Procédure normalisée de fonctionnement Contrôle de l'accès à l'information			
Catégorie:	Gestion et documentation des dossiers		
Numéro de PNF:	03.001	Version:	f2.0
Remplace:	3.1.001 f1.0	Date d'entrée en vigueur:	30 mai 2012

Approuvée par:	Comité administratif du RCBT (CAR)	01 mai 2012
	Par: Brent Schacter	30 mai 2012

1.0 INTENTION

Les banques de tumeurs doivent sauvegarder les données cliniques et les autres informations associées aux échantillons dont elles sont dépositaires. Les banques du RCBT sont responsables de limiter la divulgation de l'information, de maintenir la vie privée des participants et de sauvegarder l'intégrité de l'information.

2.0 PORTÉE

Cette procédure normalisée de fonctionnement (PNF) trace les grandes lignes des éléments généraux et des caractéristiques qui devraient être mis en place pour assurer que l'accès à l'information du participant et de l'échantillon soit contrôlé afin d'être limiter aux personnes autorisées seulement.

3.0 RÉFÉRENCES À D'AUTRES PNF OU POLITIQUES

Remarque: Lors de l'adoption de cette PNF pour un usage local, s'il vous plaît faire référence au RCBT.

3.1 *Politique du RCBT POL 4 : Vie privée et sécurité*
3.2 *Politique du RCBT POL 7 : Manipulation du matériel et de l'information*

4.0 RÔLES ET RESPONSABILITÉS

Cette PNF s'applique aux membres du personnel des banques membres du RCBT qui sont responsables du système de base de données ainsi que de sauvegarder l'information relative au participant et à l'échantillon.

Personnel de la banque de tumeurs	**Responsabilité/Rôle**
Personnel des technologies informatiques	Mise en œuvre et audit des politiques de sécurité adoptées par la banque. Utilisation des meilleures pratiques pour la sécurité des ordinateurs et des logiciels.
Directeur, administrateur et chercheur principal de la banque de tumeurs	Mise en œuvre et définition des procédures pour contrôler l'accès à l'information.

5.0 MATÉRIEL, ÉQUIPEMENT ET FORMULAIRES

Le matériel, l'équipement et les formulaires inscrits sur la liste suivante ne sont que des recommandations et peuvent être substitués par des produits alternatifs ou équivalents plus appropriés aux tâches et aux procédures spécifiques de chaque site.

Matériel et équipement	**Matériel et équipement (spécifiques au site)**
Aucun équipement physique requis	

6.0 DÉFINITIONS

Voir le glossaire du programme du RCBT: http://www.ctrnet.ca/glossary

7.0 PROCÉDURES

Aux installations des lieux de collecte et d'entreposage, un processus devrait être mis en place pour limiter l'accès à l'information sensible et précieuse détenue par la banque.

7.1 Accès aux données – Limite de l'accès sur la base de "nécessité de savoir".

7.1.1 Les infirmières, les techniciens, l'administration et les informaticiens sont impliqués dans l'entrée, la préparation et l'accès aux données entreposées à l'intérieur de la banque. Définir les rôles afin de limiter l'accès.

7.1.2 Permettre l'accès seulement si un rôle défini le justifie pour accomplir la tâche et après que l'éducation et la formation aient été complétées et que les lois, les règlements et les politiques institutionnelles sur la confidentialité aient été examinées. Le cas échéant, les accords de confidentialité nécessaires ont été signés.

7.1.3 Enlever l'accès une fois que les rôles changent ou qu'une activité spécifique est complétée.

7.1.4 Vérifier toutes les autorisations dans le cadre d'un bilan régulier de l'accès aux données qui est recommandé à tous les 6 mois ou à toutes les fois que des changements importants sont effectués.

7.2 Accès aux données – Transfert des données de recherche

7.2.1 Le transfert de l'information codée aux chercheurs devrait suivre les mêmes pratiques mises en place pour le transfert du matériel biologique humain. Pour plus d'informations, voir la PNF du RCBT 9.1.004 *Requête et transfert de matériel.*

7.2.2 L'information sélectionnée et dénominalisée d'un participant ou d'un échantillon particulier devrait être extraite de la base de données (à la biobanque) dans un formulaire et envoyée aux chercheurs de façon électronique ou par copie papier.

7.2.3 Toutes les données transférées doivent avoir un code de transfert (également connu comme le numéro de référence ou l'identifiant de la biobanque) permettant à cette biobanque (uniquement sous l'autorité de son directeur) de relier les données à l'échantillon et de retracer son origine. À aucun moment, un code transféré ne contient des données qui peuvent être interprétées pour identifier un donneur (p.ex. date de naissance, numéro de carte d'assurance maladie, etc.).

Le code de transfert utilisé pour les données et les échantillons devient un identificateur public. Selon les circonstances, la biobanque peut décider de rendre le code de transfert différent du code utilisé par la biobanque, de rendre le code unique pour chacun des cas utilisés pour chaque étude ou encore d'attribuer le même code pour chaque étude recevant un matériel spécifique.

La première stratégie signifie que les chercheurs ne peuvent croiser les cas référés et les données pour effectuer des recherches secondaires sans la participation de la biobanque empêchant ainsi de compromettre les identités individuelles ou la portée du consentement original. Cette stratégie signifie également que les résultats de recherche peuvent être partagés plus efficacement et que leur valeur en est amplifiée.

Des exemples d'identifiants de transfert pour des études peuvent être :

- Des numéros séquentiels associés à l'échantillon (p.ex.1001, 1002, 1003).
- Des numéros d'échantillons primaires pouvant être utilisés avec une prolongation pour la portion aliquotée (1001-1, 1001-2, 1001-3).
- Des numéros uniques et attribués au hasard.
- L'archivage des données peut uniquement être identifié par le numéro de l'échantillon (en combinaison avec un emplacement d'entreposage si nécessaire – p.ex. microétalages de tissus (TMAs).

7.2.4 Prendre note et archiver les transferts de données. Spécifier:

a. La date du transfert

b. Les noms du chercheur et de l'institution vers qui les données ont été transférées

c. L'étude pour laquelle les données ont été transférées

7.2.5 Les numéros de référence individuelle associés avec le transfert.

7.3 Autres questions d'accès aux données électroniques

7.3.1 Lorsque c'est possible, les biobanques devraient s'assurer que l'information sensible est entièrement contenue au sein du réseau de l'institution hôte et protégée par celui-ci.

7.3.2 Si un réseau institutionnel hôte n'existe pas, des murs pare-feu configurés doivent être mis en place et gérés par un personnel formé.

7.3.3 Des systèmes de détection d'intrusion avec des alertes/alarmes devraient être mis en place et suivis dans le cas d'infraction à la sécurité.

7.3.4 Vérifier, surveiller et documenter l'accès à l'information en enregistrant les circonstances où elle a été consultée ou transférée.

7.3.5 Vérifier les enregistrements pour s'assurer que les procédures limitent l'accès au personnel et aux usagés autorisés seulement.

7.3.6 Rapporter les déviations à l'accès au directeur de la biobanque.

7.3.7 Investiguer les déviations pour déterminer leur cause et la source.

7.3.8 Prendre les actions correctives pour éviter que le cas ne se répète dans le futur.

7.3.9 Encourager l'utilisation des mots de passe "forts" (voir l'annexe A pour des exemples de mots de passe "forts" et "faibles").

7.3.10 Ne pas utiliser les mêmes de mots de passe pour les accès à la banque de tumeurs que ceux utilisés pour des accès autres que la banque de tumeurs (ex : compte personnel de votre fournisseur de service internet, accès à un compte bancaire, etc.). Si possible, ne pas utiliser le même mot de passe pour les besoins d'accès à plusieurs banques de tumeurs.

7.3.11 Ne pas partager des mots de passe avec quiconque, incluant les assistants ou les secrétaires d'administration. Tous les mots de passe doivent être traités comme de l'information confidentielle.

7.3.12 Liste à éviter :

- Ne pas révéler de mot de passe par téléphone à quiconque.
- Ne pas révéler de mot de passe par courriel ou autre forme de communication électronique.
- Ne pas parler du mot de passe devant personne.
- Ne pas laisser insinuer le contenu du mot de passe (p.ex. "mon nom de famille")
- Ne pas révéler de mot de passe sur des questionnaires ou des formulaires de sécurité.
- Ne pas partager de mot de passe avec les membres de sa famille.
- Ne pas révéler de mot de passe à des collègues.

7.3.13 Ne écrire de mots de passe ni les entreposer n'importe où dans votre bureau. N'entreposer de mots de passe dans aucun dossier sur aucun système informatique (p.ex. en utilisant un logiciel de cryptage tel la plateforme Trucrypt pour les fichiers numériques)

7.3.14 Les intervalles recommandés pour changer les mots de passe sont conformément à la politique institutionnelle.

7.3.15 Si un mot de passe est soupçonné d'être compromis, rapporter l'incident au personnel technologique et changer le mot de passe.

7.3.16 Les développeurs d'application doivent s'assurer que leurs programmes contiennent les précautions de sécurité suivantes:

a. Devrait supporter l'authentification des usagers individuels, non des groupes.
b. Ne devrait pas entreposer de mots de passe dans un texte clair ou dans une forme facilement réversible.
c. Devrait fournir pour certains genres de rôles administratifs, un moyen tel qu'un utilisateur puisse reprendre les fonctions d'un autre sans avoir à connaître le mot de passe de ce dernier.

8.0 RÉFÉRENCES, RÈGLEMENTS ET DIRECTIVES

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 ANNEXES

9.1 Annexe A –caractéristiques des mots de passe

10.0 HISTORIQUE DES RÉVISIONS

Numéros des PNFs	Dates des modifications	Auteurs	Résumé des modifications
3.1.001 e1.0	2008	JdSH	Version initiale
3.1.001 e1.0	Mai 2012	CMC	• Section 1: Intention, formulation modifiée • Section 4: Changement du titre de *Rôles et responsabilités*, suppression de la coordination de la biobanque du personnel. • Suppression des définitions • Section 7.1: modification mineure à la formulation, délétion des points #3 et 5. Addition du point #4 • Section 7.2: #2-addition de " sélectionnée et dénominalisée" au début du paragraphe, changement au #3 • Section 7.3: Regroupement des points 7.3, 7.4, et 7.5 dans la section 7.3. • Grammaire et mise en page • Retrait des définitions • Historique des révisions déplacé au bas du document • Mise à jour des liens pour les références • Mise à jour des références aux PNFs

CARACTÉRISTIQUES DES MOTS DE PASSE

Caractéristiques de mots de passe "forts":

- Contiennent des caractères minuscules et majuscules (ex : a-z, A-Z)
- Contiennent des chiffres et des caractères de ponctuation aussi bien que des lettres ex : 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Ont au moins une longueur de 8 caractères alphanumériques
- Ne sont pas des mots dans aucun langage, argot, dialecte, jargon, etc.
- Ne sont pas basés sur une information personnelle, noms de famille, etc.
- Les mots de passe ne devraient jamais être écrits nulle part ou entreposés en ligne. Essayer de créer des mots de passe qui peuvent être facilement retenus. Une façon de faire est de créer un mot de passe basé sur le titre d'une chanson, d'une affirmation ou d'une autre phrase. Par exemple, la phrase peut être : "Un moyen de se rappeler cette phrase" et le mot de passe pourrait être : "1MDSR7p!" ou "1mdesr7p" ou autres variations.

Caractéristiques de mots de passe "faibles":

- Les mots de passe contiennent moins de 8 caractères
- Les mots de passe sont des mots que l'on trouve dans un dictionnaire (français ou autre)
- Les mots de passe sont des mots d'un usage commun tels que :
    - Nom de famille, d'un animal de compagnie, d'un ami, d'un collègue, etc.
    - Termes et noms de l'ordinateur, d'une commande, d'un site, d'une compagnie, d'un logiciel
    - Les mots "<Nom de compagnie>", "Mtl", "CHUM" ou des dérivations
    - Anniversaires ou autres informations personnelles comme des adresses et des numéros de téléphone
    - Suite ou patron de mots ou de chiffres comme aaabbb, zyxwvuts, 123321, etc.
    - Aucun de ces derniers à rebours
    - Aucun de ces derniers suivis d'un chiffre (p.ex. secret1, 1secret)