Records Management

Reviewed Date		**Number**	*IM0110*
Revised Date	*November 24, 2003*	**Approved Date**	*September 25, 1996*

Introduction

Information is recorded in the day to day operations of the agency. How this information is collected, stored, accessed and released is governed by legislation and regulations including the Municipal Freedom of Information and Protection of Privacy Act and Regulated Health Professions Act. The health unit also has policies which influence how records are managed (Confidentiality and Release of Information Policy, Consent to Treatment Policy, Compliance with MFIPPA Policy). Regulating bodies for the various professions working within the agency have also set standards related to records management.

This policy outlines the general expectations of the agency with respect to management of records created in carrying out the functions and mandates of the Board of Health.

Purpose

Legislative Authority

Policy Definitions and Interpretation

Policy

Every file or document used by the Board of Health or on behalf of the Board to carry out its functions and mandates is deemed to be a record. This includes correspondence, ledgers, completed forms, maps, plans, photographs, microfilms, minutes, books, tapes, client records, personnel records, computer discs, hard drives, CD-ROMs or other technological means.

Records of the health unit are the property of the Board of Health. Records will be created and destroyed according to an established records management system within the requirements of legislation and regulations.

Recognizing that each Service Area may have different legal requirements for records management, the Director of each Service Area is responsible to the Medical Officer of Health for ensuring that a records management system is in place for the service. The system will describe methods for the creation, maintenance, security and disposal of records and be consistent with agency policies and relevant legislation.

It is the responsibility of each staff member who is in possession of an official record to ensure the security of that record. *(See also Policy A 1.030 Confidentiality)*. Records will be stored under lock and key when not in use by the staff member. Records temporarily left in a vehicle should be placed out of view, in the locked trunk of the vehicle.

Procedures

A) Creation of Records:

Every record will have a person identified, by function or title, as responsible for the original record. Every record will have a specific physical location. All staff in possession of the original record share in the responsibility to ensure protection and location. Often this person is the originator of the record but this may change over time.

The original record is the permanent record, although the form of retention may vary. Judgment of the "next best evidence" e.g. microfilming to replace paper copy, or the form or format of the record is made at the time the record is created. Discretion is used during the creation of a record as to whether working notes and drafts of documents are kept as part of the document or destroyed. Copies of records will only be retained temporarily based on an operational need.

B) Maintenance and Security of Records:

The Director of each Service Area will ensure that person(s) are assigned responsibility for maintenance, securing and providing appropriate access to records.

Records will be kept in the most efficient manner with respect to storage and access. Unless paper records are required by law, records may be retained on computer disc, hard drive files, CD-ROM or other technological means.

Records will be secured, usually in locked cabinets. Only operational current records and working documents may be taken off site. Records and copies of records will be kept confidential and only be accessible to appropriate personnel.

Records that are current and operational must be easily retrieved. Frequency of need and user need will determine record location and ease of access.

C) Procedure in the Event of Lost or Stolen Records:

1. If a record has been stolen, the staff member will report the theft and the circumstances involved to the local police authority and then proceed with the steps below
2. If a record is missing (i.e. cannot be located when needed), the staff member will notify his/her program manager, verbally and in writing.
3. A "Breach of Security" report will be created by the staff member, detailing:
    - essential identifying information,
    - the last known location of the record,
    - efforts made to locate the record,
    - circumstances related to the loss,
    - date last signed out and by whom and
    - other relevant information e.g. Police report
    - manager who took the report

    Upon completion of the report, the staff member and the manager will sign prior to forwarding to the Service Area Director.
4. The original of the report will be forwarded to the Service Area Director, who reviews the report, signs it and forwards to the Administrative Assistant for filing in the central corporate file established in the Administrative Service. A copy of the report will be retained by the staff member and by the program manager. (If the record is

subsequently located, a follow-up communication will be sent to the same people, and the new record will be merged with the recovered record.)

5. The staff member will create a new record and document the fact that the original record has been lost, as well as any information from the original record that can be accurately recalled. The “Breach of Security” report will be cross-referenced on the record.
6. The program manager will review, with the staff member the circumstances associated with the loss/theft of the record and determine what actions could be undertaken to avoid a reoccurrence. In the event of a record loss, with no indication of third party involvement, the client may be informed at the discretion of the program manager.
7. If it is determined that a record has come into the possession of a third party (e.g. through theft), the MOH will be notified of the circumstances both verbally and in writing. The client will also be informed about the circumstances of the event.

D) Record Retention and Disposal

Service Area Directors are responsible for developing a record retention schedule based on legislation and the needs of the Service. Directors are also responsible for ensuring a system is is place for review and disposal of records.

In the absence of legal requirements with respect to record retention, an original record will be kept for three years. No records will be kept beyond their retention period.

E) Historical and Archival Materials

The Director of Resource Services will determine if records have a historical significance for the health unit and how these records will be retained.

Service Area Directors will determine if records have historical significance for a service or profession and how these records will be retained.

Related Forms

Related Procedures

Records Destruction Procedure – March 5, 2008
Preparation of Inactive Records for Storage – November 30, 2010
Inactive Records Transfer – January 4, 2013

Related Policies

Policy IM0101 Personal Information Including Personal Health Information Privacy – Principles
Policy IM0102 Personal Information Including Personal Health Information Privacy – Accountability
Policy IM0103 Personal Information Including Personal Health Information Privacy – Consent
Policy IM0104 Personal Information Including Personal Health Information Privacy – Collection & Use
Policy IM0105 Personal Information Including Personal Health Information Privacy – Disclosure
Policy IM0106 Personal Information Including Personal Health Information Privacy – Access
Policy IM0107 Personal Information Including Personal Health Information Privacy – Correction
Policy IM0108 Personal Information Including Personal Health Information Privacy – Privacy Breach

Final Approval Signature: _____

Review/Revision History:
September 2010 Policy re-numbered, previous number C4.020