Manitoba
Health, Seniors and Active Living

GUIDELINES

for

Records of User Activity (RoUA)

Approved by: Karen Herd, Deputy Minister
Approval Date: June 3, 2014
Effective Date: June 3, 2014

Table of Contents

PART 1: LEGISLATIVE REFERENCE 3
The Personal Health Information Act (PHIA) 3
The Personal Health Information Regulation 3
Schedule B: Demographic and Eligibility Information 3
PART 2: DEFINITIONS 4
PART 3: CREATING A RECORD OF USER ACTIVITY (RoUA) 4
1. Determining if RoUA Required 4
2. Providing RoUA to Individuals 5
3. Fees 5
4. Security and Confidentiality of RoUA 5
PART 4: AUDITING RECORDS OF USER ACTIVITY 5
5. Description 5
6. Designated Individual 5
7. Random Audits 6
Process 6
Audit Triggers 6
Frequency 6
8. Focused Audits 7
9. Checking the Checker 7
10. Notification to Users 7

PART 1: LEGISLATIVE REFERENCE

The Personal Health Information Act (PHIA)

Additional safeguards for information in electronic form

18(3) A Trustee who maintains personal health information in electronic form shall implement any additional safeguards for such information required by the regulations.

The Personal Health Information Regulation

4(1) In accordance with guidelines set by the minister, a Trustee shall create and maintain or have created and maintained, a record of user activity for any electronic information system it uses to maintain personal health information.

4(2) A record of user activity may be generated manually or electronically.

4(3) In the following circumstances, a record of user activity is not required under this section:

(a) if personal health information is demographic or eligibility information listed in Schedule B, or is information that qualifies or further describes information listed in Schedule B [of the Regulation];

(b) if personal health information is disclosed under the authority of clause 22(2)(h) of the Act (disclosure to a computerized health information network) in a routine and documented transmission from one electronic information system to another;

(c) if personal health information is accessed or disclosed while a Trustee is generating, distributing or receiving a statistical report, as long as the Trustee

(i) maintains a record of the persons authorized to generate, distribute and receive such reports, and

(ii) regularly reviews the authorizations.

4(4) A Trustee shall audit records of user activity to detect security breaches, in accordance with guidelines set by the minister.

4(5) A Trustee shall maintain a record of user activity for at least three years.

4(6) A Trustee shall ensure that at least one audit of a record of user activity is conducted before the record is destroyed.

Schedule B: Demographic and Eligibility Information

- Name
- Signature
- Address
- Telecommunications information
- Sex
- Date of birth
- Date of death
- Family associations
- Eligibility for health care coverage
- Jurisdiction of residence
- Manitoba Health family registration number
- Personal Health Identification Number(PHIN)
- A unique identifier equivalent to the PHIN assigned by another Jurisdiction that pays for health care
- A unique identifier — not including a social insurance number or, except as provided in this Schedule, any other pre-existing identifier — assigned to an individual by a Trustee for its own purposes, when accessed by any Trustee
- A non-Canadian unique health identification number

PART 2: DEFINITIONS

In these guidelines,

Access refers to viewing or reading personal health information maintained within an electronic information system.

Audit Data means data obtained from one or more records of user activity

Audit Trigger means an access to information in an electronic information system that may indicate inappropriate use of personal health information in contravention of legislation and/or organizational policy. An audit trigger may prompt a focused audit.

Focused Audit is an audit of specific user activity based on the need to investigate suspected unauthorized access.

Random Audit is an audit of user activity for randomly selected users.

Record of User Activity (RoUA) means a record about access to personal health information maintained on an electronic information system, which, at minimum, identifies the following:

a) individuals whose personal health information has been accessed,
b) persons who accessed personal health information,
c) when personal health information was accessed,
d) the electronic information system or component of the system in which personal health information was accessed, and
e) whether personal health information that has been accessed is subsequently disclosed under section 22 of the Act.

Security Breach includes a privacy breach.

User Access Role refers to the functionality assigned to a specific user or group of users who require access to personal health information maintained in an electronic information system to do their job (e.g. read/view, add, modify, delete).

PART 3: CREATING A RECORD OF USER ACTIVITY (RoUA)

1. Determining if RoUA Required

A Trustee must review Subsection 4(3) and Schedule B of the Regulation to determine whether a record of user activity is required or whether the electronic information system is exempt (see PART 1: LEGISLATIVE REFERENCE above).

Legacy systems (i.e. systems that were in place or being implemented prior to December 12, 2000) are exempt from the requirement to create and maintain a record of user activity if they lack the functionality to do so, until such time as the system is replaced.

The trustee will work towards becoming compliant when considering an upgrade of any non-compliant legacy system.

2. Providing RoUA to Individuals

Upon request, and in accordance with PART 2 of *The Personal Health Information Act* (PHIA), and subject to the reasons for refusing access set out in Section 11 of the Act, a record of user activity must be provided to the individual the information is about, within the timeframe required by PHIA. This must enable individuals to:

- assess which authorized users, by name, have accessed their information and when, and
- determine compliance with the individual's directives on access to or disclosure of personal health information.

3. Fees

When providing a RoUA to an individual, a trustee may charge a search and preparation fee not exceeding $15.00 for each half-hour in excess of two hours whenever the trustee estimates that search and preparation related to the RoUA will take more than two hours.

When calculating search and preparation time, a trustee shall not include time spent

a. preparing an estimate of fees under this section; or
b. preparing an explanation of an RoUA.

4. Security and Confidentiality of RoUA

Trustees must ensure that sufficient security measures are in place to protect the confidentiality, integrity and availability of records of user activity and audit data. This must include:

- securing access to the records of user activity and audit data,
- safeguarding access to system audit tools to prevent misuse or compromise, and
- documenting all occasions when the audit trail has been out of service or turned off.

PART 4: AUDITING RECORDS OF USER ACTIVITY

5. Description

Auditing records of user activity enables Trustees to assess compliance with organizational and legislative requirements by detecting unauthorized access to personal health information maintained in electronic information systems by authorized system users.

There are two types of audits: 1) random audits, and 2) focused audits.

6. Designated Individual

A Trustee must designate one or more persons who will be responsible for creating and/or auditing records of user activity. The designated individual(s) must:

a) have good working knowledge of what information is maintained in the system and the purpose for which the information was collected, and
b) have a good working knowledge of the levels of access to the system and purposes of user access roles.

7. Random Audits

Process

Trustees will establish a process for conducting random audits. Random audits are conducted to identify possible inappropriate access by users of electronic information systems maintaining personal health information.

The process for a random audit of records of user activity includes:

a) determining reasonable/attainable numbers of users for review as part of an audit,
b) determining reasonable/attainable frequency of audits, and
c) establishing a rotation for routine audits (i.e. varying day/week/month/time of day).

Audit Triggers

Trustees are responsible for determining the triggers appropriate to the system being audited. In determining appropriate triggers for a system, trustees must consider the following:

- information accessed where:
  - the user has the same last name as the individual the record is about
  - the user accesses records of co-workers or staff from another department/facility
  - the user accesses their own record
  - a higher than normal number of users access a particular record
  - a user accesses a particular record an unusually high number of times
  - no action was taken when a record was accessed and the record is of a type which should not be accessed unless action is to be taken
  - the access is outside the user's normal working hours
  - the access does not correspond to the user's role

- access to records of individuals related to
  - publicized/media events (news/crime)
  - VIPs (board members, celebrities, government or community figures, physicians, management staff or other highly publicized individual)
  - highly sensitive diagnosis (HIV, Psychiatric disorders)
  - human resource related events (new hires, employee departures)

Frequency

The following are key issues/risks that should be assessed to determine the frequency of random audits of each electronic information system maintaining personal health information:

- Scope of system
  - Size and complexity
  - Number of users
  - Sensitivity of the information
  - Inter-departmental/facility
  - Systems shared by multiple trustees
  - Cross jurisdictional, cross border systems
  - Third party access (vendors or information managers)

The greater quantity and significance of key issues/risks identified with an electronic information system, the greater the frequency of random audits that should be conducted on that system. Random audits must be of a frequency that reasonably would be expected to act as a deterrent to inappropriate access to and use of personal health information.

8. Focused Audits

Trustees will establish a process for conducting focused audits. A focused audit can be initiated as a result of:

- a trigger in a random audit,
- a complaint filed by the individual the information is about, a staff member or any other person, or
- management/policy requirements.

9. Checking the Checker

Trustees will establish a process for the occasional audit of system administrator records of activity.

10. Notification to Users

Trustees will establish a process to inform system users that auditing occurs. This may be accomplished through:

- staff orientation/refreshers
- user agreements/terms of use
- organizational policies
- splash screens

For more information, contact:

Legislative Unit
Manitoba Health, Seniors and Active Living
300 Carlton Street, Winnipeg, MB R3B 3M9
Phone: (204) 788-6612
Fax: (204) 945-1020
Email: PHIAinfo@gov.mb.ca