BC CHILDREN'S HOSPITAL BIOBANK

Title	Records and Documentation
Policy number	POL 5
Effective Date	1 Dec 2014
Approved by	Suzanne Vercauteren

1.0 BACKGROUND

Recent developments in molecular biology and genomics have essentially enhanced the value of clinically annotated biospecimens in translational research and drug discovery. Adherence to best practices in the generation and maintenance of complete and accurate documentation is important in ensuring the value and utility of resources within a biobank. Intellectual property rights (IPR) can only be protected adequately if all records and documents are thorough, accurate and contemporaneous.

2.0 PURPOSE

The BC Children's Hospital BioBank (BCCHB) is committed to adherence to high ethical standards and practices in the collection and storage of human biospecimens - particularly from pediatric and maternal sources - for research purposes. The generation of clear, accurate, comprehensive and retrievable records and documents are vital to the BCCHB's compliance and success. The purpose of this BCCHB policy is to outline general principles that can be used by the BCCHB to insure that all records and documents are maintained with essential standards.

3.0 SCOPE

This policy applies to all records and documents that have to be generated and maintained as part of the operation of the BCCHB. The policy covers written notebooks, original paper records, true copies such as photocopies as well as electronic records (e.g. databases, spreadsheets, etc.) and documents (e.g. CD, DVD, USB, etc.).

4.0 REFERENCE TO OTHER SOPs OR POLICIES

BCCHB SOPs:

- FMO 003 Maintenance of Biospecimen Storage Facility and Equipment
- MHD 002 Inventory Verification
- MHD 006 Blood Collection
- MHD 007 Blood Processing and Storage
- MHD 011 Tissue Collection and Transportation
- MHD 012 Tissue Harvesting
- MHD 013 Snap Freezing of Tissue
- MHD 022 Biospecimen Retrieval
- MHD 024 Image Management
- MTR 001 Biospecimen Shipping and Transportation
- MTR 003 Material Request and Release
- PRM 003 Obtaining Informed Consent
- PRM 004 Withdrawal of Consent
- SFT 001 Handling Hazardous Chemical Waste
- SFT 002 Handling Biohazardous Substances
- TRN 001 Education and Training
- RMD 001 Information Access Control
- RMD 005 Data Entry Procedures
- RMD 007 Request and Creation of Accounts

PHSA Policies:

- IA_020 Privacy and Confidentiality

BCCHB Policies:

- POL 1 Informed Consent
- POL 3 Education and Training
- POL 4 Privacy and Security
- POL 7 Material and Information Handling

CFRI Policies:

- 167 Network Acceptable Use
- 168 Network Security
- 169 Systems Security
- 172 Account and Password
- 173 Electronic Data Storage
- 177 Personal Device
- 179 Loss, Damage, Theft and Disposal of Electronic Data
- 200 Performing and Retaining Data Backups

This Policy is modified from the Canadian Tumour Repository Network (BCCHB) Records and Documentation (POL 005 v.2.0).

5.0 RESPONSIBILITY

As custodian of biospecimens and associated information, the BCCHB has a responsibility to maintain complete and auditable records. This policy applies to BCCHB personnel involved in generating, maintaining and managing records and documents within the biobank.

6.0 POLICY STATEMENTS

The use of biospecimens and accompanying data is critical for medical research. Clear, accurate and complete records are essential to any research program. As custodian of biospecimens, biobanks are responsible for keeping proper records. The following principles will guide the BCCHB in maintaining compliant records and documents.

6.1 Collecting and managing information and data

6.1.1 Confidentiality of personal information as well as data associated with biospecimens is essential. All personal information will be de-identified as early as possible after collection.

6.1.2 Data records will be monitored to ensure completeness and accuracy.

6.1.3 As custodian of biospecimens, the BCCHB is responsible for keeping proper records of all uses that have been made of the material.

6.1.4 The BCCHB will ensure that all biospecimens and data uses have appropriate Research Ethics Board (REB) approval. All required documentation for REB approval will be kept for easy reference.

See **BCCHB Pol 4 Privacy and Security** for more information on confidentiality of personal information.

6.2 Retaining information and data

6.2.1 Retention of accurately recorded and retrievable information, data and results are essential for the operation of a biobank and should be retained indefinitely to be of value to translational researchers. Indefinite storage of biospecimens and data is a common practice in biobanking.

6.2.2 Researchers (who are leaving an establishment) that generated data and who wish to retain de-identified data/copies of data for future use must get specific permission to do so from both the BCCH BioBank and from the appropriate Research Ethics Board (REB). A material transfer agreement (MTA) should govern this transaction.

6.3 Retention of Data in the Case of Withheld or Revoked Consent

6.3.1 For cases of withheld consent, all case related information and data held (electronically or on paper) by the BCCHB will be removed or destroyed (**see BCCHB SOPs: RMD 005-01 Data Entry Procedures; PRM 003-01 Obtaining Informed Consent; PRM 004-01 Withdrawal of Consent).**

6.3.2 For cases of revoked consent, all case related information and data will be processed as outlined in BCCHB SOP **PRM 003-01 Obtaining Informed Consent; PRM 004-01 Withdrawal of Consent.** Biospecimens may be retained in an anonymized form for the purpose of education and protocol development.

6.4 Notebooks and Electronic Records

6.4.1 All raw data should be recorded and retained in laboratory notebooks or in an electronic database dedicated to that purpose. Note, personal information will be entered into a secure BCCHB Database. Raw data and non-identifiable information may be entered onto paper copies.

6.4.2 Machine print-outs, consent forms, questionnaires, chart recording, autoradiographs, forms, letters, etc. which cannot be attached to the main record should be retained in a separate manila folder that is cross-indexed by use of the BCCHB Biospecimen ID (**BCCHB SOP: MHD-001 Labeling and Tracking Materials**).

6.4.3 Electronic records (e.g. imaging records, gross or microscopic images etc.) should be de-identified and entered into the system as soon as possible after the data is collected or generated. Recorded data should be identified by date of the record and date of collection if the two do not coincide. Subsequent modifications or additions to records should be clearly identified and dated. See **BCCHB SOP: RMD 006 De-Identification of Data**.

6.4.4 Processes in place with regard to quality assurance of data collected and recorded electronically are described in **BCCHB SOP: MHD 002 Inventory Verification**.

6.4.5 Where feasible, internally annotated digitized data/images should be recorded and retained in a “raw” or original format as well. This is especially relevant where data/images undergoing digitization are subsequently enhanced. If possible, both the original and enhanced forms should be stored in the BCCHB data system. This is described further in **BCCHB SOP: MHD 024 Image Management**.

6.4.6 Any electronic document including images will be de-identified before being released to researchers. See **BCCHB SOP: RMD 006 De-Identification of Data**.

6.4.7 Electronic records will be backed-up regularly; duplicate copies should be held on a disc in a secure but readily accessible archive. These processes will take place in accordance with **CFRI Policy: 200 Performing and Retaining Data Backups.**

6.5 Personnel and Users Access to Information and Records

User accounts will be authorized and access privileges assigned by the BCCHB Data Coordinator based on business applicability, efficiency, effectiveness and appropriate security arrangements.

- All user accounts will be approved by the BCCHB Administrative Manager or BCCHB director.
- User accounts will only be provided once the user has read and acknowledged the PHSA Agreement on Terms and Conditions of Use and the PHSA Confidentiality Acknowledgment and BCCHB Confidentiality Agreement have been signed.
- Access privileges will be based on need-to-know in combination with the user’s role and assigned responsibilities.
- A unique user account will be set up to ensure individual accountability and audit capability. No generic or departmental accounts will be allowed.

- The BCCHB Administrative Manager is responsible for communicating job changes to the BCCHB Data Coordinator
- Regular reviews of user accounts will occur every 6 months.
- User accounts will be terminated at the first reasonable time after a user has vacated a position and is no longer with the BCCHB.
- If the user remains with the organization but vacates their current position, the account will be amended to reflect the roles required to support the user's new function.
- If data or functions available to a departed user are required by someone else, that other person will be provided with the original user's data and functionality not their original account.
- Users may have more than one role but care must be taken with consolidated access privileges in order to guard against security risk of a more highly privileged account being made available in an insecure environment.
- To prevent security risk, such users may be required to have separate accounts for their different functions. When and how this principle is applied will be based on risk and is at the discretion of the BCCHB Data Coordinator.

Full details on the process for data access, and information given to each user is explicitly laid out in **BCCHB SOPs: RMD 001 Information Access Control; RMD 007 Request and Creation of Accounts** and is related to CFRI Policies: **167 Network Acceptable Use; 172 Account and Password.**

6.6 Transmission of Information and Data

6.6.1 Users must not use e-mail to distribute "confidential information" over un-trusted networks such as the Internet.
6.6.1.1 Information from incoming sources (such as faxes, intercampus mail) should be transmitted in a secure manner.
6.6.1.2 Users must not use e-mail systems such as AOL, Hotmail or local ISP websites to access BCCHB related e-mail. Access to such sites is considered high risk.

6.6.2 Computer monitors, printers, fax machines displaying personal information should be positioned out of public view.

6.6.3 Attaching a confidentiality warning to emails and faxes may be considered by the BCCHB. An example of this is may be:

"Confidentiality Warning: This message and any attachments are intended only for the use of the intended recipient(s), are confidential, and may be privileged. If you are not the intended recipient, you are hereby notified that any review, retransmission, conversion to hard copy, copying, circulation or other use of this message and any attachments is strictly prohibited. If you are not the intended recipient, please notify the sender immediately by return e-mail, and delete this message and any attachments from your system. Thank you."

6.7 Physical Storage of Information and Data

6.7.1 Identifiable information should be stored in as few places as possible.

6.7.2 Data and records should be stored securely and with appropriate contingency plans. **(see CFRI Policy: 179 Loss, Damage, Theft and Disposal of Electronic Data).**

6.7.3 Data and records should be stored in a manner to permit retrospective audit if needed.

6.7.4 Data must be stored in a form that allows its inactivation if the research subject/partner withdraws consent.

6.7.5 Records and back-up discs should be stored to maximize protection from factors such as flooding, fire or theft. (**see: CFRI Policy: 200 Performing and Retaining Data Backups**).

6.7.6 Archival of identifiable information on WORM media such as CD's is strongly discouraged, and should be avoided at all costs:
- This includes archival for temporary usage, such as making a local copy of a database;
- When storage equipment is taken out of service, the storage media must be physically destroyed, rather than simply erased;
- Hard drives, CD's, etc. must be rendered physically unusable;
- No storage media/devices are to be sold, or passed on to third parties, or reused;
- Regular equipment is erased according to US DOD 5220.22-M guidelines

See CFRI Policy: 173 Electronic Data Storage

7.0 REFERENCES

1. Tri-Council Policy Statement 2: Ethical Conduct for Research Involving Humans; Medical Research Council of Canada; Natural Sciences and Engineering Council of Canada; Social Sciences and Humanities Research Council of Canada, December 2010. http://www.pre.ethics.gc.ca/archives/tcps-eptc/docs/TCPS%20October%202005_E.pdf

2. Human Tissue and Biological Samples for use in Research. Operational and Ethical Guidelines. Medical Research Council Ethics Series. http://www.mrc.ac.uk/news-events/publications/human-tissue-and-biological-samples-for-use-in-research/

3. International Conference on Harmonisation (ICH) Good Clinical Practice (GCP) Guidelines, section 4.8. http://www.ich.org

4. Medical Research Council, Ethics Series. Good Research Practice. http://www.mrc.ac.uk/documents/pdf/good-research-practice-principles-and-guidelines/

5. Good Laboratory Practice for nonclinical lab studies (CFR21-Chapter1 Part 58 Subpart J (58.185, 58.190 and 58.195).

6. Canadian Tumour Repository Network (BCCHB) Policy POL 005 e2.0. Records and Documentation

8.0 REVISION HISTORY

BCCHB Policy - Records and Documentation				
Policy Code -Version No.	**Date Revised**	**Approved By**		**Summary of Revisions**
		Print Name	**Signature**	
				Original version
