Procédure normalisée de fonctionnement du RCBT **Systèmes de sauvegarde des bases de données**			
Numéro de PNF:	3.1.002	Version	f1.0
Remplace:		Date d'entrée en vigueur	
Objet:	Notification de découvertes significatives et pertinentes	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
3.1.002 f1.0	06/08/2008	LC	Traduction française de 3.1.002

1.0 INTENTION

Les banques de tumeurs se doivent de conserver et protéger les données cliniques et toute autre donnée associée aux échantillons dans leur fiducie. Les politiques du RCBT à l'égard des sauvegardes de données visent à protéger les données et les informations personnelles contre les défaillances, les pertes ou les dommages pouvant survenir lors d'erreurs d'utilisation (modification ou destruction volontaire ou accidentelle des données), de bris d'équipement (panne d'ordinateur) ou d'événements exceptionnels (feu, inondation, coupure de courant, virus ou piratage informatique). Les systèmes de sauvegarde doivent garantir que l'information contenue dans la base de données peut être intégralement restaurée. Le RCBT recommande une sauvegarde quotidienne des données afin de limiter les pertes éventuelles de données à une journée

2.0 PORTÉE

Cette procédure normalisée de fonctionnement (PNF) trace les éléments généraux et les caractéristiques qui doivent être mis en place pour s'assurer que l'information entreposée dans une base de données puisse être intégralement récupérée et dans un laps de temps raisonnable.

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 Manipulation du matériel et de l'information

4.0 RESPONSABILITÉS

La PNF s'applique au personnel des banques membres du RCBT qui sont responsables du système de base de données, de la sauvegarde des échantillons et de l'information relative au participant.

Personnel de la banque de tumeurs	**Responsabilité/Rôle**	**Site personnel spécifique et coordonnées de contact**
Personnel du département des technologies de l'information (TI)	Gère les sauvegardes et récupère les données en accord avec les règles définies par de la banque.	
Administrateur/coordonnateur de la banque, directeur	Participe au développement des besoins pour la sauvegarde et la récupération des données.	
Administrateur de la banque de tumeurs	S'assure qu'un système de sauvegarde adéquate a été mis en place.	

5.0 MATÉRIEL, ÉQUIPEMENT ET FORMULAIRES

Le matériel, l'équipement et les formulaires 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)**
Système de sauvegarde de la base de données	
Support de sauvegarde amovible	
Lieu d'entreposage extérieur	

6.0 DÉFINITIONS

Sauvegarde: Procédure routinière consistant à dupliquer et mettre en sécurité les données contenues dans un système informatique de manière automatisée ou non.

Fiducie: Responsabilité de conserver de manière sécuritaire des échantillons de tissus et leurs données et de contrôler l'utilisation et la destruction éventuelle de ces derniers en accord avec les termes du consentement donné par le participant et réglementé par le comité d'éthique à la recherche. La fiducie définit certains droits quant à l'utilisation des échantillons aux personnes autorisées et aux responsabilités afin de garantir les intérêts des donneurs.

Application de la banque de tumeurs: Logiciels et systèmes informatiques utilisés pour annoter, suivre et distribuer les biospécimens de la banque.

Sécurité: Processus, procédures et technologies mis en place pour protéger les données d'événements indésirables (bris, virus, etc.)

Système de gestion de la base de données (SGBD) : Un groupe complexe d'applications permettant de gérer l'organisation, l'entreposage et la récupération des données d'une base de données. Il existe de nombreux SGBD connus comme Oracle, DB2, Microsoft Access, Microsoft SQL Server, Postgres, MySQL et FileMaker.

7.0 PROCÉDURES

Les installations doivent comporter des systèmes de sauvegarde pour protéger les informations de la base de données des dommages et des pertes. Dans le cas d'erreurs d'utilisateurs, de bris d'équipements ou d'évènements nuisibles, le système devrait être capable de récupérer et restaurer intégralement l'information telle qu'elle était avant l'incident. On entend par «intégralement» le fait que l'information sera restaurée de manière complète et exempte de corruption.

7.1 Sauvegarde de la base de données – Description générale du processus

1. Chaque banque devrait développer une stratégie de sauvegarde basée sur :
   - La taille des données entreposées
   - Les supports de sauvegarde disponibles
   - Le SGBD utilisé
   - Les exigences de sauvegarde (définitions des données devant être obligatoirement restaurées, etc.)

- Les besoins définis dans le cadre d'une détection de donnés erronées (Problèmes d'intégrité des données qui requièrent la récupération d'archives plus ou moins vieilles afin de localiser la source de l'erreur et la corriger).

2. Se basant sur un plan de sauvegarde acceptable, le personnel IT de la banque devrait implanter et gérer des processus de sauvegardes régulières.
3. Entreposer de manière régulière des copies des sauvegardes sur des sites extérieures afin de protéger les données d'événements nuisibles pouvant détruire le site principal d'archivage (feu, inondations, tremblements de terre, etc).
4. Tester la récupération des données à des intervalles réguliers tel que spécifié dans le plan de sauvegarde/récupération et archiver les résultats. Tester à la fois la récupération des données individuelles ainsi que la totalité des données. Les sauvegardes entreposées sur des sites extérieurs doivent faire l'objet de tests similaires.

7.2 Sauvegarde de la base de données – Processus de routine

1. Les processus de sauvegarde dépendront du support utilisé. Idéalement, le système de sauvegarde devrait être automatisé et ne pas requérir une intervention humaine quotidienne de l'utilisateur (changement manuel du support de sauvegarde par exemple) afin de réduire les risques d'erreur.
2. Procéder à des validations afin de garantir que la sauvegarde quotidienne a été complétée avec succès. Toute erreur de sauvegarde doit être analysée et corrigée de manière prioritaire.

7.3 Sauvegarde de la base de données – Fréquence

1. La fréquence est dépendante des besoins de récupération de la banque. La base de données devrait être sauvegardée quotidiennement durant la nuit. Une telle configuration limiterait la perte de données à une journée en cas de dommage ou de perte de données.
2. Conserver une partie des sauvegardes sur une période de un an à compter de leur date de création (recommandation du RCBT)
    a. Garder des copies mensuelles complètes durant un an.
    b. Utiliser un ensemble de cinq (5) copies hebdomadaires pour chaque mois
    c. Utiliser des supports différents pour chacun des jours d'opération (excluant les journées de congé, comme les fins de semaine et les copies de fin de semaine)
    d. Entreposer les sauvegardes en protégeant l'accès à ces dernières.
3. Entreposage hors site
    a. Le RCBT recommande (au minimum) que des copies mensuelles soient envoyées hors site, de façon hebdomadaire de préférence.

b. Quand un entreposage hors site est maintenu, le fournisseur de service doit être autorisé par l'institution hôte à manipuler les données sensibles.

7.4 Sauvegarde de la base de données – Plan de récupération

1. Mettre en place un plan de récupération pour la banque définissant les pertes de données acceptables. L'habilité à récupérer les données peut dépendre du système informatique et du SGBD utilisés.

7.5 Sauvegarde de la base de données – Vérification et validation des systèmes de sécurité de récupération des données en cas de feu

1. Développer un plan de tests pour s'assurer que les sauvegardes sont lisibles et contiennent des données valides.
2. Exécuter les tests aussi bien pour la récupération intégrale de la base de données que pour la récupération des données individuelles sur une base trimestrielle.

8.0 RÉFÉRENCES, RÈGLEMENTS ET LIGNE 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

aucune