual files**

- Microsoft Office or other applications can be used to password protect and encrypt documents on a file by file basis.

Encrypt your whole drive

- **Full disk encryption** is available on Windows, Mac, iOS, and Android. This protects every file on your device so you don't need to worry about missing a file. You can also encrypt entire external drives.

Create "**virtual encrypted disks**"

- Disk Utility on Mac or VeraCrypt (3rd party software) can create encrypted virtual disks, where you can store sensitive data files

How should I protect my data?

Enable Multi-Factor Authentication (MFA)

- Also known as 2 Factor Authentication (2FA)
- Requires more than one code or ‘Factor’ to login – typically 2 factors: password and a security code sent to your phone number or generated by a linked authenticator app
- Many other web services (Gmail, Dropbox, etc) provide MFA

Password Best Practices

Make sure your online information is secure by ensuring your password is:

✓ **Strong**: Make a strong password by combining a series of numbers, letters, and symbols into a long series of words. Try to combine them into something memorable – like L1br@ryt1pS.

✓ **Unique**: Use a different password for each important website/service

✓ **Secret**: Never share your passwords with anybody via email or text.

✓ **Up to date**: Change your passwords in response to platform breaches

✓ **Devices**: Use a strong password on your computer and phone, too

Tip: Remembering multiple passwords can be difficult. Use a trusted password manager to keep track of your passwords for you. Some examples are BitWarden and 1Password.

Publishing Data

What do you plan to do with your data once it’s been published? How will you ensure that your data remains accessible (to you and others) long-term?

Consider whether you can publish your data in an online repository for preservation and sharing.

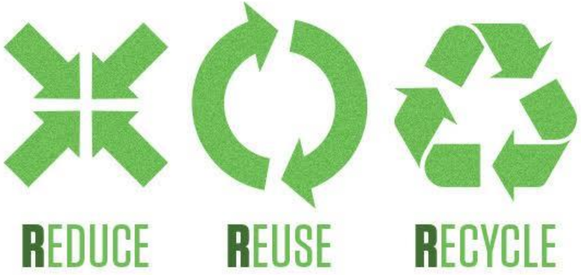
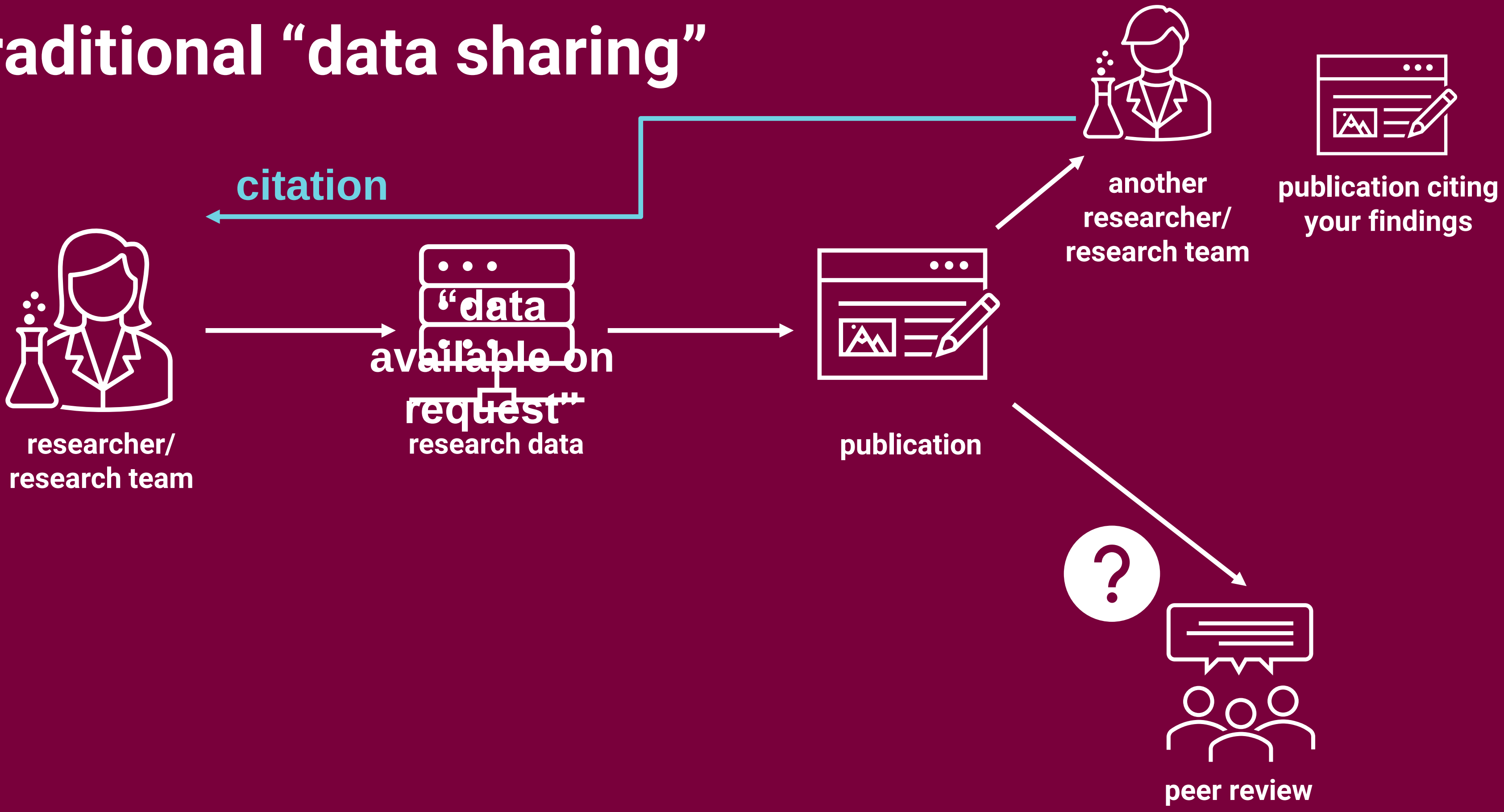


Photo by Lars Kienle on Unsplash.

Data Sharing

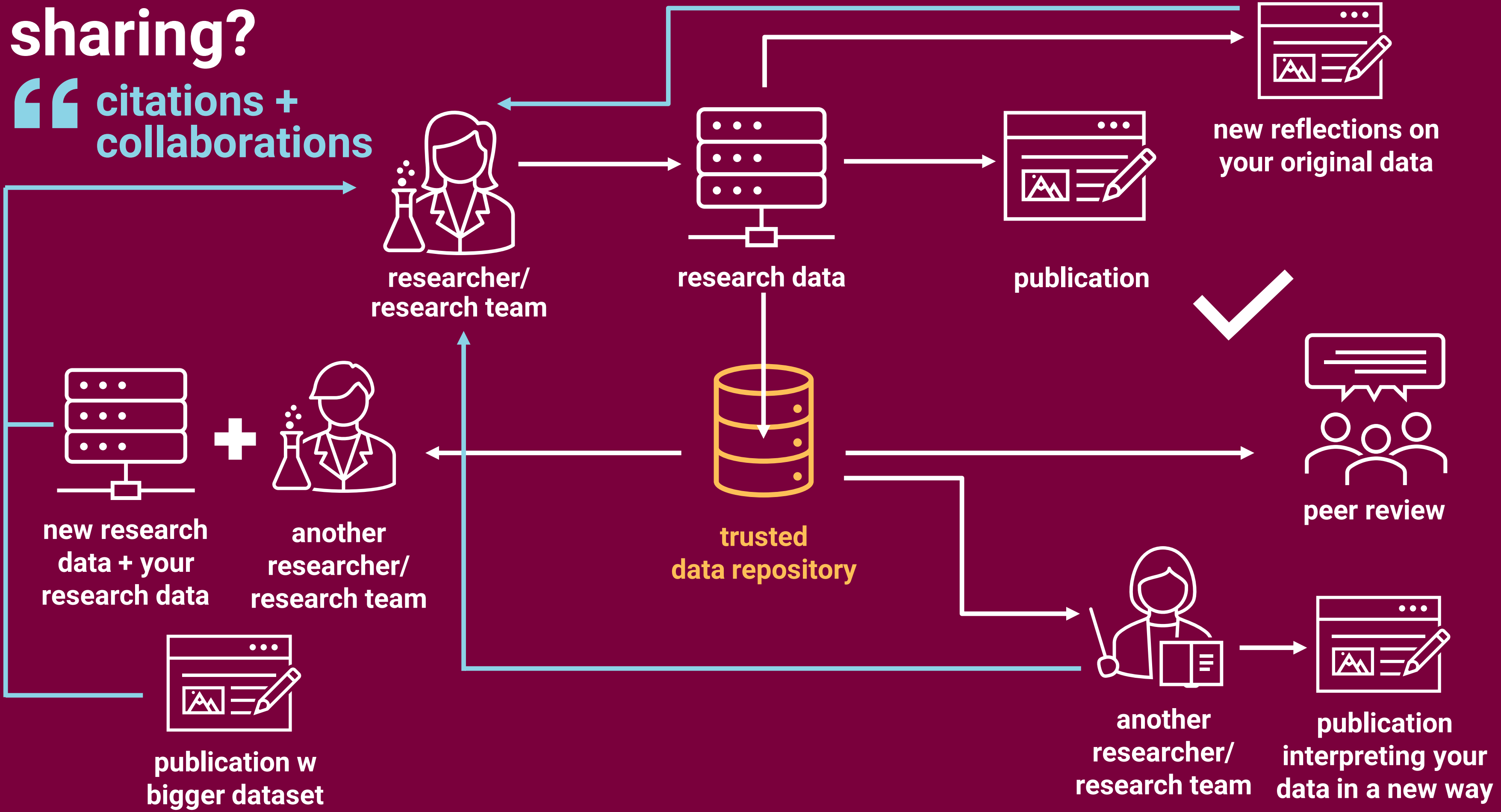
- Culture of reproducible research **increases confidence in research results** and avoids article retractions.
- Leads to new **collaborations** – potential for **meta-analyses** over a wider topic area.
- Better **informed policymakers** in healthcare and science as well as hospital stakeholders, professional associations, patient advocates.
- Long term **preservation** and **archiving** of data by established repositories.

Traditional “data sharing”



The future of data sharing?

“ citations + collaborations



researcher/ research team
research data
publication
new reflections on your original data
peer review
trusted data repository
new research data + your research data
another researcher/ research team
publication w bigger dataset
another researcher/ research team
publication interpreting your data in a new way

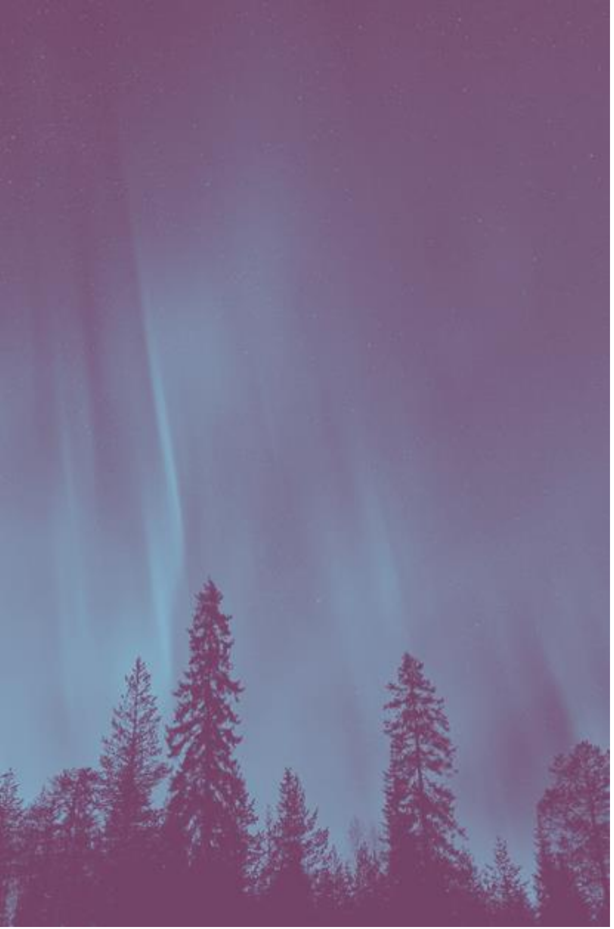
Sharing sensitive data

If you want to publish or share sensitive data, there a few main options:

- **Anonymize the dataset:** remove, replace, or redact all sensitive information from datasets prior to upload in an open repository.
- Data can be shared through closed access portals with restricted access mechanisms and **Data Sharing/Transfer Agreements**
  - Examples of this kind of web portal include ICES and CIHI

Remember you must have patient/participant consent to share data

- Portage's Research Data Management Language for Informed Consent

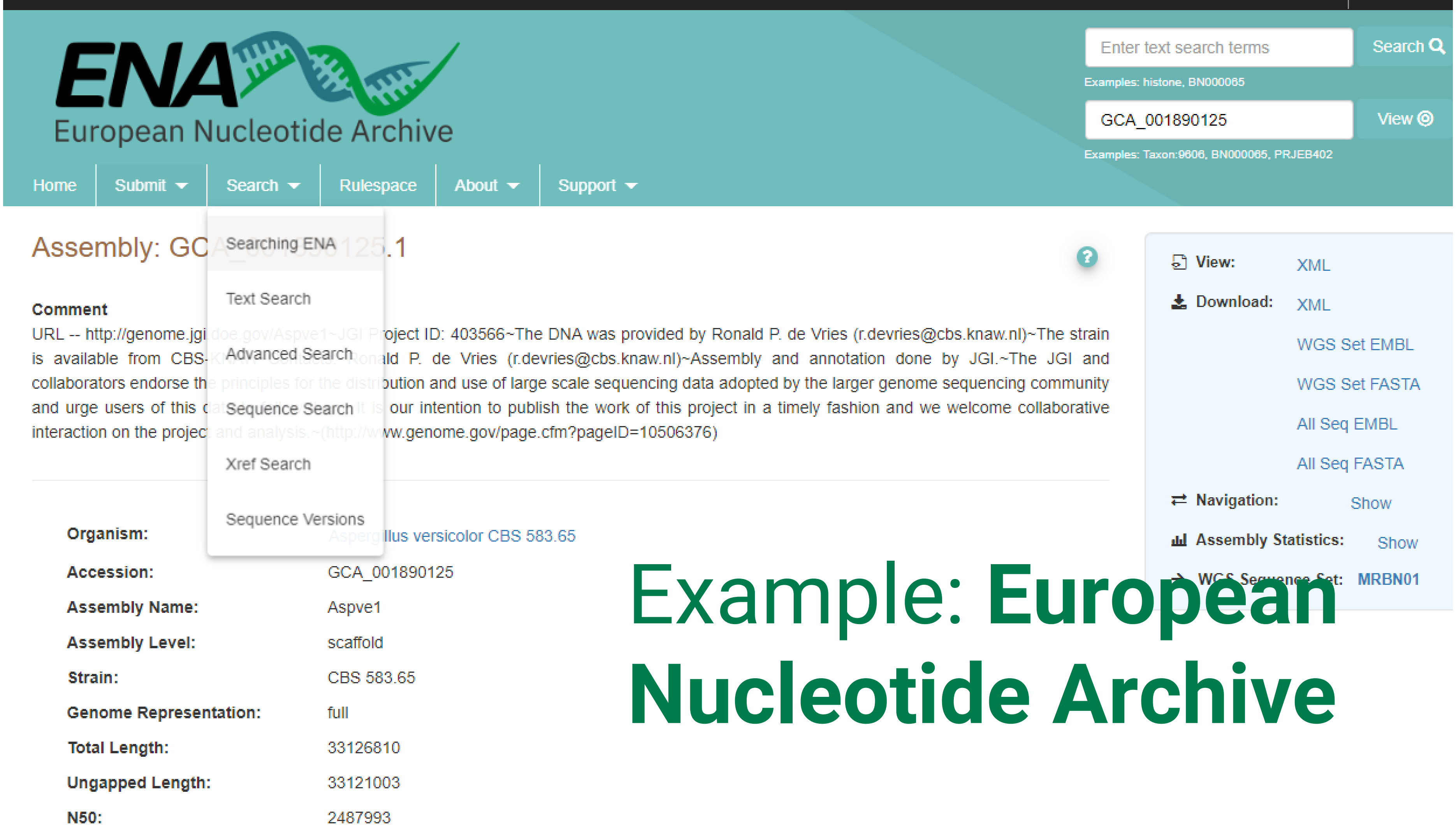


? *Ok, so where do I put everything?*

A **data repository** is a web platform and storage space for researchers to deposit data sets associated with their research.

Repositories provide:

- long-term storage and access to research data beyond the life of a grant, research project, or individual careers.
- Discoverability and findability for datasets through features like indexing and DOIs.
- Easy-to-use shared platforms made for research.



Assembly: GCA_001890125.1

Comment

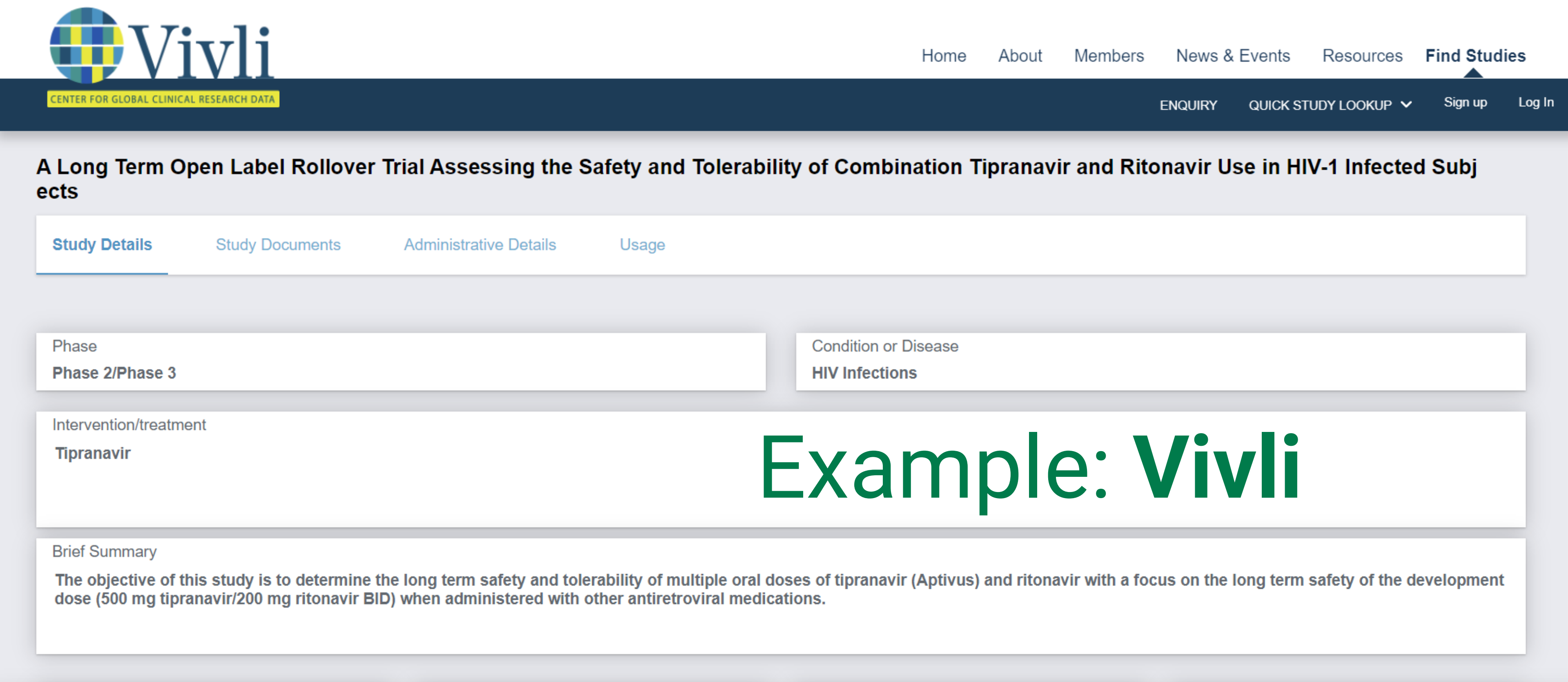
URL -- http://genome.jgi.doe.gov/Aspve1~JGI Project ID: 403566~The DNA was provided by Ronald P. de Vries (r.devries@cbs.knaw.nl)~The strain is available from CBS-KNAW. Contact Ronald P. de Vries (r.devries@cbs.knaw.nl)~Assembly and annotation done by JGI.~The JGI and collaborators endorse the principles for the distribution and use of large scale sequencing data adopted by the larger genome sequencing community and urge users of this data to follow them. It is our intention to publish the work of this project in a timely fashion and we welcome collaborative interaction on the project and analysis.~(http://www.genome.gov/page.cfm?pageID=10506376)

Organism:	Aspergillus versicolor CBS 583.65
Accession:	GCA_001890125
Assembly Name:	Aspve1
Assembly Level:	scaffold
Strain:	CBS 583.65
Genome Representation:	full
Total Length:	33126810
Ungapped Length:	33121003
N50:	2487993

View:	XML
Download:	XML WGS Set EMBL WGS Set FASTA All Seq EMBL All Seq FASTA
Navigation:	Show
Assembly Statistics:	Show
WGS Sequence Set:	MRBN01

Example: **European Nucleotide Archive**

Example: **Vivli**



A Long Term Open Label Rollover Trial Assessing the Safety and Tolerability of Combination Tipranavir and Ritonavir Use in HIV-1 Infected Subj ects

Phase
Phase 2/Phase 3

Condition or Disease
HIV Infections

Intervention/treatment
Tipranavir

Brief Summary
The objective of this study is to determine the long term safety and tolerability of multiple oral doses of tipranavir (Aptivus) and ritonavir with a focus on the long term safety of the development dose (500 mg tipranavir/200 mg ritonavir BID) when administered with other antiretroviral medications.

FRDR Zero knowledge encryption for sensitive data

- FRDR is working on a pilot project to add optional zero-knowledge encryption to the repository.
- “**Zero-knowledge encryption**” means that FRDR will never be able to access your data. All datasets are encrypted, and their keys stored in a separate researcher-managed platform. This allows you to deposit your data in a trusted repository for archival but maintain complete control over access to the data.
- Interested in piloting this service? Email us: rdm@mcmaster.ca

FRDR
FEDERATED RESEARCH DATA REPOSITORY

Lewis & Ruth
Sherman Centre
for Digital Scholarship
scds.ca

McMaster University | Library

Research Data Management Services

McMaster RDM webpage:	rdm.mcmaster.ca
Contact RDM services at:	rdm@mcmaster.ca
Upcoming RDM webinars:	rdm.mcmaster.ca/events
Recorded RDM webinars:	u.mcmaster.ca/learn-rdm

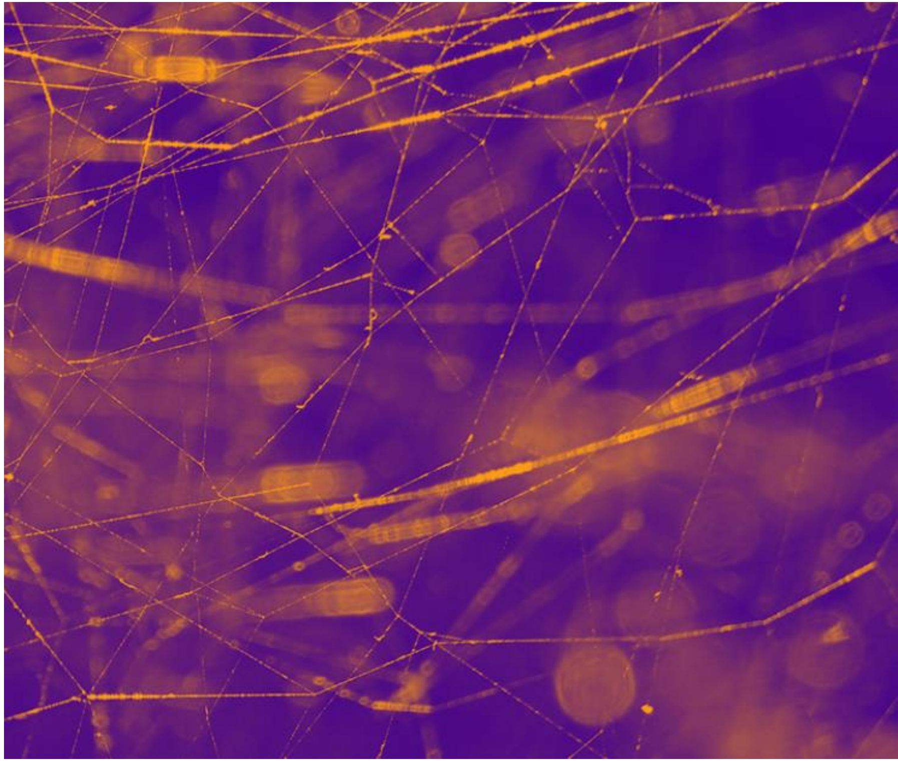
Make an appointment with a Research Data Management Specialist:
u.mcmaster.ca/rdm-appointments

Lewis & Ruth
Sherman Centre
for Digital Scholarship
scds.ca

McMaster University | Library

RDM Community of Practice

- Monthly meetings of people interested in RDM at McMaster
- February - Allison Van from Spark on RDM in Social Sciences.
  - **Thursday Feb. 23 – 11 AM**
- March – Dr. Claudia Emerson on medical ethics.
  - **Thursday March 30th – 11 AM**
- Connect with other researchers practicing RDM across the university!
- https://u.mcmaster.ca/rdm-community



RDM

February 15 | 10:30-11:30am

Hybrid Workshop

Persistent Identifiers For All

u.mcmaster.ca/scds-events

SCDS

Library | McMaster University

RDM

March 15 | 10:30-11:30am

Virtual Workshop

Before You Dig: Finding and Reusing Datasets

u.mcmaster.ca/scds-events

SCDS

Library | McMaster University

RDM

April 5 | 10:30-11:30am

Hybrid Workshop

Qualitative Data: Practices for RDM Planning & Sharing

u.mcmaster.ca/scds-events

SCDS

Library | McMaster University