med.data.edu.au

Navigating data-driven medical researchers through the IT privacy/security landscape

Jeff Christiansen, Jared Winton and Kathy Dallest

INTERSECT

VicNode

qcif

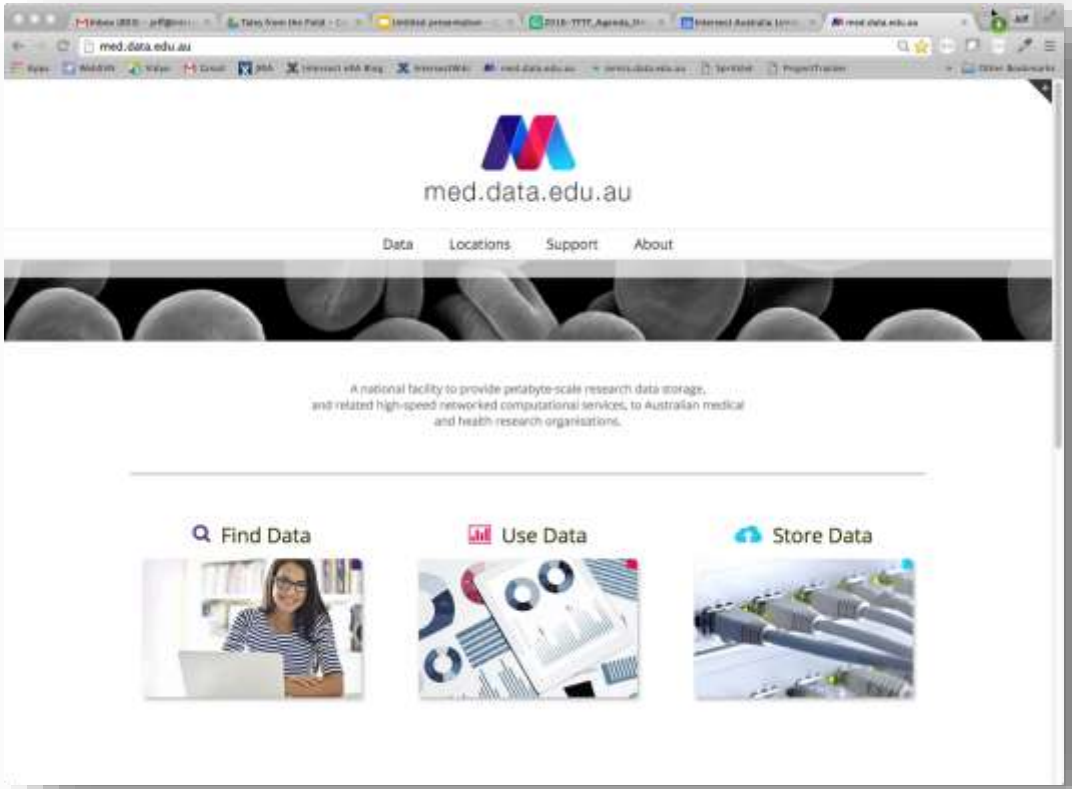
med.data.edu.au

NCRIS-funded project

RDSI Research Data Storage Infrastructure

RDS www.rds.edu.au

A national facility for petabyte scale research data storage and high-speed networked computational services to Australian Health and Medical Research organisations

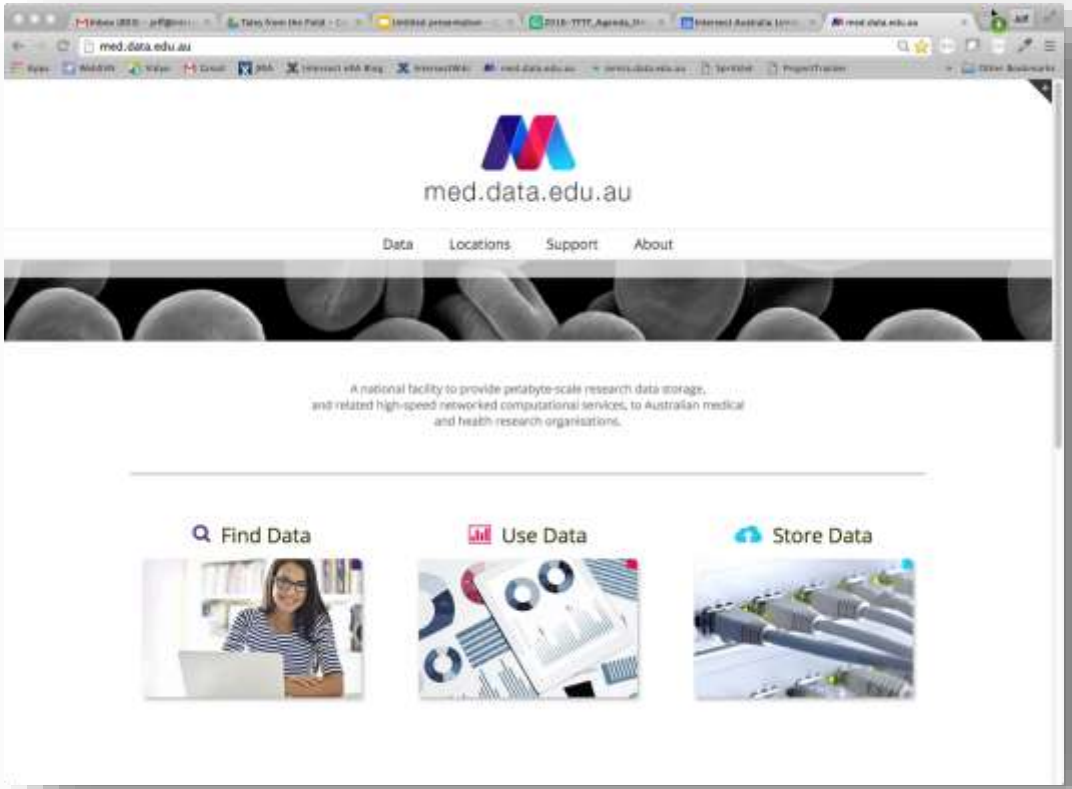


med.data.edu.au

4 RDS nodes:
Intersect, VicNode, eRSA, QCIF

Health/medical research data:
4 states
7 Universities
12 Medical Research Institutes

2.2PB (91 data collections)
Human genomic data ~85%
Human 3D imaging ~10%
Other health datasets <5%



med.data.edu.au

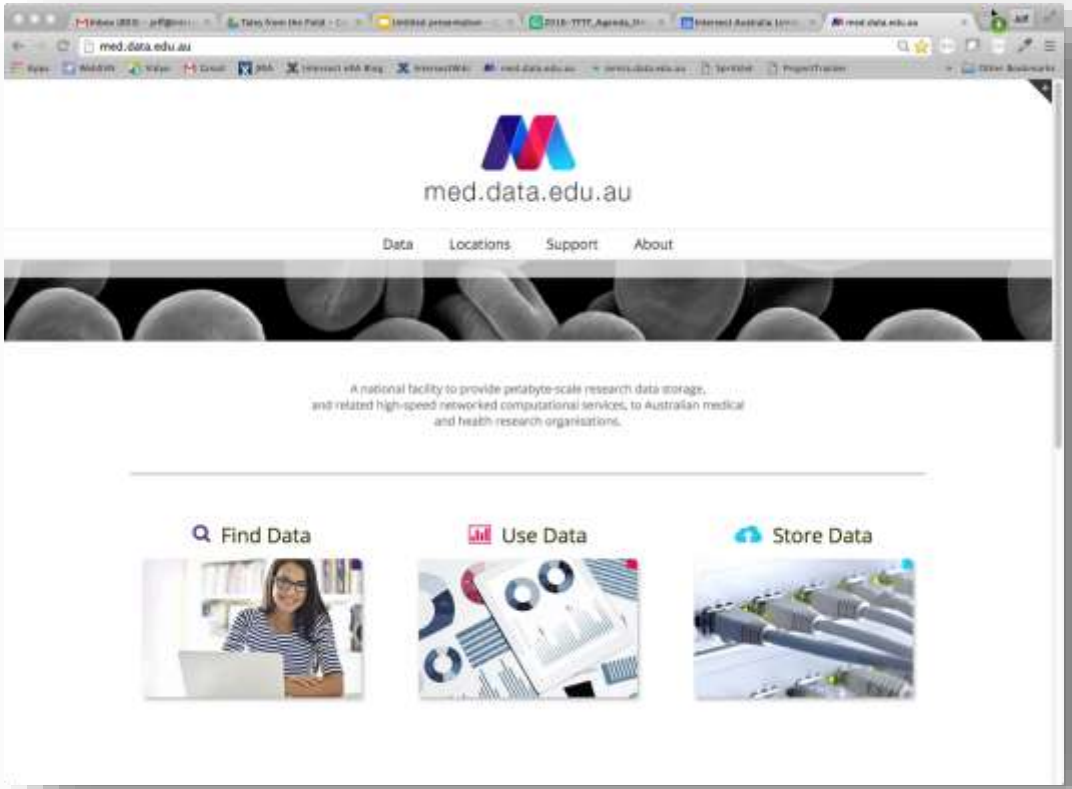
Advisory Board:

med.data.edu.au

FIND DATA

USE DATA

STORE DATA



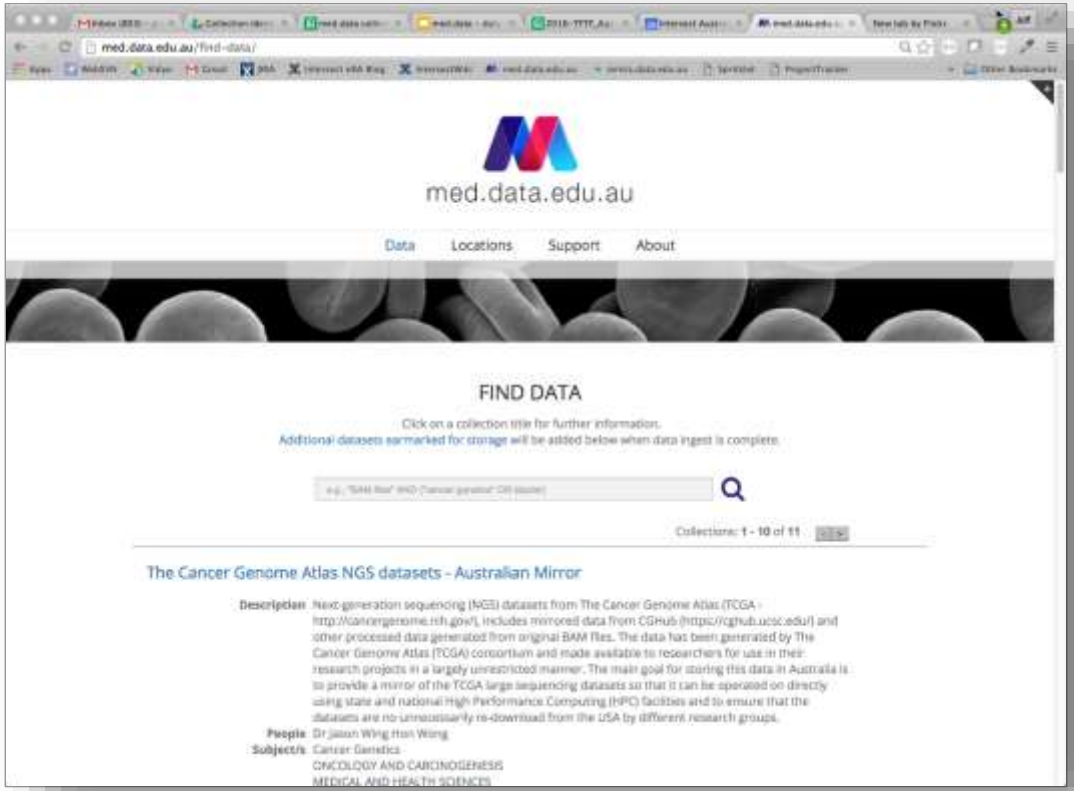
med.data.edu.au

FIND DATA

Dataset descriptions listed

Tools and processes to publish dataset descriptions

Leverages institutional and national infrastructure (ANDS)

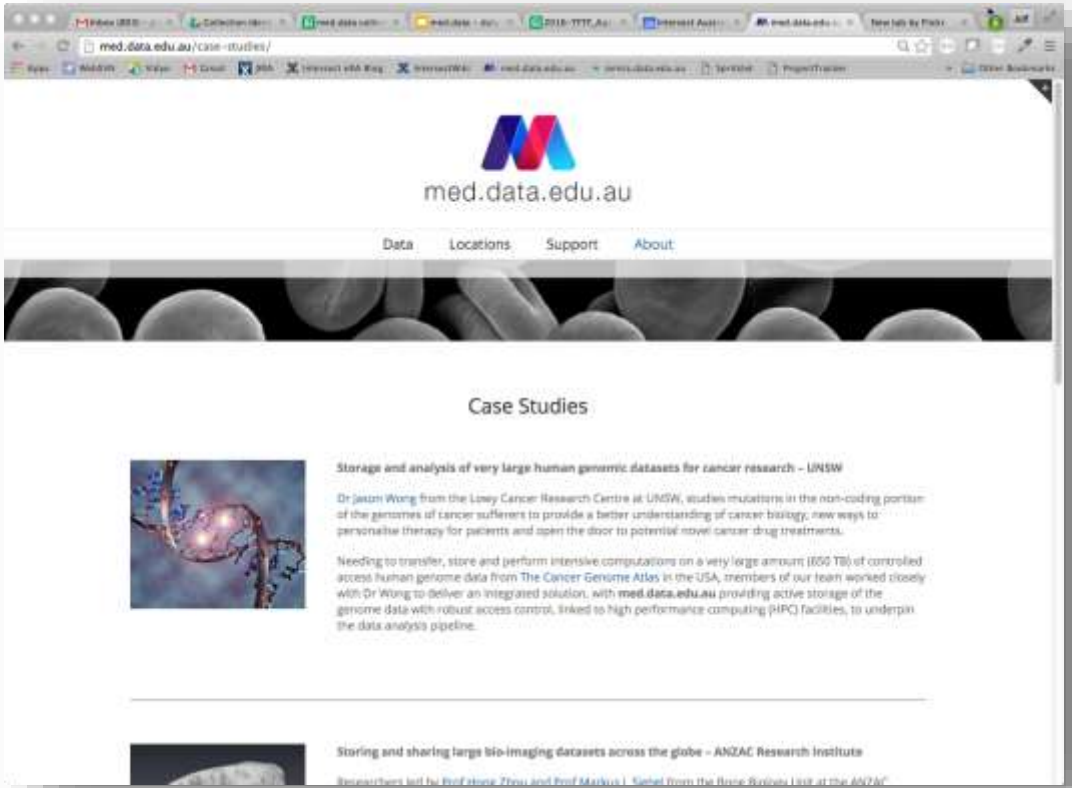


med.data.edu.au

USE DATA

Generally, users requiring large data storage and associated HPC or cloud (Nectar) compute, or
Collaborative research across Institutions

BYO software

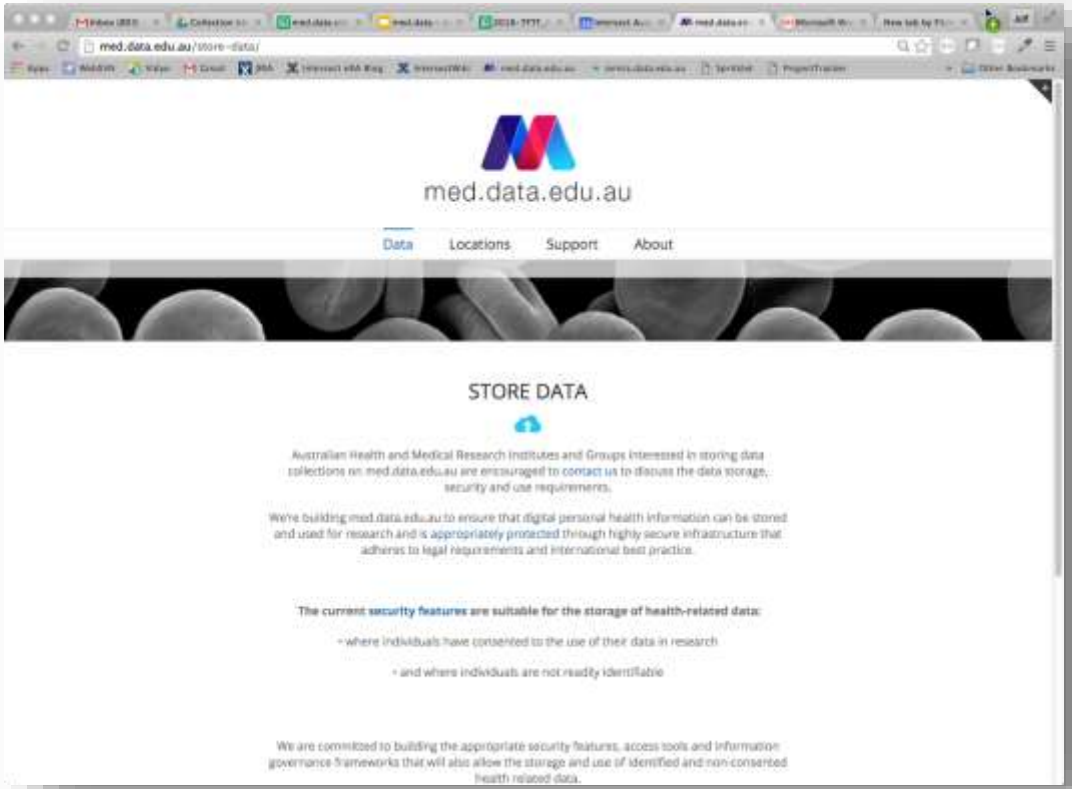


med.data.edu.au

STORE DATA

Data is managed using various platforms
(Mediaflux, Aspera, MyTardis)

Human-derived data is subject to a higher level of protection than other data



Health and Medical information

Collected for healthcare provision

Held by health service providers

Derived from or relating to human individuals

It is personal* info: i.e. about an identified or reasonably identifiable individual

It is sensitive* info: i.e. about an individual’s Health; or Genetic or Biometric info.

* As defined by The Privacy Act 1988 (Cth)

Health and Medical information

Collected for healthcare provision

Held by health service providers

Derived from or relating to human individuals

It is personal* info: i.e. about an identified or reasonably identifiable individual

It is sensitive* info: i.e. about an individual's Health; or Genetic or Biometric info.

Must be protected (Privacy Act (Cth) and various state health privacy legislation)

Health and Medical information in research

Collected for healthcare provision OR specifically collected for use in research studies

Held by researchers

Derived from or relating to human individuals (i.e. is personal and sensitive)

Health and Medical information in research

Collected for healthcare provision OR specifically collected for use in research studies

Held by researchers

Derived from or relating to human individuals (i.e. is personal and sensitive)

Must be protected from misuse, interference and loss,

and from unauthorised access, modification or disclosure.

Health and Medical information in research

POINTS FOR CONSIDERATION

Privacy Protection Legislation

Privacy Protection Legislation

Protecting an individual's privacy (and health privacy) is enshrined in Commonwealth and State Legislation:

Commonwealth
- Privacy Act (1988)

NSW
- Privacy and Personal information Protection Act 1998
- Health Records and Information Privacy Act 2002 (HRIPA)

VIC
- Information Privacy Act 2000 (Vic)
- Privacy and Data Protection Act 2014
- Health Records Act 2001 (Vic)
- Charter of Human Rights and Responsibilities Act 2006 (Vic)

QLD
- Information Privacy Act 2009 (Qld)
- Health Services Act 1991 (Qld)
- Information Standards 42 (general) & 42A (health)
- Public Health Act 2005 Chapter 6, Part 4, Division 2, s281

SA
- Department of the Premier and Cabinet IPPs

WA
- Information Privacy Bill 2007

TAS
- No health specific privacy legislation.
- Personal Information and Protection Act 2004

ACT
- Information Privacy Act 2014 (ACT) (ACT Public Sector Agencies)
- Health Records (Privacy and Access) Act 1997

NT
- No health specific privacy legislation.

Ethics

Ethics

When health data is collected for research purposes, Human Research Ethics Committee (HREC) approval is required first.

HREC approval is also required for its use (usually only approved for use in a specific research study).

Must not be shared in an identifiable form with those outside the HREC-approved research project(s).

Consent

Consent

The guiding principle for researchers is that a person’s decision to participate in research is to be voluntary, and based on sufficient information and adequate understanding of both the proposed research and the implications of participation in it.

“Informed consent”

As defined in the *National Statement on Ethical Conduct in Human Research* (NHMRC, ARC, Universities Australia)

Consent

When consent has not been given to use personal health data in research, the use of health data use may still be permitted for research purposes:

Cth Privacy Act Section 95 – allows Commonwealth managed health data to be used for research in an identifiable form if the proposed research has been approved by a HREC.

Cth Privacy Act Section 95A – allows private sector data to be used for research where gaining consent is not practical, and the research has been approved by a HREC.

Note – neither are applicable for data from State Health Departments - however some states e.g. NSW have comparable legislation (e.g. NSW – HRIPA)

Identifiability of data

Identifiability of data

Individually identifiable data – where the identity of a specific individual can *reasonably be ascertained* (e.g. a name, image, date of birth or address.

Re-identifiable data - where identifiers have been removed and replaced by a code, but it remains possible to re-identify a specific individual by, for example, using the code or linking different data sets.

Non-identifiable data - has never been labelled with individual identifiers or from which identifiers have been permanently removed, and by means of which no specific individual can be identified.

As defined in the *National Statement on Ethical Conduct in Human Research* (NHMRC, ARC, Universities Australia)

Identifiability of data

Making data non-identifiable, decreases risks associated with inadvertent release

Removal of overt identifying information or identifiers - e.g. name, image, date of birth, address, medicare/patient numbers.

Statistical methods - applied by an expert and the methods must be documented

As defined in the *Guidelines for the disclosure of Secondary Use Health Information for Statistical Reporting, Research and Analysis 2015* (National Health Information Standards and Statistics Committee)

Legislation affecting trans-border dataflow

Legislation affecting trans-border dataflow

Commonwealth – Privacy Act (1988) Australian Privacy Principle (APP)-8 cross-jurisdictional transfer of personal information out of Australia.

NSW – NSW Health Records and Information Privacy Act 2002 Health Privacy Principle (HPP)-14 Trans-border data flows and data flow to Commonwealth agencies.

VIC – Health Records Act 2001 (Vic) Health Privacy Principle (HPP)-9 Transborder Data Flows

WA – Information Privacy Bill 2007 (WA) Information Privacy Principle 8: Transborder data flows

TAS – Personal Information Protection Act 2004

NT – Information Act: Information Privacy Principle (IPP)-9 Transborder data flows

What controls are needed to protect HM data in research?

What controls are needed to protect HM data in research?

What controls are needed to protect HM data in research?

There IS no definitive checklist - It's about risk management

Discussion paper

Legislative framework (Commonwealth, State and International)

Best Practice (Ethics, Research etc)

IT Security requirements for Health (Human-derived) data

Roles and Responsibilities (Data Custodians, Users, Nodes)

Discussion paper

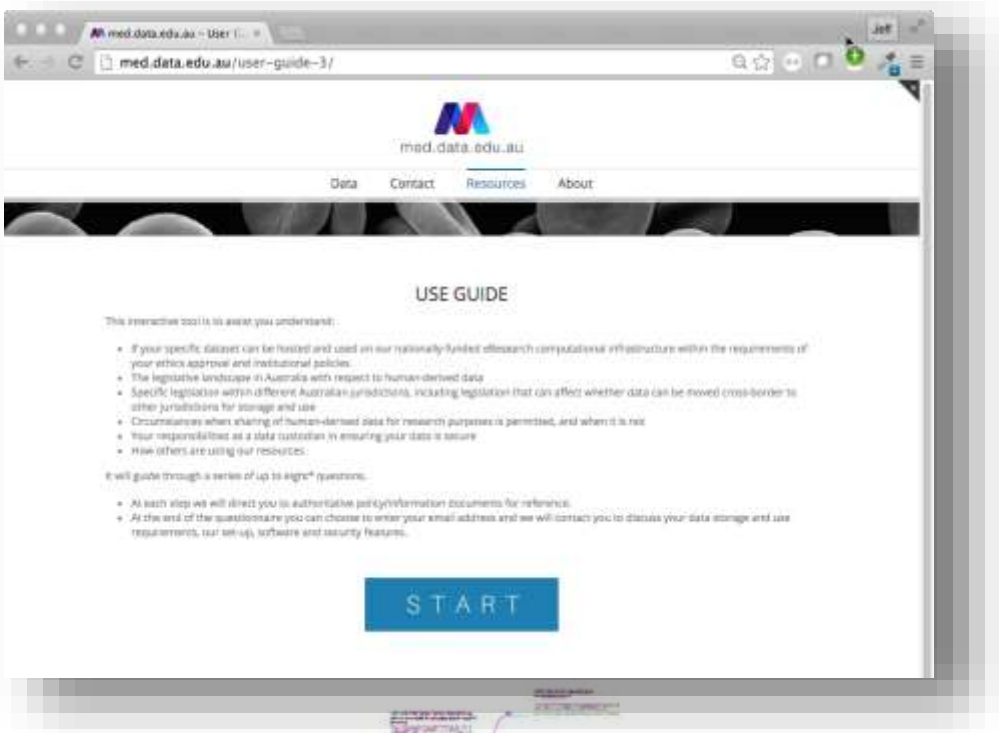
41 pages and heavy going

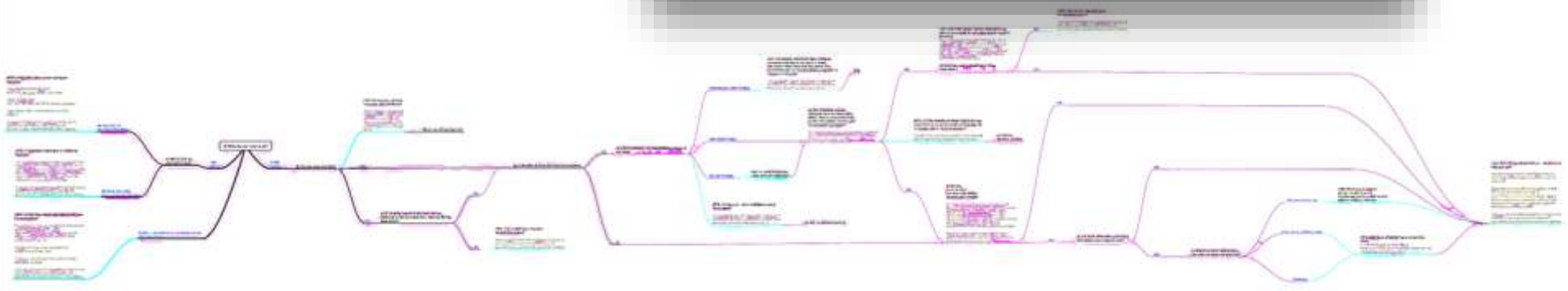
Need something simpler

Use Guide

On-line wizard

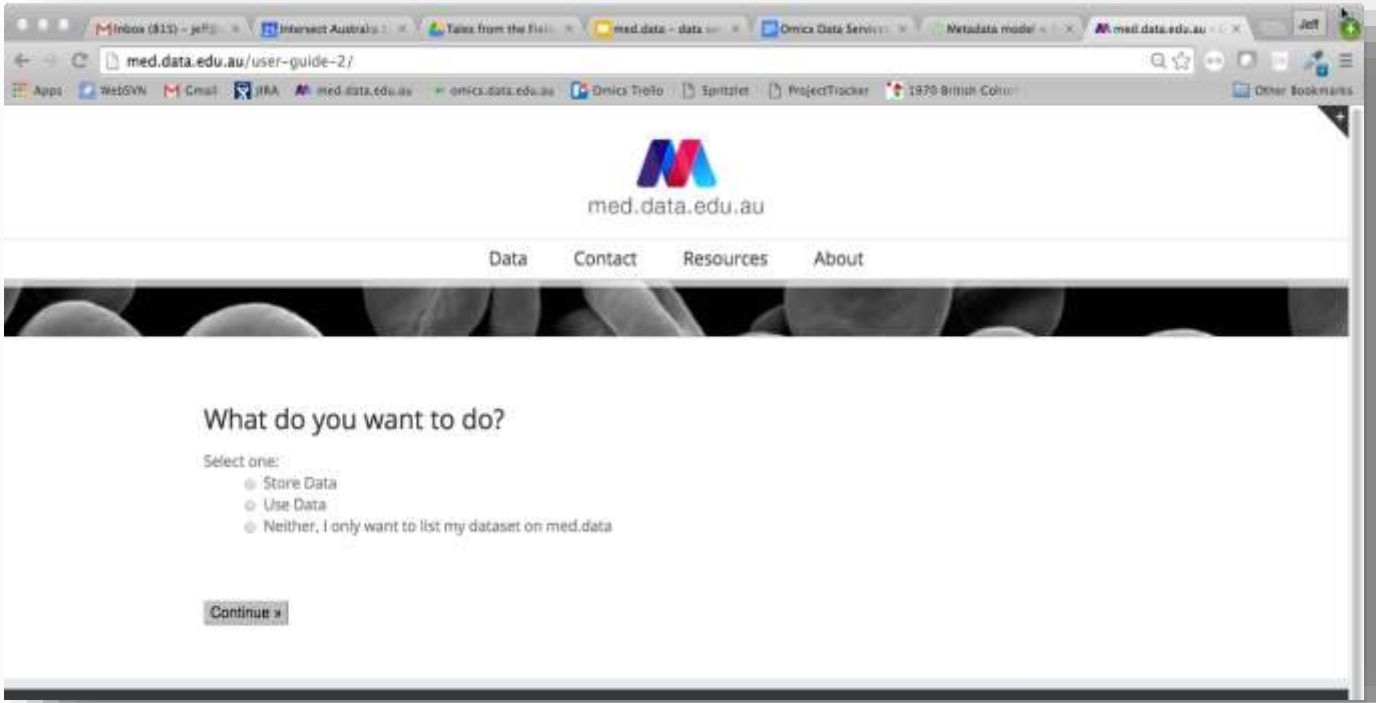
Navigates the user through relevant info





Use Guide

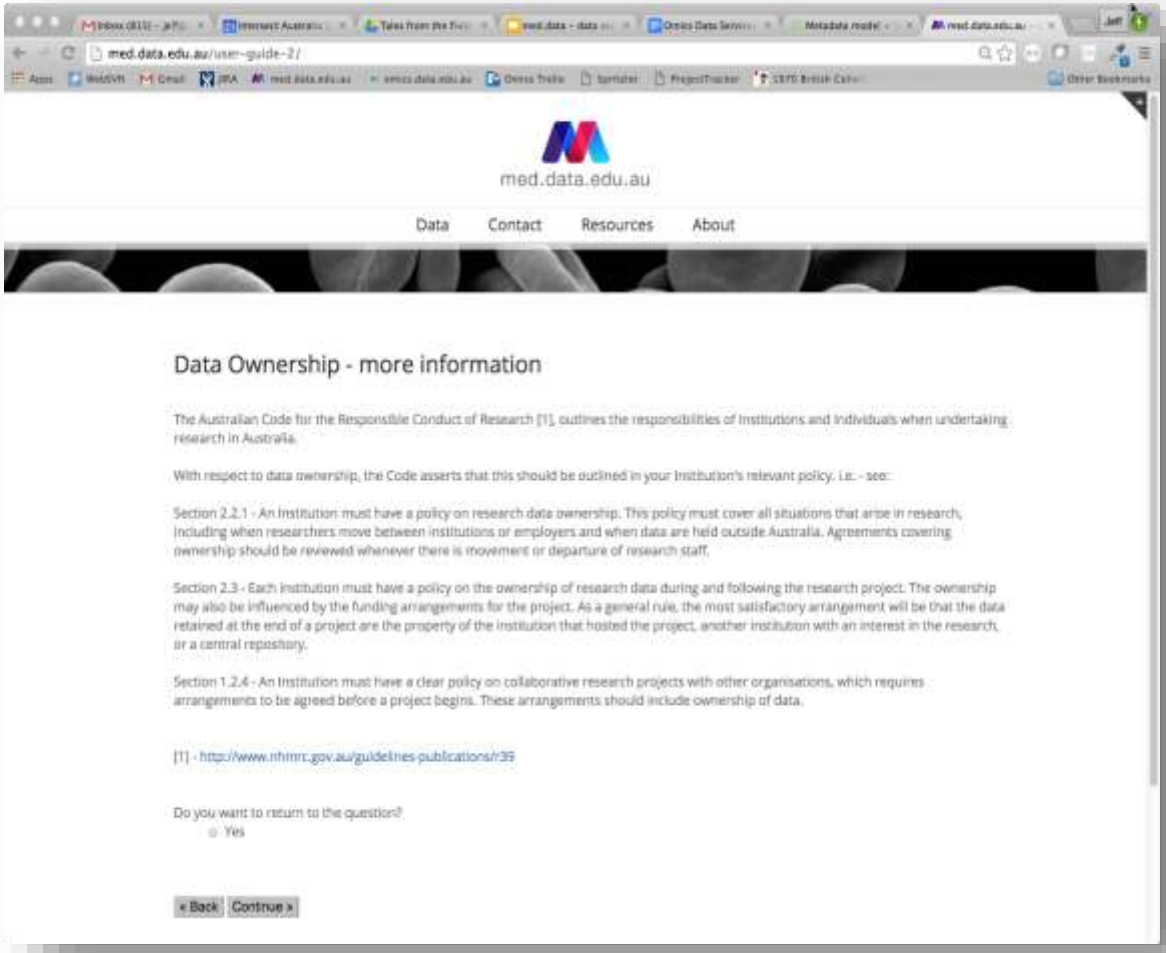
Simple questions



Use Guide

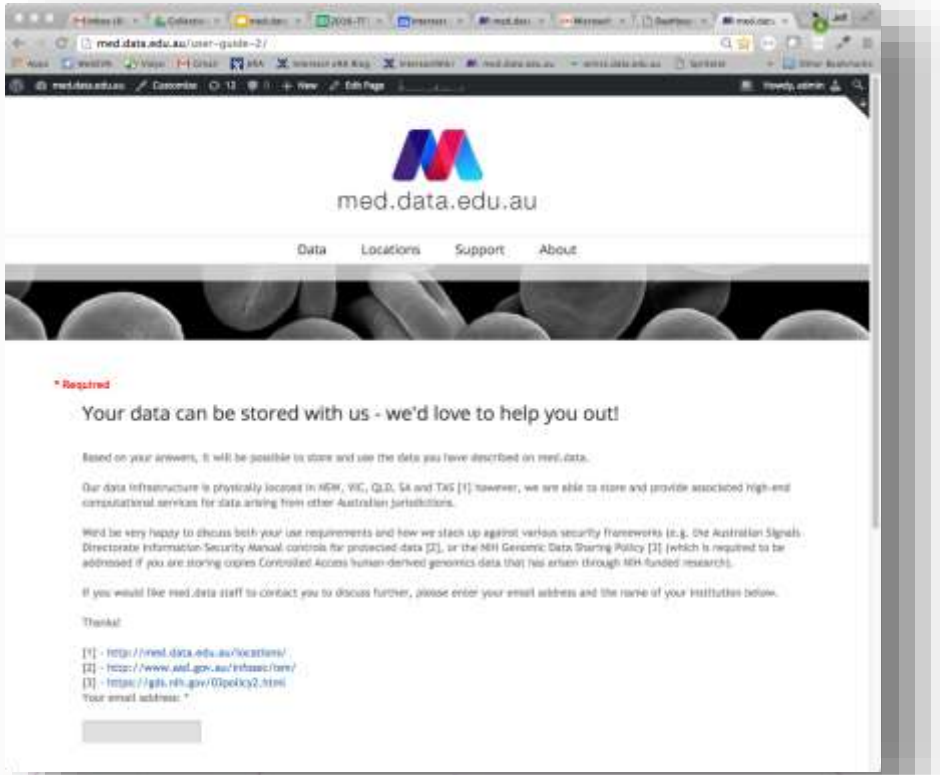
Info when requested

Authoritative references



Use Guide

Option to be contacted for Node Specific Information



Use Guide

Node Specific Security Info

How do each Node’s Storage, HPC and Cloud compute stack up against…

- National Standards for Protected or Sensitive Info (ASD ISM)?

What controls are needed to protect HM data in research?

User identity

User authentication

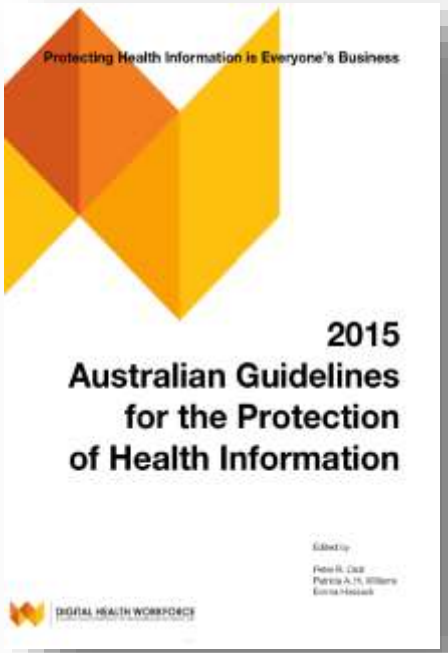
Access control

Encryption

Secure audit

General security

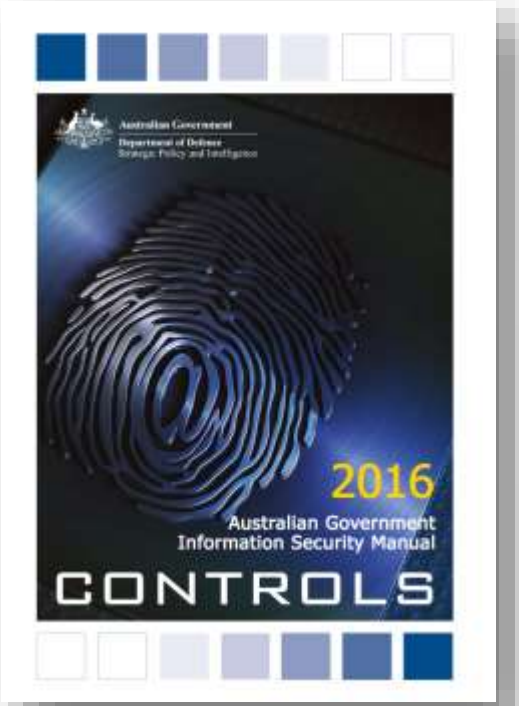
Anonymisation



Controls for "Protected" and "Sensitive" Data

IT Security set-up

Security Policy



Use Guide

Node Specific Security Info

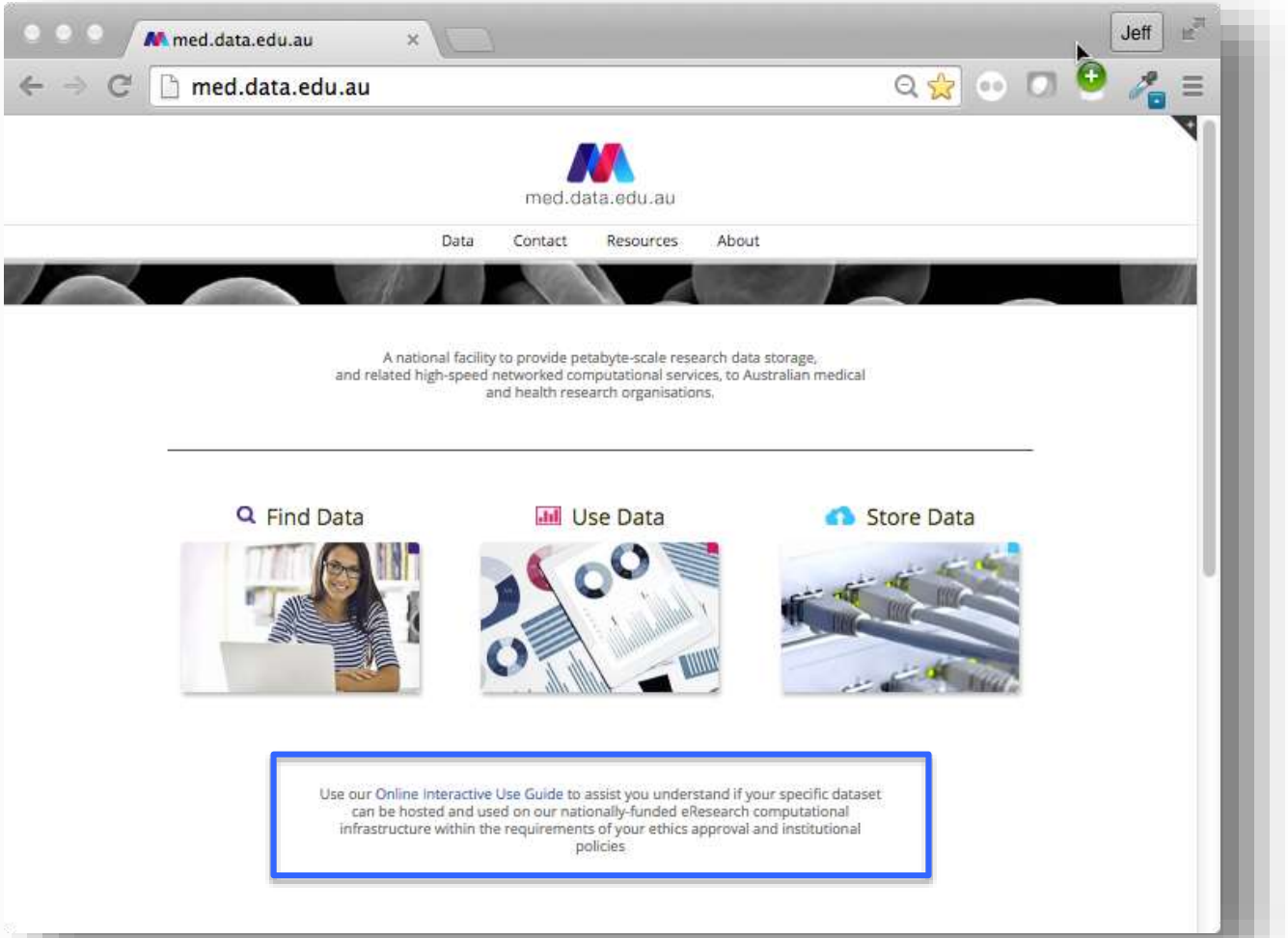
How do each Node’s Storage, HPC and Cloud compute stack up against…

- National Standards for Protected or Sensitive Info (ASD ISM)?
- Common other standards (e.g. NIH Best Practices for storage of Human Genomic Sequence)?

Required for an informed conversation about risk with each Data Custodian (Node set-up, Roles and Responsibilities of Data Custodians, Data Users and Node Operators).

Use Guide

Available Now



THANK YOU

jeff@intersect.org.au

Acknowledgements