Procédure normalisée de fonctionnement du RCBT **Contrôle de l'accès à l'information**			
Numéro de PNF:	3.1.001	Version	
Remplace:		Date d'entrée en vigueur	
Objet:	Contrôle de l'accès à l'information	Catégorie	Gestion des données et documentation

Préparée par:		Aaron Suggit/Jean de Sousa-Hitzler		
	Signature	Nom	Titre	jjmmaa
Approuvée par:		Peter Geary	CEO	
	Signature	Nom	Titre	jjmmaa
Approuvée par:				
	Signature	Nom	Titre	jjmmaa

Historique des révisions

Numéro de PNF	Date des modifications	Auteur (Initiales)	Résumé des révisions
3.1.001 f1.0	05/08/2008	LC	Traduction française de 3.1.001

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. Le RCBT a des politiques en regard de la protection des données et de l'information personnelle.

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 de limiter l'accès aux personnes autorisées seulement.

3.0 RÉFÉRENCES À D'AUTRES POLITIQUES ET PNFS

1. Politique du RCBT: POL 004.001 Vie privée et sécurité
2. Politique du RCBT: POL 007.001 Politique de la manipulation du matériel et de l'information

4.0 RESPONSABILITÉ

La PNF s'applique au personnel des banques membres du RCBT qui est responsable du système de base de données et de sauvegarder l'information relative au participant et à l'échantillon.

Personnel de la banque de tumeurs	**Responsabilité/Rôle**	**Site personnel spécifique et coordonnées de contact**
Personnel technologique de l'information	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.	
Administrateur/coordonnateur de la banque, directeur de la banque	Mise en œuvre et définition des procédures pour contrôler l'accès à l'information.	
Administrateur de la banque de tumeurs	Assurance que les procédures adéquates sont en place pour contrôler l'accès à l'information.	

5.0 MATÉRIEL, ÉQUIPEMENT ET FORMULAIRES

Les items inscrits dans la liste suivante ne sont que recommandés et peuvent être substitués par des produits alternatifs/équivalents plus appropriés aux tâches ou aux procédures spécifiques aux sites.

Matériel et équipement	**Matériel et équipement (spécifiques au site)**
Pas d'exigences d'équipement physique	

6.0 DÉFINITIONS

Fiduciaire: Personne responsable de conserver de manière sécuritaire des échantillons de tissus et leurs données associées et qui contrôle leur utilisation et leur destruction éventuelle en accord avec les termes du consentement donné par le participant et réglementé par le comité d'éthique de la recherche. La fiducie implique certains droits à décider comment les échantillons sont utilisés et par qui, et implique également la responsabilité de sauvegarder les intérêts des donneurs.

Application de la banque de tumeurs: Système de logiciels et d'ordinateurs nécessaires pour annoter, suivre et distribuer les biospécimens entreposés dans la biobanque.

Déviation: Un événement intentionnel ou non-intentionnel qui provoque une sortie de la procédure ou de la pratique normale.

Sécurité: Processus, procédures et technologies pour s'assurer d'être à l'abri du danger ou du bris.

7.0 PROCÉDURES

Aux installations des lieux de collecte et d'entreposage, un processus fondamental devrait être suivi 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".

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.
2. Permettre l'accès seulement si le rôle défini le justifie pour accomplir la tâche.
3. Permettre l'accès sur une base de "nécessité de savoir", limiter l'accès aux données ou aux applications personnelles
4. Enlever l'accès une fois que les rôles changent ou qu'une activité spécifique est complétée.
5. Les usagers externes (usagers venant des réseaux publics) ne devraient pas avoir accès aux informations sensibles bien qu'on puisse leur permettre l'accès à des données codées tel qu'une base de données régionales.

7.2 Accès aux données – Transfert des données de recherche

1. Le transfert de l'information codée aux chercheurs devrait suivre les mêmes pratiques mises en place pour le transfert du matériel biologique humain.
2. Pour plus d'informations, voir la PNF du RCBT 9.1.005 *Requête et transfert de matériel.*
3. L'information sur un participant ou un échantillon particulier devrait être extraite de la base de données (à la banque) dans un formulaire et envoyée aux chercheurs de façon électronique ou par copie papier.
4. Prendre note et archiver les transferts de données. Spécifier :
    - La date du transfert,
    - Les noms du chercheur et de l'institution vers qui les données ont été transférées, et
    - L'étude pour laquelle les données ont été transférées.
5. Chaque transfert d'information codée à un nouveau chercheur devrait conduire à un nouveau groupe d'identifiants publics pour s'assurer que les chercheurs ne croiseront pas leurs identifiants de référence avec d'autres pour comparer les résultats.

7.3 Accès aux données – Murs pare-feu

1. Là où c'est possible, les banques devraient s'assurer que l'information sensible est complètement contenue à l'intérieur du réseau de l'institution et protégée par celui-ci.

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.

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 Accès aux données – Audit et surveillance de l'accès et utilisation

1. Vérifier, surveiller et documenter l'accès à l'information en enregistrant les circonstances où l'information a été consultée ou transférée.
2. Vérifier les enregistrements pour s'assurer que les procédures limitent l'accès au personnel et aux usagés autorisés seulement.

7.4 Accès aux données – Archives des déviations

1. Rapporter les déviations à l'accès au directeur de la banque.
2. Investiguer les déviations pour déterminer leur cause et la source.
3. Prendre les actions correctives pour éviter que le cas ne se répète dans le futur.

7.5 Accès aux données – Utilisation d'un mot de passe

1. Dans la mesure du possible, utiliser des mots de passe "forts".
2. Essayer de ne pas utiliser de mots de passe "faibles". Les caractéristiques pour "forts" et "faibles" sont décrites dans l'annexe 1.
3. 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.
4. 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.
5. 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 (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 pendant les vacances.
6. Ne pas écrire de mots de passe ni l'entreposer n'importe où dans votre bureau. N'entreposer de mots de passe dans aucun dossier sur aucun système informatique (incluant les Palm Pilots ou appareil similaire) sans cryptage.
7. Changer les mots de passe au moins à tous les 6 mois (excepté les mots de passe du système qui doivent être changés tous les 3 mois). L'intervalle de changement recommandé est aux 4 mois.
8. Si on suspecte qu'un mot de passe est compromis, rapporter l'incident au personnel technologique et changer le mot de passe.
9. Les développeurs d'application doivent s'assurer que leurs programmes contiennent les précautions de sécurité suivantes :
   - devrait supporter l'authentification des usagers individuels, non des groupes.
   - ne devrait pas entreposer de mots de passe dans un texte claire ou dans une forme facilement réversible.
   - 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 l'autre.
   - devrait supporter TACACS+ , RADIUS et/ou X.509 avec retrait de sécurité, si possible.

8.0 RÉFÉRENCES, RÈGLEMENTS ET LIGNES DIRECTRICES

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 ANNEXES

1. Caractéristiques de mot de passe

Annexe 1.

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 (e.g., secret1, 1secret)