

CTRNet Standard Operating Procedure Information Access Control			
SOP Number:	3.1.001	Version	e1.0
Supersedes:	SR 001.001	Effective Date	09 Jan 08
Subject:	Information Access Control	Category	Records Management and Documentation

Prepared By:		Jean de Sousa-Hitzler		
	Signature	Name	Title	ddMmmyy
Approved By:		Peter Geary	CEO	09 Jan 08
	Signature	Name	Title	ddMmmyy
Approved By:				
	Signature	Name	Title	ddMmmyy

REVISION HISTORY

SOP Number	Date Issued	Author (Initials)	Summary of Revisions
3.1.001	2008	JdSH	Initial release.

1.0 PURPOSE

Tumour banks or repositories are intended to manage the safekeeping of clinical data and other sample associated data their custody. CTRNet banks are accountable for limiting disclose of information, maintaining privacy of the participants and safeguarding the integrity of the information. CTRNet has policies regarding protection of data and personal 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 POLICIES AND SOPS

1. CTRNet Policy: POL 004.001 Privacy and Security
2. CTRNet Policy: POL 007.001 Material and Information Handling Policy

4.0 RESPONSIBILITY

The policy applies to personnel from CTRNet member repositories that are responsible for the database system and the safekeeping of sample and participant related information.

Tumour Bank Personnel	Responsibility/Role	Site Specific Personnel and Contact Information
Information Technology Staff	Implements and audits security policies adopted by the bank. Uses best practices for computer hardware and software security.	
Bank Manager/Coordinator Bank Director	Implementing and defining procedures to control access to information	
Tumour Bank Management	Ensuring adequate procedures are in place to control access to information	

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

Custodianship: Responsibility for safe keeping of tissue samples and associated data and control of their use and eventual disposal in accordance with the terms of the consent given by the participant and as regulated by the Research Ethics Board. Custodianship implies some rights to decide how the samples are used and by whom, and also responsibility for safeguarding the interests of donors.

Tumour Bank Application: Software and hardware system needed to annotate, track and distribute bio-specimens stored within the bio-repository.

Deviation: An intentional or unintentional event that is a departure from procedure or normal practice.

Safety: Processes, procedures and technologies to ensure freedom from danger or harm.

7.0 PROCEDURES

The facility should employ fundamental process to limit access to sensitive and valuable information held by the repository.

7.1 Data Access – Limit Access to “Need-to-know” Basis.

1. Nurses, technicians, administration, and informaticians are involved in entering, preparing and accessing data stored within the repository. Define roles so as to limit access.
2. Grant access only if the role defined warrants it to perform their duty.
3. Grant access on a “need-to-know” basis, limit records or application personnel have access to.
4. Remove access once a role changes or a specific activity is completed.
5. External users (Users coming from public networks) should not be granted access to sensitive information although they may be allowed to access de-identified data such as a regional data mart.

7.2 Data Access – Release of data for research.

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 9.1.005 Material Request and Release.
2. Information on a particular participant or sample should be extracted from the database (at the repository) in a report form and sent to the researchers electronically or by hard copy.

All released data must have an identifier that permits the bank (under the authority of the Bank Director only) to trace to the sample origin. At no time should any released reference number contain any data which can be interpreted (ex. Year of collection, birth date, cancer registration number, etc) to identify the donor.

3. As a best practice, each release of de-identified information to a new researcher should issue a new set of public identifiers to ensure researchers cannot cross reference identifiers with each other to compare results.

Where, owing to physical constraints, it is not possible to provide a release specific public identifier, acceptable bank assigned sample reference number options are:

- Sequential participant based sample numbers (e.g 1001,1002,1003)
- Primary sample numbers may be used 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 – ex TMA's)

4. Log and record data release. Specify:
 - Date released,
 - Name of researcher and institution released to, and
 - Study released for.
 - Individual reference numbers

7.3 Data Access – Firewalls

1. Where possible banks should ensure sensitive information is fully contained within and protected by the institution network.
2. If an institutional host network does not exist Enterprise class firewalls configured by trained personnel must be used and monitored.
3. Intrusion detection systems with alarms/alerts should be implemented and followed up on in case of security breaches.

7.3 Data Access – Auditing and Monitoring Access and Use

1. Audit, monitor and document access to information by logging events when information is accessed or released.
2. Audit logs to ensure that the procedures are limiting access to authorized personnel and users only.

7.4 Data Access – Record of Deviations

1. Report deviations to access to the repository director
2. Investigate deviations to determine cause and source.
3. Take corrective action to avoid future occurrence.

7.5 Data Access – User Passwords

1. Try to use choose “strong” passwords.
2. Try not to choose “weak” passwords. Characteristics for “strong” and “weak” passwords are described in Appendix 1.
3. Do not use the same password for tumour bank accounts as for other non-tumour bank access (e.g. personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various tumour bank access needs.
4. Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.
5. 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 reveal a password to the boss
 - 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 while on vacation
6. Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption
7. Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.
8. If an account or password is suspected to have been compromised, report the incident to your information technology staff and change all passwords.
9. Application developers must ensure that their programs contain the following security precautions:
 - should support authentication of individual users, not groups.
 - should not store passwords in clear text or in any easily reversible form.
 - 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.
 - should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

8.0 APPLICABLE REFERENCES, REGULATIONS AND GUIDELINES

1. Tri-Council Policy Statement; 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, August 1998. <http://www.pre.ethics.gc.ca/english/policystatement/policystatement.cfm>
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>
3. US National Biospecimen Network Blueprint
http://www.ndoc.org/about_ndc/reports/NBN_comment.asp

9.0 APPENDICES

1. Password Characteristics

Appendix 1.

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)