

The Personal Health Information Act

A Brief Summary for

INFORMATION MANAGERS

INTRODUCTION

As an information manager, you may be affected by *The Personal Health Information Act*. If you have a service contract with a trustee, then the Act will affect the way you deal with the personal health information maintained by a trustee.

This brief summary is intended to give you some idea of your responsibilities under the Act. *It is not comprehensive*. For a better understanding, you should review the actual legislation and its regulations. Copies are available from Statutory Publications, 200 Vaughan St., Winnipeg, MB R3C 1T5, phone 945-3101. To assist you, this summary will refer to specific sections in the Act.

What is “personal health information”?

Personal health information is any information that:

- is recorded in any form;
- can be linked to an identifiable individual; and
- relates to an individual’s health, health history, genetic makeup, health care, personal health identification number (PHIN) or other identifying information collected in the course of providing health care. *See s. 1(1) of the Act.*

Whom does the Act affect?

For the most part, the Act focuses on the obligations of “trustees” of personal health information. The Act divides trustees into four categories:

- health care facilities (such as hospitals, laboratories, psychiatric facilities and medical clinics);

- some health professionals;
- health-services agencies (organizations that provide health care under an agreement with another trustee—the Victorian Order of Nurses and We Care are two examples); and
- public bodies (such as provincial government departments and agencies, municipal governments, educational institutions and regional health authorities) *See s. 1(1) of the Act.*

However, the Act also recognizes the importance of “information managers” in the health care system and imposes obligations on them in their dealings with personal health information. *See s. 1(1), 25, 63(2) and (3) of the Act.*

What is an “information manager”?

An information manager is a person or body that:

- processes, stores or destroys personal health information;
- provides information management; or
- provides information technology services

for or to a trustee. *See s. 1(1) of the Act.*

What are my obligations as an information manager?

The Personal Health Information Act imposes two types of obligations on information managers:

1. Restrictions and duties set out in the Act or regulations.
2. Restrictions and duties contained in agreements with trustees.



What specific restrictions are imposed on information managers by the Act and the regulations?

As an information manager you must abide by two restrictions:

1. You may take possession of or gain access to the personal health information contained in records only if this is necessary to perform your legitimate functions within the health care system. That is, you can use personal health information only to:
 - process, store or destroy personal health information;
 - provide information management; or
 - provide information technology services for or to a trustee. *See s. 25(2) of the Act.*
2. Further to these limits, you may use personal health information only in circumstances in which the trustee on whose behalf you are acting would be permitted to access the information. In other words, it would be a violation of the Act for you to possess or access personal health information if the trustee who had contracted that service was not permitted to do so. *See s. 25(2) of the Act.*

Clearly, you should learn as much as possible about the limitations and duties the Act places on the trustees with which you do business. You would be well advised to examine the Act to determine the limitations placed on these trustees.

What duties are imposed by the Act on information managers?

Essentially, the Act imposes only one duty—to comply with the Act and the regulations in ensuring the security of the personal health information in your control.

What are the security safeguards set out in the Act and regulations?

You must create and comply with written security policies. Among other things, these policies must contain:

- methods to identify individuals (people/employees) who are required to have access to specific personal health information;
- procedures for preventing unauthorized access to personal health information; and
- plans for recording security breaches and responding to them.

In addition, each employee and agent of an information manager must sign a pledge of confidentiality before dealing with personal health information.

Specific regulations address physical and environmental security arrangements used by information managers, as well as safeguards for personal health information stored or transferred electronically.

Like trustees, information managers must conduct an annual review of their security arrangements and remedy any deficiencies that are identified.

What obligations are imposed on information managers by contracts with trustees?

By definition, individuals or corporations cannot be information managers unless they provide specific services to a trustee. Trustees may not provide personal health information without a written agreement, which must contain provisions that ensure that the personal health information will be adequately protected from unauthorized access, use, disclosure, destruction or alteration. *See s. 25(3) of the Act.* Information managers who fail to observe such an agreement will violate the Act. *See s. 25(4)(b) of the Act.*

What penalties does the Act provide for?

The Act permits a judge to impose a fine of up to \$50,000 for a violation of the Act. ***See s. 64(1) of the Act.*** Moreover, this fine may be imposed for every day that a violation continues. ***See s. 63(5) of the Act.***

The Act applies to all information managers, whether individuals or corporations. However, in addition to allowing the prosecution of a corporation, the Act specifically permits the prosecution and punishment of any director or officer of a corporation who has “authorized, permitted or acquiesced” in an offence. ***See. s. 64(2) of the Act.***

CONCLUSION

The obligations and restrictions placed on information managers by the Act are similar, and in many cases, identical to those placed on the trustees for which they provide information services. In order to comply with the Act and avoid significant penalties for non-compliance, you should fully acquaint yourself with how the Act applies to the trustees with which you do business.