

The James Hogg Research Centre (JHRC) BioBank: A review and update of Privacy Initiatives

Dr. M. Allard
JHRC BioBank Director and Privacy Officer
June 21, 2010



Overview

- History of the BioBank
- Privacy Initiatives
- Accessing BioBank Tissues
- BioBank and Research Database Review
- Privacy and the PROOF Centre



The BioBank History

- Dr Hogg established the Pulmonary Registry at St. Paul's Hospital ~30 yrs ago
- Dr. McManus established a Cardiovascular Registry at the University of Nebraska Medical Center in 1982 and relocated it to UBC in 1993.






What are these cardiovascular and pulmonary tissues used for?

- Research and education
 - Stereology
 - Evaluation of tissue constituents (protein, RNA, DNA)
 - Participation in worldwide studies and novel therapy development
 - Anonymized" vs. "de-identified" specimens



Privacy at the James Hogg Research Centre

- **Privacy Task Force** established in Jan 2005
- **Privacy Impact Assessment (PIA)** for the Heart, Lung and Blood Vessel Disease Tissue Registry
- **Privacy Policy Manual**
 - Procedures are compliant with Privacy Legislation
 - A “living document”
 - Reviewed annually

BioBank and Privacy Team

Team Leaders

- Mike Allard: Director (On Leave)
- Peter Paré, Jim Hogg and Bruce McManus, Principal Investigators

BioBank and Histology Staff

- Mark Elliott, Lise Matzke, Crystal Leung and Amrit Samra

Information Technology




- Joe Comeau

Staff and Trainees

- Anna Meredith, Beth Whalen, Simone Thair

Additional Members

- Jacqui Brinkman, Privacy Facilitator
- Debbie Langstaff, Data Ambassador, PROOF Centre
- Janet Scott, Leader, Information Access & Privacy, PHC
- Michelle Storms, REB Manager, Corresponding Member

Privacy on the intranet: <http://home.hli.ubc.ca/>



Jacqui Brinkman is our Privacy Facilitator.

Centre Privacy and Confidentiality

Protecting Patient Privacy is very important at the UBC James Hogg Research Centre. As a public body and a steward of personal information, the JHRC is responsible for the protection of all personal information under its custody and control and is accountable for protecting the privacy and security of all personal information in accordance with existing legislation, public expectations and internationally accepted fair information practices.

The responsible use of JHRC Computer Systems will aid in protecting our data.

To read all of our policies, please refer to the Privacy Policy Manual.

You are responsible to read and understand the following policies at the start of your term with the UBC James Hogg Research Centre:

- Privacy Policy 7.5: Password Policy
- Privacy Policy 7.6: Acceptable Use of Computer Accounts
- Privacy Policy 8.7: Managing Privacy Breaches
- Acceptable Use of Computer Systems Manual
- Privacy Policy 10.1: Privacy Policy

You must then sign the accompanying agreements, BEFORE being able to access your computer account, and return them to the HR Manager:

- Agreement to abide by the JHRC policy concerning acceptable use of IT resources
- Confidentiality Agreement

Other Forms and Policies:

- Data Access Form
- Biobank Standard Operating Procedures (SOPs)

Memos:

- March 2006: Storage of Personally Identifiable Patient Research Subject Information
- May 2006: Signing of the Confidentiality Agreement
- November 2006: Fax and Email Confidentiality (new fax cover sheet)

If you have any questions or concerns regarding the privacy of patient research subject information, please contact:

Jacqui Brinkman, Privacy Facilitator
 Lise Matzke / Crystal Leung or Dr. Mark Elliott, Biobank Managers
 Dr. Michael Allard, Biobank Director
 Joe Comeau, Manager, IT Services

Privacy Policy 8.7

Managing Privacy Breaches

- Minimize the potential risk to the James Hogg Research Centre and its research subjects/partners, patients/residents/clients and staff;
- Enable a prompt, effective and orderly response to privacy incidents;
- Comply with the requirements of the FOIPPA*; and
- Prevent recurrence.

*FOIPPA = Freedom of Information & Protection of Privacy Act



Privacy Policy 8.7: Managing Privacy Breaches

Procedure:

1. Contain the Breach
2. Evaluate the Risks Associated with the Breach
3. Notification, Reporting the Privacy Breach
4. Prevention



Responsibilities

(excerpt from Privacy Policy 10.1)

Senior Leadership:

- Communicate the privacy policy (10.1) and ensure all individuals covered by this policy are clear on their role and how it relates to privacy and security of personal info.

Supervisor/Manager Responsibilities:

- Ensure all new and existing staff receive appropriate orientation/training on how to treat and protect personal info
- Ensure processes are in place to protect personal info
- Ensure non employees working within the Centre (trainees, physicians, researchers) read and understand the policy and sign the *Confidentiality Agreement*.



Responsibilities

(excerpt from Privacy Policy 10.1)

Human Resources:

- Ensure all new staff receive privacy documents as part of their orientation manual, sign the *Confidentiality Agreement* and place such document in the personnel file.

Trainee, Employee, Investigator:

- Sign the *Confidentiality Agreement* signifying they have read and understood the policy.
- Follow the policy and become aware of how to appropriately collect, use, disclose and protect personal information.



BioBank Processes: Frequently Asked Questions

- How do I access tissues in the BioBank?
- Who can access BioBank tissues?
- Do I need ethics approval?
- How can I access clinical data?
- Are there charges associated with accessing tissues?
- Can I do a pilot study without REB approval?
- To whom do I speak?
- Do I need to report my findings back?



BioBank Processes

- Access to, and use of, BioBank Tissues
 - Must present proposal to Scientific Advisory Committee
 - Must obtain ethics approval
 - Some 'test' tissues for pilot projects, protocol dev't (results cannot be used in publication without ethics approval)
 - Method development DOES NOT EQUAL control blood for your study (you cannot use this consent form to enroll actual control patients for your study, you must have ethics approval)



BioBank Processes: Important Notes

BioBank Fees

http://home.hli.ubc.ca/tech/registry/biobank_prices.html

- BEFORE submitting your next grant budget, please consult BioBank staff to include necessary items

BioBank/Histology Contacts:

- Lise Matzke/Crystal Leung, Cardiovascular
- Mark Elliott, Pulmonary
- Amrit Samra /Crystal Leung, Histology







BioBank Processes: Frequently Asked Questions

- How do I access tissues in the BioBank?
- Who can access BioBank tissues?
- Do I need ethics approval?
- How can I access clinical data?
- Are there charges associated with accessing tissues?
- Can I do a pilot study without REB approval?
- To whom do I speak?
- Do I need to report my findings back?



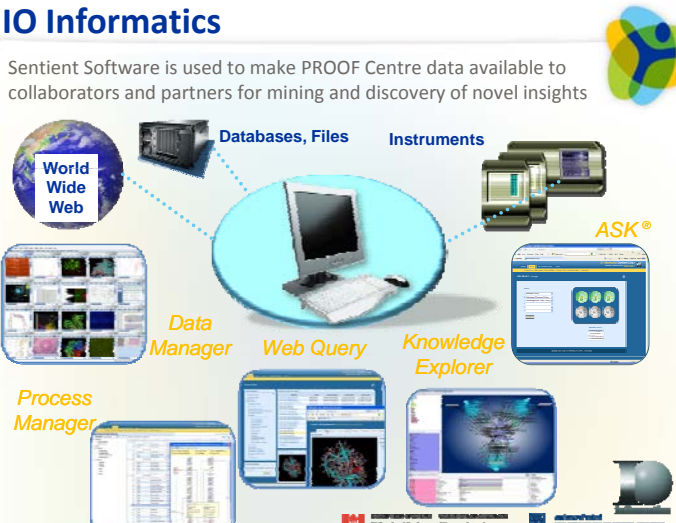
The JHRC BioBank Database

- A new BioBank Database is in the works!
- Anyone working with personal identifying information, especially patient information, must save data on the P: drive (encrypted volume)
(NOT the O: drive and NOT on personal laptops)
- Access should be limited to only those who “need to know” the personal information to do their jobs.
- Who has access to P? Anyone, with Manager/PI approval.

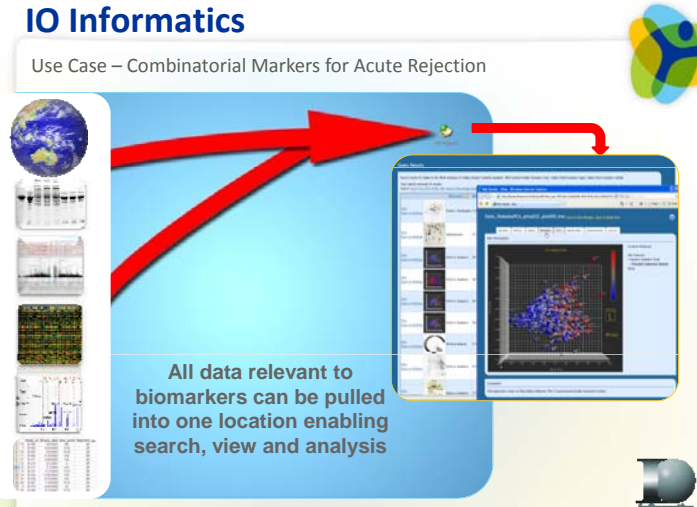
IO Informatics

Sentient Software is used to make PROOF Centre data available to collaborators and partners for mining and discovery of novel insights

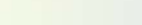





IO Informatics

Use Case – Combinatorial Markers for Acute Rejection







All data relevant to biomarkers can be pulled into one location enabling search, view and analysis

Tips for Protecting Privacy

(excerpts from SPH Medical Staff Orientation)

- Don't store personal info on the hard drives of desktop computers, laptops or other electronic devices (e.g., Blackberrys, USB, CDs) unless **absolutely** necessary. If necessary, ensure personal info is encrypted & password protected.
- Store personal info on a network server so if there is a theft, or the device is damaged; the personal info is not accessible or compromised.
- Use “good” passwords - 8 characters long and a combination of upper and lowercase letters, numbers and characters.
- Never share your username and password

Password Protection

- Do not write your passwords down!
- Do not keep them in your wallet or purse!
- Do not use the same password to access different systems or accounts.
- If you have a hard time remembering your accounts and passwords – Use a password safe.
- Store your accounts and passwords along with important info such as: when the account was created, what e-mail address it was associated with.
- Use a difficult password to gain access to your password safe !
- Make sure you have a backup of your password safe !!



Tips for Protecting Privacy

- Taking personal info off-site is discouraged, but in the rare case when it may be required, minimize the amount. Talk to IT about using a VPN.
- If personal info must be taken home, it must be stored in a locked drawer or cabinet when not being used.
- Personal info stored on computers should be encrypted & password protected.
- Personal computers should have effective Internet security measures such as anti-virus software and firewalls.
- Don't leave personal info unattended; ensure it is stored in a secure (locked) location.



Faxing

- If you have to fax documents containing personal info, verify fax number using a second source, double check the number entered and follow other faxing guidelines.
- Receipt of Faxes with Patient Information
 - When possible, faxes should be sent to clinical offices
 - If received, put inside a clearly labeled envelop and place in a secure location (not in a hallway mail slot).
 - Misdirected faxes are privacy 'breaches' and should be treated and reported as per Privacy Breach Policy.



E-mail

- Files with personal information should NOT be e-mailed
 - Alternatives include:
 - Faxing (use safe faxing procedures)
 - Using a secure FTP site (ask HelpDesk)
- If Email is the only way to communicate personal info, minimize the information & identifiers used.
- Remember – once you press SEND, you have lost CONTROL



Information Access & Privacy Office at St. Paul's Hospital

privacy@providencehealth.bc.ca
604-806-8336

Janet Scott Leader, Information Access & Privacy
jscott@providencehealth.bc.ca

Zulie Sachedina VP Human Resources & General
Counsel
zsachedina@providencehealth.bc.ca



Be Aware of Social Engineering

- One of the more interesting uses is something called "Tabnabbing"
- This feature is available with all new browsers and targets the Social sites like Facebook, Twitter, Hotmail, Gmail etc...
- How to avoid it?
- Always open a new browser and open the Website you wish to visit from your favorites or your password Safe !
- Demo(time permitting)



Upcoming events!

- Tuesday, June 29th
 - Breakfast Bike Ride Potluck
 - Hot Dog Day
- Thursday, July 22nd: Summer Staff BBQ (Stanley Park)
- Wednesday, Aug 25th: Hot Dog Day
- Lunch and Learns (Thursday, 12 – 1, Gourlay):
 - June 24th: Effective oral presentations
 - July 8th: Effective poster presentations
 - July 15th: Graduate Student Experiences



Acknowledgements

The Privacy Team, especially
Janet Scott and Elaine Sawatsky

UBC and PHC CREB

Peter Paré and Rick Hegele

