CTRNet Standard Operating Procedure Information Access Control			
SOP Number:	03.001	Version:	e2.0
Supersedes:	3.1.001 e1.0	Category:	Records Management and Documentation

Approved By:	CTRNet Management Group (CMG)	01-May-2012
	Per: Brent Schacter	30-May-2012

1.0 PURPOSE

Tumour biobanks are intended to manage the safekeeping of clinical and sample data in their custody. CTRNet biobanks are accountable for limiting disclosure of information, maintaining privacy of the participants and safeguarding the integrity of the information.

2.0 SCOPE

This standard operating procedure (SOP) outlines general elements and features that should be in place to ensure that access to participant and sample information is controlled so as to limit access to authorized personnel only.

3.0 REFERENCE TO OTHER CTRNET SOPS OR POLICIES

Note: When adopting this SOP for local use please reference CTRNet.

3.1 *CTRNet Policy: POL 4 Privacy and Security*
3.2 *CTRNet Policy: POL 7 Material and Information Handling*

4.0 ROLES AND RESPONSIBILITIES

This SOP applies to personnel from CTRNet member biobanks that are responsible for the database system and the safekeeping of sample and participant related information.

Tumour Biobank Personnel	**Responsibility/Role**
Information Technology Staff	Implements and audits security policies adopted by the biobank. Uses best practices for computer hardware and software security.
Tumour Biobank Director, Manager, or Principal Investigator	Implementing and defining procedures to control access to information

Copyright©2012 Canadian Tumour Repository Network (CTRNet).

5.0 MATERIALS, EQUIPMENT AND FORMS

Items listed in the following list are recommendations only and may be substituted by alternative/equivalent products more suitable for the site-specific task or procedure.

Materials and Equipment	Materials and Equipment (Site Specific)
No physical equipment requirements	

6.0 DEFINITIONS

See the CTRNet Program Glossary: http://www.ctrnet.ca/glossary

7.0 PROCEDURES

The facility should employ processes to limit access to sensitive and valuable information held by the biobank.

7.1 Data Access – Limit Access to "Need-to-Know" Basis

7.1.1 Nurses, technicians/technologists, administration, and IT staff are involved in entering, preparing, auditing, accessing and releasing data stored within the biobank. Define roles so as to limit access.

7.1.2 Grant access only if the role defined warrants it to perform their duty and after specified education/training has been completed and relevant privacy laws, regulations, and institutional policies have been reviewed. Where appropriate, necessary confidentiality agreements have been signed.

7.1.3 Remove or modify access once a role changes or a specific activity is completed.

7.1.4 Audit all permissions as part of a regular data access checkup recommended every 6 months or whenever major changes to data access systems are made.

7.2 Data Access – Release of Data for Research

7.2.1 Release of de-identified information to researchers should follow the same practices in place for the release of Human Biological Material. For more information see *CTRNet SOP 09.004 Material Request and Release.*

7.2.2 Selected and de-identified information on a particular participant or sample should be extracted from the database (at the biobank) in a report form and sent to the researchers electronically or by hard copy.

7.2.3 All released data must have a release code (also known as biobank reference number or biobank identifier) that permits the biobank (under the authority of the Biobank Director only) to link the data to the sample and to trace their origins. At no time should any release code contain any data that can be interpreted to identify the donor (e.g. birth date, cancer registration number, etc.).

The release code used for data and samples is a public identifier. Depending on the circumstances, the biobank may decide to make the release code different from the code used within the biobank, and unique for each case used for each study release or the same for each study receiving the same materials. The former strategy means that researchers

Copyright©2012 Canadian Tumour Repository Network (CTRNet).

cannot cross reference cases and data to conduct secondary research without involvement of the biobank where this might compromise individual identities or the scope of the original consent. The latter strategy means that research results can be shared more effectively and the value of the research data amplified.

Some examples of study release identifiers are:

- Sequential participant based sample numbers (e.g. 1001,1002,1003).
- Primary sample numbers may be used with an extension for the aliquot 1001-1, 1001-2,1001-3).
- Unique and randomly assigned numbers.
- Data records can be uniquely identified by the sample number. (In combination with a storage location where required – e.g. Tissue Micro Arrays (TMA's).)

7.2.4 Log and record data release. Specify:

a. Date released,

b. Name of researcher and institution released to, and

c. Study released for.

d. Individual reference numbers associated with the release

7.3 Other Electronic Data Access Issues

7.3.1 Where possible biobanks should ensure sensitive information is fully contained within and protected by the institution network.

7.3.2 If an institutional host network does not exist effective firewalls configured by trained personnel must be used and monitored.

7.3.3 Intrusion detection systems should be implemented and followed up in case of security breaches.

7.3.4 Audit, monitor and document access to information by logging events when information is accessed or released.

7.3.5 Audit logs to ensure that the procedures are limiting access to authorized personnel and users only.

7.3.6 Report deviations to access to the biobank director.

7.3.7 Investigate deviations to determine cause and source.

7.3.8 Take corrective action to avoid future occurrence.

7.3.9 Encourage the use of "strong" passwords (See Appendix A for "strong" and "weak" password examples)

7.3.10 Do not use the same password for tumour biobank accounts as for other non-tumour biobank access (e.g. personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various tumour biobank access needs.

Copyright©2012 Canadian Tumour Repository Network (CTRNet).

7.3.11 Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

7.3.12 A list of “don’ts”:

- Don't reveal a password over the phone to anyone.
- Don't reveal a password in an email message or other forms of electronic communication.
- Don't talk about a password in front of others.
- Don’t hint at the format of a password (e.g., “my family name”).
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers.

7.3.13 Do not write passwords down and store them anywhere in your office. Do not store passwords in a paper or digital file without proper encryption (e.g. by using encryption software such the open source cross platform True crypt program for digital files).

7.3.14 The recommended intervals for changing user level passwords are as per institutional policy.

7.3.15 If an account or password is suspected to have been compromised, report the incident to your IT staff and change all passwords.

7.3.16 Application developers must ensure that their programs contain the following security precautions:

a. Should support authentication of individual users, not groups.
b. Should not store passwords in clear text or in any easily reversible form.
c. Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

8.0 APPLICABLE REFERENCES, REGULATIONS AND GUIDELINES

8.1 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/eng/policy-politique/initiatives/tcps2-eptc2/Default/

8.2 Best Practices for Repositories I. Collection, Storage and Retrieval of Human Biological Materials for Research. International Society for Biological and Environmental Repositories (ISBER).
http://www.isber.org/Search/search.asp?zoom_query=best+practices+for+repositories

8.3 US National Biospecimen Network Blueprint
http://biospecimens.cancer.gov/resources/publications/reports/nbn.asp

9.0 APPENDICES

9.1 Appendix A – Password Characteristics

Copyright©2012 Canadian Tumour Repository Network (CTRNet).

10.0 REVISION HISTORY

SOP Number	Date revised	Author	Summary of Revisions
3.1.001 e1.0	2008	JdSH	Original document
3.1.001 e1.0	May 2012	CMG	• Section 1: Purpose, wording changed • Section 4: Changed title to Roles and Responsibilities, Deleted Tumour Bank Management from personnel • Removed definitions • Section 7.1: minor wording changes, deleted point #'s 3 and 5. Added point #4 (e2.0) • Section 7.2: #2-added "selected and de-identified" in the beginning of the paragraph. #3-changed • Section 7.3: Combined the points from 7.3, 7.4, and 7.5 all into section 7.3. • Grammatical and formatting throughout • Definitions removed • Revision History moved to bottom • Reference links updated • SOP References updated

Copyright©2012 Canadian Tumour Repository Network (CTRNet).

PASSWORD CHARACTERISTICS

Characteristics of "strong" passwords:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Characteristics of "weak" passwords:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software
    - The words "<Company Name>", "sanjose", "sanfran" or any derivation
    - Birthdays and other personal information such as addresses and phone numbers
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Copyright©2012 Canadian Tumour Repository Network (CTRNet).