IPC GUIDE TO HIPA

The Health Information Protection Act

The following is a tool which can be used by Trustees as a guide to interpreting The Health Information Protection Act (HIPA). The guidance provided is non-binding and every matter should be considered on a case-by-case basis. In some instances, trustees wish to seek legal advice.
## IPC GUIDE TO HIPA

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed Table of Contents</td>
<td>2</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>11</td>
</tr>
<tr>
<td>When Does HIPA Apply?</td>
<td>12</td>
</tr>
<tr>
<td>Who is ‘THE’ Trustee?</td>
<td>12</td>
</tr>
<tr>
<td>Rights of the Individual (Part II of HIPA)</td>
<td>15</td>
</tr>
<tr>
<td>Diagram – Types of Consent</td>
<td>21</td>
</tr>
<tr>
<td>Duty of a Trustee to protect personal health information (Part III of HIPA)</td>
<td>24</td>
</tr>
<tr>
<td>Limit on Collection, Use, and Disclosure of Personal Health Information by Trustees (Part IV of HIPA)</td>
<td>35</td>
</tr>
<tr>
<td>Access of Individuals to Personal Health Information (Part V of HIPA)</td>
<td>67</td>
</tr>
<tr>
<td>Diagram – Steps to Respond to an Access to Personal Health Information Request</td>
<td>73</td>
</tr>
<tr>
<td>Diagram - How to grant access to a record that contains personal health information of two individuals (s. 38(1)(b))</td>
<td>81</td>
</tr>
<tr>
<td>Diagram – Steps to Responding to a request for Amendment</td>
<td>90</td>
</tr>
<tr>
<td>Review and Appeal (PART VI of HIPA)</td>
<td>91</td>
</tr>
<tr>
<td>Preliminary Matters (Part I of HIPA)</td>
<td>100</td>
</tr>
<tr>
<td>Commissioner (Part VII of HIPA)</td>
<td>102</td>
</tr>
<tr>
<td>General (Part VIII of HIPA)</td>
<td>107</td>
</tr>
<tr>
<td>The HIPA Regulations</td>
<td>123</td>
</tr>
<tr>
<td>Appendix A – Glossary</td>
<td>149</td>
</tr>
<tr>
<td>Appendix B – Detailed Examples of Safeguards</td>
<td>160</td>
</tr>
<tr>
<td>Appendix C – Privacy Breach Guidelines</td>
<td>165</td>
</tr>
<tr>
<td>Appendix D – What to Expect During a Review with the IPC</td>
<td>173</td>
</tr>
<tr>
<td>Appendix E – Faxing Personal Health Information</td>
<td>180</td>
</tr>
<tr>
<td>Appendix F – When to Disclose Personal Health Information to Family and Friends</td>
<td>186</td>
</tr>
<tr>
<td>Appendix G – De-identified Personal Health Information</td>
<td>187</td>
</tr>
<tr>
<td>Appendix H – Information Sharing Agreements</td>
<td>189</td>
</tr>
<tr>
<td>Appendix I – Sample Request for Disclosure to Police Forms</td>
<td>191</td>
</tr>
<tr>
<td>Appendix J – Checklist for Searching for Personal Health Information</td>
<td>193</td>
</tr>
</tbody>
</table>
## DETAILED TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed Table of Contents</td>
<td>2</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>11</td>
</tr>
<tr>
<td>When Does HIPA Apply?</td>
<td>12</td>
</tr>
<tr>
<td>Who is ‘THE’ Trustee?</td>
<td>12</td>
</tr>
<tr>
<td>Rights of the Individual (Part II of HIPA)</td>
<td>15</td>
</tr>
<tr>
<td>Consent required for use or disclosure (section 5)</td>
<td>15</td>
</tr>
<tr>
<td>5(1)</td>
<td>15</td>
</tr>
<tr>
<td>5(2)</td>
<td>15</td>
</tr>
<tr>
<td>Consent (section 6)</td>
<td>18</td>
</tr>
<tr>
<td>6(1)</td>
<td>18</td>
</tr>
<tr>
<td>6(2)</td>
<td>19</td>
</tr>
<tr>
<td>6(3)</td>
<td>19</td>
</tr>
<tr>
<td>6(4)</td>
<td>19</td>
</tr>
<tr>
<td>6(5)</td>
<td>20</td>
</tr>
<tr>
<td>6(6)</td>
<td>20</td>
</tr>
<tr>
<td>Diagram – Types of Consent</td>
<td>21</td>
</tr>
<tr>
<td>Right to revoke consent (section 7)</td>
<td>22</td>
</tr>
<tr>
<td>7(1)</td>
<td>22</td>
</tr>
<tr>
<td>7(2)</td>
<td>22</td>
</tr>
<tr>
<td>7(3)</td>
<td>22</td>
</tr>
<tr>
<td>Right to be informed (section 9)</td>
<td>22</td>
</tr>
<tr>
<td>9(1)</td>
<td>22</td>
</tr>
<tr>
<td>9(2)</td>
<td>23</td>
</tr>
<tr>
<td>9(3)</td>
<td>23</td>
</tr>
<tr>
<td>Right to information about disclosures without consent (section 10)</td>
<td>23</td>
</tr>
<tr>
<td>Right to designate (section 15)</td>
<td>23</td>
</tr>
<tr>
<td>Duty of a Trustee to protect personal health information (Part III of HIPA)</td>
<td>24</td>
</tr>
<tr>
<td>Duty to Protect (section 16)</td>
<td>24</td>
</tr>
<tr>
<td>16(a)</td>
<td>24</td>
</tr>
<tr>
<td>16(b)</td>
<td>25</td>
</tr>
<tr>
<td>16(c)</td>
<td>25</td>
</tr>
<tr>
<td>Retention and Destruction Policy (section 17)</td>
<td>25</td>
</tr>
<tr>
<td>17(1)</td>
<td>25</td>
</tr>
<tr>
<td>IPC Guide to HIPA</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>17(2)(a)........................................................................................................................................... 26</td>
<td></td>
</tr>
<tr>
<td>17(2)(b)........................................................................................................................................... 27</td>
<td></td>
</tr>
<tr>
<td>Information management service provider (section 18) ....................................................................... 28</td>
<td></td>
</tr>
<tr>
<td>18(1)............................................................................................................................................... 28</td>
<td></td>
</tr>
<tr>
<td>18(3)............................................................................................................................................... 29</td>
<td></td>
</tr>
<tr>
<td>18(5)............................................................................................................................................... 30</td>
<td></td>
</tr>
<tr>
<td>Comprehensive Health Record (section 18.1) ...................................................................................... 30</td>
<td></td>
</tr>
<tr>
<td>Duty to collect accurate information (section 19) ............................................................................ 31</td>
<td></td>
</tr>
<tr>
<td>Duty where one trustee discloses to another (section 20) .............................................................. 31</td>
<td></td>
</tr>
<tr>
<td>Duty where disclosing to persons other than trustees (section 21) ................................................ 32</td>
<td></td>
</tr>
<tr>
<td>21(a)............................................................................................................................................... 32</td>
<td></td>
</tr>
<tr>
<td>21(b)............................................................................................................................................... 32</td>
<td></td>
</tr>
<tr>
<td>Continuing duties of trustees (section 22) ......................................................................................... 33</td>
<td></td>
</tr>
<tr>
<td>22(1)............................................................................................................................................... 33</td>
<td></td>
</tr>
<tr>
<td>22(2) and 22(2.1)........................................................................................................................... 33</td>
<td></td>
</tr>
<tr>
<td>22(3)............................................................................................................................................... 33</td>
<td></td>
</tr>
<tr>
<td>Limit on Collection, Use, and Disclosure of Personal Health Information by Trustees (Part IV of HIPA)</td>
<td>35</td>
</tr>
<tr>
<td>Collection, use and disclosure on need-to-know basis (section 23) .............................................. 35</td>
<td></td>
</tr>
<tr>
<td>23(1)............................................................................................................................................... 35</td>
<td></td>
</tr>
<tr>
<td>Need-to-know principle ..................................................................................................................... 35</td>
<td></td>
</tr>
<tr>
<td>Data minimization principle .............................................................................................................. 35</td>
<td></td>
</tr>
<tr>
<td>Circle of Care vs. Need-to Know ...................................................................................................... 35</td>
<td></td>
</tr>
<tr>
<td>23(2)............................................................................................................................................... 36</td>
<td></td>
</tr>
<tr>
<td>23(4)............................................................................................................................................... 36</td>
<td></td>
</tr>
<tr>
<td>Restrictions on collection (section 24) .............................................................................................. 37</td>
<td></td>
</tr>
<tr>
<td>24(1)............................................................................................................................................... 37</td>
<td></td>
</tr>
<tr>
<td>24(2)............................................................................................................................................... 37</td>
<td></td>
</tr>
<tr>
<td>24(3)............................................................................................................................................... 37</td>
<td></td>
</tr>
<tr>
<td>Manner of collection (section 25) ...................................................................................................... 38</td>
<td></td>
</tr>
<tr>
<td>25(1)............................................................................................................................................... 38</td>
<td></td>
</tr>
<tr>
<td>25(1)(a)............................................................................................................................................ 39</td>
<td></td>
</tr>
<tr>
<td>25(1)(b)............................................................................................................................................ 39</td>
<td></td>
</tr>
<tr>
<td>25(1)(c)............................................................................................................................................ 39</td>
<td></td>
</tr>
</tbody>
</table>
42(3) ....................................................................................................................................... 94
Review or refusal to review (section 43).................................................................................. 94
43(1) ....................................................................................................................................... 94
43(2) ....................................................................................................................................... 94
Notice of intention to review (section 44) ................................................................................ 97
Conduct of review (section 45) ................................................................................................. 97
45(1) ....................................................................................................................................... 97
45(2) ....................................................................................................................................... 97
45(3) ....................................................................................................................................... 97
Powers of commissioner (section 46) ....................................................................................... 98
46(1) ....................................................................................................................................... 98
46(2)-(3) .................................................................................................................................. 98
Burden of proof (section 47) .................................................................................................... 98
Commissioner to report (section 48) ........................................................................................ 99
Decision of trustee (section 49) ................................................................................................ 99
Appeal to court (section 50) .................................................................................................... 99
Preliminary Matters (Part I of HIPA) ...................................................................................... 100
Application of Act (section 3) ................................................................................................. 100
3(2) ....................................................................................................................................... 100
Act prevails (section 4) ........................................................................................................... 101
4(1) – (3) ............................................................................................................................... 101
4(4) and 4(6) ........................................................................................................................ 101
Commissioner (Part VII of HIPA) .......................................................................................... 102
Privacy powers of commissioner (section 52) ........................................................................ 102
52(a) ..................................................................................................................................... 102
52(b) ..................................................................................................................................... 102
52(c) ...................................................................................................................................... 103
52(d) ..................................................................................................................................... 103
52(e) ..................................................................................................................................... 104
General powers of commissioner (section 53) ....................................................................... 104
Confidentiality (section 54)..................................................................................................... 104
54(1) – (2) ............................................................................................................................. 105
54(3) ..................................................................................................................................... 105
54(4) ..................................................................................................................................... 105
Administrative safeguards ................................................................. 160
Technical Safeguards ........................................................................... 163
Physical Safeguards ............................................................................ 164
Appendix C – Privacy Breach Guidelines .................................................. 165
What is a Privacy Breach? ................................................................. 165
When does a Privacy Breach Occur? ...................................................... 165
What is Privacy? .................................................................................. 165
There’s been a Privacy Breach – Now What? ........................................ 166
Contain the Breach .............................................................................. 166
Notification .......................................................................................... 166
Investigate the Breach ........................................................................ 167
Prevent Future Breaches ..................................................................... 167
Privacy Breach Report ......................................................................... 168
When Employee Snooping is Suspected .................................................. 168
What Can I Expect if the IPC is involved? .............................................. 169
What are the advantages of proactively reporting a breach to the IPC? ...... 169
Summary of Investigation Process ........................................................ 169
Informal Resolution ............................................................................. 170
What will be the IPC’s focus? ............................................................... 171
Draft Report ........................................................................................ 171
Commissioner’s Report ...................................................................... 172
The IPC is Paperless ............................................................................. 172
Appendix D – What to Expect During a Review with the IPC. .................. 173
Summary of Review Process ................................................................. 173
Informal Resolution ............................................................................. 174
Preliminary Objections ....................................................................... 174
Notification of the Review ................................................................. 175
Preparing the Record/Index of Records .................................................. 175
Preparing the Submission ................................................................... 176
Timelines and Escalation Policy ............................................................ 177
Sharing of Submissions ...................................................................... 177
Draft Report ........................................................................................ 178
Commissioner’s Report ...................................................................... 178
The IPC is Paperless ............................................................................. 178
ACKNOWLEDGEMENTS

We gratefully acknowledge the numerous sources that were utilized in the development of this resource. This document could not have been created without the many resources published by other Information and Privacy Commissioner’s Offices across the country, other government, and non-government publications. This includes:

- *How to avoid Abandoned Records: Guidelines on the Treatment of Personal Health Information, in the Event of a Change in Practice* – Information and Privacy Commissioner, Ontario
- *Time Extension Request Guidelines for Public Bodies* – Office of the Information and Privacy Commissioner, British Columbia
- *Guidelines on Requirements and Good Practices for Protecting Personal Health Information and Privacy FAQ* – Saskatchewan Medical Association (SMA)
- *Checklist for Compliance with HIPA* – The College of Physicians and Surgeons of Saskatchewan (CPSS)

We have also quoted resources from Canada’s Heath Informatics Association (COACH). For more information on the Coach’s resources, please see [www.coachorg.com](http://www.coachorg.com).
WHEN DOES HIPA APPLY?

In order for HIPA to be engaged, two things must exist:

1. There must be personal health information involved as defined by subsection 2(m) of HIPA; and

2. There must be a trustee involved as defined by subsection 2(t) of HIPA.

In order for there to be a trustee that is required to comply with HIPA, the organization in question must have two things:

1. The organization must be listed at subsection 2(t) of HIPA; and

2. The organization must have custody or control of the personal health information involved.

WHO IS ‘THE’ TRUSTEE?

Subsection 2(t) of HIPA defines who can qualify as a trustee. However, simply because an individual or an organization qualifies as a trustee, it does not mean they would qualify as ‘the’ trustee of personal health information in every circumstance. In order to determine who is ‘the’ trustee, in other words the person or organization who has accountability for the protection of the personal health information in question, the individual must also have custody or control of the personal health information.

Custody is the physical possession of a record by a trustee.

Control connotes authority. A record is under the control of a trustee when the trustee has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. Custody is not a requirement.

The 15 criteria suggested for determining any measure of control is:

1. The record was created by the trustee or a staff member of the trustee in the course of his or her duties performed for the trustee;

2. The record was created by an outside consultant for the trustee;

3. The trustee possesses the record, either because it has been voluntarily provided by the creator or pursuant to a mandatory or statutory or employment requirement;

4. An employee of the trustee possesses the record for the purposes of his or her duties performed for the trustee;

5. The record is specified in a contract as being under the control of a trustee and there is no understanding or agreement that the records are not to be disclosed;

6. The content of the record relates to the trustee’s mandate and core, central or basic functions;

7. The trustee has a right of possession of the record;
8. The trustee has the authority to regulate the record’s use and disposition;
9. The trustee paid for the creation of the records;
10. The trustee has relied upon the record to a substantial extent;
11. The record is closely integrated with other records held by the trustee;
12. A contract permits the trustee to inspect, review and/or possess copies of the records the contractor produced, received or acquired;
13. The trustee’s customary practice in relation to possession or control of records of this nature in similar circumstances;
14. The customary practice of other trustees in relation to possession or control of records of this nature in similar circumstances; and
15. The owner of the records.

All 15 criteria do not have to be met in order to find that a trustee has a measure of control. The Saskatchewan Medical Association’s Guidelines on Requirements and Good Practices for Protecting Personal Health Information reference manual provides the following considerations to determine who is ‘the’ trustee (which we have adapted for this Guide):

NOTE: In this context, the term “health professional” is used to describe an individual who could qualify as a trustee. (As an example: physician, nurses, dentists, etc.)

1. Is the health professional collecting, using or disclosing personal health information as an employee of a trustee?
   If so, the health professional is not ‘the’ trustee. The health professional needs to be aware of and meet the obligations contained within HIPA, as there are specific offence provisions for the employees of trustees. They would also be expected to be aware of and follow all of the trustees’ privacy policies and procedures.

   However, if the health professional is an employee of a non-trustee such as a private company the health professional should consider whether he/she has custody or control of the personal health information.

2. Is the health professional part of a group practice?
   It is very common for a group of health professionals to establish a group practice, whether it is a legal entity or a group of health professionals in a shared space using some common services.

   Health professionals must determine if they have sole custody or control of their patients’ records or if this responsibility is shared with the other health professionals in the practice.

   Where health professionals in one medical practice each have their own separate database within the EMR and accordingly, sole custody or control of their patient’s personal health information there is an expectation that they develop common approaches to protecting the personal health information, including a single policy manual for the entire practice.

   Three questions to consider are:
   1. Does each health professional have his/her own EMR or a separate patient list within a common EMR?
2. Do employees, medical students and residents, work for just one health professional?

3. If the health professional were to leave the current location of practice could he/she take the records or a copy of them to a new practice location?

If the answers to these questions are yes then each health professional is solely accountable for the personal health information under his/her custody or control and must meet his/her duties under HIPA.

If a health care professional is in any group practice situation, they should have strong information sharing agreements in place with the other healthcare professionals involved. See Appendix H – for more information about information sharing agreements.

Where several physicians in one medical practice share a single, common database within the EMR, it is essential the physicians develop a common approach to protecting the personal health information and develop a single policy manual for the entire practice.
RIGHTS OF THE INDIVIDUAL (PART II OF HIPA)

Consent required for use or disclosure (section 5)

5(1) Subject to subsection (2), an individual has the right to consent to the use or disclosure of personal health information about himself or herself.

(2) A trustee shall use or disclose personal health information about an individual only:
   
   (a) with the consent of the subject individual; or

   (b) in accordance with a provision of this Act that authorizes the use or disclosure.

(3) Repealed. 2003, c.25, s.5.

(4) Repealed. 2003, c.25, s.5.

5(1)
This subsection provides an individual the right to consent to the use or disclosure of his/her personal health information by a trustee.

See section 6 of HIPA.

5(2)
A trustee can only use or disclose personal health information if:

- they have the consent of the individual; or

- a section of HIPA allows a trustee to use or disclose the information without consent.
### Circumstances Where Consent is not Required for the Use or Disclosure of Personal Health Information by a Trustee

<table>
<thead>
<tr>
<th>Section</th>
<th>Explanation of Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>27(2)(a)</td>
<td>For the purpose for which the information was collected by the trustee or for a purpose that is consistent with that purpose.</td>
</tr>
<tr>
<td>27(2)(b)</td>
<td>For the purpose of arranging, assessing the need for, providing, continuing or supporting the provision of, a service requested or required by the subject individual.</td>
</tr>
</tbody>
</table>
| 27(2)(c) | To the subject individual’s next of kin or someone with whom the subject individual has a close personal relationship if:  
• the disclosure relates to health services currently being provided to the subject individual; and  
• the subject individual has not expressed a contrary intention to a disclosure of that type. |
| 27(4)(a) | Where the trustee believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person. |
| 27(4)(b) | Where the opinion believes that disclosure is necessary for monitoring, preventing or revealing fraudulent, abusive or dangerous use of publicly funded health services. |
| 27(4)(c) | Where the disclosure is being made to a trustee that is the successor of the trustee that has custody or control of the information, if the trustee makes a reasonable attempt to inform the subject individuals of the disclosure. |
| 27(4)(d) | To a person who, pursuant to *The Health Care Directives and Substitute Health Care Decision Makers Act*, is entitled to make a health care decision, as defined in that Act, on behalf of the subject individual, where the personal health information is required to make a health care decision with respect to that individual. |
| 27(4)(e) | If the subject individual is deceased:  
• where the disclosure is being made to the personal representative of the subject individual for a purpose related to the administration of the subject individual’s estate; or  
• where the information relates to circumstances surrounding the death of the subject individual or services recently received by the subject individual, and the disclosure:  
  o is made to a member of the subject individual’s immediate family or to anyone else with whom the subject individual had a close personal relationship; and  
  o is made in accordance with established policies and procedures of the trustee, or where the trustee is a health professional, made in accordance with the ethical practices of that profession. |
<p>| 27(4)(f) | Where the disclosure is being made in accordance with section 22 to another trustee or an information management service provider that is a designated archive. |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Explanation of Act</th>
</tr>
</thead>
</table>
| 27(4)(g)  | Where the disclosure is being made to a standards or quality of care committee established by one or more trustees to study or evaluate health services practice in a health services facility, health region or other health service area that is the responsibility of the trustee, if the committee:  
• uses the information only for the purpose for which it was disclosed;  
• does not make a further disclosure of the information; and  
• takes reasonable steps to preserve the confidentiality of the information. |
| 27(4)(h)  | Subject to subsection (5), where the disclosure is being made to a health professional body or a prescribed professional body that requires the information for the purposes of carrying out its duties pursuant to an Act with respect to regulating the profession. |
| 27(4)(i)  | Where the disclosure is being made for the purpose of commencing or conducting a proceeding before a court or tribunal or for the purpose of complying with:  
• an order or demand made or subpoena or warrant issued by a court, person or body that has the authority to compel the production of information; or  
• rules of court that relate to the production of information. |
| 27(4)(j)  | Subject to subsection (6), where the disclosure is being made for the provision of health or social services to the subject individual, if, in the opinion of the trustee, disclosure of the personal health information will clearly benefit the health or well-being of the subject individual, but only where it is not reasonably practicable to obtain consent. |
| 27(4)(k)  | Where the disclosure is being made for the purpose of:  
• obtaining payment for the provision of services to the subject individual; or  
• planning, delivering, evaluating or monitoring a program of the trustee. |
| 27(4)(l)  | Where the disclosure is permitted pursuant to any Act or regulation.                                                                                                                                               |
| 27(4)(m)  | Where the disclosure is being made to the trustee’s legal counsel for the purpose of providing legal services to the trustee.                                                                                           |
| 27(4)(n)  | In the case of a trustee who controls the operation of a pharmacy as defined in The Pharmacy Act, 1996, a physician, a dentist or the minister, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to The Medical Profession Act, 1981 and approved by the minister. |
| 27(4)(o)  | In the case of a trustee who controls the operation of a pharmacy as defined in The Pharmacy Act, 1996, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to The Pharmacy Act, 1996 and approved by the minister. |
| 27(4)(p)  | In prescribed circumstances.                                                                                                                                                                                    |
Consent (section 6)

6(1) Where consent is required by this Act for the collection, use or disclosure of personal health information, the consent:

(a) must relate to the purpose for which the information is required;
(b) must be informed;
(c) must be given voluntarily; and
(d) must not be obtained through misrepresentation, fraud or coercion.

(2) A consent to the collection, use or disclosure of personal health information is informed if the individual who gives the consent is provided with the information that a reasonable person in the same circumstances would require in order to make a decision about the collection, use or disclosure of personal health information.

(3) A consent may be given that is effective for a limited period.

(4) Consent may be express or implied unless otherwise provided.

(5) An express consent need not be in writing.

(6) A trustee, other than the trustee who obtained the consent, may act in accordance with an express consent in writing or a record of an express consent having been given without verifying that the consent meets the requirements of subsection (1) unless the trustee who intends to act has reason to believe that the consent does not meet those requirements.

Note: See the diagram related to the types of consent that appears in this Guide.

6(1)
In order to obtain true consent, a trustee must ensure it meets all of the elements listed in subsections 6(1)(a) through (d) which includes:

(a) Once consent has been given, a trustee can only use personal health information required for the purposes for which consent has been applied. In other words, the data-minimization principle applies and a trustee should collect, use or disclose the least amount of identifying information as necessary.

(b) True consent must be informed consent. It is best practice that the subject individual understand:

i) The specific personal health information to be collected, used or disclosed;
ii) Anticipated uses and/or disclosures;
iii) To whom the personal health information may be disclosed;
iv) The date the consent is effective and the date on which the consent expires; and
v) Any potential risks associated with the collection, use or disclosure.

See section 9 and section 6(2) of HIPA for more information.

(c) Must be given voluntarily.

(d) Must not be obtained through misrepresentation, fraud or coercion.
When a trustee is obtaining consent, they must provide the subject individual with as much information as a reasonable person in the same circumstances would require in order to make a decision about the collection, use or disclosure. This would generally include:

- The specific personal health information to be collected, used or disclosed;
- Anticipated uses and/or disclosures;
- To whom the personal health information may be disclosed;
- The date the consent is effective and the date on which the consent expires; and
- Any potential risks associated with the collection, use or disclosure.

Consent may be given for a limited period. If consent is given orally, the trustee should make note of this time period in the individual’s record.

Unless explicitly noted in HIPA, consent may be express or implied.

**EXPRESS CONSENT**

Express consent can be written (e.g. form or letter) or verbal (see subsection 6(5) of HIPA). It must be informed. It is best practice that the subject individual understand the following conditions:

- The specific personal health information to be collected, used or disclosed;
- Anticipated uses and/or disclosures;
- To whom the personal health information may be disclosed;
- The date the consent is effective and the date on which the consent expires; and
- Any potential risks associated with the collection, use or disclosure.

See the diagram related to the types of consent that appears in this Guide or subsection 6(5).

**IMPLIED CONSENT**

For implied consent to be valid trustees must first meet a number of conditions. The consent to the collection, use or disclosure of personal health information by a trustee may only be implied if:

- In all circumstances, the purpose of the collection, use or disclosure is or will become reasonably obvious to the individual.
- It is reasonable to expect that the individual would consent to the collection use or disclosure.
- The trustee is not aware that the individual withdrew consent.
- The trustee uses or discloses the information for no other purpose other than the purpose for which it was collected.
- The individual has the right to “opt out”.
The intent of an implied consent is to enable a trustee to use or disclose personal health information for a purpose that is consistent with the purposes for which it was originally collected, without seeking further consent.

See the diagram related to the types of consent that appears in this Guide

6(5)
An express consent need not be in writing. It can be given orally by the patient. The trustee, however, should note the consent in the individual’s record. This would include the date consent was given as well as:

- The specific personal health information to be collected, used or disclosed;
- Anticipated uses and/or disclosures;
- To whom the personal health information may be disclosed;
- The date the consent is effective and the date on which the consent expires; and
- Any potential risks associated with the collection, use or disclosure that were discussed with the individual.

6(6)
A trustee may rely on the express consent obtained by another trustee if it involves the same personal health information and collections, uses and disclosures. However, if the trustee does not believe that the original consent meets all of the requirements, then the trustee should obtain consent again. Trustees should have a process in place to ensure consent has been obtained before collecting personal health information.

For example, if Trustee A obtains consent to disclose personal health information with Trustee B than Trustee B can rely on the consent to collect the personal health information.
Diagram – Types of Consent

Types of Consent in HIPA

Consent means informed, voluntary agreement with what is being done or proposed with respect to the collection, use or disclosure of personal health information.

Express Consent

Implied Consent

No Consent (Deemed)

What Is It and What Is Required?

The highest standard of consent. Express consent can be written or verbal (s. 6.5 of HIPA). Express consent must be informed and meet all the following conditions:

- the specific personal health information to be collected, used or disclosed;
- anticipated uses and/or disclosures;
- to whom the personal health information may be disclosed;
- the date the consent is effective and the date on which the consent expires; and
- any potential risks associated with the collection, use or disclosure.

For implied consent to be valid trustees must first meet a number of conditions:

- in all circumstances, the purpose of the collection, use or disclosure is or will become reasonably obvious to the individual;
- it is reasonable to expect that the individual would consent to the collection, use or disclosure;
- the trustee is not aware that the individual withdrew consent;
- the trustee uses or discloses the information for no other purpose other than the purpose for which it was collected;
- the individual has the right to "opt out".

A trustee can forgo express or implied consent in certain circumstances, such as when an individual is unable to give consent, is unconscious or in emergency circumstances. See subsection 27(1) of HIPA.

When Is It Appropriate?

Abigail HIPA requires the patient’s express consent for providing his or her personal health information in response to a third party request (e.g., insurance company, patient’s lawyer, research) that is not directly related to the patient’s health care or treatment.

The intent of an implied consent is to enable a trustee to use or disclose personal health information for a purpose that is consistent with the purposes for which it was originally collected, without seeking further consent.

Only in emergency circumstances:

- individual is unable (i.e., unconscious);
- urgent/imminent risk to health or safety.

This relates to The Health Information Protection Act (HIPA).

Office of the Saskatchewan Information and Privacy Commissioner

www.oipc.sk.ca
Right to revoke consent (section 7)

7(1) An individual may revoke his or her consent to the collection of personal health information or to the use or disclosure of personal health information in the custody or control of a trustee.

(2) A consent may be revoked at any time, but no revocation shall have retroactive effect.

(3) A trustee must take all reasonable steps to comply with a revocation of consent promptly after receiving the revocation.

7(1)
At any time, an individual may revoke consent previously given to a trustee to collect, use or disclose personal health information. This applies to implied consent and express consent.

7(2)
Consent maybe revoked at any time. However, a trustee does not have to take steps to undo the actions it took when the consent was in effect.

Example: Consent was obtained to allow a trustee to disclose personal health information of an individual on a weekly basis. Consent was then revoked. The trustee must stop the weekly disclosure of personal health information but does not have to retrieve the personal health information that has already been disclosed.

7(3)
Once a revocation of consent is made, a trustee should take immediate steps to honour the individual's wishes.

Right to be informed (section 9)

9(1) An individual has the right to be informed about the anticipated uses and disclosures of the individual's personal health information.

(2) When a trustee is collecting personal health information from the subject individual, the trustee must take reasonable steps to inform the individual of the anticipated use and disclosure of the information by the trustee.

(3) A trustee must establish policies and procedures to promote knowledge and awareness of the rights extended to individuals by this Act, including the right to request access to their personal health information and to request amendment of that personal health information.

9(1)
An individual has a right to know any anticipated uses or disclosures of his/her personal health information. A trustee should be able to let the individual know if asked. Best practice would be to promote the individual's awareness before he/she asked.
9(2)
When collecting personal health information, a trustee should let the individual know how the information is likely to be used and to whom it is likely to be disclosed.

9(3)
A trustee must have policies and procedures to promote patient/client awareness of:

- Privacy rights described in HIPA;
- Right to access personal health information;
- Right to request an amendment; and
- Right of a review of a decision by the Commissioner.

Right to information about disclosures without consent (section 10)

10(1) A trustee must take reasonable steps to ensure that the trustee is able to inform an individual about any disclosures of that individual’s personal health information made without the individual’s consent after the coming into force of this section.

(2) This section does not apply to the disclosure of personal health information for the purposes or in the circumstances set out in subsection 27(2).

Trustees should be able to notify the subject individual of any disclosure made without the individual’s consent, unless made in accordance with subsection 27(2) of HIPA.

This includes disclosures made on purpose or by accident. Disclosures made that are not in compliance with sections 27, 28 or 29 of HIPA constitute privacy breaches. For more information, please see Appendix C – Privacy Breach Guidelines.

Right to designate (section 15)

15 An individual may designate in writing another person to exercise on behalf of the individual any of the individual’s rights or powers with respect to personal health information.

Any individual can provide authorization to another person to act on his/her behalf. Such authorization must be in writing, and can provide authority to the representative to exercise any right or undertake any power, including the right to provide consent under various provisions of the Act, or simply the right to access the individual’s health information.

The authorization must be signed by the individual, and preferably witnessed.

Please see Appendix F – When to Disclose Personal Health Information to Family and Friends.
Duty of a Trustee to Protect Personal Health Information (Part III of HIPA)

Part III of HIPA outlines general duties for trustees with respect to protecting personal health information. This section of this guide will discuss these duties. It will guide trustees on what is required to meet these sections of HIPA.

Duty to Protect (section 16)

Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:

(a) protect the integrity, accuracy and confidentiality of the information;
(b) protect against any reasonably anticipated:
   (i) threat or hazard to the security or integrity of the information;
   (ii) loss of the information; or
   (iii) unauthorized access to or use, disclosure or modification of the information; and
(c) otherwise ensure compliance with this Act by its employees.

See also subsection 23(2) of HIPA.

Section 16 of HIPA requires that a trustee have administrative, technical and physical safeguards to protect personal health information.

Administrative safeguards are controls that focus on internal organization, policies, procedures and maintenance of security measures that protect personal health information.

Technical Safeguards are the technology and the policy and procedures for its use that protect personal health information and control access to it.

Physical Safeguards are physical measures, policies, and procedures to protect personal health information and related buildings and equipment, from unauthorized intrusion and natural and environmental hazards.

See Appendix B - Detailed Examples of Safeguards for more information.

16(a)

Integrity refers to the condition of information being whole or complete; not modified, deleted or corrupted.

Confidentiality implies a trust relationship between the person supplying information and the individual or organization collecting or using it.
16(b)

**Threat** means a sign or cause of possible harm.

**Hazard** means a risk, peril or danger.

**Security** means a condition of safety or freedom from fear or danger.

**Unauthorized access** occurs when individuals have access to personal health information that they do not need-to-know, either by accident or on purpose. This would also qualify as either an unauthorized use or unauthorized disclosure.

**Unauthorized collection** occurs when personal health information is collected, acquired, received or obtained by any means for purposes that are not allowed under sections 23, 24 or 25 of HIPA.

**Unauthorized use** refers to the use of personal health information for a purpose that is not authorized under sections 23 and 26 of HIPA.

**Unauthorized disclosure** refers to the act of revealing, showing, providing copies, selling, giving, or relaying the content of personal health information in ways that are not permitted under sections 23, 27, 28, 29, and 30.

16(c)

**Trustees** should have education programs in place for their employees which addresses the trustee’s duties under HIPA, safeguards the trustee has established, the need-to-know and consequences for violating HIPA.

---

**Retention and Destruction Policy (section 17)**

17(1) Not yet proclaimed.

(2) A trustee must ensure that:

(a) personal health information stored in any format is retrievable, readable and useable for the purpose for which it was collected for the full retention period of the information established in the policy mentioned in subsection (1); and

(b) personal health information is destroyed in a manner that protects the privacy of the subject individual.

Section 17 of HIPA places duties on trustees to store (or retain) and destroy personal health information in secure ways.

17(1)

Subsection 17(1) is not yet proclaimed by the legislature. However, the intent of this clause is to provide trustees with guidance on how long personal health information is to be kept.

Even though subsection 17(1) is not proclaimed, trustees should still have a written records retention and disposition schedule (see Appendix B - Detailed Examples of Safeguards for
This outlines all the types of personal health information that a trustee possesses and how long it will be retained. Trustees should consult with their respective regulatory body for guidance when setting these timelines.

Some of the advantages of having a written retention and disposition schedule are as follows:

- HIPA compliance;
- A trustee can better respond to an access request for personal health information that has been destroyed; and
- Holding on to personal health information when it is no longer necessary to do so can be expensive and be a liability with respect to potential privacy breaches.

Further the trustee should have had destruction policies and procedures that explicitly describe all steps that the trustee and staff must take to prepare records for destruction. A trustee should keep records of what has been destroyed, such as destruction certificates.

When an IMSP is used for the destruction of personal health information proper agreements should be in place (see section 18 of HIPA).

Other considerations include The Hospital Standards Regulations, 1980 which reads as follows:

15(1) Subject to subsection (2), the patient’s health record shall be retained by the hospital for a minimum period of ten years from the date of last discharge or until age nineteen if the patient is a minor, whichever period is the longer or for such further period as may be deemed necessary by the hospital after consultation with the medical staff.

(2) Where microfilming is employed, the health record must be retained in its original form for a minimum period of six complete years, and the microfilm must be retained for the remainder of the retention period mentioned in subsection (1).

The Saskatchewan Medical Association’s website recommends the following:

- The College of Physician and Surgeons requires that records be held for six years after the patient was last seen. Records of pediatric patients shall be retained until two years past the age of majority or six years after the date last seen, whichever may be the later date.
- The Canadian Medical Protective Association recommends that members keep medical records for at least 10 years from the date of last entry or, in the case of minors, 10 years from when the age of majority is reached or 10 years from the last entry, whichever is greater.
- The trustee needs to ensure that they have a policy and procedure in place that establishes the retention period and the process for destruction and storage of the medical records.

17(2)(a) Not only do trustees have a duty to protect personal health information from inappropriate disclosure, accidental or otherwise, they also have a duty to ensure it is retrievable, readable and usable. In other words, subsection 17(2)(a) requires trustees to organize personal health information in its custody or control.
**Retrievable** means that the trustee must be able to access personal health information with reasonable ease when required to do so. For example, personal health information should not be stored in an outdated format that can no longer be processed or interpreted by current software (ie. microfiche).

**Readable** means that the personal health information is able to be read or legible. For example, paper files containing personal health information that experience water damage may no longer be legible.

Maintaining personal health information properly allows trustees to more easily respond to the access provisions of HIPA and provide care to individuals.

**17(2)(b)**

Subsection 17(1)(b) requires trustees to destroy personal health information in a secure manner. The IPC has issued several reports discussing the practices used by trustees for destruction of personal health information.

Cross shredding of physical copies of personal health information is reliable and standard. However, the lead up to shredding is just as important. It is important that the decision to destroy personal health information is made by someone with a need-to-know and destruction occurs as soon as possible after the decision has been made. The following are some examples of non-compliance by trustees:

- Investigation Report H-2011-001 – The trustee had lost track of some physical files containing personal health information under its custody and control. The files eventually wound up in a recycle bin without having been shredded.

- Investigation Report H-2013-002 – The trustee hired an IMSP to destroy records containing personal health information on its behalf. However, they were found in the yard of the IMSP. Even though the displacement of the personal health information was the result of actions by an employee of the IMSP, the Commissioner found the trustee was responsible for the actions of its IMSP. The Commissioner found that the trustee had inadequate safeguards in place to ensure the proper destruction of the addressograph cards in question.

- Investigation Report H-2013-003 – This trustee’s process for destruction of personal health information was long and convoluted. It involved those without a need-to-know having responsibility for the destruction of personal health information. Personal health information was also found in a dumpster.

- Investigation Report 077-2014 – The trustee did not keep track of those who were assigned to “strip files” and then destroy personal health information. Many did not have a need-to-know. Those staff members did not receive helpful or consistent instructions. Further, proper safeguards were not in place during the process.

- Investigation Report 107-2015 – A trustee had an agreement with a chicken farm to destroy personal health information. The Commissioner found this was an inappropriate practice and the trustee did not meet its obligation under 17(2)(b).

Trustees must also be mindful of the destruction of electronic personal health information. This includes the safe destruction of hardware from computers, fax machines, photocopiers, mobile devices, etc. that may retain personal health information once the device is no longer useable.
Trustees who also qualify as government institutions must also be aware of the requirements of *The Archives and Public Records Management Act*.

### Information management service provider (section 18)

18(1) A trustee may provide personal health information to an information management service provider:

(a) for the purpose of having the information management service provider process, store, archive or destroy the personal health information for the trustee;

(b) to enable the information management service provider to provide the trustee with information management or information technology services;

(c) for the purpose of having the information management service provider take custody and control of the personal health information pursuant to section 22 when the trustee ceases to be a trustee; or

(d) for the purpose of combining records containing personal health information.

(2) Not yet proclaimed.

(3) An information management service provider shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection (1).

(4) Not yet proclaimed.

(5) If a trustee is also an information management service provider and has received personal health information from another trustee in accordance with subsection (1), the trustee receiving the information is deemed to be an information management service provider for the purposes of that personal health information and does not have any of the rights and duties of a trustee with respect to that information.

18(1) A trustee can engage an IMSP for the purposes described in subsection 18(1). However, trustees must understand that they continue to be responsible for the personal health information that they have provided to the IMSP. HIPA continues to apply to both the trustee and the personal health information.

It is essential for trustees to have detailed written agreements in place when engaging an IMSP. This includes:

- identifying the objectives of the agreement and the principles to guide the agreement;
- whether the IMSP is permitted to collect personal health information and if so, a description of that information and the purposes for which it may be collected;
- whether the IMSP may use personal health information provided to it by the trustee and if so, a description of that information and the purposes for which it may be used;
- whether the IMSP may disclose personal health information provided to it by the trustee and if so, a description of that information and the purpose for which it may be disclosed;
• the process for the IMSP to respond to access requests or requests to amend or correct personal health information or for the IMSP to refer access requests to the trustee;
• where applicable, how the IMSP should address an individual’s express wish relating to the disclosure of personal health information; and
• how personal health information is to be protected, managed, returned, or destroyed by the IMSP in accordance with HIPA.

Information sharing agreements should have the following components:

- Define what personal health information means.
- Describe the purpose for information sharing.
- Reference all applicable legislation that provides the legal authority for collection.
- Establish an understanding of who has custody and control.
- Identify the type of information that each party will share with each other.
- Identify the uses for the information and limitations on the uses to the specified purpose.
- Describe who will have access and under what conditions.
- Describe how the information will be exchanged.
- Describe the process for ensuring accuracy.
- Describe the process for managing privacy breaches, complaints, and incidents.
- Identify retention periods.
- Identify secure destruction methods when retention expires.
- Describe the security safeguards in place to protect information.
- Describe termination of the agreement procedures.

Also see the IPC’s resource Best Practices for Information Sharing Agreements available at: https://oipc.sk.ca/assets/best-practices-for-information-sharing-agreements.pdf

18(3)
An IMSP may collect, use, disclose or access the personal health information provided by the trustee only for the purposes authorized by an agreement. The IMSP must comply with HIPA and the regulations as described in an agreement. An IMSP cannot collect, use, disclose or access the personal health information for any other purpose.

Trustee should periodically audit the policies, procedures and performance of the IMSP to ensure compliance with HIPA. The trustee’s ability to do so should be outlined in the agreement. There should also be provision for remedies such as cancellation of the agreement in the event that the IMSP fails to meet its terms and conditions or fails to comply with HIPA or the regulations.

See section 64(2) for consequences for IMSPs
In the event that a trustee is taking on an IMSP role for another trustee, it is especially important to have clear, detailed agreements in place. The trustee who is the IMSP can only use personal health information under the control of the other IMSP for the purposes described in the agreement.

For example, if one physician is storing personal health information for another trustee, the physician would not be able to use this personal health information to treat a patient unless the agreement specifically permitted it.

**Comprehensive Health Record (section 18.1)**

18.1(1) Subject to the terms of any agreements made pursuant to subsection 18(2), eHealth Saskatchewan or a prescribed person may create comprehensive health records with respect to individuals.

(2) A comprehensive health record with respect to an individual:

(a) consists of records containing the individual’s personal health information that are provided by two or more trustees;

(b) is created for the purposes of:

(i) compiling a complete health history of the individual; and

(ii) providing access to that history to any trustee; and

(c) is stored and controlled by eHealth Saskatchewan or the prescribed person that created it.

(3) eHealth Saskatchewan or a prescribed person shall provide a trustee with access to a comprehensive health record only if:

(a) access is authorized by each trustee whose records were used to compile the comprehensive health record; and

(b) either:

(i) the subject individual has provided consent in writing authorizing the trustee to have access; or

(ii) one of the purposes or circumstances set out in subsection 27(2) or (4) exists and the subject individual has not made a direction pursuant to subsection 8(2) or (3).

(4) Nothing in this section prevents the combining of records of personal health information where the combination is not for the purpose of creating a comprehensive health record.

There is currently no other prescribed person that may create a comprehensive health record, other than eHealth Saskatchewan.

eHealth Saskatchewan also functions as an IMSP for certain trustees. As such, it is important for a trustee to have detailed agreements with eHealth Saskatchewan if using the comprehensive health record.
Duty to collect accurate information (section 19)

In collecting personal health information, a trustee must take reasonable steps to ensure that the information is accurate and complete.

Before collecting, using or disclosing personal health information, a trustee must make a reasonable effort to ensure that the information is accurate and complete.

Part of this duty is ensuring that the source of personal health information can be clarified and all accesses, uses, disclosures and changes can be tracked and audited.

“Take reasonable steps” means that the trustee will be thorough in identifying practicable means to ensure that personal health information is accurate and complete.

Trustees trying to ensure accuracy and completeness may find it helpful to answer the following questions:

- Is there a system of verification for personal health information collected and for its entry on the system?
- Does the record indicate the last update date?
- Who is authorized to add, change or delete personal health information from records held by the system? Are these actions tracked?
- Is there a procedure for correcting or amending the information in the record?
- Does the system have the necessary audit trails to determine who may have previously relied on the incorrect information?
- Are procedures in place for disposition of personal health information and are actual records retention and disposition schedules agreed upon and signed, for all the information in the system?

Certain trustees can collect registration information for the purpose of verifying accuracy. See subsection 28(1)(c) of HIPA and subsection 6.4(1)(c) of the HIPA Regulations in this Guide.

Duty where one trustee discloses to another (section 20)

Where one trustee discloses personal health information to another trustee, the information may become a part of the records of the trustee to whom it is disclosed, while remaining part of the records of the trustee that makes the disclosure.

Where personal health information disclosed by one trustee becomes a part of the records of the trustee to whom the information is disclosed, the trustee to whom the information is disclosed is subject to the same duties with respect to that information as the trustee that discloses the information.

Section 20 of HIPA permits trustees to disclose personal health information between each other. When this occurs, both trustees are responsible for the protection of the personal health information in question. Disclosures, of course, must always be made in accordance with sections 23, 27, 28, 29 and 30 of HIPA.
Duty where disclosing to persons other than trustees
(Section 21)

21 Where a trustee discloses personal health information to a person who is not a trustee, the trustee must:

(a) take reasonable steps to verify the identity of the person to whom the information is disclosed; and

(b) where the disclosure is made without the consent of the subject individual, take reasonable steps to ensure that the person to whom the information is disclosed is aware that the information must not be used or disclosed for any purpose other than the purpose for which it was disclosed unless otherwise authorized pursuant to this Act.

21(a)
A trustee who discloses personal health information must make a reasonable effort to ensure that the person to whom the disclosure is made is the person intended and authorized to receive the information.

“Take reasonable steps” in the context of this section would mean verifying the identity of any individual to whom personal health information will be disclosed prior to the disclosure occurring.

In person, trustees should require proof of an individual’s identity. That proof could be in the form of photo identification (i.e. driver’s license, passport, etc.). Copies of such identification do not need to be collected for this purpose, although a note of the verification and disclosure should be made in the file.

The most common way of verifying or authenticating identity electronically is through the use of passwords. However, it could also include requiring proof of identity using tokens, biometrics, challenge/response scenarios, digital signatures and certification authorities.

21(b)
Disclosures without consent must be made in accordance with sections 23, 27, 28, 29 and 30. Although a trustee does not have responsibility over what an individual does with personal health information once it has been disclosed if it had the requisite authority to disclose, it does have a responsibility to communicate to the individual that the personal health information is being disclosed without consent in accordance with HIPA and must not be used or disclosed for any purpose other than the purpose for which it was disclosed.
Continuing duties of trustees (section 22)

22(1) Where a trustee ceases to be a trustee with respect to any records containing personal health information, the duties imposed by this Act on a trustee with respect to personal health information in the custody or control of the trustee continue to apply to the former trustee until the former trustee transfers custody and control of the personal health information to another trustee or to an information management service provider that is a designated archive.

(2) Where a former trustee fails to carry out the duties continued pursuant to subsection (1), the minister may appoint a person or body to act in place of the former trustee until custody and control of the personal health information is transferred to another trustee or to an information management service provider that is a designated archive.

(2.1) If a trustee fails to keep secure personal health information in the custody or control of the trustee, the minister may appoint a person or body to act in place of the trustee until custody or control of the personal health information is re-established, transferred to another trustee or transferred to an information management service provider that is a designated archive.

(3) Where a trustee dies, the duties imposed by this Act on a trustee with respect to personal health information in the custody or control of the trustee become the duties of the personal representative of the trustee and continue to apply to the personal representative until the personal representative transfers custody and control of the personal health information to another trustee or to an information management service provider that is a designated archive.

22(1) A trustee of personal health information (or their personal representative) remains a trustee until complete custody and control of the personal health information passes to another trustee or designated archive. Section 4 of the HIPA Regulations lists the current designated archives.

A trustee may need to pass custody or control of personal health information for a variety of circumstances – death, bankruptcy, retirement or relocation, to name a few. The failure to adequately protect personal health information in such an event of a change in practice may have harmful consequences for the individuals to whom the personal health information relates and the trustee.

22(2) and 22(2.1) When there is a concern that personal health information is abandoned, the Minister of Health may step in and appoint a body or person to secure the records. Examples of this include when patient records found in a public space or when a physician leaves the province, abandoning personal health information.

22(3) Pursuant to subsection 22(3) of HIPA, the personal representative of a deceased trustee becomes the trustee of any personal health information under the custody or control of the deceased trustee. The personal representative must pass custody and control of the personal health information to another person who is legally authorized to hold it. As a result, the
personal representative must comply with the duties and obligations imposed on trustees under HIPA.

The IPC has defined *personal representative* as an executor under a will or an administrator appointed by the court as Executor Administrator of an estate.
LIMIT ON COLLECTION, USE, AND DISCLOSURE OF PERSONAL HEALTH INFORMATION BY TRUSTEES (PART IV OF HIPA)

Collection, use and disclosure on need-to-know basis (section 23)

23(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.

(2) A trustee must establish policies and procedures to restrict access by the trustee’s employees to an individual’s personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.

(3) Repealed. 2003, c.25, s.13.

(4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

23(1)
Section 23 of HIPA is based on two principles:

1) Need-to-Know
2) Data minimization

Section 23 underlies all of Part IV of HIPA.

Need-to-know principle

The need-to-know principle is self-explanatory. Trustees and their staff should only collect, use or disclose personal health information needed for the diagnosis, treatment or care of an individual. Personal health information should only be available to those employees in an organization that have a legitimate need-to-know that information for the purpose of delivering their mandated services. A trustee should limit collection and use of personal health information to what he/she needs-to-know to do his/her job, not collect or use information that is ‘nice to know’.

Data minimization principle

The data minimization principle means that a trustee or employee should collect, use or disclose the least amount of identifying information necessary for the purpose.

Circle of Care vs. Need-to Know

Circle of Care is a popular term among Saskatchewan trustees. In this concept, the patient is at the centre of the circle. Health care professionals involved in the diagnosis treatment
and care of the patient are also in the circle and would be entitled to view and use personal health information. Diagrams of this concept are complex.

However, need-to-know is the concept used in HIPA and is more simple and accurate. A trustee should only view and use personal health information if they have a need-to-know. Need-to-know will vary with each episode of care.

23(2)
Our office has said that the biggest threat to personal health information is employee snooping. In addition to section 16, a trustee must ensure that it has policies and procedures to ensure that its employees understand and follow the need-to-know and data minimization principles to adhere with this section of HIPA. This would include:

- HIPA training with an emphasis on need-to-know and data minimization;
- Employee oath or undertaking of confidentiality;
- Trustee specific policies and procedures;
- Cautionary reminders to users when they sign in to view personal health information in the electronic health record;
- Audit log of viewing activity for individual patients;
- Identification of the risks of snooping such as:
  - discipline by the trustee including dismissal;
  - discipline by a professional body;
  - sharing details of discipline with staff or affected individuals; or
  - prosecution under HIPA.

Further, it would be a violation of subsection 23(2) of HIPA if an employee of a trustee views or handles personal health information by accident or through an established process without the need-to-know. (e.g. A misdirected fax from a regional health authority is sent to the wrong number within the same regional health authority.)

See the HIPA Offences and their Consequences Table found in this Guide for more information about the potential consequences to snooping.

23(4)
De-identified personal health information is defined in section 2(d) as follows:

2(d) “de-identified personal health information” means personal health information from which any information that may reasonably be expected to identify an individual has been removed.

See Appendix G – Deidentified Personal Health Information for more information on de-identified personal health information. See also section 3(2)(a) of HIPA.
Restrictions on collection (section 24)

24(1) A trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.

(2) A trustee may collect personal health information for a secondary purpose if the secondary purpose is consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.

(3) Nothing in this Act prohibits the collection of personal health information where that collection is authorized by another Act or by a regulation made pursuant to another Act.

(4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

24(1)
Section 24(1) contains three key elements:

- The collection must be for a service of the trustee.
- That service must be one that can reasonably be expected to benefit the patient.
- The service to the patient must be the primary purpose for the collection activity.

24(2)
Secondary purpose refers to the collection of personal health information for a purpose other than described in subsection 24(1) such as research, health system planning, fundraising, etc.

Personal health information can be collected for a secondary purpose only if it is described in sections 27, 28 or 29 of HIPA.
See sections 27, section 28 or 29 section of HIPA for further details.

24(3)
Trustees may collect personal health information if permitted to do so by other legislation.
Manner of collection (section 25)

25(1) Subject to subsection (2), a trustee shall collect personal health information directly from the subject individual, except where:

(a) the individual consents to collection of the information by other methods;

(b) the individual is unable to provide the information;

(c) the trustee believes, on reasonable grounds, that collection directly from the subject individual would prejudice the mental or physical health or the safety of the subject individual or another individual;

(d) the information is collected, and is necessary, for the purpose of:
   (i) determining the eligibility of the individual to participate in a program of the trustee or receive a product or service from the trustee, in the course of processing an application made by or on behalf of the individual; or
   (ii) verifying the eligibility of the individual who is participating in a program of the trustee or receiving a product or service from the trustee;

(e) the information is available to the public;

(f) the trustee collects the information by disclosure from another trustee pursuant to section 27, 28 or 29; or

(g) prescribed circumstances exist.

(2) Where the collection is for the purpose of assembling the family health history of an individual, a trustee may collect personal health information from the individual about other members of the individual’s family.

(3) Where a trustee collects personal health information from anyone other than the subject individual, the trustee must take reasonable steps to verify the accuracy of the information.

(3.1) Subsection (3) does not apply to personal health information collected by the Saskatchewan Archives Board for the purposes of *The Archives Act, 2004*.

25(1)

Section 25(1) states that a trustee must collect personal health information directly from the subject individual, unless it is a circumstance described in subsections (a) – (g).

Direct collection is the preferred method for obtaining personal health information. This provides an opportunity for the trustee and subject individual to discuss the type of personal health information being collected and how it will be used and by whom.

If the trustee receives an access request from the subject individual for personal health information collected indirectly, the personal health information would not necessarily be protected. In some circumstances, a trustee may only withhold personal health information if it would reveal the source of the information (See subsection 38(1)(c) of HIPA).

Pursuant to subsection 9(2) of HIPA, when collecting personal health information, a trustee should let the individual know how the information is likely to be used and to whom it is likely to be disclosed.
25(1)(a)
A trustee may collect personal health information if it has the consent of the subject individual prior to collection. See the sections on consent.

25(1)(b)
A trustee may collect personal health information indirectly where the individual is unable to provide the information (e.g. a senior with dementia, someone who is unresponsive, etc.)

25(1)(c)
A trustee may collect personal health information indirectly where the trustee believes, on reasonable grounds, that collection directly from the subject individual would prejudice the mental or physical health or the safety of the subject individual or another individual.

“On reasonable grounds” means using logical, sensible or rational thought as the basis for drawing a fair conclusion on a matter.

Examples of this would be:

- where a patient may not be honest with a trustee. Necessary, accurate information about the patient’s health, effectiveness of medication may, therefore, not be obtained;
- where a patient is likely to modify his or her behavior in such a way that it could prevent an effective diagnosis or assessment of the patient’s treatment;
- where an individual does not know the information that is needed (e.g., a senior dealing with a pharmacist and neither the senior nor the pharmacist is aware of all the medications the senior may be taking);
- direct collection would delay the provision of emergency treatment;
- requesting the information could cause the individual to react violently; or
- in the case of a psychotic patient, another person’s perspective on symptoms and the effect of a particular medication may be required.

25(1)(d)

25(1)(d)(i)
This section provides authority for indirect collection where a trustee is determining the eligibility of an individual to participate in a program of the trustee or to receive a product or health service from the trustee. This may require the trustee to approach several different sources of information besides the individual to determine whether the criteria or qualifications are met. This collection can only take place in the course of processing an application from the individual, or from his or her personal guardian or legal custodian. The individual may not be informed that verification is taking place.

25(1)(d)(ii)
This section provides authority for a trustee to verify the eligibility of an individual who is already participating in a program or receiving a product or service from a trustee to continue to participate in the program or to continue to receive the product or service.
This provision is intended to allow for cases where an individual has already qualified for a program, product or service and the trustee needs to check or verify whether the eligibility remains valid. In this case, personal health information may be collected from a variety of sources other than the individual the information is about and the individual may not be informed that verification is taking place.

25(1)(e)
This section provides authority for a trustee to collect personal health information indirectly without the consent or knowledge of the individual where the information can be readily found in published or other public sources.

Examples include:

- Information published in any form such as in print form, audiotape or videotapes.
- Birth, marriage or obituary notices, newspaper reports, clipping files and articles in periodicals.
- Recorded information available for a fee or for free, such as information that is available on the Internet, a written biographical sketch provided to participants at a public function, or information in public registry records.

Information of a more personal nature, based upon personal acquaintance, friendship, observation, social media or gathered through surveillance, would not be included.

Trustees should always ensure the accuracy of the personal health information it collects. See section on accuracy of personal health information.

25(1)(f)
Even though sections 27, 28 and 29 of HIPA outline the reasons for disclosing personal health information, a trustee may also collect personal health information for the same reasons.

See section 27, section 28 and section 29 in this guide for more information.

25(1)(g)
Prescribed circumstances refer the reader to the HIPA Regulations. Currently, only section 7.1 of the Regulations address the collection of personal health information. That is for fundraising purposes.

25(2)
A trustee may collect personal health information about family members of an individual for the purpose of assembling a family history where the information collected is to be used in the context of providing a health service to the individual who is the subject of the information.

The information can only be collected under the authority of this section in the context of providing a health service to the patient. It cannot be collected for research or other purposes without the subject individual's authorization.
25(3)
When a trustee collects personal health information from anyone other than the subject individual, the trustee must take reasonable steps to verify the accuracy of the information.

See section 19 in this guide for tips on how to verify the accuracy of personal health information.

Restrictions on use (section 26)

26(1) A trustee shall not use personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section.

(2) A trustee may use personal health information:

(a) for a purpose for which the information may be disclosed by the trustee pursuant to section 27, 28 or 29;

(b) for the purposes of de-identifying the personal health information;

(c) for a purpose that will primarily benefit the subject individual; or

(d) for a prescribed purpose.

(3) Nothing in subsection (2) authorizes a trustee as an employer to use or obtain access to the personal health information of an individual who is an employee or prospective employee for any purpose related to the employment of the individual without the individual's consent.

HIPA defines use in section 2(u) as follows:

2(u) use includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

Another helpful definition of use is as follows:

Use indicates the internal utilization of personal health information by a trustee and includes sharing of the personal health information in such a way that is remains under the control of that trustee. For example, in a regional health authority and its facilities, the sharing of information between employees constitutes ‘use’ of the personal health information since the sharing happens under the control of the regional health authority.

Use does not include disclosure of personal health information.
26(1)
A trustee may only use personal health information for a purpose listed in subsection 26(2) or with the consent of an individual.

See the section of this Guide about consent.

If personal health information is used for the purposes of research, there are special provisions that a trustee must follow, even if the subject individual has given express consent. See section 29 of this Guide.

26(2)

26(2)(a)
Even though sections 27, 28 and 29 of HIPA outline the reasons for disclosing personal health information, a trustee may also use personal health information for the same reasons.

Subsection 27(2)(b) of HIPA describes a health service; the core activities that occur in the healthcare sector.

This allows trustees to use personal health information for the purpose of arranging, assessing the need for, providing, continuing or supporting the provision of, a service requested or required by the subject individual.

Subsection 2.2 of The Regional Health Services Administration Regulations defines health services as follows:

(2.2) For the purposes of sub clause 2(1)(j)(i) of the Act, the following services are health services:

(a) alcohol, drug or substance abuse or addiction assessment, education and treatment services;
(b) chronic disease management services;
(c) community health services;
(d) convalescent care and palliative care services;
(e) counselling services;
(f) diagnostic imaging services;
(g) disability management services;
(h) disease and injury prevention services;
(i) emergency medical response services;
(j) emergency stabilization services;
(k) health assessment and screening services;
(l) health education services;
(m) health promotion services;
(n) home care services;
(o) hospital services;
(p) laboratory services;
(q) long-term care services;
(r) medical services;
(s) mental health services;
(t) nursing services;
(u) personal care services;
(v) physician services;
(w) provision of drugs, medical supplies and surgical supplies;
(x) public health services;
(y) registered nurse or nurse practitioner services;
(z) rehabilitation services;
(aa) specialty and subspecialty medical services and surgical services;
(bb) therapy services;
(cc) any other goods and services ancillary or incidental to health promotion and protection or respecting the care, treatment or transportation of sick, infirm or injured individuals.

This list would apply to all trustees for the purposes of HIPA.

See section 27, section 28 and section 29 in this Guide for more information.

26(2)(b)
De-identified personal health information is defined in subsection 2(d) of HIPA as follows:

2(d) “de-identified personal health information” means personal health information from which any information that may reasonably be expected to identify an individual has been removed;

Subsection 26(2)(b) allows the trustee to de-identify personal health information for other purposes. For more information, see the section of this Guide on de-identification of personal health information.

26(2)(c)
The benefit contemplated by subsection 26(2)(c) must primarily benefit the specific subject individual. This provision would not apply if the primary benefit was for the trustee or a third party.

26(2)(d)
Prescribed circumstances refer the reader to the HIPA Regulations. Currently, only section 7.1 of the Regulations addresses the use of personal health information. That is for fundraising purposes.
26(3) Trustees cannot use personal health information in its custody or under its control to evaluate the suitability of a potential employee without consent of the subject individual. Consent should be express consent.

Trustees cannot use personal health information in its custody or under its control of an employee for an employment related matter without consent of the subject individual. Consent should be express consent.

See sections in this Guide about consent.

Disclosure (section 27)

27(1) A trustee shall not disclose personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section, section 28 or section 29.

A trustee may only disclose personal health information for a purpose listed in section 27, 28 or 29 or with the consent of an individual.

See the sections in this Guide about consent.

NOTE: If personal health information is disclosed for the purposes of research, there are special provisions that a trustee must follow, even if the subject individual has given express consent. See section 29 of this Guide.

27(2) A subject individual is deemed to consent to the disclosure of personal health information:

(a) for the purpose for which the information was collected by the trustee or for a purpose that is consistent with that purpose;

(b) for the purpose of arranging, assessing the need for, providing, continuing or supporting the provision of, a service requested or required by the subject individual; or

(c) to the subject individual’s next of kin or someone with whom the subject individual has a close personal relationship if:

(i) the disclosure relates to health services currently being provided to the subject individual; and

(ii) the subject individual has not expressed a contrary intention to a disclosure of that type.

Subsection 27(2) is based on deemed consent. Deemed consent means a trustee can forgo express or implied consent in certain circumstances, such as when an individual is unable to
give consent, is unconscious or in emergent circumstances. If any trustee wishes to rely on deemed consent, they must ensure that they are in compliance with both the general duties and the specific duties prescribed in HIPA. The data minimization and need-to-know principles are especially important. See Part III of HIPA in this Guide.

In our view, the disclosure must not be contrary to the express request of the individual.

27(2)(a)
A consistent purpose is one that has a direct and reasonable connection to the original purpose that the personal health information was collected such as providing the program, activity or service of the trustee that can reasonably be expected to benefit the subject individual. Under this subsection, personal health information is typically disclosed to another trustee.

In our view, the disclosure must not be contrary to the express request of the individual.

27(2)(b)
This provision describes the core activities that occur in the healthcare sector. These include the primary purposes for collecting personal health information.

27(2)(c)
Under this provision, a trustee may disclose information about an individual’s location, presence, condition, diagnosis, progress and prognosis on that day to family members of the individual or to another person with whom the individual is believed to have a close personal relationship, without the individual’s consent.

In our view, the disclosure must not be contrary to the express request of the individual.

Immediate family and Next of Kin – the IPC recommends that trustees in Saskatchewan adopt the list for “nearest relative” provided by subsection 15(1) of The Health Care Directives and Substitute Health Care Decision Makers Act for the definition of immediate family. The list is as follows:

- the spouse or person with whom the person requiring treatment cohabits and has cohabited as a spouse in a relationship of some permanence;
- an adult son or daughter;
- a parent or legal custodian;
- an adult brother or sister;
- a grandparent;
- an adult grandchild;
- an adult uncle or aunt;
- an adult nephew or niece.

Person in a close personal relationship could include a common-law spouse, a close friend or other person who can demonstrate that he or she has such a relationship with the individual who is the subject of the information.

This provision enables a trustee to discuss the diagnosis or condition of a patient or their location with a patient’s relative or close friend.
Please see Appendix F – When to Disclose Personal Health Information to Family and Friends.

27(3)

27(3) A trustee shall not disclose personal health information on the basis of a consent pursuant to subsection (2) unless:

(a) in the case of a trustee other than a health professional, the trustee has established policies and procedures to restrict the disclosure of personal health information to those persons who require the information to carry out a purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act; or

(b) in the case of a trustee who is a health professional, the trustee makes the disclosure in accordance with the ethical practices of the trustee’s profession.

27(3)(a)

A trustee should have all the requirements of section 16 of HIPA in place before disclosing personal health information to other health professionals. See section 16 in this Guide for more information. Information sharing agreements are a crucial best practice for sharing personal health information with other trustees.

See Appendix H – for more information on information sharing agreements.

27(3)(b)

The trustee should take into account the ethical practices of his/her profession. However, ethical practices should not override any provisions of HIPA.

27(4)

The following subsections consider scenarios where trustees can collect, use or disclose personal health information without the consent of the subject individual.

In accordance with section 10 of HIPA, trustees should be able to notify the subject individual of any disclosure made without the individual’s consent.
27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

(a) where the trustee believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person;

(b) where, in the opinion of the trustee, disclosure is necessary for monitoring, preventing or revealing fraudulent, abusive or dangerous use of publicly funded health services;

(c) where the disclosure is being made to a trustee that is the successor of the trustee that has custody or control of the information, if the trustee makes a reasonable attempt to inform the subject individuals of the disclosure;

(d) to a person who, pursuant to The Health Care Directives and Substitute Health Care Decision Makers Act, is entitled to make a health care decision, as defined in that Act, on behalf of the subject individual, where the personal health information is required to make a health care decision with respect to that individual;

(e) if the subject individual is deceased:

(i) where the disclosure is being made to the personal representative of the subject individual for a purpose related to the administration of the subject individual's estate; or

(ii) where the information relates to circumstances surrounding the death of the subject individual or services recently received by the subject individual, and the disclosure:

(A) is made to a member of the subject individual’s immediate family or to anyone else with whom the subject individual had a close personal relationship; and

(B) is made in accordance with established policies and procedures of the trustee, or where the trustee is a health professional, made in accordance with the ethical practices of that profession;

(f) where the disclosure is being made in accordance with section 22 to another trustee or an information management service provider that is a designated archive;

(g) where the disclosure is being made to a standards or quality of care committee established by one or more trustees to study or evaluate health services practice in a health services facility, health region or other health service area that is the responsibility of the trustee, if the committee:

(i) uses the information only for the purpose for which it was disclosed;

(ii) does not make a further disclosure of the information; and

(iii) takes reasonable steps to preserve the confidentiality of the information;

(h) subject to subsection (5), where the disclosure is being made to a health professional body or a prescribed professional body that requires the information for the purposes of carrying out its duties pursuant to an Act with respect to regulating the profession;
(i) where the disclosure is being made for the purpose of commencing or conducting a proceeding before a court or tribunal or for the purpose of complying with:

(ii) rules of court that relate to the production of information;

(j) subject to subsection (6), where the disclosure is being made for the provision of health or social services to the subject individual, if, in the opinion of the trustee, disclosure of the personal health information will clearly benefit the health or well-being of the subject individual, but only where it is not reasonably practicable to obtain consent;

(k) where the disclosure is being made for the purpose of:

(ii) planning, delivering, evaluating or monitoring a program of the trustee;

(l) where the disclosure is permitted pursuant to any Act or regulation;

(m) where the disclosure is being made to the trustee’s legal counsel for the purpose of providing legal services to the trustee;

(n) in the case of a trustee who controls the operation of a pharmacy as defined in The Pharmacy Act, 1996, a physician, a dentist or the minister, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to The Medical Profession Act, 1981 and approved by the minister;

(o) in the case of a trustee who controls the operation of a pharmacy as defined in The Pharmacy Act, 1996, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to The Pharmacy Act, 1996 and approved by the minister;

(p) in prescribed circumstances.

27(4)(a)

27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

(a) where the trustee believes, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person;

This provision is meant to provide the ability to disclose personal health information if it could avoid or minimize a danger to the safety, physical or mental health of an individual.

Threaten means to expose to risk or harm.

Safety implies relative freedom from danger or risks.

Physical health refers to the well-being of an individual’s physical body.

Mental health refers to the functioning of a person’s mind in a normal state.
In order to determine whether a threat to the safety, physical or mental health of any person exists, the trustee should apply the following test:

1. there must be a reasonable expectation of probable harm;
2. the harm must constitute damage or detriment and not more inconvenience;
3. must be a causal connection between disclosure and avoiding or minimizing the anticipated harm.

Generally, this means the trustee must make an assessment of the risk and determine whether there are reasonable grounds for concluding there is a danger to the health or safety of any person. That assessment must be specific to the circumstances of the case under consideration. The inconvenience, upset or unpleasantness of dealing with difficult or unreasonable people is not sufficient to trigger this section. The threshold cannot be achieved on the basis of unfounded, unsubstantiated allegations.

The trustee should be able to detail what the harm is and to whom the harm threatens before the personal health information is released.

27(4)(b)

27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

...  
(b) where, in the opinion of the trustee, disclosure is necessary for monitoring, preventing or revealing fraudulent, abusive or dangerous use of publicly funded health services;

This provision authorizes a trustee to disclose limited personal health information without the individual’s consent when the trustee “reasonably believes” that the personal health information will detect, limit or prevent fraud or abuse in the use of health services. This type of disclosure would usually be made to the police or the Minister of Justice and Attorney General or Minister of Health.

Reasonably believes means having a view that is supported by logic and knowledge of the relevant circumstances.

27(4)(c)

27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

...  
(c) where the disclosure is being made to a trustee that is the successor of the trustee that has custody or control of the information, if the trustee makes a reasonable attempt to inform the subject individuals of the disclosure;

Under this provision, a trustee may disclose personal health information without the individual’s consent to its successor if:

• the successor is a trustee;
• it is for the purpose of the trustee transferring its records to the successor as a result of the trustee ceasing to be a trustee or ceasing to provide health services within the geographic area in which the successor provides health services; and

• The trustee has made a reasonable attempt to inform the subject individuals of disclosure. This could include contacting former patients directly, having posters in the office informing of the move for a prolonged period of time (6-12 months) or taking out and advertisement in a newspaper.

**Successor** would be the person or organization that obtains ownership of or title to a trustee’s facility or practice when the trustee ceases to be a trustee. A successor could be an individual, a partnership, corporation or other unincorporated organization or sole proprietorship.

This provision would, for example, enable a physician or other health professional in the publicly funded health system to transfer his or her patient files to another physician who is taking over the practice of that physician.

For more information, see section 22 of this Guide, and/or **Who is “THE” Trustee** section of this Guide.

27(4)(d)

27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

...  
(d) to a person who, pursuant to *The Health Care Directives and Substitute Health Care Decision Makers Act*, is entitled to make a health care decision, as defined in that Act, on behalf of the subject individual, where the personal health information is required to make a health care decision with respect to that individual;

This subsection allows a trustee to make a disclosure about the subject individual to someone who is entitled to make a decision pursuant to *The Health Care Directives and Substitute Health Care Decision Makers Act*.

Such a person may be a proxy, nearest relative or personal guardian.

As defined in 2(1)(g) of *The Health Care Directives and Substitute Health Care Decision Makers Act*, a proxy is “a person appointed in a directive to make health care decisions for the person making the directive.” See sections 11, section 12 and section 13 of *The Health Care Directives and Substitute Health Care Decision Makers Act* for more details.

As outlined in subsection 15(1) of *The Health Care Directives and Substitute Health Care Decision Makers Act*, the nearest relative is as follows:

“the person first described in the following clauses who is willing, available and has the capacity to make a health care decision:”

(a) the spouse or person with whom the person requiring treatment cohabits and has cohabited as a spouse in a relationship of some permanence;

(b) an adult son or daughter;
(c) a parent or legal custodian;
(d) an adult brother or sister;
(e) a grandparent;
(f) an adult grandchild;
(g) an adult uncle or aunt;
(h) an adult nephew or niece.

As defined in 2(1)(f) of The Health Care Directives and Substitute Health Care Decision Makers Act, a personal guardian is “appointed pursuant to The Adult Guardianship and Co-decision-making Act who has the authority to make health care decisions for a dependent adult and who acts in accordance with the authority granted to the personal guardian pursuant to that Act”.

The trustee should ensure the disclosure is made for a purpose discussed in The Health Care Directives and Substitute Health Care Decision Makers Act.

In our view, disclosures should not be made against the express wish of the subject individual.

See The Health Care Directives and Substitute Health Care Decision Makers Act for more details.

See section 22 and section 56(b) of this Guide for more details.

27(4)(e)

27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

... 

(e) if the subject individual is deceased:

(i) where the disclosure is being made to the personal representative of the subject individual for a purpose related to the administration of the subject individual’s estate; or

(ii) where the information relates to circumstances surrounding the death of the subject individual or services recently received by the subject individual, and the disclosure:

(A) is made to a member of the subject individual’s immediate family or to anyone else with whom the subject individual had a close personal relationship; and

(B) is made in accordance with established policies and procedures of the trustee, or where the trustee is a health professional, made in accordance with the ethical practices of that profession;
27(4)(e)(i)
A trustee may disclose personal health information to the personal representative of a deceased individual if the purpose relates to the administration of the deceased person’s estate.

The IPC has defined personal representative as an executor under a will or an administrator appointed by the court as Executor Administrator of an estate. See subsection 56(a) of this Guide.

27(4)(e)(ii)
A trustee may disclose information relates to circumstances surrounding the death of the subject individual or services recently received by the subject individual if:

- The disclosure is made to an immediate family member or someone in a close personal relationship with the deceased AND
- It is made in accordance with any policies and procedures or ethical practices of the trustee.

Any personal health information disclosed should not go beyond the circumstances of the subject individual's death and the care received at that time.

Ethical practices should not override any provisions of HIPA.

27(4)(f)

27 A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

... 

(f) where the disclosure is being made in accordance with section 22 to another trustee or an information management service provider that is a designated archive;

This subsection allows a trustee to disclose personal health information to another trustee or an IMSP that is a designated archive for the purposes described in section 22. See section 22 of this Guide.

27(4)(g)

27 A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

... 

(g) where the disclosure is being made to a standards or quality of care committee established by one or more trustees to study or evaluate health services practice in a health services facility, health region or other health service area that is the responsibility of the trustee, if the committee:

(i) uses the information only for the purpose for which it was disclosed;

(ii) does not make a further disclosure of the information; and

(iii) takes reasonable steps to preserve the confidentiality of the information;
This provision enables a trustee to disclose personal health information without the individual’s consent to a standards or quality of care committee that has as its primary purpose the carrying out of quality of care activities pursuant to section 10 of The Evidence Act of Saskatchewan if:

a) The committee uses the personal health information only for the purposes for which it was disclosed;

b) Does not make further disclosures of the information; and

c) Take reasonable steps to preserve the confidentiality of the information.

Pursuant to subsection 10(1) of The Evidence Act, a quality improvement committee means a committee designated as a quality improvement committee by a health services agency to carry out a quality improvement activity the purpose of which is to examine and evaluate the provision of health services for the purpose of:

(a) educating persons who provide health services; or

(b) improving the care, practice or services provided to patients by the health services agency;

HIPA also considers standards of care committees and quality of care committees which may be internal to an organization or made up of several trustees.

In order to meet the conditions imposed by 27(4)(g), a trustee should have strong information sharing agreements with any committee outside of the organization and strong terms of reference for a committee within the organization.

See Appendix H – for more information about information sharing agreements.

27(4)(h)

27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

... 

(h) subject to subsection (5), where the disclosure is being made to a health professional body or a prescribed professional body that requires the information for the purposes of carrying out its duties pursuant to an Act with respect to regulating the profession;

This subsection authorizes a trustee to disclose personal health information without the individual’s consent to a health professional body for the carrying out its duties pursuant to an Act with respect to regulating the profession.

Health professional body is a body that regulates the members of a health profession or health discipline pursuant to an Act. Examples of these bodies include the College of Physicians and Surgeons of Saskatchewan, Saskatchewan Registered Nurses Association, Chiropractors’ Association of Saskatchewan, etc.

There are currently no prescribed professional bodies listed in the HIPA Regulations.

Investigation refers to a systematic process of examination, inquiry and observation.
**Discipline proceeding** refers to a formal process of determining whether a practitioner has displayed a lack of skill or judgment in the practice of his or her profession; has displayed unbecoming and/or unprofessional, disgraceful or dishonorable conduct; or is incapable or unfit to practice his or her profession.

**Practice review** refers to an assessment or evaluation of the professional performance or competence of a practitioner.

**Inspection** refers to the examination or viewing of the physical premises or of the books, records, papers or other documents of a practitioner as part of an investigation.

The **health professional body** must agree in writing not to disclose the information except as authorized under the Act governing that health professional body. An **information sharing agreement** is a good idea. See Appendix – H for more information on information sharing agreements.

In addition section this section authorizes a trustee to disclose **personal health information** to a health professional body for the purpose of lodging a complaint with the health professional body.

**NOTE:** If sharing personal health information of a member of a health professional body see subsection 27(5) of HIPA.

**27(4)(i)**

27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

... 

(i) where the disclosure is being made for the purpose of commencing or conducting a proceeding before a court or tribunal or for the purpose of complying with:

   (i) an order or demand made or subpoena or warrant issued by a court, person or body that has the authority to compel the production of information; or

   (ii) rules of court that relate to the production of information;

This provision enables the disclosure of personal health information without the individual’s consent for the purpose of complying with legal processes that require the production of information. These processes include subpoenas, warrants or orders issued or made by a court, person or body having jurisdiction in Saskatchewan to compel the production of information or with a rule of court that relates to the production of information.

**Subpoena** is a command or summons requiring the attendance of someone as a witness at a court or hearing. It will specify a place and time when testimony on a certain matter will be required and may also order a person to meet the requirements of a court in Saskatchewan to disclose information.

**Warrant** is a judicial authorization to search for and collect something, which may include personal health information. The warrant will state in writing what information, or what thing, its authority covers.
**Order** is an authoritative command, direction or instruction to produce something – in this context, personal health information.

When considering responding to a foreign subpoena or other court order, trustees must take reasonable steps to ensure it has been recognized by a court with jurisdiction in Saskatchewan or Canada, or obtain consent from the subject individual to disclose their health information.

27(4)(j)

27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

... 

(j) subject to subsection (6), where the disclosure is being made for the provision of health or social services to the subject individual, if, in the opinion of the trustee, disclosure of the personal health information will clearly benefit the health or well-being of the subject individual, but only where it is not reasonably practicable to obtain consent;

See also subsection 27(6) of HIPA.

A trustee is able to disclose personal health information to arrange a health or social service for the subject individual disclosure of the personal health information will clearly benefit the health or well-being of the subject individual. Also, a trustee may only make the disclosure if the trustee cannot obtain the consent of the subject individual.

Examples of social services include:

- income support and financial assistance
- child and family services (child care subsidies, adoption services, child protection, foster care, etc)
- housing programs
- supports for persons with disabilities

Not reasonably practicable refers to something that is not feasible or possible from a realistic or practical standpoint.

27(4)(k)

27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

... 

(k) where the disclosure is being made for the purpose of:

(i) obtaining payment for the provision of services to the subject individual; or
(ii) planning, delivering, evaluating or monitoring a program of the trustee;
27(4)(k)(i)
This subsection allows a trustee to disclose personal health information for the purpose of obtaining payment for services provided to the subject individual.

Some scenarios this provision might cover include the following:

- Where the subject individual is not from Saskatchewan to the government of that province or territory or to the government of Canada. Disclosure would be permitted where the individual is a resident of the other province or territory or where the government of Canada is responsible for payments for health services provided to the individual.

- To a third party insurer who is responsible for the payment of that individual’s health product or service claim.

27(4)(k)(ii)
Typically activities related to planning, delivering, evaluating or monitoring a program of the trustee would be done internally and would qualify as a use and not a disclosure. This provision also allows the trustee to disclose personal health information for the purposes of these activities as well.

Trustees should have strong written information sharing agreements in place before disclosing personal health information for these purposes.

See Appendix H – for more information on information sharing agreements.

27(4)(l)

A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

- where the disclosure is permitted pursuant to any Act or regulation;

This provision permits a trustee to disclose personal health information without the individual’s consent if another Act or regulation of Saskatchewan or Canada authorizes or requires the disclosure.

Since disclosures under this provision are discretionary, unless another enactment expressly prevails over the HIPA, trustees must still exercise their discretion in terms of disclosures of personal health information that are authorized or required by another enactment.

Some examples of other statutes that authorize or require, in particular situations, the disclosure of certain types of personal health information are:

- Criminal Code (Canada) provides authority to compel disclosure of information by way of warrants or subpoenas specifying the health information requested. Also authorizes the release of information to a board of review appointed under the Criminal Code;

- The Gunshot and Stab Wounds Mandatory Reporting Act requires some trustees to disclose certain personal health information of gunshot and stab wound victims to police.
27(4)(m)

A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

... (m) where the disclosure is being made to the trustee's legal counsel for the purpose of providing legal services to the trustee;

A trustee may disclose personal health information to the subject individual's legal counsel for the purpose of providing legal services to the trustee.

27(4)(n)

A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

... (n) in the case of a trustee who controls the operation of a pharmacy as defined in *The Pharmacy Act, 1996*, a physician, a dentist or the minister, where the disclosure is being made pursuant to a program to monitor the use of drugs that is authorized by a bylaw made pursuant to *The Medical Profession Act, 1981* and approved by the minister;

A physician, dentist or the Minister of Health or a trustee who operates a pharmacy pursuant to *The Pharmacy Act, 1996* may disclose personal health information to a program that monitors the use of a certain drug. The program must be authorized by a bylaw made pursuant to *The Medical Profession Act, 1981* and approved by the Minister of Health.

27(4)(o)

A trustee who operates a pharmacy pursuant to *The Pharmacy Act, 1996* may disclose personal health information to a program that monitors the use of a certain drug. The program must be authorized by a bylaw made pursuant to *The Pharmacy Act, 1996* and approved by the minister;

27(4)(p)

A trustee who operates a pharmacy pursuant to *The Pharmacy Act, 1996* may disclose personal health information to a program that monitors the use of a certain drug. The program must be authorized by a bylaw made pursuant to *The Pharmacy Act, 1996* and approved by the Minister of Health.
A trustee may disclose personal health information without the consent of the subject individual for a reason listed in The Health Information Protection Regulations.

Currently, the HIPA Regulations describes the following circumstances where personal health information can be disclosed without consent of the subject individual:

- Disclosures to the Saskatchewan Health Quality Council (section 5 of the HIPA Regulations);
- Disclosures to police officers or RCMP (section 5.1 of the HIPA Regulations);
- Disclosures to a party to an information sharing agreement (section 5.2 of the HIPA Regulations);
- Disclosures for a program to monitor the prescribing, dispensing, or use of drugs (sections 6.1 to 6.3 of the HIPA Regulations);
- Disclosures for fundraising activities (section 7.1 of the HIPA Regulations).

27(5)

27(5) For the purposes of clause (4)(h), where the personal health information in question is about a member of the profession regulated by the health professional body or prescribed professional body, disclosure may be made only:

(a) in accordance with clause (4)(i);

(b) with the express consent of the subject individual; or

(c) if the trustee has reasonable grounds to believe that the personal health information is relevant to the ability of the subject individual to practise his or her profession, on the request of the health professional body or prescribed professional body.

A trustee may only disclose personal health information of a member of a health professional body if:

- The disclosure is also being made pursuant to 27(4)(i);
- The subject individual (the member) has given express consent (see the sections on consent); or
- the trustee has reasonable grounds to believe that the personal health information is relevant to the ability of the subject individual to practise his or her profession, on the request of the health professional body.

On reasonable grounds means using logical, sensible or rational thought as the basis for drawing a fair conclusion on a matter.
27(6) Disclosure of personal health information pursuant to clause (4)(j) may be made only where the person to whom the information is to be disclosed agrees:

(a) to use the information only for the purpose for which it is being disclosed; and
(b) not to make a further disclosure of the information in the course of carrying out any of the activities mentioned in that clause.

If a trustee is disclosing personal health information to arrange a social service for the subject individual pursuant to 27(4)(j), the trustee must ensure that the recipient of the personal health information:

- uses the information only for the purpose for which it was disclosed; and
- will not to make a further disclosure of the information in the course of carrying out any of the activities for arranging the social services.

These conditions would normally be reached through the use of information sharing agreement. See Appendix H – for more information on information sharing agreements.

Disclosure is the exposure of personal health information to a separate entity, not a division, branch or employee of the trustee in custody or control of that information.

Even with deemed or implied consent, the IPC’s view is that, in most circumstances, in our view, a use or disclosure should not be contrary to the subject individual’s express wishes. This is best practice.

Trustees should document any disclosure of personal health information in the individual’s file. The trustee should also note the section of HIPA upon which he/she is relying upon to make that disclosure.

Disclosure of registration information (section 28)

28(1) The minister may disclose registration information without the consent of the subject individual:

(a) to a trustee in connection with the provision of health services by the trustee;
(b) to another government institution, a regional health authority or an affiliate, for the purpose of verifying the eligibility of an individual to participate in a program or, receive a service from, the government institution, regional health authority or affiliate:

(i) in the course of processing an application made by or on behalf of the individual; or
(ii) if the individual is already participating in the program or receiving the service;
(c) to another government institution, a regional health authority or an affiliate, for the purpose of verifying the accuracy of registration information held by the government institution, regional health authority or affiliate; or
(d) with the approval of the Lieutenant Governor in Council, to another government institution on any terms or conditions that the Lieutenant Governor in Council may
(2) For the purposes set out in subsection (3), registration information may be disclosed without the consent of the subject individual:

(a) by the minister to a regional health authority or affiliate;

(b) by a regional health authority or affiliate to the minister; or

(c) by one regional health authority or affiliate to another regional health authority or affiliate.

(3) Registration information may be disclosed pursuant to subsection (2) for the purpose of planning, delivering, evaluating or monitoring a program of the minister, a regional health authority or an affiliate that relates to the provision of health services or payment for health services.

(4) The minister or a regional health authority may, without the consent of the subject individuals, disclose the names, dates of birth, telephone numbers and addresses of individuals under the age of seven years to a board of education or the Conseil scolaire fransaskois within the meaning of The Education Act, 1995 for the purpose of planning or administration by the board of education or the Conseil scolaire fransaskois.

(5) With the approval of the Lieutenant Governor in Council, the minister may enter into agreements for the sharing of registration information with:

(a) the Government of Canada or the government of a province or territory of Canada; or

(b) a prescribed person or body.

(6) An agreement pursuant to subsection (5) must specify that the party to whom the registration information is disclosed shall use the information only for the purposes specified in the agreement.

(7) The minister may disclose registration information without the consent of the subject individual in accordance with an agreement entered into pursuant to subsection (5).

(8) Registration information may be disclosed without the consent of the subject individual in accordance with the regulations.

Registration information is defined in subsection 2(q) of HIPA as follows:

(q) registration information means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations.

Registration information also qualifies as personal health information. However, for the purposes of section 28, trustees must take care to only disclose registration information in these circumstances, and no other types of personal health information.

28(1)
Subsection 28(1) only allows the Minister of Health (or more practically, the Ministry of Health) to disclose personal health information for the reasons listed in subsections (a)-(d) without the consent of the subject individual.
28(1)(a)
The Minister of Health may disclose personal health information to a trustee for the purposes of arranging, assessing the need for, providing, continuing or supporting the provision of, a service requested or required by the subject individual without the consent of the subject individual.

28(1)(b)
The Minister of Health may disclose personal health information to a government institution, a regional health authority or an affiliate for the purpose of verifying the eligibility of an individual to participate in a program of, or receive a service from, the government institution, regional health authority or affiliate if:

- the Minister is processing an application made by or on behalf of the individual; or
- if the individual is already participating in the program or receiving the service.

See section 25(1)(d) of this Guide.

A government institution means:

- the office of Executive Council or any department, secretariat or other similar agency of the executive government of Saskatchewan; or
- any board, commission, Crown corporation or other body, prescribed in The Freedom of Information and Protection of Privacy Regulations, whose members or directors are appointed, in whole or in part:
  - by the Lieutenant Governor in Council;
  - by a member of the Executive Council; or
  - in the case of:
    - a board, commission or other body, by a Crown corporation; or

28(1)(c)
Without the consent of the subject individual, the Minister of Health may disclose personal health information to a government institution, a regional health authority or an affiliate for the purpose of verifying the accuracy of registration information held by the government institution, regional health authority or affiliate.

See section 19 of this Guide for info on how to collect accurate personal health information.

28(1)(d)
The Minister of Health may disclose the registration information to another government institution without the consent of the subject individual with the approval of the Lieutenant Governor in Council. The Lieutenant Governor in Council may impose certain conditions. This would typically occur through an order-in-council.

28(2) and 28(3)
Personal health information may be disclosed without the consent of the subject individual in the circumstances described in (a)-(c).
28(2)(a)  
Registration information may be disclosed by the Minister of Health to a regional health authority or an affiliate for the purpose of planning, delivering, evaluating or monitoring a program of the minister, a regional health authority or an affiliate that relates to the provision of health services or payment for health services.

28(2)(b)  
Registration information may be disclosed by a regional health authority or affiliate to the Minister of Health for the purpose of planning, delivering, evaluating or monitoring a program of the minister, a regional health authority or an affiliate that relates to the provision of health services or payment for health services.

28(2)(c)  
Registration information may be disclosed by one regional health authority or affiliate to another regional health authority or affiliate for the purpose of planning, delivering, evaluating or monitoring a program of the minister, a regional health authority or an affiliate that relates to the provision of health services or payment for health services.

28(4)  
The Minister of Health or a regional health authority may, without the consent of the subject individual, disclose the names, dates of birth, telephone numbers and addresses of individuals under the age of seven years to a board of education or the Conseil scolaire fransaskois within the meaning of The Education Act, 1995 for the purpose of planning or administration by the board of education or the Conseil scolaire fransaskois.

28(5), 28(6) and 28(7)  
The Minister of Health may enter into an agreement to share registration information with the Government of Canada or the government of a province or territory of Canada or a prescribed person or body (there are currently no prescribed persons or body) if:

- the Lieutenant Governor in Council approves (typically through an order-in-council); and
- the agreement specifies that the party to whom the registration information is disclosed shall use the information only for the purposes specified in the agreement.

This registration information may be disclosed without the consent of the subject individual.

28(8)  
Subsection 28(8) allows registration information to be disclosed without the consent of the subject individual in accordance with the regulations.

Currently, the HIPA Regulations describes the following circumstances where registration information can be disclosed without the consent of the subject individual:

- to the Saskatchewan Cancer Agency (section 6 of the HIPA Regulations);
- to eHealth Saskatchewan (section 6.4 of the HIPA Regulations);
- to the Ministry of Education (section 7 of the HIPA Regulations).
Use and disclosure for research (section 29)

29(1) A trustee or a designated archive may use or disclose personal health information for research purposes with the express consent of the subject individual if:

   (a) in the opinion of the trustee or designated archive, the research project is not contrary to the public interest;

   (b) the research project has been approved by a research ethics committee approved by the minister; and

   (c) the person who is to receive the personal health information enters into an agreement with the trustee or designated archive that contains provisions:

     (i) providing that the person who is to receive the information must not disclose the information;

     (ii) providing that the person who is to receive the information will ensure that the information will be used only for the purpose set out in the agreement;

     (iii) providing that the person who is to receive the information will take reasonable steps to ensure the security and confidentiality of the information; and

     (iv) specifying when the person who is to receive the information must do all or any of the following:

         (A) return to the trustee or designated archive any original records or copies of records containing personal health information;

         (B) destroy any copies of records containing personal health information received from the trustee or designated archive or any copies made by the researcher of records containing personal health information received from the trustee or designated archive.

(2) Where it is not reasonably practicable for the consent of the subject individual to be obtained, a trustee or designated archive may use or disclose personal health information for research purposes if:

   (a) the research purposes cannot reasonably be accomplished using de-identified personal health information or other information;

   (b) reasonable steps are taken to protect the privacy of the subject individual by removing all personal health information that is not required for the purposes of the research;

   (c) in the opinion of the research ethics committee, the potential benefits of the research project clearly outweigh the potential risk to the privacy of the subject individual; and

   (d) all of the requirements set out in clauses (1)(a) to (c) are met.

29(1)
Subsection 29(1) details the circumstances in which a trustee or a designated archive may use or disclose personal health information for the purposes of research if the subject individual has given express consent. However, the conditions described in subsections (a)-(c) must be met.
29(1)(a)
The trustee or designated archive must be of the opinion that the research project is not contrary to the public interest. When making an assessment to whether the research project is not contrary to the public interest in the trustee or designated archive should consider the degree to which the proposed research may contribute to:

- identification, prevention or treatment of illness or disease;
- scientific understanding relating to health;
- promotion and protection of the health of individuals and communities;
- improved delivery of health services; or
- improvements in health system management.

29(1)(b)
Before a trustee or designated archive uses or discloses personal health information for the purposes of research, they must ensure that the research project has been approved by a research ethics committee approved by the Minister.

The role of a research ethics committee is to assess whether, in the opinion of the research ethics board:

- the proposed research is of sufficient importance that the public interest in the proposed research outweighs to a substantial degree the public interest in protecting the privacy of the individuals who are the subjects of the health information to be used in the research;
- the researcher is qualified to carry out the research and review the agreement discussed in subsection 29(1)(c); and
- adequate safeguards will be in place at the time the research will be carried out to protect the privacy of the individuals who are the subjects of the health information to be used in the research and the confidentiality of that information.

Note: For further information please contact the Ministry of Health

29(1)(c)
The trustee or designated archive must enter in to a written agreement with the researcher before the personal health information is used or disclosed. The agreement must address the following:

- an assurance that the researcher will not disclose the personal health information;
- a statement about how the personal health information will be used and that the researcher will only use it for those purposes;
- a statement indicating the researcher will take reasonable steps to ensure the security and confidentiality of the personal health information. “Reasonable steps” means putting physical, administrative and technical safeguards in place as discussed in Part III of HIPA; and
- describe what will occur with the personal health information once the research is complete. This would be either:
  - returning the personal health information to the original trustee or designated archive; or
o if copies of the personal health information were made and provided to the researcher, destroying personal health information in a secure manner. See section 17 of this Guide.

To make an agreement as strong as possible, see Appendix H – on information sharing agreements.

29(2)
Subsection 29(2) details the circumstances in which a trustee or a designated archive may use or disclose personal health information for the purposes of research if it is not reasonably practical to obtain express consent. However, the conditions described in subsections (a)-(d) must be met.

Not reasonably practicable refers to something that is not feasible or possible from a realistic or practical standpoint.

29(2)(a)
The trustee or designated archive must first consider whether the personal health information can reasonably be de-identified.

Subsection 2(d) of HIPA defines de-identified personal health information as “personal health information from which any information that may reasonably be expected to identify an individual has been removed”.

See Appendix G – for more information on de-identification of personal health information.

29(2)(b)
Trustees and designated archives must ensure that only personal health information that is absolutely necessary for the purposes of the research. This might include severing information from documents or providing print outs from electronic systems with only the relevant data fields.

29(2)(c)
When making an assessment as to whether the public interest in the potential benefits of the research outweighs protecting the privacy of the subject individuals, a research ethics board must consider the degree to which the proposed research may contribute to:

• identification, prevention or treatment of illness or disease;
• scientific understanding relating to health;
• promotion and protection of the health of individuals and communities;
• improved delivery of health services; or
• improvements in health system management.

29(2)(d)
Before a trustee uses or discloses personal health information for research purposes without consent from the subject individuals, it must follow the conditions set out in subsections 29(1)(a)-(c).
Use or disclosure prohibited (section 30)

30(1) No person who is aware, or should reasonably be aware, that he or she has received personal health information in contravention of this Act shall use or disclose the information without the consent of the subject individual or, where the subject individual is deceased, without the consent of a prescribed person.

(2) Subsection (1) does not apply to personal health information disclosed by a trustee to a member of the subject individual’s immediate family or to anyone else with whom the subject individual has a close personal relationship.

30(1)
Section 30(1) prohibits anyone from using or disclosing personal health information that has been received in error if that person is aware or should reasonably be aware that it is not in accordance with HIPA.

People who should reasonably be aware, that he or she has received personal health information in contravention of HIPA would include trustees or employees of trustees and designated archives.

30(2)
Subsection 30(1) does not apply to personal health information disclosed by a trustee to a member of the subject individual’s immediate family or to anyone else with whom the subject individual has a close personal relationship.
ACCESS OF INDIVIDUALS TO PERSONAL HEALTH INFORMATION (PART V OF HIPA)

Note: Please see diagram Steps to Respond to an Access to Personal Health Information Request found in this Guide.

Interpretation of Part (section 31)

31 In this Part:

(a) “applicant” means an individual who makes a written request for access to personal health information about himself or herself;

(b) “written request for access” means a request made pursuant to section 34.

This part addresses an individual’s requests for personal health information about himself/herself. This is a right provided by section 12 of HIPA.

An applicant can designate certain representatives to request personal health information on his/her behalf. See sections 15 and section 56 of HIPA.

Right of access (section 32)

32 Subject to this Part, on making a written request for access, an individual has the right to obtain access to personal health information about himself or herself that is contained in a record in the custody or control of a trustee.

A trustee must provide an individual with personal health information about himself or herself, even if it exists in an electronic form.

There are limited circumstances where a trustee can deny access to personal health information which are listed in section 38.

Control connotes authority. A record is under the control of a trustee when the trustee has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. Custody is not a requirement for control.

The 15 criteria suggested for determining any measure of control is:

1. The record was created by the trustee or a staff member of the trustee in the course of his or her duties performed for the trustee;
2. The record was created by an outside consultant for the trustee;
3. The trustee possesses the record, either because it has been voluntarily provided by the creator or pursuant to a mandatory or statutory or employment requirement;
4. An employee of the trustee possesses the record for the purposes of his or her duties performed for the trustee;
5. The record is specified in a contract as being under the control of a trustee and there is no understanding or agreement that the records are not to be disclosed;

6. The content of the record relates to the trustee’s mandate and core, central or basic functions;

7. The trustee has a right of possession of the record;

8. The trustee has the authority to regulate the record’s use and disposition;

9. The trustee paid for the creation of the records;

10. The trustee has relied upon the record to a substantial extent;

11. The record is closely integrated with other records held by the trustee;

12. A contract permits the trustee to inspect, review and/or possess copies of the records the contractor produced, received or acquired;

13. The trustee’s customary practice in relation to custody or control of records of this nature in similar circumstances;

14. The customary practice of other trustees in relation to possession or control of records of this nature in similar circumstances; and

15. The owner of the records.

All 15 criteria do not have to be met in order to find that a trustee has a measure of control.

Custody is the physical possession of a record by a trustee.

**Oral request for access (section 33)**

33 Nothing in this Act precludes:

(a) an individual from making an oral request for access to personal health information about himself or herself that is contained in a record in the custody or control of a trustee; or

(b) a trustee from responding to an oral request.

Oral request means an applicant is verbally asking for personal health information.

Pursuant to section 12 of HIPA, an applicant’s access rights for under HIPA is limited to his/her personal health information. HIPA enables applicants to request access to his/her personal health information by simply asking to see it.

A trustee can choose to respond to an oral request or require the applicant to submit a written request. It is best practice for a trustee to document an oral request and the date it was made.

Things to consider:

- Does the Applicant have a language barrier or disability that would make it difficult for him/her to make a written request?
- It would be best to get a written request if:
The request is complex, large or decentralized;  
Fees will be applied;  
Records are missing; or  
Records may be denied.

Trustees should also inform applicants that make an oral request that the Office of the Information and Privacy Commissioner can only review responses to written requests. (See subsection 34(4) of this Guide.)

Written request for access (section 34)

34(1) An individual may, in accordance with the regulations, make a written request for access to personal health information about himself or herself that is contained in a record in the custody or control of a trustee.

(2) A written request for access must:
   a. be made to the trustee that the applicant believes has custody or control of the record containing the personal health information; and
   b. contain sufficient detail to enable the trustee to identify the personal health information requested.

(3) An applicant must prove his or her identity to the satisfaction of the trustee.

(4) The right to make an application for review pursuant to section 42 applies only to written requests for access.

Once in receipt of a written application, the trustee must comply with the provisions in section 34 of HIPA.

34(1)
The HIPA Regulations do not specifically address an applicant’s written request for access.

34(2)(a)
If a trustee does not have custody or control of the personal health information that an individual is seeking, the trustee should either inform the applicant or transfer the request to a trustee that may have the records. See subsections 36(1)(b) and subsection 36(1)(d) of HIPA.

34(2)(b)
If the trustee does not know or understand what the Applicant is requesting, the trustee should contact the applicant to clarify. This is part of the duty to assist (see subsection 35(1) of HIPA).
34(3)
For the purposes of verifying someone’s identity, a trustee should not collect information (such as photocopying photo identification). A note in the individual’s file that photo identification was verified is sufficient.

See section 21(a)

Duty to assist (section 35)

35(1) Subject to sections 36 to 38, a trustee shall respond to a written request for access openly, accurately and completely.

(2) On the request of an applicant, a trustee shall:

(a) provide an explanation of any term, code or abbreviation used in the personal health information; or

(b) if the trustee is unable to provide an explanation in accordance with clause (a), refer the applicant to a trustee that is able to provide an explanation.

35(1)
Subsection 35(1) indicates that trustees have a duty to respond to an applicant openly, accurately and completely. The standard the trustee must meet to respond openly, accurately and completely is not a standard of perfection, but rather what is reasonable for a trustee to do in order to assist the applicant who is making an access request.

Examples of ways a trustee can meet the duty to assist include:

- **Assisting applicants clarifying.** The applicant is not fully knowledgeable as to what records may exist or how they are organized, for example, the trustee has a duty to tell the applicant what they need-to-know in order for them to obtain as much of the information they are seeking as possible.

- **Transferring requests when appropriate.** If there is an indication that another trustee may also have personal health information about the individual, as part of the duty to assist, applicants should be advised that another trustee or other organization may have personal health information about them. The trustee should still provide any relevant personal health information to the applicant. If the trustee does not have any of the requested personal health information, the trustee must transfer the request to the other trustee (see subsection 36(1)(d) and subsection 36(2) of HIPA).

- **Undertake an adequate search for records.** A reasonable search is one in which an employee, experienced in the subject matter, expends a reasonable effort to locate records which are reasonably related to the request. The threshold that must be met is one of “reasonableness”. In other words, it is not a standard of perfection, but rather what a fair and rational person would expect to be done or consider acceptable. HIPA does not require the trustee to prove with absolute certainty that records do not exist.
More about searching for personal health information

When a patient makes an access to information request for his or her personal health information, the search for responsive records may not be as easy as just checking out the health records department. HIPA applies to all personal health information in the custody or control of the trustee. All records, in any form, that are responsive to the request, must be identified, located and retrieved within 30 calendar days.

The right of access by a patient or an applicant extends to all personal health information that is in the custody or under the control of the trustee regardless of who created it, where it came from or how it is stored.

Records may be in paper or electronic form whether found in a file drawer, legacy system, electronic medical record (EMR) or electronic health record (EHR). Electronic or digital records include electronic documents, such as word processed documents, spreadsheets, email, digital photographs and scanned images and electronic data, such as information stored in databases or registries or in rarer cases, back-up tapes.

Regardless of the medium, a thorough search needs to be conducted. For instance, the IPC dealt with a request for access to records from the 1960s. The records existed on microfiche only so the trustee had to find a way to read and copy even though the trustee no longer had the technical capability. The take away lesson, as long as records have not been destroyed, access rights of the individual remain intact and records need to be produced wherever they reside.

A request for access may be unduly general or vague because the applicant lacks knowledge of the trustee’s operations or programs and the type of health records that may exist. These types of requests may prove challenging for a large trustee organization (i.e. a regional health authority) as would require a search of all facilities, program areas and information systems. This is why communicating with the applicant early on in the process to clarify the request is critical. This communication is also in keeping with a trustee’s obligations under section 35 of HIPA.

Section 35 is the express duty to assist which requires a trustee to make every reasonable effort to assist an applicant and to respond to each openly, accurately and completely. This means that if the applicant does not understand what records may exist or how they are organized, the trustee should clarify to assist the applicant in obtaining as much information as possible that he or she is entitled to under the Act.

The responsibility to maintain records may fall to many different individuals at different times resulting in records being temporarily retained on the unit, in individual employee’s offices, vehicles or homes, managed off-site by an information management service provider (IMSP) or put into storage while waiting to be culled (i.e. non-active files). When applicable, records in the physical possession of contracted agencies may also have to be located as may have records responsive to an access request (e.g. independent medical examination).

Also, a search at one time may reveal responsive records, but not necessarily all. For instance, what about records that are in the queue, (i.e. not yet dictated)? Patient care is not static. There will always be new responsive records being generated.

Best practice is to start with a search strategy by talking to the ‘people in the know’ before proceeding (e.g. record managers). It will save you a lot of time in the long run! And don’t
forget to document both your search strategy and keep details of the actual search. In the event a review is undertaken by the IPC, those details may be requested and should speed up the process for all involved.

Appendix J – Checklist for searching for personal health information is meant to be a guide to assist in searching for personal health information.

Please note, that providing those details is not a guarantee that the IPC will find the search conducted was reasonable. Each case will require different search strategies and details depending on the records requested.

35(2)
In addition to providing the record, the trustee must provide, at the applicant’s request, an explanation of any term, code or abbreviation used in the record. If the trustee is unable to provide the necessary explanations to the applicant, the trustee must refer the applicant to a trustee who would be able to do so.
Diagram – Steps to Respond to an Access to Personal Health Information Request

Step to Responding to an Access to Information Request for Personal Health Information

HIPA provides an individual with the right to access personal health information about himself or herself that is contained in a record in the custody or control of a trustee (s. 32). If the trustee does not have control of the information that the individual is seeking, the trustee should either inform the applicant or transfer the request.

<table>
<thead>
<tr>
<th>Request received from applicant</th>
</tr>
</thead>
<tbody>
<tr>
<td>The clock starts now! HIPA provides that a trustee must respond to a written request for access within 30 days (s. 36). Within this period a trustee can inform the applicant they will extend this deadline by another 30 days (s. 37).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Duty to assist (s. 35)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A trustee has a duty to assist. The trustee shall provide open, accurate and complete information. The trustee must provide an explanation of terms, codes or abbreviations. If the trustee is unable to provide an explanation they should refer the applicant to a trustee that is able to.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clarify Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the trustee does not know or understand what the applicant is requesting, the trustee should contact the applicant to clarify.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently there is no fee schedule for HIPA; however, the OIPC recommends trustees use the fee schedule provided in the LA FOIP Regulations for guidance. This fee schedule appears in the IPC Guide to HIPA in section 39.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Was the request made in writing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A written request must:</td>
</tr>
<tr>
<td>• Be made to the trustee that the applicant believes has custody or control of the PHI.</td>
</tr>
<tr>
<td>• Contain sufficient detail to enable the trustee to identify the PHI requested.</td>
</tr>
<tr>
<td>• Allow the identity of the applicant be proven. For the purposes of verification of identity, photocopies should not be collected and added to the record.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Should access be denied?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notify Applicant of denial in writing as prescribed in s. 36(1)(c).</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPA provides a trustee authority to refuse access to an applicant. This may occur if (s. 36):</td>
</tr>
<tr>
<td>• It is the opinion of the trustee that the information may result in danger to the health or safety of any person.</td>
</tr>
<tr>
<td>• The PHI is about an individual other than the applicant.</td>
</tr>
<tr>
<td>• The PHI may lead to the identification of another individual.</td>
</tr>
<tr>
<td>• The information was collected for the principle use of a civil, criminal or quasi-judicial proceeding.</td>
</tr>
<tr>
<td>• The disclosure could interfere with a lawful investigation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Advise that best-practice is a written request</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPA provides that a request may be made orally. It is best practice that the request is made in writing as the OIPC can only review responses to written requests (s. 33).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Will the request be subject to fees?</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Should access be denied?</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ask for the request to be made in writing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Release the requested PHI to the applicant.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The original copy of the patient health record must remain intact. Photocopy reproduction is best practice. Important: verify the identity of the applicant before releasing the record. For the purposes of verification of identity, photocopies should not be collected and added to the record.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Severing PHI (s. 38)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPA provides that if the option is available where the portion of the PHI that the trustee refuses to release can be severed and the rest of the PHI can be released this would be an appropriate action.</td>
</tr>
</tbody>
</table>

This relates to The Health Information Protection Act (HIPA).
Response to written request (section 36)

36(1) Within 30 days after receiving a written request for access, a trustee must respond to the request in one of the following ways:

(a) by making the personal health information available for examination and providing a copy, if requested, to the applicant;
(b) by informing the applicant that the information does not exist or cannot be found;
(c) by refusing the written request for access, in whole or in part, and informing the applicant:
   (i) of the refusal and the reasons for the refusal; and
   (ii) of the applicant’s right to request a review of the refusal pursuant to Part VI;
(d) by transferring the written request for access to another trustee if the personal health information is in the custody or control of the other trustee.

(2) A trustee that transfers a written request for access pursuant to clause (1)(d) must notify the applicant of the transfer as soon as reasonably possible, and the trustee to whom the written request for access is transferred must respond to it within 30 days after the date of transfer.

(3) The failure of a trustee to respond to a written request for access within the period mentioned in subsection (1) or (2) is deemed to be a decision to refuse to provide access to the personal health information, unless the written request for access is transferred to another trustee pursuant to clause (1)(d).

Section 36(1) provides that a trustee must make every reasonable effort to respond to a request within 30 days after receiving the request. In limited circumstances, a trustee may extend this timeline by 30 days pursuant to section 37 of HIPA (see section 37 of HIPA). The trustee’s response must be in accordance with subsections 36(1)(a)-(d) of HIPA.

The 30 day limit is based on calendar days. The time period begins on the date the request is received by the trustee. The short time period in which HIPA requires a request to be processed emphasizes the usefulness of having a written request so that the starting date is clear. It is best practice to date stamp any written request.

If the request is incomplete and further information is required from the applicant, trustee should seek this information immediately (See subsection 35(1) – Duty to assist). The need to clarify with an applicant would “stop the clock”. For example, the time from when the trustee received the request to the time it made attempts to contact the applicant would count in the 30 days; however, the time a trustee spent waiting for an applicant to respond would not count (eg. waiting for the applicant to return a phone call).

If a trustee does not respond within 30 days, it is considered a deemed refusal. (See subsection 36(3) of HIPA).
36(1)(a)
If access to personal health information is to be granted to the subject individual, the trustee’s response must inform the applicant of one of two things:

1. If it can be reasonably reproduced, provide a copy of the personal health information to the applicant. This can be done once fees have been paid. (See section 39 - Fees).

2. If it is not possible to provide a copy of the records, the applicant should be told when and where the records will be available for examination.

36(1)(b)
If the trustee does not have the records that the applicant is seeking, it should inform the applicant. If the trustee is aware of another trustee that may have personal health information relevant to the applicant’s request, the trustee should transfer the request to that trustee pursuant to subsections 36(1)(d) and 36(2).

If records do not exist or the request is being transferred, it is best practice to advise the applicant of his/her right to request a review by the Information and Privacy Commissioner. Suggested wording is as follows:

- If you are unsatisfied and would like to exercise your right to request a review of this decision, you may do so within one year of this notice by contacting the Saskatchewan Information and Privacy Commissioner at (306) 787-8350 or www.oipc.sk.ca.

36(1)(c)
If a trustee intends to deny the applicant access to personal health information within its custody or control, it must only do so in accordance with section 38 of HIPA. (See section 38 – Refusing access).

If section 38 applies, a trustee should give access to as much as the record as possible. Records may contain both information that can be released and other information that should be excepted from disclosure. When information that falls within an exception can reasonably be severed from a record, an applicant has a right of access to the remainder of the record. A trustee should sever the portions to which section 38 applies and grant access to the rest of the personal health information. See section 38 of HIPA.

If access is refused, the trustee must inform the applicant of the decision. This includes which subsection of 38 the trustee is relying upon to refuse access. The trustee should also provide a brief explanation of the subsection and how it applies to the personal health information in question.

The trustee must also advise the applicant of his/her right to request a review by the Information and Privacy Commissioner. Suggested wording is as follows:

- If you are unsatisfied and would like to exercise your right to request a review of this decision, you may do so within one year of this notice by contacting the Saskatchewan Information and Privacy Commissioner at (306) 787-8350 or www.oipc.sk.ca.

36(1)(d)
If the trustee does not have the records that the applicant is seeking, and is aware of another trustee that may have custody or control of the personal health information relevant to the
applicant’s request, the trustee should transfer the request to that trustee pursuant to this subsection and 36(2).

It is best practice to obtain the applicant’s consent before transferring the request.

Once the request has been transferred, the trustee should confirm in writing with the trustee that the request has been transferred.

If the request is being transferred, it is best practice to advise the applicant of his/her right to request a review by the Information and Privacy Commissioner. Suggested wording is as follows:

- If you are unsatisfied with the transfer and would like to exercise your right to request a review of this decision, you may do so within one year of this notice by contacting the Saskatchewan Information and Privacy Commissioner at (306) 787-8350 or www.oipc.sk.ca.

36(2)
Pursuant to subsection 36(1)(d), a trustee must transfer the request within 30 days of receiving it.

A trustee who receives a transferred request must then respond within 30 days of the date of transfer. Part V of HIPA applies to the request.

36(3)
If a trustee does not respond to a written request for access it is considered a deemed refusal. Subsection 36(3) clearly establishes that the failure of a trustee to respond to a request within the 30 day period or any extended period is to be treated as a decision to refuse access to the particular records. Such action qualifies the request for complaint and review.

Extension of time (section 37)

37(1) A trustee may extend the period set out in subsection 36(1) for a reasonable period not exceeding 30 days where:

(a) the request is for access to a large number of records or necessitates a search through a large number of records or there is a large number of requests, and completing the work within the original period would unreasonably interfere with the operations of the trustee; or

(b) consultations that are necessary to comply with the request cannot reasonably be completed within the original period.

(2) A trustee who extends a period pursuant to subsection (1) shall give notice of the extension to the applicant within 30 days after the request is made.

There are two circumstances where a trustee may delay in responding to a written access request past the 30 days prescribed in section 36 of HIPA.
37(1)(a)
In order to extend the time to respond to an access request pursuant to subsection 37(1)(a), the trustee must consider the following:

- a large number of records have been requested or must be searched, and
- that meeting the time limit would unreasonably interfere with the operations of the trustee.

In its resource entitled Time Extension Request Guidelines for Public Bodies, the Office of the Information and Privacy Commissioner for British Columbia has suggested these considerations when extending timelines:

**Volume:**
- How many pages?
- Do the records require special handling?
- Does the type of record require different methods of searching or handling?
- How does volume compare with average request volume?

**Circumstances that may contribute to unreasonable interference:**
- Significant increase in requests (e.g., sharp rise over 1-4 months)
- Computer systems or technical problems
- Unexpected leave of staff
- Unusual number (high percentage) of new staff
- Type of records
- Number of program areas searched
- Location of records

**Invalid Circumstances:**
- Long term or systemic problems
- Vacations
- Office processes (e.g. sign-off)
- Personal commitments
- Pre-planned events
- Type of applicant

37(1)(b)
In order to extend the time to respond to an access request pursuant to subsection 37(1)(b), the trustee must consider the following again taken from the Time Extension Request Guidelines for Public Bodies resource:

The trustee should be able to explain why it is necessary to consult with a third party or other trustee in order to make a decision about access, including how the third party or other trustee is expected to assist. Also, the trustee needs to explain why it needs more time to do this.

**Some valid reasons for consulting:**
- Third party or other trustee has an interest in the records
- Records created or controlled jointly

**Other Relevant Information:**
- When did trustee initiate consultation?
- Large number of consultations required
- Availability of third party or trustee contacts
- Did trustee set deadline expectations for third party or other trustee?
- Is time required for consultation reasonable?
- Has the trustee followed up on consultation request?
Invalid Circumstances:
• Consultations with staff of the same trustee organization
• Consultations for a purpose other than deciding whether to give access

37(2)
A trustee who extends the time period to respond to a written request should advise the applicant in writing of the extension within the original 30 day period.

Refusing access (section 38)

38(1) Subject to subsection (2), a trustee may refuse to grant an applicant access to his or her personal health information if:

(a) in the opinion of the trustee, knowledge of the information could reasonably be expected to endanger the mental or physical health or the safety of the applicant or another person;

(b) disclosure of the information would reveal personal health information about another person who has not expressly consented to the disclosure;

(c) disclosure of the information could reasonably be expected to identify a third party, other than another trustee, who supplied the information in confidence under circumstances in which confidentiality was reasonably expected;

(d) subject to subsection (3), the information was collected and is used solely:
   (i) for the purpose of peer review by health professionals, including joint professional review committees within the meaning of The Saskatchewan Medical Care Insurance Act;
   (ii) for the purpose of review by a standards or quality of care committee established to study or evaluate health services practice in a health services facility or health services agency, including a committee as defined in section 10 of The Evidence Act; or
   (iii) for the purposes of a body with statutory responsibility for the discipline of health professionals or for the quality or standards of professional services provided by health professionals;

(e) the information was collected principally in anticipation of, or for use in, a civil, criminal or quasi-judicial proceeding; or

(f) disclosure of the information could interfere with a lawful investigation or be injurious to the enforcement of an Act or regulation.

(2) Where a record contains information to which an applicant is refused access, the trustee shall grant access to as much of the record as can reasonably be severed without disclosing the information to which the applicant is refused access.

(3) Where access to personal health information is refused pursuant to clause (1)(d), a trustee must refer the applicant to the trustees from which the personal health information was collected.
Note: Please see the diagram Steps to How to grant access to a record that contains personal health information of two individuals found in this Guide.

38(1)
Section 38(1) lists the reasons for which a trustee can deny access to an individual's own personal health information.

38(1)(a)
Endanger means the act of putting someone or something in danger; exposure to peril or harm.

Safety implies relative freedom from danger or risks.

Physical health refers to the well-being of an individual's physical body.

Mental health refers to the functioning of a person’s mind in a normal state. In order to determine whether a threat to the safety, physical or mental health of any person exists, the trustee should apply the following test:

1. there must be a reasonable expectation of probable harm;
2. the harm must constitute damage or detriment and not more inconvenience; and
3. must be a causal connection between disclosure and the anticipated harm.

The trustee must make an assessment of the risk and determine whether there are reasonable grounds for concluding there is a danger to the health or safety of any person. That assessment must be specific to the circumstances of the case under consideration. The trustee should consider if there is documented evidence of the individual's background that suggests mental or physical problems/concerns or instability that would lead the trustee to conclude that release would result in harm to the requestor or another individual (i.e., a history of violence or mental breakdown that, upon accessing information, would likely trigger a violent response directed at him/herself or others).

The inconvenience, upset or unpleasantness of dealing with difficult or unreasonable people is not sufficient to trigger this section. The threshold cannot be achieved on the basis of unfounded, unsubstantiated allegations.

The trustee should be able to detail what the harm is and to whom the harm threatens if the information were released.

For example, the mental or physical health of a person would be threatened if information were disclosed to an applicant that would cause severe stress such as suicidal ideation or that could result in verbal or physical harassment or stalking. Individual safety could be threatened if information were released that allowed someone who had threatened to kill or injure the individual to locate him or her. Examples of individuals whose safety might be threatened would include an individual fleeing from a violent spouse, a victim of harassment or a witness to harassment, an employee who has been threatened.

Could versus could reasonably be expected to have different requirements. The requirement for could is simply that the release of information could have the specified result. The threshold test for a reasonable expectation is somewhat higher.

Could reasonably be expected to provides a middle ground between that which is probable and that which is merely possible. The trustee must provide evidence well beyond or
considerably above a mere possibility of harm in order to reach that middle ground. This inquiry, of course, is contextual and what is needed to meet this standard will ultimately depend on the nature of the issue and inherent probabilities or improbabilities or the seriousness of the allegations or consequences.

38(1)(b)
Subsection 38(1)(b) requires a trustee to refuse to disclose personal health information to an applicant if the personal health information is also about an individual other than the applicant, unless the other individual has consented to the disclosure.

The trustee can attempt to obtain consent from the other individual; however, the trustee should check to see if the identity of the applicant can be disclosed to the other individual.

There may be situations where an applicant has provided personal health information about family members or other relatives to his or her physician in the context of providing a medical history. The information about other individuals provided by the applicant as part of their medical history could be disclosed to the applicant requesting access to his or her personal health information.
Diagram - How to grant access to a record that contains personal health information of two individuals (s. 38(1)(b))

Subsection 38(1)(b) of The Health Information Protection Act

- Is the applicant (or representative) requesting their own personal health information that includes the personal health information of another individual? 
  - Yes
  - Ask the applicant if you can disclose his/her identity to the other individual
    - Yes
    - Ask the other individual if he/she consents to the disclosure of his/her personal health information to the applicant
      - Yes
      - Release the record to applicant (s. 38(1))
      - No
      - Can the record be severed?
        - Yes
        - Sever the record (s. 38(2))
        - No
        - Access denied, notify applicant (s. 38(1)(c))
    - No
    - No
  - No
  - Section 38(1)(b) not applicable
38(1)(c)
Under section 38(1)(c) a trustee may refuse to disclose personal health information that could reasonably lead to the identification of a person who provided the personal health information to the trustee explicitly or implicitly in confidence. To fit within the subsection, collection of the personal health information in question should have been in accordance with subsection 25(1) of HIPA.

The person who provided the personal health information must also have done so in circumstances where it would be appropriate that the name of the person be kept confidential.

The subsection does not require a trustee to demonstrate that harm could come to the source but must make a determination, based on the relevant circumstances, that it is appropriate to protect the identity of the source.

Could versus could reasonably be expected to have different requirements. The requirement for could is simply that the release of information could have the specified result. The threshold test for a reasonable expectation is somewhat higher.

Could reasonably be expected to provides a middle ground between that which is probable and that which is merely possible. The trustee must provide evidence well beyond or considerably above a mere possibility of harm in order to reach that middle ground. This inquiry, of course, is contextual and what is needed to meet this standard will ultimately depend on the nature of the issue and inherent probabilities or improbabilities or the seriousness of the allegations or consequences.

It is common to privacy laws in Saskatchewan and other jurisdictions that the “personal information” of an individual includes opinions of others about that subject individual. It appears that in drafting HIPA, section 38(1)(c) was carefully written in such a way that the focus is not on whether someone views the opinions about another as confidential or not but rather whether providing access will identify a source who provided information with a reasonable expectation of confidentiality.

38(1)(d)(ii)
This provision enables a trustee to withhold personal health information from the subject individual if it was collected and used solely by a standards or quality of care committee that has as its primary purpose the carrying out of quality of care activities pursuant to section 10 of The Evidence Act of Saskatchewan.

Pursuant to subsection 10(1) of The Evidence Act, a quality improvement committee means a committee designated as a quality improvement committee by a health services agency to carry out a quality improvement activity the purpose of which is to examine and evaluate the provision of health services for the purpose of:

(a) educating persons who provide health services; or

(b) improving the care, practice or services provided to patients by the health services agency;

HIPA also considers standards of care committees and quality of care committees which may be internal to an organization or made up of several trustees.

The personal health information also should have been collected in accordance with subsection 27(4)(g) of HIPA. For more information, see subsection 27(4)(g) of HIPA. See also subsection 38(3) of HIPA.
38(1)(d)(iii)
This subsection authorizes a trustee to withhold personal health information of an individual if it was collected or used solely by a health professional body for the carrying out its duties pursuant to an Act with respect to regulating the profession.

The personal health information must have been collected in accordance with subsection 27(4)(h) of HIPA.

See also subsection 38(3) of HIPA.

38(1)(f)
The trustee must be able to demonstrate that it anticipated such a proceeding before the collection was made.

Legal proceedings are proceedings governed by rules of court or rules of judicial or quasi-judicial tribunals that can result in a judgment of a court or a ruling by a tribunal. Legal proceedings include all proceedings authorized or sanctioned by law, and brought or instituted in a court or legal tribunal, for the acquiring of a right or the enforcement of a remedy.

38(2)
Personal health information may contain both information that can be released and other information that should not be disclosed pursuant to subsection 38(1) of HIPA. When information that falls within an exception can reasonably be severed, the applicant has a right of access to the remainder of the personal health information.

In some cases, personal health information cannot be severed. The trustee must then refuse access to the whole record and must be prepared to demonstrate to the Information and Privacy Commissioner the technical reasons underlying the inability to sever.

Some methods of severing can include:
- the use of non-permanent white tape over the portion to be withheld on a copy of the record and recopying to obtain the record to be released to the applicant;
- use of liquid eraser over the portion to be withheld on a copy of the record and recopying to obtain the record to be released; or
- use of a photocopier or scanner with editing features suitable for severing.

A trustee should indicate the section number of any exception used to sever information, either in the space left after the severing or in the margin closest to the severed information.

38(3)
If personal health information has been collected for one of the reasons discussed in subsection 38(1)(d), the trustee should refer the applicant to the other trustees. See also 36(1)(d) of HIPA.
Fee (section 39)

39 A trustee may charge a reasonable fee not exceeding the prescribed amount to recover costs incurred in providing access to a record containing personal health information.

Currently, the HIPA Regulations do not address the subject of fees. However, the Office of the Information and Privacy Commissioner recommends that trustees use the fee schedule provided in The Freedom of Information and Protection of Privacy Regulations or The Local Authority Freedom of Information and Protection of Privacy Regulations for guidance.

There are three kinds of fees that a trustee can charge:

1. Fees for searching for a responsive record.

   Search time consists of every half hour of manual search time required to locate and identify responsive records. A trustee can charge $15 per half hour of search time. Activities that qualify as search time include:
   - staff time involved with searching for records;
   - examining file indices, file plans or listings of records either on paper or electronic;
   - pulling paper files/specific paper records out of files; and
   - reading through files to determine whether records are responsive.

   Search time does not include:
   - time spent to copy the records;
   - time spent going from office to office or off-site storage to look for records; or
   - having someone review the results of the search.

2. Fees for preparing the record for disclosure.

   Preparation includes time spent preparing the record for disclosure. A trustee can charge $15 per half hour of preparation time. Activities that qualify as preparation time include:
   - time anticipated to be spent physically severing exempt information from records. See section 38 of HIPA.

   Preparation time does not include:
   - Deciding whether or not to claim an exemption;
   - Identifying records requiring severing;
   - Identifying and preparing records requiring third party notice;
   - Packaging records for shipment;
   - Transporting records to the mailroom or arranging for courier service;
   - Time spent by a computer compiling and printing information;
• Assembling information and proofing data;
• Photocopying; and
• Preparing an index of records.

The test related to reasonable time spent on preparation is:
• Generally, it should take an experienced employee 2 minutes per page to physically sever only.

3. Fees for the reproduction of records.

Fees for reproduction of the record are taken right out of The Freedom of Information and Protection of Privacy Regulations or The Local Authority Freedom of Information and Protection of Privacy Regulations. The most common fees are as follows:
• for a photocopy, $0.25 per page;
• for a computer printout, $0.25 per page;
• for a paper print from microfilm, $0.50 per page; (g) for a print of a photograph or slide:
  • $5 per 4” x 6” black and white print;
  • $8 per 4” x 6” colour print;

For further guidance, see the LA FOIP Regulations.

The convention is to waive any fees less than $50. However, some trustees may charge an application fee of $20.

If a trustee believes fees will be more than $50, it is a good idea to provide the applicant with a fee estimate. This includes a rough estimate of the total cost broken down into the three types of fees noted above. A trustee should also make the applicant aware of any reasons why personal health information might be severed (pursuant to section 38 of HIPA). It is reasonable to ask for a deposit of 50% of the estimate. If the actual cost is less than the estimate, the trustee should only charge the actual cost.
Right of amendment (section 40)

40(1) An individual who is given access to a record that contains personal health information with respect to himself or herself is entitled:

(a) to request amendment of the personal health information contained in the record if the person believes that there is an error or omission in it; or

(b) if an amendment is requested but not made, to require that a notation to that effect be made in the record.

(2) A request for amendment must be in writing.

(3) Within 30 days after a request for amendment is received, the trustee shall advise the individual in writing that:

(a) the amendment has been made; or

(b) a notation pursuant to clause (1)(b) has been made.

(4) Subject to subsection (6), where a trustee makes an amendment or adds a notation pursuant to clause (1)(b), the trustee must, where practicable, give notice of the amendment or notation to any other trustee or person to whom the personal health information has been disclosed by the trustee within the period of one year immediately before the amendment was requested.

(5) A trustee that receives a notice pursuant to subsection (4) must make the amendment or add the notation to any record in the custody or control of the trustee that contains personal health information respecting the individual who requested the amendment.

(6) A trustee is not required to notify other trustees where:

(a) an amendment or a notation cannot reasonably be expected to have an impact on the ongoing provision of health services to the individual; or

(b) the personal health information was disclosed to the other trustees for any of the purposes or in any of the circumstances set out in subsection 27(2).

(7) An amendment required to be made pursuant to this section must not destroy or obliterate existing information in the record being amended, other than registration information.

Note: Please see diagram Steps to Responding to a request for Amendment found in this Guide.

40(1)
Pursuant to section 13 of HIPA, an individual has a right to request an amendment to his/her personal health information or have a notation made in lieu. If an individual has been given access to a record that contains his/her personal health information and wishes that it be changed, it may do one of two things as listed in subsections (a) and (b).

40(1)(a)
An individual can request that an amendment be made to his/her personal health information if there is an error or an omission.

An error is a mistake or something wrong or incorrect.

An omission means that something is missing, left out or overlooked.
40(1)(b)
If an individual has requested that an amendment be made to his/her personal health information, and was not made by the trustee, the individual can require that a notation be made on the record explaining this.

40(2)
An individual’s request for an amendment as described in subsection 40(1) must be made in writing. See subsection 34(2) of HIPA for more details.

40(3)
Subsection 40(3) provides that a trustee must make every reasonable effort to respond to a request for amendment within 30 days after receiving the request.

The 30 day limit is based on calendar days. The time period begins on the date the request is received in an office duly authorized to deal with it. It is best practice to date stamp a written request.

If the request is incomplete and further information is required from the applicant, trustee should seek this information immediately (See subsection 35(1) – Duty to assist).

The following factors should be considered for an amendment:

1. the information at issue must be personal health information;
2. the information must be inexact, incomplete or ambiguous; and
3. the correction cannot be a substitution of opinion.

If a trustee does not respond within 30 days it is considered a deemed refusal. See subsection 36(3) of HIPA.

The trustee’s response must do one of two things as described in subsections (a) and (b).

40(3)(a)
Once a trustee has made an amendment to an individual's personal health information it should advise the individual in writing within 30 days.

The applicant must initially provide some argument to support the request for amendment. A request for correction must, at a minimum:

1. Identify the personal health information the applicant believes is in error. It must be the personal health information of the applicant and not of a third party;
2. The alleged error must be a factual error or omission;
3. The request must include some evidence to support the allegation of error or omission. Mere assertions will not suffice; and
4. The proposed correction must be clearly stated and cannot be a substitution of opinion.

See also subsection 40(4) of HIPA for additional requirements.
40(3)(b)
If a trustee disagrees with the requested amendment for reasons discussed under subsection 40(3)(a), the trustee should, instead, make a notation.

A notation should include the date, who requested the amendment, what the requested amendment was and a signature of the decision maker. The notation should be made on the record near the information in question. Trustees should build ways to incorporate notations in their electronic record systems. Trustees should also record the reason why the notation instead of the change was made in the event of a review. See section 42(1)(b) of HIPA.

40(4)
Subsection 40(4) requires a trustee to inform any person to whom the personal health information has been disclosed, that the correction or amendment has been made. Notification must be given to any person who has received the information within one year prior to the request for correction or amendment. This ensures that other parties have accurate and complete information for their own decision-making processes.

Best practice is that this notice be made in writing. It should include the same details as described in subsection 32(4) of HIPA.

See also subsection 40(6) of HIPA.

40(5)
If a trustee receives a notification from another trustee, the same amendment or notation should be made to personal health information as made by the first trustee.

40(6)
A trustee does not have to notify other trustees of an amendment or notation made to an individual's personal health information pursuant to subsection 40(4) in two circumstances described in (a) and (b).

40(6)(a)
A trustee does not have to notify other trustees of an amendment or notation made to an individual's personal health information pursuant to subsection 40(4) if he/she believes it will not impact the ongoing care received by the individual.

*Could* versus *could reasonably be expected* to have different requirements. The requirement for *could* is simply that the release of information *could* have the specified result. The threshold test for a *reasonable expectation* is somewhat higher.

*Could reasonably be expected* to provides a middle ground between that which is probable and that which is merely possible. The trustee must provide evidence well beyond or considerably above a mere possibility of harm in order to reach that middle ground. This inquiry, of course, is contextual and what is needed to meet this standard will ultimately depend on the nature of the issue and inherent probabilities or improbabilities or the seriousness of the allegations or consequences.
40(6)(b)
A trustee does not have to notify other trustees of an amendment or notation made to an individual's personal health information pursuant to subsection 40(4) if the disclosure of the personal health information was made pursuant to subsection 27(2) of HIPA.

40(7)
When making an amendment or notation, a trustee should not completely erase or destroy what is to be corrected or replaced. It is important to make a record of the transaction.
Diagram – Steps to Responding to a request for Amendment

Steps to Responding to an Amendment

Section 40 of The Health Information Protection Act (HIPA)

Was the request made in writing?

Yes

No

Was the request made in writing?

Ask that the request be made in writing

Yes

Does it relate to an error or omission?

No

Does it relate to an opinion?

Yes

Collect supporting documentation if necessary

Do you agree with the request?

No

A notation is required in the patient record to the effect that there was a request for amendment, but none was made.

Yes

Where practicable, give notice of the amendment or notation to any other trustee or person to whom the personal health information has been disclosed within the period of one year immediately before the amendment was requested.

Within 30 days the individual must be informed in writing on whether the amendment was made or not made.

An amendment is the act of making a change to the personal health information of the subject individual who believes there is an error or omission.

An amendment required to be made pursuant to this section must not destroy or obliterate existing information in the record being amended, other than registration information. Example:

**Appendectomy** Splenectomy

A notation is a note made on the individual’s personal health information or in an electronic medical record indicating that the individual has requested an amendment to the personal health information. A notation should include the date, who requested the amendment, what the requested amendment was and a signature of the decision maker.
**Review and Appeal (Part VI of HIPA)**

**Interpretation of Part (section 41)**

41 In this Part:

(a) “applicant” means a person who makes an application for review;

(b) “application for review” means an application pursuant to section 42;

(c) “court” means the Court of Queen’s Bench.

An individual’s right to a review is established in section 14 of HIPA.

A review refers to the examination by the Office of the Information and Privacy Commissioner (IPC) of a decision, act or failure to act by a trustee in the course of processing a request for access to records or information under the HIPA. A review is different from a breach of privacy investigation by the IPC. For information on a privacy breach investigation, see Appendix C – Privacy Breach Guidelines.

The IPC can only review a matter if the original access request to the trustee is made in writing.

**Application for review (section 42)**

42(1) A person may apply to the commissioner for a review of the matter where:

(a) the person is not satisfied with the decision of a trustee pursuant to section 36;

(b) the person requests an amendment of personal health information pursuant to clause 40(1)(a), and the amendment is not made; or

(c) the person believes that there has been a contravention of this Act.

(2) Subject to subsection (3), an application must be made in accordance with the regulations:

(a) in the case of an application pursuant to clause (1)(a), within one year after:

   (i) the applicant is given written notice of the decision of the trustee; or

   (ii) the period mentioned in subsection 36(2) or 37(1) expires;

(b) in the case of an application pursuant to clause (1)(b), within one year after the expiry of the period mentioned in subsection 40(3); and

(c) in the case of an application pursuant to clause (1)(c), within one year after the discovery of the alleged contravention.

(3) Where a person has commenced another review process, procedure or mechanism of a trustee, an application pursuant to subsection (1) must be made within one year after the day on which the other review process, procedure or mechanism is completed.
**42(1)**

Subsection 42(1) lists circumstances where the [Commissioner](#) may undertake a [review](#). However, below is a more detailed list of potential reviewable issues.

<table>
<thead>
<tr>
<th>Reason</th>
<th>Explanation</th>
<th>During an IPC Review...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Refusal of records</strong></td>
<td>Section 38 of HIPA lists certain specific reasons why a trustee can withhold records. A trustee should specifically list which part of section 38 it is relying upon in its response to the applicant.</td>
<td>The IPC will ask the trustee to show that the subsection of 38 would apply to the record. The IPC uses certain established tests to make a determination.</td>
</tr>
<tr>
<td><strong>The record does not exist / cannot be found</strong></td>
<td>This means that the trustee does not have records that the applicant is looking for, pursuant to subsection 36(1)(b) of HIPA. A trustee does not have to create new records to answer a request.</td>
<td>The IPC would ask the trustee for a very detailed explanation of its search for records. The IPC would measure the search against best practices.</td>
</tr>
<tr>
<td><strong>No reply to an access request</strong></td>
<td>A trustee has 30 days to reply to a request once they have received it.</td>
<td>The IPC will contact the trustee and ask that a response be issued within 7 days.</td>
</tr>
<tr>
<td><strong>A request for correction to a personal health information record was not accepted</strong></td>
<td>If a trustee denies a request for amendment or, the individual may request a review.</td>
<td>The IPC will attempt to gather facts and submissions from the individual and the trustee and then make a determination if the correction should be made or only a notation be placed in the file.</td>
</tr>
<tr>
<td><strong>Fees</strong></td>
<td>Trustees are allowed to charge the applicant fees for responding to an access request (subsection 39 of HIPA). There are no legislated guidelines for the amount of fees, but the Commissioner can review to ensure fees are reasonable.</td>
<td>The IPC will ask the trustee for a detailed breakdown of the fee including how they were determined. It will be measured against established formulas from The Freedom of Information and Protection of Privacy Regulations or The Local Authority Freedom of Information and Protection of Privacy Regulations.</td>
</tr>
<tr>
<td><strong>Transfer of application</strong></td>
<td>Pursuant to subsection 36(1)(d), if a trustee receives a request for information, it may transfer the request to another trustee if it believes that the records requested are in the custody or control of that other trustee. If an applicant disagrees, they can request a review.</td>
<td>The IPC would ask for submissions from the trustee and possibly for search efforts to make a determination if the transfer was reasonable.</td>
</tr>
</tbody>
</table>
During an IPC Review...

<table>
<thead>
<tr>
<th>Reason</th>
<th>Explanation</th>
<th>IPC will assess on a case-by-case basis.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manner of providing access</strong></td>
<td>A trustee can grant access to records in several ways such as giving the applicant copies, inviting the applicant to come on premise to examine a record or providing a transcript. An applicant can request a review if he/she disagrees with the way in which access is given.</td>
<td></td>
</tr>
<tr>
<td><strong>Extension of the 30-day response period</strong></td>
<td>Pursuant to subsections 36(1) and 37, a trustee has 30 days to reply to a request once it has received it. Within this period a trustee can inform the applicant they will extend this deadline by another 30 days.</td>
<td>The IPC will ask the trustee to explain the reason for delay and make a determination if it was warranted under the circumstances.</td>
</tr>
</tbody>
</table>

For more information on what to expect during a review with the IPC, see Appendix D – What to Expect During a Review with the IPC.

42(2)

The following is a table that reflects the time period in which an Applicant can request a review:

<table>
<thead>
<tr>
<th>Section</th>
<th>Reason for review</th>
<th>Time period to request a review</th>
</tr>
</thead>
<tbody>
<tr>
<td>42(2)(a)(i)</td>
<td>Refusal of records</td>
<td>Within one year of receipt of the trustee’s response</td>
</tr>
<tr>
<td>42(2)(a)(i)</td>
<td>The record does not exist / cannot be found</td>
<td>Within one year of receipt of the trustee’s response</td>
</tr>
<tr>
<td>42(2)(a)(ii)</td>
<td>No reply to an access request</td>
<td>An applicant can request a review 60 days after the trustee receives the Applicant’s request. The request must be made within one year of that date.</td>
</tr>
<tr>
<td>42(2)(b)</td>
<td>A request for correction to a personal health information record was not accepted</td>
<td>Within one year of receipt of the trustee’s response</td>
</tr>
<tr>
<td>42(2)(c)</td>
<td>Fees</td>
<td>Within one year of receipt of the trustee’s response indicating that fees would be applied</td>
</tr>
<tr>
<td>42(2)(a)(i)</td>
<td>Transfer of application</td>
<td>Within one year of receipt of the trustee’s response indicating that the request was transferred</td>
</tr>
<tr>
<td>42(2)(a)(i)</td>
<td>Manner of providing access</td>
<td>Within one year of receipt of the trustee’s response</td>
</tr>
<tr>
<td>42(2)(a)(ii)</td>
<td>Extension of the 30-day response period</td>
<td>Within one year of receipt of the trustee’s notification</td>
</tr>
</tbody>
</table>
42(3) After a review from the IPC, the applicant can request a second review of a different issue involving the same access to information request or request for amendment within one year of the end of the review.

Review or refusal to review (section 43)

43(1) Where the commissioner is satisfied that there are reasonable grounds to review any matter set out in an application for review, the commissioner shall review the matter.

(2) The commissioner may refuse to conduct a review or may discontinue a review if, in the opinion of the commissioner, the application for review:

(a) is frivolous or vexatious;
(b) is not made in good faith;
(c) concerns a trivial matter;
(d) does not affect the applicant personally;
(e) concerns a trustee that has an internal review process that the applicant has not used;
(f) concerns a professional who is governed by a health professional body or prescribed professional body mentioned in clause 27(4)(h) that regulates its members pursuant to an Act, and the applicant has not used a complaints procedure available through the professional body; or
(g) is normally considered pursuant to another Act that provides a review or other mechanism to challenge a trustee’s decision with respect to the access to or collection, amendment, use or disclosure of personal health information, and the applicant has not used that review or mechanism.

(3) The commissioner may suspend a review where the applicant has used another review process, procedure or mechanism and that process, procedure or mechanism has not been completed.

43(1) The IPC can undertake a review if there are reasonable grounds. The reasonable grounds are described in the table in subsection 42(1) of this Guide.

43(2) Subsection 43(2) of HIPA permits the Commissioner to dismiss or discontinue a review where it appears the access provisions are not being utilized appropriately by an applicant. The Commissioner may refuse to undertake a review if one or more of the circumstances described in subsections (a) – (g) exists.

A trustee can request the Commissioner dismiss or discontinue a review based on subsection these subsections. The trustee should provide its arguments in support of its position to the IPC.
43(2)(a)  
*A frivolous* is typically associated with matters that are trivial or without merit, lacking a legal or factual basis or legal or factual merit; not serious; not reasonably purposeful; of little weight or importance.

*Vexatious* means without reasonable or probable cause or excuse. A request is *vexatious* when the **primary purpose** of the request is not to gain access to information but to continually or repeatedly harass a *trustee* in order to obstruct or grind a trustee to a standstill. It is usually taken to mean with intent to annoy, harass, embarrass, or cause discomfort. It is a pattern or type of conduct that amounts to an abuse of the **right of access**.

43(2)(b)  
*Not in good faith* means the opposite of “good faith”, generally implying or involving actual or constructive fraud, or a design to mislead or deceive another, or a neglect or refusal to fulfill some duty or other contractual obligation, not prompted by an honest mistake as to one’s rights, but by some interested or sinister motive.

When an *applicant* refuses to cooperate with a *trustee* in the process of accessing information or if a party misrepresents events to the *IPC*, this could suggest the party is not acting in good faith. Bad faith is not simply bad judgement or negligence, but rather it implies the conscious doing of a wrong because of dishonest purpose or moral obliquity; it is different from the negative idea of negligence in that it contemplates a state of mind affirmatively operating with furtive design or ill will.

43(2)(c)  
A *trivial matter* is something insignificant, unimportant or without merit. It is similar to *frivolous*.

43(2)(a)-(c)  
Some factors that may support a finding that a *request for review* will be dismissed by the *Commissioner* include (not exhaustive):

- **Number of requests**: is the number excessive?

  There is no particular number that equates to requests being found to be excessive. It is a measure of what is considered reasonable in the circumstance. Determining whether an *applicant’s* requests are excessive involves consideration of the volume of requests and the pattern or type of conduct displayed by the applicant. This must be done on a case-by-case basis, considering all relevant circumstances and not just focusing on a single factor.

  Where the volume of requests interferes with the operations of a *trustee* it can be argued the requests are excessive. In order to interfere with operations, the volume of requests must obstruct or hinder the range of effectiveness of the trustee’s activities.

  Other factors to consider include whether the numerous requests are similar, unusually detailed or indicate that the Applicant wishes to revisit an issue over and over again that has already been addressed.

- **Nature and scope of the requests**: are they excessively broad and varied in scope or unusually detailed? Are they identical to or similar to previous requests?
When considering an applicant’s purpose for requests we consider if there is an objective other than to gain access to records. For example, multiple requests aimed at harassing or overwhelming a trustee. Again, a review of the requests may indicate a theme, pattern or type of conduct that indicates that access to records is not the intent of the Applicant. In many cases, ascertaining the applicant’s purpose requires the drawing of inferences from behavior as applicants seldom admit to a purpose other than access.

- **Purpose of the requests:** are the requests intended to accomplish some objective other than to gain access? For example, are they made for “nuisance” value, or is the applicant’s aim to harass the trustee or to break or burden the system?

- **Timing of the requests:** is the timing of the requests connected to the occurrence of some other related event, such as a court or tribunal proceeding?

- **Wording of the request:** are the requests or subsequent communications in their nature offensive, vulgar, derogatory or contain unfounded allegations?

  Offensive or intimidating conduct or comments by applicants is unwarranted and harmful. They can also suggest that an applicant’s objectives are not legitimately about access to records. Requiring employees to be subjected to and to respond to offensive, intimidating, threatening, insulting conduct or comments can have a detrimental effect on well-being.

  The use of derogatory or vulgar language, or the making of unfounded accusations, has been held to constitute an abuse of process in many court and tribunal cases across the country. In such cases the persons using such language have been denied the exercise of what would otherwise be their rights, or have been denied remedies. In some cases, the decision-maker has required undertakings that the person conduct themselves appropriately, or has awarded costs against them.

  Depending on the nature of the case, one factor alone or multiple factors in concert with each other can lead to a finding that a request is an abuse of the right of access.

43(2)(d)
The reviews described in HIPA are about access to an individual’s own personal health information. The Commissioner will not undertake a review from an individual about another person’s personal health information, except if the individual is acting in a role described in sections 15 or 56 of HIPA.

43(2)(e) – (g)
The IPC is a place of last resort. Applicants are encouraged to resolve complaints with the trustee before requesting a review from the IPC. If a trustee has an internal review process that the applicant has not engaged, the Commissioner may wait until that option has been exhausted and undertake a review only if the Applicant remains dissatisfied.
**Notice of intention to review (section 44)**

44 Not less than 30 days before commencing a review, the commissioner shall inform the trustee of:

(a) the commissioner's intention to conduct the review; and
(b) the substance of the application for review.

The **IPC** will typically contact the trustee by telephone when it first receives an application for review. An Early Resolution Officer will attempt to informally resolve a complaint. If unsuccessful, a trustee will receive written notice by e-mail or letter.

Please see *Appendix D – What to Expect during a Review with the IPC* for more information about what to expect during a review.

**Conduct of review (section 45)**

45(1) The commissioner shall conduct a review in private.

45(2) The applicant and the trustee whose decision is the subject of a review are entitled to make representations to the commissioner in the course of the review.

45(3) No one is entitled as of right:

(a) to be present during a review; or
(b) before or after a review, to have access to, or to comment on, representations made to the commissioner by any other person.

45(1)
All information, including personal health information, collected by the Commissioner will be held as confidential. The Commissioner will not share the information without the consent of the relevant parties.

Please see *Appendix D – What to Expect during a Review with the IPC* for more information about what to expect during a review.

45(2)
The IPC will ask both the trustee and the applicant for written representations. The trustee will be asked for permission to share representation with the applicant, but won't do it without consent. Please see *Appendix D – What to Expect During a Review with the IPC* for more information about what to expect during a review.

45(3)
Please see *Appendix D – What to Expect During a Review with the IPC* for more information about what to expect during a review.
Powers of commissioner (section 46)

46(1) Notwithstanding any other Act or any privilege that is available at law, the commissioner may, in a review, require to be produced and examine any personal health information that is in the custody or control of a trustee.

(2) For the purposes of conducting a review, the commissioner may summon and enforce the appearance of persons before the commissioner and compel them to give oral or written evidence on oath or affirmation and to produce any documents or things that the commissioner considers necessary for a full review, in the same manner and to the same extent as the court.

(3) For the purposes of subsection (2), the commissioner may administer an oath or affirmation.

46(1)
The Commissioner may require any record to be produced and may examine any information in a record, whether or not the record is subject to the provisions of HIPA. A trustee must produce any record or copy of a record requested by the Commissioner under section 46(1). Records must be produced despite any privilege of the law of evidence that might otherwise apply.

If a trustee is required to produce a record and it is not practicable to make a copy of it, the trustee may request that the Commissioner examine the original at the site of the trustee. The Commissioner will destroy all records at the end of a review or investigation, but can return the records at the request of a trustee.

46(2)-(3)
In rare cases, the Commissioner may question trustees and other witnesses under oath in the same manner as the court.

Burden of proof (section 47)

47 Where a review relates to a decision to refuse an individual access to all or part of a record, the onus is on the trustee to prove that the individual has no right of access to the record or part of the record.

With respect to decisions related to access to personal health information, it is up to the trustee to persuade the Commissioner that the decision was made in accordance with HIPA. The trustee’s submission is its opportunity to convince the Commissioner that certain exemptions apply to the records at issue.

Please see Appendix D – What to Expect During a Review with the IPC for more information about what to expect during a review.
Commissioner to report (section 48)

48(1) On completing a review, the commissioner shall:

(a) prepare a written report setting out the commissioner’s recommendations with respect to the matter and the reasons for those recommendations; and

(b) forward a copy of the report to the trustee and to the applicant.

(2) In the report, the commissioner may make any recommendations with respect to the matter under review that the commissioner considers appropriate.

Please see Appendix D – What to Expect During a Review with the IPC for more information about what to expect during a review.

Decision of trustee (section 49)

49 Within 30 days after receiving a report of the commissioner pursuant to subsection 48(1), the trustee shall:

(a) make a decision to follow the recommendations of the commissioner or any other decision that the trustee considers appropriate; and

(b) give written notice of the decision to the commissioner and the applicant.

Once a trustee has provided a copy of the written report, the trustee has 30 days to notify the Commissioner whether or not it will follow the recommendations.

To fulfill this duty, a short e-mail or letter will suffice. The trustee should address each recommendation and indicate if it will comply with the recommendation. The e-mail/letter should be sent to both the Commissioner and the applicant.

Appeal to court (section 50)

50(1) Within 30 days after receiving a decision of the trustee pursuant to section 49 that the trustee will or will not comply with the recommendations of the commissioner, an applicant may appeal that decision to the court.

(2) The commissioner shall not be a party to an appeal.

If the applicant is still dissatisfied after receiving the report from the Commissioner and the response from the trustee, he/she can appeal to the Court of Queen’s Bench.

The Commissioner will not play a role in an appeal.
PRELIMINARY MATTERS (PART I OF HIPA)

Application of Act (section 3)

3(1) This Act binds the Crown.

(2) This Act does not apply to:

(a) statistical information or de-identified personal health information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to enable the subject individuals to be identified;

(b) personal health information about an individual who has been dead for more than 30 years; or

(c) records that are more than 120 years old.

3(2) HIPA does not apply to the following types of personal health information:

- Records containing personal health information that are over 120 years old;
- Personal health information of an individual who has been dead for more than 30 years;
- Statistical information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to enable the subject individuals to be identified;
- De-identified personal health information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to enable the subject individuals to be identified;

Pursuant to subsection 2(d) of HIPA, “de-identified personal health information” means personal health information from which any information that may reasonably be expected to identify an individual has been removed.

Personal health information has not been properly de-identified if:

- the identity of the individual can be determined by combining available data or information within the same or in several different records held by those who have access to the information; or
- the identity of the individual can be determined by comparing information representing distinguishing characteristics with other information sources having both the distinguishing characteristics and the names or other identifiers of individuals.

See Appendix G – for more information on de-identified personal health information
Act prevails (section 4)

4(1) Subject to subsections (3) to (6), where there is a conflict or inconsistency between this Act and any other Act or regulation with respect to personal health information, this Act prevails.

(2) Subsection (1) applies notwithstanding any provision in the other Act or regulation that states that the provision is to apply notwithstanding any other Act or law.

(3) Except where otherwise provided, The Freedom of Information and Protection of Privacy Act and The Local Authority Freedom of Information and Protection of Privacy Act do not apply to personal health information in the custody or control of a trustee.

(4) Subject to subsections (5) and (6), Parts II, IV and V of this Act do not apply to personal health information obtained for the purposes of:
   (a) The Adoption Act or The Adoption Act, 1998;
   (b) Part VIII of The Automobile Accident Insurance Act;
   (c) Repealed. 2006, c.C-1.1, s.26.
   (d) The Child and Family Services Act;
   (e) Repealed. 2014, c.16, s.47.
   (f) The Public Disclosure Act;
   (g) The Public Health Act, 1994;
   (g.1) The Vital Statistics Act, 2009 or any former Vital Statistics Act;
   (g.2) The Vital Statistics Administration Transfer Act;
   (h) The Workers’ Compensation Act, 2013;
   (h.1) The Youth Drug Detoxification and Stabilization Act; or
   (i) any prescribed Act or regulation or any prescribed provision of an Act or regulation.

(5) Sections 8 and 11 apply to the enactments mentioned in subsection (4).

(6) The Freedom of Information and Protection of Privacy Act and The Local Authority Freedom of Information and Protection of Privacy Act apply to an enactment mentioned in subsection (4) unless the enactment or any provision of the enactment is exempted from the application of those Acts by those Acts or by regulations made pursuant to those Acts.

4(1) – (3)
These subsections state that HIPA supersedes other laws unless a law specifically states otherwise. The only exceptions are the laws listed in subsection 4(4) of HIPA.

4(4) and 4(6)
These subsections provides a list of laws that have special access or privacy provisions that effect the application of Parts II, IV and V of HIPA.
COMMISSIONER (PART VII OF HIPA)

Privacy powers of commissioner (section 52)

52 The commissioner may:

(a) offer comment on the implications for personal health information of proposed legislative schemes or programs of trustees;

(b) after hearing a trustee, recommend that the trustee:
   (i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and
   (ii) destroy collections of personal health information collected in contravention of this Act;

(c) in appropriate circumstances, comment on the collection of personal health information in a manner other than directly from the individual to whom it relates;

(d) from time to time, carry out investigations with respect to personal health information in the custody or control of trustees to ensure compliance with this Act;

(e) comment on the implications for protection of personal health information of any aspect of the collection, storage, use or transfer of personal health information.

Section 52 describes the powers of the Information and Privacy Commissioner with respect to the safeguarding, collection, use and disclosure of personal health information.

52(a)
It is within the Commissioner and his office's mandate to offer comments on:

- Proposed legislation currently under consideration of the legislative assembly that might affect the protection of personal health information.
- Proposed programs of a trustee (eg. a new EMR, a program where personal health information will be shared, etc).

A trustee may request comments on its proposed program through the IPC Consultation process. For more information, see www.oipc.sk.ca/Resources_PublicBodies_Consultations.htm.

52(b)
The Commissioner might recommend that a trustee:

- stop a practice of collecting, using or disclosing personal health information if the practice contravenes this HIPA; or
- destroy personal health information if the collection was not authorized by sections 23, 24 or 25 of HIPA.

Such a recommendation might come about either through an Investigation by the Commissioner or through a consultation file.
For information about an investigation by the Commissioner, see *Appendix C – Privacy Breach Guidelines*.

For information about a consultation with the IPC see www.oipc.sk.ca/Resources_PublicBodies_Consultations.htm.

52(c)
The Commissioner can comment on the collection of personal health information if it is not collected directly from the subject individual. These comments might come about either through an investigation by the Commissioner or through a consultation file.

For information about an investigation by the Commissioner, see *Appendix C – Privacy Breach Guidelines*. For information about a consultation with the IPC see www.oipc.sk.ca/Resources_PublicBodies_Consultations.htm.

52(d)
The Commissioner may undertake an investigation to ensure that personal health information is protected. The investigation can focus on the collection, use, disclosure, accuracy or safeguarding of personal health information.

The Commissioner can learn of a privacy breach and begin an investigation in several different ways. Some of them include:

- the trustee can proactively report a breach to the IPC.
- A citizen could come to the IPC with a complaint about a trustee’s actions or practices.
- A third party in possession of personal health information could notify the IPC.
- Employees of a trustee could inform the IPC of inappropriate practices within the organization.
- The IPC could act on media reports.

While not mandatory, the IPC does encourage organizations to proactively report. Some of the benefits include:

- Timely, expert advice.
- The IPC will monitor the situation and if satisfied with your organization’s internal investigation report may close the file rather than conducting a formal investigation.
- Should affected individuals contact the IPC, it can assure the individuals that it is working with your organization to address the breach which may prevent a formal investigation by the IPC.
- Should the media get wind of the privacy breach, your organization can assure the public that they are working with the IPC to address the matter.

For more information about investigations by the Commissioner and what to do if a privacy breach occurs, see *Appendix C – Privacy Breach Guidelines*. 
52(e) The Commissioner can comment on the implications for protection of personal health information of any aspect of the collection, storage, use or transfer of personal health information.

These comments might come about either through an Investigation by the Commissioner or through a consultation file.

For information about an investigation by the Commissioner, see Appendix C – Privacy Breach Guidelines.

For information about a consultation with the IPC see www.oipc.sk.ca/Resources_PublicBodies_Consultations.htm.

General powers of commissioner (section 53)

53 The commissioner may:

(a) engage in or commission research into matters affecting the carrying out of the purposes of this Act;

(b) conduct public education programs and provide information concerning this Act and the commissioner's role and activities;

(c) receive representations concerning the operation of this Act.

Section 53 of HIPA lists other activities within the scope of the Commissioner's mandate such as:

- Researching best practices and other matters relating to personal health information and the activities described in HIPA.
- Produce resources, such as this Guide, presentations and other educational material related to HIPA and his role.
- Hear feedback from other stakeholders regarding HIPA.

Confidentiality (section 54)

54(1) Except as provided in this section, the commissioner shall not disclose any information that comes to the knowledge of the commissioner in the exercise of the powers, performance of the duties or carrying out of the functions of the commissioner pursuant to this Act.

(2) Subsection (1) applies, with any necessary modification, to the staff of the commissioner.

(3) In the course of a review pursuant to section 45, the commissioner may disclose any information that the commissioner considers necessary to disclose to facilitate the review.

(4) In a report prepared pursuant to this Act, the commissioner may disclose any information that the commissioner considers necessary to disclose to establish grounds for
the findings and recommendations in the report.

(5) When making a disclosure pursuant to subsection (3) or (4), the commissioner shall take every reasonable precaution to avoid disclosure of, and shall not disclose:

(a) any information or other material if the nature of the information or material could justify a refusal by a trustee to give access to a record or part of a record; or

(b) any information as to whether a record exists if the trustee, in refusing to give access, does not indicate whether the record exists.

(6) If, in the opinion of the commissioner, there is evidence of the commission of an offence against an Act, a regulation, an Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada, the commissioner may disclose to the Attorney General for Saskatchewan or the Attorney General of Canada information that relates to the commission of the offence.

54(1) – (2)
Section 54 indicates that the Commissioner, and his staff, may not disclose any information that comes to their knowledge in the course of their work except in situations described in subsections (3)-(6).

The IPC is very cautious not to disclose personal health information at any time, unless in a situation described below.

54(3)
In the course of a review described in section 45 of HIPA, the Commissioner may disclose any information he/she deems necessary to facilitate the review.

See Appendix D – What to Expect During a Review with the IPC for more information.

54(4)
The Commissioner may disclose any information he/she deems necessary to support the findings and recommendations made in a review or investigation report.

See Appendix C – Privacy Breach Guidelines or Appendix D – What to Expect During a Review with the IPC for more information.

54(5)
During a review, or in a review or investigation report, the Commissioner will take extra caution not to disclose:

- Any information that could justify a refusal by a trustee to give access to a record or part of a record.

- Any information that confirms records exist if the trustee has not acknowledged they exist. Note: there is no provision in section 36 of HIPA that allows a trustee to deny the existence of records.
54(6)
If the Commissioner has received information that indicates that a crime has been committed, he/she may disclose that information to the Attorney General of Saskatchewan or of Canada. The crime does not have to be HIPA related.

Non-compellability (section 55)

55(1) The commissioner is not compellable to give evidence in a court or in a proceeding of a judicial nature concerning any information that comes to the knowledge of the commissioner in the exercise of the powers, performance of the duties or carrying out of the functions of the commissioner pursuant to this Act.

(2) Subsection (1) applies, with any necessary modification, to the staff of the commissioner.

The Commissioner, and his/her staff, cannot be compelled to testify in a court of law regarding any information they have learned in the course of their duties.
**Exercise of rights by other persons (section 56)**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>56</strong></td>
<td>Any right or power conferred on an individual by this Act may be exercised:</td>
</tr>
<tr>
<td></td>
<td>(a) where the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate;</td>
</tr>
<tr>
<td></td>
<td>(b) where a personal guardian has been appointed for the individual, by the guardian if the exercise of the right or power relates to the powers and duties of the guardian;</td>
</tr>
<tr>
<td></td>
<td>(c) by an individual who is less than 18 years of age in situations where, in the opinion of the trustee, the individual understands the nature of the right or power and the consequences of exercising the right or power;</td>
</tr>
<tr>
<td></td>
<td>(d) where the individual is less than 18 years of age, by the individual's legal custodian in situations where, in the opinion of the trustee, the exercise of the right or power would not constitute an unreasonable invasion of the privacy of the individual;</td>
</tr>
<tr>
<td></td>
<td>(e) where the individual does not have the capacity to give consent:</td>
</tr>
<tr>
<td></td>
<td>(i) by a person designated by the Minister of Community Resources and Employment if the individual is receiving services pursuant to <em>The Residential Services Act</em> or <em>The Rehabilitation Act</em>; or</td>
</tr>
<tr>
<td></td>
<td>(ii) by a person who, pursuant to <em>The Health Care Directives and Substitute Health Care Decision Makers Act</em>, is entitled to make a health care decision, as defined in that Act, on behalf of the individual; or</td>
</tr>
<tr>
<td></td>
<td>(f) by any person designated in writing by the individual pursuant to section 15.</td>
</tr>
</tbody>
</table>

**56(a)**

If an individual is deceased, the individual's personal representative may make decisions related to the individual's personal health information. However, the personal representative may only do so if it relates to the administration of the individual's estate. See IPC Report H-2009-001/LA-2009-002 for an in-depth discussion.

The IPC has defined personal representative as an executor under a will or administrator appointed by the court as Executor Administrator of an estate.

If, however, an individual has designated someone by writing to Act on his/her behalf, and the written designation specifically states that it extends past the individual's death, then more personal health information may be shared.

Trustees may also disclose personal health information that relate to circumstances surrounding the death of the subject individual if made to an immediate family member or someone in a close personal relationship with the individual. See section 27(4)(c) of HIPA for more information.

**56(b)**

A personal guardian may exercise the rights afforded by HIPA on behalf of another individual.
For the purposes of subsection 56 of HIPA, a personal guardian is one defined in *The Adult Guardianship and Co-decision-making Act*. In general:

A **guardian** is someone who has the authority to make decisions for an adult. A personal guardian makes decisions about an adult's personal welfare and a property guardian makes decisions about an adult's finances and property.

A **decision-maker** is someone who can make or assist in making decisions for an adult. The term is used to describe a personal guardian, a property guardian, a personal co-decision maker, a property co-decision-maker, a temporary personal guardian or a temporary property guardian. A decision-maker can be one person or more than one person.

A **co-decision-maker** is someone who has the authority to assist an adult in making decisions and to make joint decisions with the adult. A personal co-decision-maker makes decisions with the adult about personal matters and a property co-decision-maker makes decisions with the adult about finances and property. A co-decision-maker must ensure that the adult has and understands all the information needed to make a decision, and knows the alternatives and likely results of any choice.

A **temporary personal or property guardian** is someone who has the authority to make decisions for an adult in emergency situations for a limited time, to a maximum of six months. The authority of a temporary guardian is limited to doing what is necessary to protect the adult or the adult's property from serious or financial harm.

**56(c)**

Trustees may allow individuals less than 18 years of age to exercise their own rights or powers under HIPA. This provision is at the discretion of the trustee.

Where a minor understands the nature of the right or power and the consequences of exercising the right or power, he or she may exercise that right or power.

For example, some factors to consider when deciding if a youth might emotionally and

- intellectually have the *capacity* to give *consent* are:
- maturity;
- economic status (i.e. self-supporting or not);
- living arrangements;
- mental state;
- risk assessment;
- and the complexity and intrusiveness of the treatment situation.

Allowing a mature minor to exercise their own rights under HIPA may be decided on a case by case basis. For more information, see the Commissioner's blog entitled *Who Signs for a Child* available at [www.oipc.sk.ca](http://www.oipc.sk.ca).
56(d)
If an individual is under 18 years of age, and subsection 56(c) does not apply, the child’s guardian may exercise a right or power extended by HIPA on behalf of the individual.

A guardian is a person who is legally responsible for the care and custody of the minor. This definition may not extend to the biological parents of a child in all circumstances. Other guardians may be a child’s grandparent or other relative or other individual who has been granted a guardianship order by the Court.

When responding to access requests for personal health information of minor, a trustee must:

1) determine whether the subject individual can be considered a mature minor pursuant to subsection 56(c) of HIPA; and/or
2) Take reasonable steps to ensure the applicant is the legal guardian of the minor.

56(e)
If an adult does not have the capacity to consent to exercise the rights afforded by HIPA, then other individuals can do so in certain situations.

Capacity is defined in subsection 2(c) of The Adult Guardianship and Co-decision-making Act as follows:

Capacity means the ability:
- to understand information relevant to making a decision; and
- to appreciate the reasonably foreseeable consequences of making or not making a decision.

56(e)(i)
If an individual does not have capacity to exercise rights or give consent with respect to personal health information and is receiving services from The Residential Services Act or The Rehabilitation Act, then a person who is designated by the Minister responsible for those Acts may do so on his/her behalf.

Currently, the Minister of Health, Minister of Justice and Attorney General, Minister of Social Services and Minister Responsible for Corrections and Policing all have joint responsibility for The Residential Services Act. The Minister of Social Services has responsibility for The Rehabilitation Act.

56(e)(ii)
This subsection allows someone who is entitled to make a decision pursuant to The Health Care Directives and Substitute Health Care Decision Makers Act to exercise the rights afforded by HIPA on behalf of the subject individuals.

Such a person may be a proxy, immediate family or personal guardian.

As defined in 2(1)(g) of The Health Care Directives and Substitute Health Care Decision Makers Act, a proxy is “a person appointed in a directive to make health care decisions for the person making the directive.” See sections 11, 12 and 13 of The Health Care Directives and Substitute Health Care Decision Makers Act for more details.
As defined in 2(1)(f) of *The Health Care Directives and Substitute Health Care Decision Makers Act*, a personal [guardian](#) is “appointed pursuant to *The Adult Guardianship and Co-decision-making Act* who has the authority to make health care decisions for a dependent adult and who acts in accordance with the authority granted to the personal guardian pursuant to that Act”. [See subsection 56(b) of HIPA.](#)

The [trustee](#) should ensure the exercise of the rights is for a purpose discussed in *The Health Care Directives and Substitute Health Care Decision Makers Act*.

See *The Health Care Directives and Substitute Health Care Decision Makers Act* for more details.

### 56(f)
Any individual can provide authorization to another person to act on his/her behalf. Such authorization must be in writing, and can provide authority to the representative to exercise any right or undertake any power, including the right to provide [consent](#) under various provisions of the Act, or simply the right to [access](#) the individual's health information.

The authorization must be signed by the individual, and preferably witnessed.

### Information about trustees (section 57)

57 Where information about a trustee or the activities of a trustee is collected in conjunction with the collection of personal health information and regulations are made pursuant to clause 63(1)(w) governing that information, no person shall use or disclose the information about the trustee or the trustee’s activities except in accordance with those regulations.

Currently, no [regulations](#) exist pursuant to clause 63(1)(w).

### Decisions of trustees (section 58)

58(1) Where this Act or the regulations require a decision to be made or an opinion to be formed by a trustee that is a government institution as defined in *The Freedom of Information and Protection of Privacy Act*, the person who is the head, as defined in that Act, of the government institution, or the designate of the head, shall make the decision or form the opinion on behalf of the trustee.

(2) Where this Act or the regulations require a decision to be made or an opinion to be formed by a trustee that is a local authority as defined in *The Local Authority Freedom of Information and Protection of Privacy Act*, the person who is the head, as defined in that Act, of the local authority, or the designate of the head, shall make the decision or form the opinion on behalf of the trustee.

(3) Where this Act or the regulations require a decision to be made or an opinion to be formed by a trustee to whom subsection (1) or (2) does not apply, the trustee shall designate a person to make the decision or form the opinion on behalf of the trustee.
Organizations that qualify as a trustee are required to designate a person to make decisions related to HIPA.

58(1) The 'head' of an organization that is both a trustee and a government institution pursuant to The Freedom of Information and Protection of Privacy Act (FOIP) will also be responsible for making HIPA related decisions.

58(2) The 'head' of an organization that is both a trustee and a local authority pursuant to The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP) will also be responsible for making HIPA related decisions.

58(3) Organizations that qualify as a trustee, but not a government institution or local authority, are required to designate a person to make decisions related to HIPA.

Typically a head is the chairperson of the governing board or the person with the most authority in the organization. However, sometimes the powers of the head are transferred to a different individual in the organization, such as the privacy officer. It is best practise to have a written delegation that indicates who has decision making authority in matters related to HIPA.

Annual report (section 60)

60(1) Within three months after the end of each fiscal year, the commissioner shall prepare and submit an annual report to the Speaker of the Assembly, and the Speaker shall cause the report to be laid before the Assembly in accordance with section 13 of The Executive Government Administration Act.

(2) The annual report of the commissioner is to provide details of the activities of the office in relation to the commissioner's responsibilities pursuant to this Act during that fiscal year and, in particular, concerning any instances where the commissioner's recommendations made after a review have not been complied with.

Each year, the Commissioner submits an annual report to the legislative assembly. In addition to reporting on his activities, the report indicates whether trustees have complied with the recommendations made in both review reports and investigation reports.
Proceedings prohibited (section 61)

61(1) No action or proceeding lies or shall be commenced against a trustee, an information management service provider or the Government of Saskatchewan or an officer or employee of a trustee, an information management service provider or the Government of Saskatchewan with respect to:

(a) the use or disclosure in good faith of personal health information pursuant to this Act; or

(b) any consequences that flow from the use or disclosure mentioned in clause (a).

(2) No action or proceeding lies or shall be commenced against the commissioner or any employee or agent of the commissioner for any loss or damage suffered by a person by reason of anything in good faith done, caused, permitted or authorized to be done, attempted to be done or omitted to be done, by any of them, pursuant to or in the exercise of or supposed exercise of any power conferred by this Act or the regulations or in the carrying out or supposed carrying out of any order made pursuant to this Act or any duty imposed by this Act or the regulations.

No proceedings can be commenced against a trustee, the Commissioner or his staff related to actions taken to comply with HIPA.

Immunity from prosecution (section 62)

62 No person is liable to prosecution for an offence against any Act or regulation by reason of that person’s compliance with a requirement or recommendation of the commissioner pursuant to this Act.

No one can be charged for any offence related to actions taken to comply with HIPA or recommendations of the Commissioner.
Regulations (section 63)

63(1) For the purpose of carrying out this Act according to its intent, the Lieutenant Governor in Council may make regulations:

(a) defining, enlarging or restricting the meaning of any word or expression used in this Act but not defined in this Act;

(b) for the purposes of sub clause 2(t)(xii), designating classes of persons as health professionals;

(c) for the purposes of sub clause 2(t)(xv), prescribing persons, bodies or classes of persons or bodies as trustees;

(d) for the purposes of clause 4(4)(i), prescribing Acts or regulations or provisions of Acts or regulations to which Parts II, IV and V of this Act do not apply with respect to personal health information;

(e) Repealed. 2003, c.25, s.18.

(e.1) for the purposes of section 8, prescribing a form for a written direction;

(f) for the purposes of subsection 11(1), prescribing other identifying numbers;

(g) for the purposes of clause 11(3)(b), prescribing circumstances in which a person may require the production of another person’s health services number;

(h) prescribing and governing administrative, technical and physical safeguards for the protection of personal health information;

(i) prescribing and governing standards for the retention and destruction of personal health information and governing retention and destruction policies;

(j) governing agreements between trustees and information management service providers;

(j.1) for the purposes of subsection 18.1(1), prescribing persons who may create and control comprehensive health records;

(k) for the purposes of section 22, designating information management service providers as archives to which trustees and former trustees can transfer custody and control of personal health information and governing access to and use, disclosure, processing, storing, archiving, modification and destruction of personal health information by designated archives;

(l) for the purposes of clause 25(1)(g), prescribing circumstances in which a trustee may collect personal health information other than directly from the subject individual;

(m) prescribing purposes for which a trustee may use personal health information pursuant to clause 26(2)(d);

(n) Repealed. 2003, c.25, s.18.

(o) for the purposes of clause 27(4)(p), prescribing circumstances in which personal health information in the custody or control of a trustee may be disclosed without the consent of the subject individual;

(p) for the purposes of clause 27(4)(h), prescribing professional bodies to which personal health information may be disclosed;

(q) prescribing persons with whom or bodies with which the minister may enter into agreements pursuant to clause 28(5)(b);
(r) for the purposes of subsection 28(8), prescribing and governing:

(q) prescribing persons with whom or bodies with which the minister may enter into agreements pursuant to clause 28(5)(b);

(r) for the purposes of subsection 28(8), prescribing and governing:

(i) circumstances in which registration information may be disclosed without the consent of the subject individual;

(ii) persons to whom registration information may be disclosed without the consent of the subject individual;

(iii) purposes for which registration information may be disclosed without the consent of the subject individual;

(r.1) for the purposes of subsection 30(1), prescribing persons who may give consent to the use or disclosure of personal health information where the subject individual is deceased;

(s) governing the making of written requests for access to personal health information;

(t) prescribing the maximum amounts that may be charged as fees to recover costs incurred in providing access to personal health information;

(u) governing the making of requests for amendments to personal health information and the amending of personal health information by trustees;

(v) governing applications for review pursuant to section 42;

(w) for the purposes of section 57, governing the use and disclosure of information respecting trustees and their activities;

(x) prescribing any matter or thing required or authorized by this Act to be prescribed in the regulations;

(y) respecting any other matter or thing that the Lieutenant Governor in Council considers necessary to carry out the intent of this Act.

(2) At least 30 days before the coming into force of a regulation made pursuant to clause (1)(d), (g), (l), (m), (o) or (r), the minister shall provide a copy of the proposed regulation to each of the health professional bodies that regulate members of a health profession pursuant to an Act.

Section 63 of HIPA describes the types of regulations that can be made. Typically, regulations are made by the Lieutenant Governor in council and do not require approval by the Legislative Assembly.
Below is the list of types of regulations and if any have been passed. For the actual Regulations, please see the section on the HIPA Regulations.

<table>
<thead>
<tr>
<th>Section</th>
<th>Wording</th>
<th>Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>63(1)(a)</td>
<td>defining, enlarging or restricting the meaning of any word or expression used in this Act but not defined in this Act;</td>
<td>See section 2 of the Regulations</td>
</tr>
<tr>
<td>63(1) (b)</td>
<td>for the purposes of sub clause 2(t)(xii), designating classes of persons as health professionals;</td>
<td>See section 3 of the Regulations</td>
</tr>
<tr>
<td>63(1) (c)</td>
<td>for the purposes of sub clause 2(t)(xv), prescribing persons, bodies or classes of persons or bodies as trustees;</td>
<td>See section 3 of the Regulations</td>
</tr>
<tr>
<td>63(1) (d)</td>
<td>for the purposes of clause 4(4)(i), prescribing Acts or regulations or provisions of Acts or regulations to which Parts II, IV and V of this Act do not apply with respect to personal health information;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (e)</td>
<td>Repealed. (No longer exists)</td>
<td></td>
</tr>
<tr>
<td>63(1) (e.1)</td>
<td>for the purposes of section 8, prescribing a form for a written direction;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (f)</td>
<td>for the purposes of subsection 11(1), prescribing other identifying numbers;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (g)</td>
<td>for the purposes of clause 11(3)(b), prescribing circumstances in which a person may require the production of another person’s health services number;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (h)</td>
<td>prescribing and governing administrative, technical and physical safeguards for the protection of personal health information;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (i)</td>
<td>prescribing and governing standards for the retention and destruction of personal health information and governing retention and destruction policies;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (j)</td>
<td>governing agreements between trustees and information management service providers;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (j.1)</td>
<td>for the purposes of subsection 18.1(1), prescribing persons who may create and control comprehensive health records;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (k)</td>
<td>for the purposes of section 22, designating information management service providers as archives to which trustees and former trustees can transfer custody and control of personal health information and governing access to and use, disclosure, processing, storing, archiving, modification and destruction of personal health information by designated archives;</td>
<td>See section 4 of the Regulations</td>
</tr>
<tr>
<td>63(1) (l)</td>
<td>for the purposes of clause 25(1)(g), prescribing circumstances in which a trustee may collect personal health information other than directly from the subject individual;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (m)</td>
<td>prescribing purposes for which a trustee may use personal health information pursuant to clause 26(2)(d);</td>
<td>See section 7.1 of the Regulations</td>
</tr>
<tr>
<td>Section</td>
<td>Wording</td>
<td>Regulations</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>63(1) (n)</td>
<td>Repealed. (No longer exists)</td>
<td></td>
</tr>
<tr>
<td>63(1) (o)</td>
<td>for the purposes of clause 27(4)(p), prescribing circumstances in which personal health information in the custody or control of a trustee may be disclosed without the consent of the subject individual;</td>
<td>See sections 5, 6, 6.1, 6.2, 6.3, 7.1 of the Regulations</td>
</tr>
<tr>
<td>63(1) (p)</td>
<td>for the purposes of clause 27(4)(h), prescribing professional bodies to which personal health information may be disclosed;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (q)</td>
<td>prescribing persons with whom or bodies with which the minister may enter into agreements pursuant to clause 28(5)(b);</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (r)</td>
<td>for the purposes of subsection 28(8), prescribing and governing:</td>
<td>See section 6, 6.4, 7 of the Regulations</td>
</tr>
<tr>
<td></td>
<td>• circumstances in which registration information may be disclosed without the consent of the subject individual;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• persons to whom registration information may be disclosed without the consent of the subject individual;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• purposes for which registration information may be disclosed without the consent of the subject individual;</td>
<td></td>
</tr>
<tr>
<td>63(1) (r.1)</td>
<td>for the purposes of subsection 30(1), prescribing persons who may give consent to the use or disclosure of personal health information where the subject individual is deceased;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (s)</td>
<td>governing the making of written requests for access to personal health information;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (t)</td>
<td>prescribing the maximum amounts that may be charged as fees to recover costs incurred in providing access to personal health information;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (u)</td>
<td>governing the making of requests for amendments to personal health information and the amending of personal health information by trustees;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (v)</td>
<td>governing applications for review pursuant to section 42;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (w)</td>
<td>for the purposes of section 57, governing the use and disclosure of information respecting trustees and their activities;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (x)</td>
<td>prescribing any matter or thing required or authorized by this Act to be prescribed in the regulations;</td>
<td>No regulations exist</td>
</tr>
<tr>
<td>63(1) (y)</td>
<td>respecting any other matter or thing that the Lieutenant Governor in Council considers necessary to carry out the intent of this Act.</td>
<td>No regulations exist</td>
</tr>
</tbody>
</table>
Offences (section 64)

64(1) No person shall:

(a) knowingly contravene any provision of this Act or the regulations;

(b) without lawful justification or excuse, wilfully obstruct, hinder or resist the commissioner or any other person in the exercise of the powers, performance of the duties or the carrying out of the functions of the commissioner or other person pursuant to this Act;

(c) without lawful justification or excuse, refuse or wilfully fail to comply with any lawful requirement of the commissioner or any other person pursuant to this Act;

(d) wilfully make any false statement to, or mislead or attempt to mislead, the commissioner or any other person in the exercise of the powers, performance of the duties or carrying out of the functions of the commissioner or other person pursuant to this Act;

(e) wilfully destroy any record that is governed by this Act with the intent to evade a request for access to the record; or

(f) obtain another person’s personal health information by falsely representing that he or she is entitled to the information.

Note: See the HIPA Offences and their Consequences table located in this Guide.

64(1)(a)
It is an offence to violate any section of HIPA if aware that the action is a violation. Example: It is an offense for a trustee, or an employee of a trustee, to disclose personal health information if he/she knows that the disclosure is not authorized by HIPA

64(1)(b)
It is an offence to, on purpose, obstruct, hinder or resist the Commissioner or any person in performing their duties as described in HIPA.

Example: It is an offence for a trustee not to cooperate with the Commissioner during a review or investigation

64(1)(c)
It is an offence to refuse to comply or deliberately not comply with a requirement of the Act.

Example: It is an offence not to comply produce personal health information requested by the Commissioner pursuant to section 46(1) of HIPA.

64(1)(d)
It is an offence to make false statements to the Commissioner or to mislead the Commissioner in relation to his duties as described in HIPA.

64(1)(e)
It is an offence to destroy a record that is responsive to an access request.

Example: After an individual makes a request to a trustee for information about a recent illness, it is an offence to destroy the responsive record to avoid providing it to the individual.
64(1)(f)
It is an offense for anyone to obtain another individual’s personal health information by falsely stating that they are entitled to the information.

Example: It is an offence for an individual to receive personal health information of a former spouse by indicating to the trustee that he/she is entitled to have them.

64(1.1)

64(1.1) No trustee or information management service provider, or former trustee or information management service provider, shall fail to keep secure the personal health information in its custody or control as required by this Act.

It is an offence for a current or former trustee or IMSP to fail to keep secure personal health information. When records are found abandoned or unsecured, the trustee will need to show they took all reasonable steps to prevent the abandonment.

Example: An IMSP must keep personal health information protected even if the contact/agreements with the trustee has expired. It is an offence not to do so.

64(1.2)

64(1.2) No person shall be found to have contravened subsection (1.1) if that person can establish that he or she took all reasonable steps to prevent the contravention.

A person will not be found to have made an offence if they can demonstrate that they took steps to prevent the offence (before the offence occurred).

64(2)

64(2) Every person who contravenes subsection (1) or (1.1) is guilty of an offence and is liable on summary conviction:

(a) in the case of an individual, to a fine of not more than $50,000, to imprisonment for not more than one year or to both; and

(b) in the case of a corporation, to a fine of not more than $500,000.

The consequence for any one is found guilty of an offence can be:

- A fine of up to $50,000 or up to a year in prison, or both;

- In the case of a corporation, a fine of up to $500,000.
64(3) Every director, officer or agent of a corporation who directed, authorized, assented to, acquiesced in or participated in an act or omission of the corporation that would constitute an offence by the corporation is guilty of that offence, and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the corporation has been prosecuted or convicted.

If a director, officer or agent of a corporation has:

- directed, authorized, assented to, acquiesced in or participated in an act or omission of the corporation that would constitute an offence pursuant to subsection 64(1) of HIPA.

Then the director, officer or agent may be:

- required to pay a fine of up to $50,000; or
- spend one year in jail; or
- both.

This may occur even if the corporation has not been prosecuted or convicted.
64(3.1) An individual who is an employee of or in the service of a trustee or information management service provider and who knowingly discloses or directs another person to disclose personal health information in circumstances that would constitute an offence by the trustee or information management service provider pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the trustee or information management service provider has been prosecuted or convicted.

(3.2) An individual who is an employee of or in the service of a trustee and who wilfully accesses or uses or directs another person to access or use personal health information that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the trustee has been prosecuted or convicted.

(3.3) An individual who is an employee of or in the service of an information management service provider and who wilfully accesses or uses or directs another person to access or use personal health information for a purpose that is not authorized by subsection 18(1) of this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the information management service provider has been prosecuted or convicted.

If an employee of a trustee or IMSP has:

- Knowingly disclosed personal health information that would constitute an offence pursuant to subsection 64(1) of HIPA; or
- Directed another individual to disclose personal health information that would constitute an offence pursuant to subsection 64(1) of HIPA;

Then the employee may be:

- required to pay of fine of up to $50,000; or
- spend one year in jail; or
- both.

This includes individuals in the service of a trustee or an IMSP (ie: a contractor).

This may occur even if the trustee or IMSP has not been prosecuted or convicted.

64(3.2) If an employee of a trustee has:

- Accessed or used personal health information “that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act”; or
- Directed another individual to access or use personal health information “that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act”; 

Then the employee may be:

- required to pay of fine of up to $50,000; or
• spend one year in jail; or
• both.

This includes individuals in the service of a trustee (ie: a contractor).

This may occur even if the trustee has not been prosecuted or convicted.

64(3.3)
If an employee of an IMSP has:
• Accessed or used personal health information for a purpose that is not authorized by subsection 18(1) of HIPA; or
• Directed another individual to access or use personal health information for a purpose that is not authorized by subsection 18(1) of HIPA;

Then the employee may be:
• required to pay of fine of up to $50,000; or
• spend one year in jail; or
• both.

This includes individuals in the service of an IMSP (ie: a contractor).

This may occur even if the IMSP has not been prosecuted or convicted.

64(4)

64(4) No prosecution shall be commenced pursuant to this section except with the express consent of the Attorney General for Saskatchewan.

If the Commissioner suspects that an offence has been committed, he/she cannot commence a prosecution. He/she may only refer the matter to the Attorney General for Saskatchewan or recommend that the Attorney General examine the matter.

64(5)

64(5) No prosecution shall be commenced pursuant to this section after the expiration of two years after the date of the discovery of the alleged offence.

The Attorney General cannot commence a prosecution after two years from the discovery of the alleged offence. The discovery could be made by a trustee, the affected individual, the Commissioner or others.

Section 64 describes offenses to HIPA. In other words, this section describes situations where a trustee, or the employee of a trustee, or any person could be charged for HIPA violation and what the consequences would be.

The Commissioner cannot decide if a person has violated HIPA and whether penalties should be imposed. He/she can only refer the matter to the Attorney General of Saskatchewan.
### HIPA Offences and their Consequences

<table>
<thead>
<tr>
<th>Section</th>
<th>What is the offence?</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>64(1)(a)</td>
<td>It is an offence to violate any section of HIPA if aware that the action is a violation.</td>
<td>In the case of an individual, a fine of up to $50,000 or up to a year in prison, or both;</td>
</tr>
<tr>
<td>64(1)(b)</td>
<td>It is an offence to, on purpose, obstruct, hinder or resist the Commissioner or any person in performing their duties as described in HIPA.</td>
<td>In the case of a corporation, a fine of up to $500,000.</td>
</tr>
<tr>
<td>64(1)(c)</td>
<td>It is an offence to refuse to comply or deliberately not comply with a requirement of the Act.</td>
<td></td>
</tr>
<tr>
<td>64(1)(d)</td>
<td>It is an offence to make false statements to the Commissioner or to mislead the Commissioner in relation to his duties as described in HIPA.</td>
<td></td>
</tr>
<tr>
<td>64(1)(e)</td>
<td>It is an offence to destroy a record that is responsive to an access request.</td>
<td></td>
</tr>
<tr>
<td>64(1)(f)</td>
<td>It is an offense for anyone to obtain another individual’s personal health information by falsely stating that they are entitled to the information.</td>
<td></td>
</tr>
<tr>
<td>64(1.1)</td>
<td>It is an offence for a current or former trustee or IMSP to fail to keep secure personal health information.</td>
<td></td>
</tr>
<tr>
<td>64(3)</td>
<td>It is an offence for a director, officer, or agent of a corporation to direct, authorize, assent to, acquiesce in or participate in an act or omission of the corporation that would constitute an offence pursuant to subsection 64(1) of HIPA.</td>
<td>The director, officer or agent may be required to pay a fine of up to $50,000, spend one year in jail; or both. This may occur even if the corporation has not been prosecuted or convicted.</td>
</tr>
<tr>
<td>64(3.1)</td>
<td>It is an offence for an employee of a trustee or IMSP to knowingly disclose personal health information that would constitute an offence pursuant to subsection 64(1) of HIPA; or to direct another individual to disclose personal health information that would constitute an offence pursuant to subsection 64(1) of HIPA.</td>
<td>The employee may be required to pay of fine of up to $50,000, spend one year in jail or both. This may occur even if the trustee or IMSP has not been prosecuted or convicted.</td>
</tr>
<tr>
<td>64(3.2)</td>
<td>It is an offence if an employee of a trustee or an IMSP to access or use personal health information “that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act”; or to directed another individual to access or use personal health information “that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act”.</td>
<td>The employee may be required to pay of fine of up to $50,000; or spend one year in jail; or both. This may occur even if the trustee or IMSP has not been prosecuted or convicted.</td>
</tr>
</tbody>
</table>

**This is SNOOPING!**
THE HIPA REGULATIONS

Trustees prescribed (Section 3 of the Regulations)

3 For the purposes of subclause 2(t)(xv) of the Act, the following are prescribed as trustees:
   (a) the Health Quality Council;
   (b) NYP. 30 Jne 2005 cH-0.021 Reg 1 s3.

For the purposes of subsection 2(t)(xy) of HIPA, the Saskatchewan Health Quality Council qualifies as a trustee.

Designated archives (Section 4 of the Regulations)

4(1) For the purposes of section 22 of the Act, the following are designated archives:
   (a) affiliates;
   (b) the Department of Health;
   (c) health professional bodies that regulate members of a health profession pursuant to an Act;
   (d) regional health authorities;
   (e) Saskatchewan Archives Board;
   (f) eHealth Saskatchewan;
   (g) University of Regina Archives;
   (h) University of Saskatchewan Archives.

(2) Nothing in this section requires a designated archive to accept personal health information from a trustee.

4(1) (HIPA Regulations)

Section 22 of HIPA requires trustees to take certain steps to protect personal health information. One of the possible steps is to transfer custody of personal health information to a designated archive. Below is a list of organizations that can qualify as designated archives:

- affiliates
- the Department of Health (the Ministry of Health)
- health professional bodies that regulate members of a health profession pursuant to an Act
- regional health authorities
- Saskatchewan Archives Board
- eHealth Saskatchewan
- University of Regina Archives
- University of Saskatchewan Archives

Please note subsection 4(2) of the Regulations.
4(2) (HIPA Regulations)

Even if an organization qualifies as a designated archive, it is not required to accept custody of personal health information.

Disclosure to Health Quality Council (Section 5 of the Regulations)

5 Pursuant to clause 27(4)(p) of the Act, the minister or eHealth Saskatchewan may, without the consent of the subject individual, disclose personal health information to the Health Quality Council for use by the council in carrying out any of the objects of the council set out in clauses 5(a) to (l) of The Health Quality Council Act, if:

(a) before the personal health information is disclosed to the Health Quality Council, the minister or eHealth Saskatchewan ensures that reasonable steps have been taken:

(i) to remove any information that by itself may reasonably be expected to identify the subject individual; and

(ii) to replace the subject individual’s health services number or any other number assigned to the individual as part of a system of unique identifying numbers with a unique encrypted identifier; and

(b) the Health Quality Council has entered into a written agreement with the minister or eHealth Saskatchewan that:

(i) governs the personal health information to be disclosed;

(ii) governs the Health Quality Council’s collection and use of personal health information;

(iii) requires the Health Quality Council to use the personal health information only for the objects set out in clauses 5(a) to (l) of The Health Quality Council Act;

(iv) prohibits the Health Quality Council from disclosing the personal health information without the approval of the minister;

(v) prohibits the Health Quality Council from attempting to re-identify the personal health information; and

(vi) requires the Health Quality Council to:

(A) take reasonable steps to ensure the security and confidentiality of the personal health information; and

(B) ensure that, in any publication or report made by the Health Quality Council, information is disclosed only in a manner that will prevent the direct or indirect identification of subject individuals.

The Ministry of Health or eHealth Saskatchewan can disclose personal health information to the Saskatchewan Health Quality Council without the consent of the individual if the following three conditions exist:

1. First, the purpose for the disclosure must be in line with the objects of the council as listed in Section 5 of The Health Quality Council Act. They are as follows:
5(a) to monitor existing clinical standards of health care and to research and develop new clinical standards of health care;

(b) to research and evaluate prescription drug prescribing practices, prescription drug utilization and existing processes for reviewing and approving prescription drugs;

(c) to assess the effectiveness of new and existing health technologies;

(d) to promote improvement in the quality of health care through training and education;

(e) to develop and implement training and education programs and activities to promote improvement in the quality of health care;

(f) to promote research and education leading to improvement in the quality of health care;

(g) to monitor and assess the quality of the health services available in Saskatchewan;

(h) to investigate, inquire into or study matters respecting health services and the quality of health care that are referred to it by the minister;

(i) to undertake research with respect to any of the objects described in clauses (c) to (h);

(j) to identify human resource issues associated with the objects described in clauses (a) to (h);

(k) to do any other things prescribed in the regulations;

(l) to make recommendations to the minister and others with respect to any of the objects described in clauses (a) to (k).

2. Second, the Ministry of Health or eHealth Saskatchewan must reasonably take steps to de-identify the personal health information before it is disclosed to the Saskatchewan Health Quality Council. The regulations require that any information that by itself may reasonably be expected to identify the subject individual be removed. It also requires that the subject individual's health services number or any other number assigned to the individual be replaced with a unique encrypted identifier. See Appendix G for methods to de-identify personal health information.

3. Finally, there must be a written agreement between the Saskatchewan Health Quality Council and the Ministry or eHealth Saskatchewan that dictate the terms of the disclosure of the personal health information. The regulations indicate that such an agreement must include the following:

- a description of the personal health information to be disclosed to the council;

- a description of how the council should collect and use the personal health information;

- a statement that indicated that the council may only use the personal health information for the reasons set out in clauses 5(a) to (l) of The Health Quality Council Act;
- a statement that prohibits the council from disclosing personal health information without the approval of the Minister of Health;
- a statement that prohibits the council from re-identifying the personal health information;
- a statement that requires the council to protect the personal health information;
- a statement that ensures that any personal health information in a publication made by the council will not be able to be re-identified. In other words, the council must ensure that the subject individual of any personal health information in its publications cannot be identified.

The Ministry of Health, e-Health Saskatchewan and the Saskatchewan Health Quality Council should also include other best practices in its information sharing agreements. These include citing all the relevant legislative authority and identifying retention periods. Please see Appendix H for more information on information sharing agreements.

**Disclosure to police officers (Section 5.1 of the Regulations)**

5.1(1) For the purposes of clause 27(4)(p) of the Act, personal health information may be disclosed, without the consent of the subject individual, to a member of the Royal Canadian Mounted Police, or to a member of a police service within the meaning of The Police Act, 1990, in the following circumstances:

(a) by the minister or eHealth Saskatchewan if:

(i) the personal health information is required to locate the subject individual for any of the following purposes:

(A) enforcing an outstanding warrant for arrest that has been issued by a court, person or body that has the lawful authority to issue that warrant;

(B) serving a subpoena with respect to the prosecution of an indictable offence;

(C) locating a person reported missing; and

(ii) the personal health information to be disclosed is limited to:

(A) the name, address, date of birth and telephone number of the subject individual; or

(B) information respecting the location that the subject individual last received or was offered a health service;

(b) by a trustee if:

(i) the personal health information is requested for any of the following purposes:

(A) enforcing the Criminal Code or the Controlled Drugs and Substances Act (Canada);

(B) carrying out a lawful investigation pursuant to the Criminal Code or the Controlled Drugs and Substances Act (Canada); and
(ii) the personal health information to be disclosed is limited to:

(A) the name, address, date of birth and telephone number of the subject individual; or

(B) the nature and severity of an injury that:

(I) was suffered by the subject individual or another individual; and

(II) is connected with the enforcement or lawful investigation mentioned in subclause (i);

(c) by a trustee if:

(i) an individual received or was offered health services directly as a result of an incident that has been made the subject of a lawful investigation pursuant to the Criminal Code or the Controlled Drugs and Substances Act (Canada);

(ii) the personal health information to be disclosed is limited to:

(A) the factual circumstances surrounding the incident mentioned in subclause (i); and

(B) the factual circumstances surrounding the provision of, or offer to provide, health services; and

(iii) in the opinion of the trustee, the factual circumstances mentioned in subclause (ii) do not include the health history of the subject individual prior to the incident mentioned in subclause (i).

(2) For the purposes of clause 27(4)(p) of the Act, the minister or a trustee may disclose personal health information, without the consent of the subject individual, to the chief coroner or a coroner appointed pursuant to The Coroners Act, 1999 with respect to the conduct of an investigation or inquest by the chief coroner or other coroner pursuant to that Act.

Section 5.1 of the HIPA Regulations describes when trustees can disclose personal health information to the Royal Canadian Mounted Police (RCMP) or a member of a police service. Note that any disclosures are at the trustee’s discretion unless a court order has been made.

In accordance with section 10 of HIPA, trustees should be able to notify the subject individual of any disclosure made without the individual’s consent.

**5.1(1)(a) (HIPA Regulations)**

**Disclosures to police by the Ministry of Health and eHealth Saskatchewan**

The Ministry of Health and eHealth Saskatchewan are able to disclose the personal health information of an individual without consent if the police or RCMP is looking for the individual for one of these purposes:

- enforcing an outstanding warrant for arrest that has been issued by a court, person or body that has the lawful authority to issue that warrant;
- serving a subpoena with respect to the prosecution of an indictable offence;
- locating a person reported missing.
When disclosing personal health information to the police or RCMP for the purpose of locating an individual as described above, the Ministry or eHealth Saskatchewan may only disclose the following data elements:

- Name;
- Address;
- Date of birth;
- Telephone number; or
- Information regarding the location that the individual last was offered or received a health service.

It is best practice to get a written request from the police or RCMP describing the personal health information and why the personal health information requested will be helpful for the purposes outlined above. See Appendix I for a sample request form for police from the Sunrise Health Region.

Note that any disclosures are at the trustee’s discretion unless a court order has been made.

5.1(1)(b) (HIPA Regulations)
Disclosures to police by all trustees with respect to investigations or the enforcement of certain Acts

Any trustee can disclose certain personal health information to the police or RCMP if it is requested for the purposes of enforcing or investigating an incident dealing with:

- the Criminal Code (Canada); or
- the Controlled Drugs and Substances Act (Canada).

Note that any disclosures are at the trustee’s discretion unless a court order has been made.

A trustee can only disclose the following data elements:

- Name;
- Address;
- date of birth;
- telephone number; or
- the nature and severity of an injury that was suffered by the subject individual or another individual if it is connected to the enforcement or investigation described above.

It is best practice to have the police or RCMP who is requesting the information to do so in writing. The requester should indicate the following:

- The type of personal health information being requested (as listed above);
- Whether the personal health information relates to the Criminal Code or the Controlled Drugs and Substances Act (it is even better to ask the police to cite the specific section of the legislation);
• Why the personal health information is necessary for the enforcement or investigation;
• General contact information for the police officer (Name, name of police service, badge number and telephone number).

See Appendix I for a sample request form for police from the Sunrise Health Region.

It is also best practice to document what has been disclosed to the police or RCMP.

5.1(1)(c) (HIPA Regulations)
Disclosures to police by all trustees where the personal health information directly relates to an incident

Any trustee can disclose certain personal health information to the police or RCMP if it relates to an incident that is being investigated under:
  • the Criminal Code (Canada); or
  • the Controlled Drugs and Substances Act (Canada).

Note that any disclosures are at the trustee’s discretion unless a court order has been made.

A trustee can only disclose the following data elements:
  • factual circumstances surrounding the incident;
  • factual circumstances about the health services that were offered or provided as a result of the incident.

NOTE: A trustee should not disclose any health history (personal health information of the subject individual prior to the incident) to police or RCMP.

It is best practice to have the police or RCMP who is requesting the information to do so in writing. The requester should indicate the following:
  • The type of personal health information being requested (as listed above);
  • Whether the personal health information relates to the Criminal Code or the Controlled Drugs and Substances Act (it is even better to ask the police to cite the specific section of the legislation);
  • Why the personal health information is necessary for the enforcement or investigation;
  • General contact information for the police officer (name, name of police service, badge number and telephone number).

See Appendix I for a sample request form for police from the Sunrise Health Region.

It is also best practice to document what has been disclosed to the police or RCMP.

5(2) (HIPA Regulations)
Disclosures to the Chief Coroner

A trustee may disclose personal health information to the Chief Coroner without the subject individual’s consent for the purposes of an investigation or inquest by the Coroner.
Disclosure to a party to an information sharing agreement (Section 5.2 of the Regulations)

5.2(1) In this section:

(a) “common or integrated service” means a program or activity designed to benefit the health, safety, welfare or social well-being of an individual that is delivered by a government institution and one or more of the following:

(i) another government institution;
(ii) a local authority;
(iii) a trustee as defined in The Health Information Protection Act;
(iv) a First Nation;
(v) a police service or regional police service as defined in The Police Act, 1990;
(vi) the Royal Canadian Mounted Police;
(vii) a non-profit organization that provides a service of the type to be included in the common or integrated service;
(viii) any other agency or organization that the minister determines is appropriate;

(b) “information sharing agreement” means an agreement that governs the collection, use and disclosure of personal health information by the parties involved in the provision of a common or integrated service and that meets the requirements of subsection (2).

(2) An information sharing agreement must contain the following:

(a) a description of the common or integrated service to be provided;
(b) a description of the purposes or expected outcomes of the common or integrated service;
(c) provisions setting out the obligations of a party respecting the security and safeguarding of personal health information received by that party;
(d) provisions that prohibit the subsequent use and disclosure of the personal health information for purposes not related to the common or integrated service except:

(i) with the consent of the person to whom the information relates; or
(ii) if required or authorized by law;
(e) provisions for the withdrawal of a party and, in the case of a withdrawal, provisions that:

(i) prohibit any further use or disclosure of the personal health information received by that party except:

(A) with the consent of the person to whom the information relates; or
(B) if required or authorized by law; and
(ii) specify the ongoing obligations of that party to secure and safeguard the personal health information;
(f) provisions for the termination of the information sharing agreement and, in the case of a termination, provisions that:
(i) prohibit any further use or disclosure of the personal health information received by the parties except:

(A) with the consent of the person to whom the information relates; or

(B) if required or authorized by law; and

(ii) specify the ongoing obligations of the parties to secure and safeguard the personal health information;

(g) any other provisions that the minister considers necessary.

(3) For the purposes of clause 27(4)(p) of the Act, personal health information may be disclosed to a party to an information sharing agreement entered into for the purposes of providing a common or integrated service:

(a) if that information is disclosed in accordance with the agreement for any or all of the following purposes:

(i) determining the eligibility of an individual to receive the common or integrated service;

(ii) assessing and planning the common or integrated service and delivering that service to an individual or that individual’s family; or

(b) if consent to the disclosure was obtained pursuant to any other Act or regulation that does not require the consent to be in writing.

(4) If the Royal Canadian Mounted Police participates in providing a common or integrated service, the requirements of subsection (3) are met if the Royal Canadian Mounted Police enters into a single arrangement in writing with a government institution that is involved in the provision of the common or integrated service, under which the Royal Canadian Mounted Police signifies that it will comply with the terms governing the collection, use and disclosure of personal information contained in the information sharing agreement applicable to the common or integrated service in which the Royal Canadian Mounted Police participates.

This section allows trustees to disclose personal health information with other organizations for the purposes of providing a common or integrated service if an information sharing agreement is in place.

In accordance with section 10 of HIPA, trustees should be able to notify the subject individual of any disclosure made without the individual’s consent.

A common or integrated service is a program or activity designed to benefit the health, safety, welfare or social well-being of an individual that is delivered by a government institution and one or more of the following:

- another government institution;
- a local authority;
- a trustee;
- a First Nation;
- a police service or regional police service as defined in The Police Act, 1990;
- the Royal Canadian Mounted Police;
• a non-profit organization that provides a service of the type to be included in the common or integrated service;
• any other agency or organization that the Minister of Health determines is appropriate.

One current example of a common or integrated service is the HUB set up in Prince Albert, Saskatchewan. It provides immediate, coordinated and integrated responses through the mobilization of resources to address situations facing individuals and/or families with acutely elevated risk factors, as recognized across a range of service providers.

The information can be disclosed for this purpose to:
• determining the eligibility of an individual to receive the common or integrated service;
• assessing and planning the common or integrated service and delivering that service to an individual or that individual’s family; or

Also, if an individual has consented to the disclosure in accordance with any other Act or regulation, the consent may not have to be in writing.

In order for a trustee to disclose personal health information to a common or integrated service, an information sharing agreement must be in place.

An information sharing agreement is an agreement that governs the collection, use and disclosure of personal health information by the parties involved in the provision of a common or integrated service and that meets the requirements of subsection 5.2(2). Subsection 5.2(2) of the regulations requires an information sharing agreement to contain the following:

• a description of the common or integrated service to be provided;
• a description of the purposes or expected outcomes of the common or integrated service;
• provisions setting out the obligations of each party respecting the security and safeguarding of personal health information received by that party;
• provisions that prohibit the subsequent use and disclosure of the personal health information for purposes not related to the common or integrated service except:
  o with the consent of the person to whom the information relates; or
  o if required or authorized by law;
• provisions for the withdrawal of a party and, in the case of a withdrawal, provisions that:
  o prohibit any further use or disclosure of the personal health information received by that party except:
    - with the consent of the person to whom the information relates; or
    - if required or authorized by law; and
  o specify the ongoing obligations of that party to secure and safeguard the personal health information;
• provisions for the termination of the information sharing agreement and, in the case of a termination, provisions that:
  o prohibit any further use or disclosure of the personal health information received by the parties except:
with the consent of the person to whom the information relates; or
- if required or authorized by law; and
  - specify the ongoing obligations of the parties to secure and safeguard the personal health information;
• any other provisions that the minister considers necessary.

Trustees should also add in other best practices in its information sharing agreements. These include citing all the relevant legislative authority and identifying retention periods. Please see Appendix H for more information on information sharing agreements.

The RCMP that participates in providing a common or integrated service only needs to enter into an agreement with a government institution of the agreement signifies it will comply with the terms of the information sharing agreement of the common or integrated service.

**Disclosure to the Cancer Agency (Section 6 of the Regulations)**

Pursuant to subsection 28(8) of the Act, registration information may be disclosed to the Cancer agency and by the Cancer agency for any of the purposes set out in subsections 28(1) to (3) of the Act as if the Cancer agency were a regional health authority or an affiliate.

Registration information can be disclosed to the Cancer Agency for the purposes described in section 28(1) to (3) of HIPA.

In accordance with section 10 of HIPA, trustees should be able to notify the subject individual of any disclosure made without the individual’s consent.
Disclosure by the college, health professional bodies or health professionals for the purpose of monitoring prescribing, dispensing or using drugs (Sections 6.1 to 6.3 of the Regulations)

6.1(1) In this section and in sections 6.2 and 6.3:

(a) “college” means the College of Physicians and Surgeons of the Province of Saskatchewan;

(b) “drug” means a drug that is listed in section 18.1 of the college’s bylaws and is approved by the minister;

(c) “health professional” means a person who:

   (i) is licensed pursuant to an Act for which the minister is responsible; and
   (ii) is authorized by The Drug Schedules Regulations, 1997 to prescribe or dispense a drug;

(d) “health professional body” means a body other than the college that, pursuant to an Act for which the minister is responsible, regulates health professionals;

(e) “program” means a program to monitor the prescribing, dispensing or use of drugs that is authorized by a bylaw that:

   (i) is made pursuant to The Medical Profession Act, 1981 or an Act that regulates a health professional body; and
   (ii) is approved by the minister.

(2) The college may use or disclose personal health information in its custody and control without the consent of the subject individual in one or more of the following cases:

(a) the use or disclosure is made for the purposes of a program;

(b) the disclosure is to a trustee who controls the operation of a proprietary pharmacy as defined in The Pharmacy Act, 1996;

(c) the disclosure is made to a health professional;

(d) the disclosure is made to a health professional body.

6.2(1) A health professional body to which personal health information is disclosed pursuant to clause 6.1(2)(d) or section 6.3 may disclose that information:

(a) subject to subsection (2), to the college or another health professional body, as the case may be, if the disclosure is made for the purposes of a program; or

(b) to a health professional if the disclosure is made for the purposes of a program.

(2) A health professional body to which personal health information is disclosed pursuant to clause (1)(a), clause 6.1(2)(d) or section 6.3 shall only use or disclose that personal health information for one or more of the following purposes:

(a) for a purpose authorized by a bylaw that:

   (i) is made pursuant to an Act that regulates a health professional body; and
   (ii) is approved by the minister;

(b) for the purpose of carrying out its duties with respect to regulating the members of
6.3 A health professional may disclose to the college or to a health professional body personal health information in his or her custody and control without the consent of the subject individual if the disclosure is made for the purposes of a program.

Sections 6.1, 6.2 and 6.3 of the HIPA Regulations deal with the disclosure of personal health information for the purposes of a program to monitor the prescribing, dispensing or use of drugs that is authorized by a bylaw.

Subsections 6.1(2) and 6.3 of the HIPA Regulations describe when The College of Physicians and Surgeons and health professionals can disclose or use personal health information for these purposes.

Section 6.2 describes when a health professional body can use or disclose personal health information that has been received by the College of Physicians and Surgeons or a health professional for the purpose of monitoring the prescribing, dispensing or use of drugs.

In accordance with section 10 of HIPA, trustees should be able to notify the subject individual of any disclosure made without the individual’s consent.

6.1(2) (HIPA Regulations)
The College of Physicians and Surgeons of Saskatchewan can use or disclose personal health information without the consent of the individual for the following four purposes [6.1(2)(a) to (d)]:

6.1(2)(a) (HIPA Regulations)
The use or disclosure is for a program to monitor the prescribing, dispensing or use of drugs that is authorized by a bylaw that is made pursuant to The Medical Profession Act, 1981 or an Act that regulates a health professional body. The program also has to be approved by the Minister of Health.

6.1(2)(b) (HIPA Regulations)
The disclosure is to a trustee who controls the operation of a proprietary pharmacy as defined in The Pharmacy Act, 1996.

6.1(2)(c) (HIPA Regulations)
The disclosure is made to a health professional who is licensed pursuant to an Act for which the minister is responsible and is authorized by The Drug Schedules Regulations, 1997 to prescribe or dispense a drug.
6.1(2)(d) (HIPA Regulations)
The disclosure is made to a health professional body that regulates health professionals pursuant to an Act for which the Minister of Health is responsible.

6.2(1) (HIPA Regulations)
A health professional body that has collected personal health information pursuant to subsections 6.1(2)(d) or 6.3 can disclose the personal health information for the following two purposes [6.2(1)(a) to (b)]:

6.2(1)(a) (HIPA Regulations)
To the College of Physicians and Surgeons of Saskatchewan or another health professional body if the disclosure is made for a program to monitor the prescribing, dispensing or use of drugs that is authorized by a bylaw that is made pursuant to The Medical Profession Act, 1981 or an Act that regulates a health professional body.

6.2(1)(b) (HIPA Regulations)
To a health professional for the purposes of a program to monitor the prescribing, dispensing or use of drugs that is authorized by a bylaw that is made pursuant to The Medical Profession Act, 1981 or an Act that regulates a health professional body.

6.2(2) (HIPA Regulations)
A health professional body that has collected personal health information pursuant to subsections 6.1(2)(d), 6.2(1)(a) or 6.3 can only use or disclose the personal health information for the following three purposes [6.2(2)(a) to (c)]:

6.2(2)(a) (HIPA Regulations)
The disclosure or the use is consistent with a bylaw of a health professional body that is authorized by an Act and approved by the Minister of Health.

6.2(2)(b) (HIPA Regulations)
The disclosure or the use is for the purpose of carrying out its duties with respect to regulating the members of its profession.

6.2(2)(c) (HIPA Regulations)
The disclosure or the use is for the purpose of a program to monitor the prescribing, dispensing or use of drugs that is authorized by a bylaw that is made pursuant to The Medical Profession Act, 1981 or an Act that regulates a health professional body.

6.3 (HIPA Regulations)
A health professional may disclose personal health information to the College of Physicians and Surgeons of Saskatchewan or another health professional body without the consent of the subject individual if the disclosure is made for the purposes of a program to monitor the prescribing, dispensing or use of drugs that is authorized by a bylaw that is made pursuant to The Medical Profession Act, 1981 or an Act that regulates a health professional body.
Disclosure or registration information by eHealth Saskatchewan (Section 6.4 of the Regulations)

6.4 (1) For the purposes of subsection 28(8) of the Act, eHealth Saskatchewan may disclose registration information without the consent of the subject individual:

(a) to a trustee in connection with the provision of health services by the trustee;

(b) to the minister, another government institution, a regional health authority or an affiliate for the purpose of verifying the eligibility of an individual to participate in a program of, or receive a service from, the minister, government institution, regional health authority or affiliate:

(i) in the course of processing an application made by or on behalf of the individual; or

(ii) if the individual is participating in the program or receiving the service; or

(c) to the minister, another government institution, a regional health authority or an affiliate for the purpose of verifying the accuracy of registration information held by the minister, the government institution, regional health authority or affiliate.

(2) For the purposes set out in subsection (3), registration information may be disclosed without the consent of the subject individual:

(a) by eHealth Saskatchewan to a regional health authority or affiliate;

(b) by a regional health authority or affiliate to eHealth Saskatchewan;

(c) by eHealth Saskatchewan to the minister;

(d) by the minister to eHealth Saskatchewan;

(e) by eHealth Saskatchewan to a trustee; or

(f) by a trustee to eHealth Saskatchewan.

(3) Registration information may be disclosed pursuant to subsection (2) for the purpose of planning, delivering, evaluating or monitoring a program of the minister, eHealth Saskatchewan, a regional health authority or an affiliate that relates to the provision of health services or payment for health services.

(4) eHealth Saskatchewan may, without the consent of the subject individual, disclose registration information to the Government of Canada or the government of a province or territory of Canada.

(5) Any disclosure of registration information pursuant to this section is to be:

(a) subject to subsection (6), limited to the name, address, date of birth and telephone number of the subject individual; and

(b) in accordance with an agreement that contains a provision that the party to whom the registration information is disclosed shall use the information only for the purposes specified in the agreement.

(6) Registration information in addition to the information mentioned in clause (5)(a) may be disclosed in accordance with subsection (2) only if that information is necessary to fulfil obligations under an agreement mentioned in clause (5)(b).
6.4(1) (HIPA Regulations)
eHealth Saskatchewan may disclose registration information without the consent of the subject individual if one of these three circumstances exists [6.4(1)(a) to (c)].

In accordance with section 10 of HIPA, trustees should be able to notify the subject individual of any disclosure made without the individual’s consent.

6.4(1)(a) (HIPA Regulations)
eHealth Saskatchewan may disclose registration information to another trustee if it is related to health services to be provided by that trustee.

Registration information should be limited to the name, address, date of birth and telephone number of the subject individual. Further, there must be an agreement in place that contains a provision that the party that collects the registration information can only use the information for the purposes specified in the agreement. Best practice is to have an information sharing agreement in place. See Appendix H for more information about information sharing agreements.

6.4(1)(b) (HIPA Regulations)
eHealth Saskatchewan may disclose registration information to the Ministry of Health, another government institution, a regional health authority or an affiliate for the purpose of verifying the eligibility of an individual to participate in a program of, or receive a service by that trustee. This can occur while processing an application or if the subject individual is already participating in the program or receiving the service.

Registration information should be limited to the name, address, date of birth and telephone number of the subject individual. Further, there must be an agreement in place that contains a provision that the party that collects the registration information can only use the information for the purposes specified in the agreement. Best practice is to have an information sharing agreement in place. See Appendix H for more information about information sharing agreements.

6.4(1)(c) (HIPA Regulations)
eHealth Saskatchewan may disclose registration information to the Ministry of Health another government institution, a regional health authority or an affiliate for the purpose of verifying the accuracy of registration information held by one of those trustees. See section 19 of HIPA for information about the accuracy of personal health information.

Registration information should be limited to the name, address, date of birth and telephone number of the subject individual. Further, there must be an agreement in place that contains a provision that the party that collects the registration information can only use the information for the purposes specified in the agreement. Best practice is to have an information sharing agreement in place. See Appendix H for more information about information sharing agreements.

6.4(2) and (3) (HIPA Regulations)
Registration information may be disclosed without the consent of the subject individual for the purpose of planning, delivering, evaluating or monitoring a program of the Ministry of
Health, eHealth Saskatchewan, a regional health authority or an affiliate that relates to the provision of health services or payment for health services.

In accordance with section 10 of HIPA, trustees should be able to notify the subject individual of any disclosure made without the individual’s consent.

These disclosures may occur as follows:

- by eHealth Saskatchewan to a regional health authority or affiliate;
- by a regional health authority or affiliate to eHealth Saskatchewan;
- by eHealth Saskatchewan to the minister;
- by the minister to eHealth Saskatchewan;
- by eHealth Saskatchewan to a trustee; or
- by a trustee to eHealth Saskatchewan.

Registration information should be limited to the name, address, date of birth and telephone number of the subject individual. Further, there must be an agreement in place that contains a provision that the party that collects the registration information can only use the information for the purposes specified in the agreement. Best practice is to have an information sharing agreement in place. See Appendix H for more information about information sharing agreements. In these cases, more types of registration information may be disclosed if specified in the agreement pursuant to subsection 6.4(6) of the HIPA Regulations.

6.4(4) (HIPA Regulations)
eHealth Saskatchewan may, without the consent of the subject individual, disclose registration information to the Government of Canada or the government of a province or territory of Canada.

In accordance with section 10 of HIPA, trustees should be able to notify the subject individual of any disclosure made without the individual’s consent.

Registration information should be limited to the name, address, date of birth and telephone number of the subject individual. Further, there must be an agreement in place that contains a provision that the party that collects the registration information can only use the information for the purposes specified in the agreement. Best practice is to have an information sharing agreement in place. See Appendix H for more information about information sharing agreements.
Disclosures to the Ministry of Education (Section 7 of the Regulations)

7(1) Pursuant to subsection 28(8) of the Act, the minister or eHealth Saskatchewan may disclose registration information in accordance with subsection (2) to the Ministry of Education for the purpose of enabling the Ministry of Education to administer a database for the tracking of persons of an age up to and including compulsory school age.

(2) In a disclosure made pursuant to subsection (1), the minister or eHealth Saskatchewan:

(a) may disclose registration information with respect to persons of an age up to and including compulsory school age and the parents or guardians of those persons; and

(b) shall disclose only the following types of registration information with respect to the subject individual that are necessary for the purpose described in that subsection:

(i) name;
(ii) date of birth;
(iii) name of the individual’s parents or guardians;
(iv) address and phone number of the individual’s parents or guardians.

eHealth Saskatchewan may disclose registration information to the Ministry of Education for the purpose of administering a database for the tracking of persons of an age up to and including compulsory school age.

eHealth Saskatchewan may only disclose registration information of individuals of an age up to and including compulsory school age.

eHealth Saskatchewan may only disclose the following registration information for these purposes:

- name;
- date of birth;
- name of the individual’s parents or guardians;
- address and phone number of the individual’s parents or guardians.

In accordance with section 10 of HIPA, trustees should be able to notify the subject individual of any disclosure made without the individual's consent.
Use and disclosure for fundraising purposes (Section 7.1 of the Regulations)

7.1(1) In this section:

(a) “client” means an individual who has received a health service, whether as an in-patient or an out-patient, at a hospital operated by a designated trustee;

(b) “client information” means the name and address of a client;

(c) “client list” means a client list prepared in accordance with subsection (4);

(d) “consent to fundraising statement” means a brief statement to the effect that, unless a client opts out, client information may be used by the designated trustee for fundraising purposes or disclosed to a fundraising agency for fundraising purposes;

(e) “designated trustee” means:

   (i) a regional health authority;

   (ii) an affiliate; or

   (iii) the Athabasca Health Authority;

(f) “eligible client” means a client who meets the criteria set out in subsection (5);

(g) “fundraising activity” means a fundraising activity for a health-related charitable purpose;

(h) “fundraising agency” means a registered charity as defined in the *Income Tax Act* (Canada) that:

   (i) is incorporated in Saskatchewan for the sole purpose of carrying out fundraising activities for the benefit of a designated trustee; and

   (ii) has entered into a fundraising agreement with a designated trustee;

(i) “fundraising agreement” means an agreement between a designated trustee and a fundraising agency by which the fundraising agency is authorized to carry out fundraising activities on behalf of the designated trustee;

(j) “health-related charitable purpose” means a charitable purpose related to a health services facility situated in Saskatchewan or to the provision in Saskatchewan of a health service or program;

(k) “hospital” means a facility designated as a hospital pursuant to *The Facility Designation Regulations*, and includes a hospital operated by the Athabasca Health Authority;

(l) “opt out” means to inform a designated trustee or a fundraising agency, in accordance with subsection (10), that a client does not consent to the use or disclosure of his or her client information by the designated trustee or the fundraising agency for the purposes of a fundraising activity;

(m) “opting-out procedure” means a procedure by which a client may inform a designated trustee or a fundraising agency, as the case may be, that the client wishes to opt out;

(n) “personal care home” means a personal care home as defined in *The Personal Care Homes Act*;

(o) “preparation date” means the date on which a client list is prepared;
(p) “special-care home” means a facility designated as a special-care home pursuant to The Facility Designation Regulations.

(2) A designated trustee may, in accordance with this section:

(a) use client information for fundraising purposes; or

(b) disclose client information to a fundraising agency for fundraising purposes.

(3) Before using client information for fundraising purposes or disclosing client information to a fundraising agency, a designated trustee must:

(a) prepare a consent to fundraising statement and post it, or otherwise make it available in a manner likely to come to the attention of clients, in places where health services are provided;

(b) develop an opting-out procedure;

(c) at the time of providing a health service to a client, provide the client with written information about the opting-out procedures of the designated trustee and any fundraising agencies that are authorized to carry out fundraising activities on behalf of the designated trustee; and

(d) prepare a client list in accordance with subsection (4).

(4) A designated trustee may, from time to time, use the personal health information of eligible clients in the custody or control of the trustee for the purpose of preparing a client list that sets out:

(a) the client information of clients who, as of the preparation date, are eligible clients; and

(b) the preparation date of the list.

(5) A client is an eligible client if:

(a) the client is 18 years of age or older at the date of discharge from a hospital or the date of receiving a health service;

(b) the client was not a resident of a personal care home or a special-care home immediately before being admitted to a hospital or at the time of receiving a health service;

(c) in the case of a client who was an in-patient in a hospital, the client did not become a resident of a personal care home or a special-care home on discharge from the hospital;

(d) as of the preparation date, a period of not less than 60 days has elapsed since the most recent date on which the client:

(i) was discharged from the hospital; or

(ii) received a health service at the hospital on an out-patient basis; and

(e) the client:

(i) has not opted out pursuant to subsection (10); or

(ii) has revoked a decision to opt out pursuant to subsection (11).

(6) Subject to subsections (7) to (14), a designated trustee may:

(a) use client information in a client list to carry out a fundraising activity; or

(b) provide a client list to a fundraising agency with which it has entered into a
fundraising agreement that meets the requirements of subsection (8).

(7) A designated trustee shall not reveal any personal health information other than client information:

(a) when contacting or attempting to contact a client for the purposes of a fundraising activity; or

(b) when disclosing client information to a fundraising agency.

(8) A fundraising agreement must:

(a) require the fundraising agency:

(i) to provide to any client who receives a solicitation from the agency a simple procedure for opting out of future solicitations;

(ii) to notify the designated trustee promptly of any opting out by a client that is communicated to the fundraising agency;

(iii) to protect and secure the client information disclosed to it by the designated trustee by means that include, without limiting the generality of the foregoing:

(A) establishing policies and procedures to maintain administrative, technical and physical safeguards for the client information;

(B) appointing a person to be responsible for the client information;

(C) ensuring that the client information is accessible only to those of its employees who perform fundraising activities; and

(D) providing for the continuation of all duties imposed by the fundraising agreement with respect to the protection of client information in the custody or control of the fundraising agency after the expiration or termination of the fundraising agreement until the fundraising agency transfers the custody and control of the client information back to the designated trustee or to a designated archive; and

(iv) to advise the designated trustee immediately on discovery if any client information has been compromised or any requirement of the agreement has been breached; and

(b) prohibit the fundraising agency from:

(i) soliciting a client who:

(A) is not listed in the current client list; or

(B) has opted out, unless the opting out has not been communicated to the fundraising agency; or

(ii) using or disclosing client information for any purpose other than the purposes of a fundraising activity on behalf of the designated trustee that is authorized by the agreement.

(9) Subject to subsections (10) to (14), a fundraising agency may, in accordance with the terms of a fundraising agreement with a designated trustee, use client information in a client list provided by the designated trustee for the purpose of carrying out a fundraising activity on behalf of the designated trustee.

(10) A client may, at any time, opt out of receiving fundraising solicitations:

(a) by following the opting-out procedure of the designated trustee or fundraising agency;
(b) by any other means that communicates the client’s intention to opt out to the designated trustee or fundraising agency.

(11) A client may, at any time, revoke his or her decision to opt out.

(12) If a client’s intention to opt out is communicated to a designated trustee, the designated trustee shall:

(a) promptly advise each fundraising agency with which it has entered into a fundraising agreement that the client has opted out; and

(b) immediately remove the client’s name from the current client list.

(13) If a client’s intention to opt out is communicated to a fundraising agency, the fundraising agency shall:

(a) promptly advise the designated trustee with which it has entered into a fundraising agreement that the client has opted out; and

(b) immediately remove the client’s name from the current client list.

(14) A fundraising agency shall not disclose client information to any person or agency:

(a) except for the purposes of carrying out a fundraising activity authorized by a fundraising agreement; and

(b) in accordance with the provisions of the fundraising agreement mentioned in clause (a) that are required by subclause (8)(a)(iii).

What is a fundraising activity?

For the purposes of using or disclosing personal health information, a fundraising activity must be for a health-related charitable purpose. In other words, it is a charitable purpose related to a health services facility situated in Saskatchewan or to the provision in Saskatchewan of a health service or program.

Only certain trustees may use or disclose personal health information for a fundraising activity (designated trustees). Further, only certain personal health information can be used.

Which Trustees can use or disclose personal health information for a fundraising activity?

The HIPA Regulations only allow “designated trustees” to use or disclose personal health information for fundraising activities. A designated trustee means a regional health authority, an affiliate, or the Athabasca Health Authority.

A designated trustee can:

- use client information (personal health information) for fundraising purposes; or
- disclose client information (personal health information) to a fundraising agency for fundraising purposes.
What is a fundraising agency and what is its role?
A fundraising agency is a registered charity as defined in the *Income Tax Act* (Canada) that is incorporated in Saskatchewan for the sole purpose of carrying out fundraising activities for the benefit of a designated trustee. The fundraising agency and designated trustee must also have entered into a fundraising agreement. Examples are the Hospitals of Regina Foundation and the Royal University Hospital Foundation.

A fundraising agreement is an agreement between a designated trustee and a fundraising agency by which the fundraising agency is authorized to carry out fundraising activities on behalf of the designated trustee. See Requirements of a Fundraising Agreement for more information.

When a “fundraising agreement” is in place, a fundraising agency may only use personal health information provided by the designated trustee for the purpose of carrying out a fundraising activity on behalf of the designated trustee.

A fundraising agency should not use or disclose personal health information to any person or agency except for the purposes of carrying out a fundraising activity authorized by a fundraising agreement.

What personal health information can be used or disclosed?
Designated trustees may only use or disclose certain personal health information of certain individuals for fundraising activities. It is referred to in the Regulations as “client information”.

Designated trustees can only use the name and address of a “client”. A client is an individual who has received a health service, whether as an in-patient or an out-patient, at a hospital operated by a designated trustee. A hospital is a facility designated as a hospital pursuant to *The Facility Designation Regulations*, and includes a hospital operated by the Athabasca Health Authority.

Further, a client must also qualify as an “eligible client”. An eligible client is a client that:

- is 18 years of age or older at the date of discharge from a hospital or the date of receiving a health service;
- was not a resident of a personal care home or a special-care home immediately before being admitted to a hospital or at the time of receiving a health service;
- in the case of a client who was an in-patient in a hospital, the client did not become a resident of a personal care home or a special-care home on discharge from the hospital;
- as of the preparation date, a period of not less than 60 days has elapsed since the most recent date on which the client was discharged from the hospital or received a health service at the hospital on an out-patient basis; and
- the client has not opted out or has revoked a decision to opt out. See opt-out section below.

The only personal health information that can be used for a fundraising activity is the name and address of a client. This is referred to as client information.
Designated trustees will create a client list for the purposes of a fundraising activity. The list contains client information of eligible clients. The client list should also contain the preparation date which means the date on which a client list is prepared.

Designated trustees can use the information in a client list to carry out a fundraising activity or provide a client list to a fundraising agency with which it has entered into a fundraising agreement. However, the designated trustee must ensure that all the requirements are in place as described in the HIPA Regulations before using or disclosing the personal health information.

When contacting clients for the purposes of a fundraising activity or disclosing client information to a fundraising agency, a designated trustee must ensure that no other personal health information is disclosed. For example, a designated trustee should not create lists that would reveal other personal health information such as lists of clients with cardiac problems or clients who have given birth etc.

**What needs to be in place before using or disclosing personal health information for a fundraising activity?**

Before a designated trustee uses or discloses client information for the purposes of fundraising activities, it must have the following requirements in place:

1. Prepare a “consent to fundraising statement” and post it, or otherwise make it available in a manner likely to come to the attention of clients, in places where health services are provided. A consent to fundraising statement means a brief statement to the effect that, unless a client opts out, client information may be used by the designated trustee for fundraising purposes or disclosed to a fundraising agency for fundraising purposes. Such a statement can be posted in common waiting rooms, on the trustees website or in handouts to the clients.

2. Develop an opt-out procedure. See opt-out section below.

3. At the time of providing a health service to a client, provide the client with written information about the opting-out procedures.

4. Prepare a client list.

**Requirements of a Fundraising Agreement**

Each time a designated trustee provides a client list to a fundraising agency, a fundraising agreement must be in place. A fundraising agreement is an agreement between a designated trustee and a fundraising agency by which the fundraising agency is authorized to carry out fundraising activities on behalf of the designated trustee and should contain the following:

Clauses that require the fundraising agency:

- To provide to any client who receives a solicitation from the agency a simple procedure for opting out of future solicitations. See section on opt-out.

- To notify the designated trustee promptly of any opting out by a client that is communicated to the fundraising agency. There should also be a reciprocal procedure.

- To protect and secure the client information disclosed to it by the designated trustee by means that include:
establishing policies and procedures to maintain administrative, technical and physical safeguards for the client information (See Appendix B for detailed examples of safeguards);

- appointing a person to be responsible for securing the client information, answer inquiries and handle privacy breaches;

- ensuring that the client information is accessible only to those of its employees who perform fundraising activities; and

- ensuring that the fundraising agency will protect the personal health information until a date specified in the contact. On that date, the fundraising agency will either destroy the personal health information in a secure manner or transfer it back to the designated trustee.

- To advise the designated trustee immediately on discovery if any client information has been compromised or any requirement of the agreement has been breached.

Clauses that prohibit the fundraising agency from:

- Soliciting a client who is not listed in the current client list; or has opted out; or

- Using or disclosing client information for any purpose other than the purposes of a fundraising activity on behalf of the designated trustee that is authorized by the agreement.

The list above is required in an agreement by the HIPA Regulations. However, it is best practice that designated trustees and fundraising agencies include all of the elements of an information sharing agreement when making a fundraising agreement. See Appendix H for more details of what should be included in a information sharing agreement.

**What is opt out?**

“Opt out” means to inform a designated trustee or a fundraising agency that a client does not consent to the use or disclosure of his or her client information by the designated trustee or the fundraising agency for the purposes of a fundraising activity. In other words, the designated trustee and fundraising agency may not use an individual’s personal health information for fundraising activities if he/she has opted-out.

Both the designated trustee and the fundraising agency must have “opting-out procedures” in place. An “opting-out procedure” means a procedure by which a client may inform a designated trustee or a fundraising agency, as the case may be, that the client wishes to opt out.

An individual, at any time has the right to opt-out by following the opting-out procedure of the designated trustee or fundraising agency. The individual can also opt-out by any other means he/she uses to communicate this intention to the designated trustee or fundraising agency.

An individual also has the right to revoke his/her decision to opt-out.

If a client’s intention to opt out is communicated to a designated trustee, the designated trustee must:
promptly advise each fundraising agency with which it has entered into a fundraising agreement that the client has opted out; and

immediately remove the client’s name from the current client list.

If a client’s intention to opt out is communicated to a fundraising agency, the fundraising agency shall:

promptly advise the designated trustee with which it has entered into a fundraising agreement that the client has opted out; and

immediately remove the client’s name from the current client list.

Although the HIPA Regulations provide an opt-out model for using and disclosing personal health information for fundraising purposes, an opt-in model is best practice. Opt-in provides an opportunity for all individuals to consent to the use and disclosure of personal health information for fundraising purposes for by signing up to be solicited. Designated trustees should strongly consider this approach.

In accordance with section 10 of HIPA, trustees should be able to notify the subject individual of any disclosure made without the individual’s consent.
APPENDIX A – GLOSSARY

Access means the viewing or obtaining of personal health information. See also the Right of Access.

Access request means a written or oral request of an individual to a trustee for access to his/her own personal health information. The request could also be made by a representative of an individual authorized by section 15 or 56 of HIPA. See also Written Request for Access.

Administrative safeguards are controls that focus on internal organization, policies, procedures and maintenance of security measures that protect personal health information.

Affiliate means an affiliate as defined in The Regional Health Services Act (See section 2 of HIPA).

Amendment is the act of making a change to the personal health information of the subject individual who believes there is an error or omission.

Applicant means an individual who makes a written request for access to personal health information about himself or herself. Also, an applicant can mean a person who makes an application for review (See sections 31 and s.41(a) of HIPA).

Application for Review means an application pursuant to section 42 of HIPA (See Section 41(b) of HIPA). See also Review and Request for Review.

Capacity, in the context of exercising individual rights afforded by HIPA, means the ability:
- to understand information relevant to making a decision; and
- to appreciate the reasonably foreseeable consequences of making or not making a decision.

Circle of care is not a term found in HIPA, but is a popular term among Saskatchewan trustees. It refers to an analogy where the patient is at the center of the circle. Health care professionals involved in the diagnosis treatment and care of the patient are also in the circle. The IPC prefers the need-to-know principle.

Client, for the purpose of section 7.1 of the HIPA Regulations, means an individual who has received a health service, whether as an in-patient or an out-patient, at a hospital operated by a designated trustee.

Client information, for the purpose of section 7.1 of the HIPA Regulations, means the name and address of a client, which qualifies as personal health information.

Client list means a client list prepared in accordance with subsection 7.1(4) of the HIPA Regulations.

Collect means to gather, obtain access to, acquire, receive or obtain personal health information from any source by any means (See section 2(b) of HIPA).

Collection is a term used to describe the action of having gathered, obtained access to, acquired, received or obtained personal health information.
Commissioner means the Information and Privacy Commissioner appointed pursuant to section 38 of The Freedom of Information and Protection of Privacy Act. The Commissioner is an Officer of the Legislative Assembly and is appointed by the Legislative Assembly (See HIPA s.2(c)).

Common or integrated service means a program or activity designed to benefit the health, safety, welfare or social well-being of an individual that is delivered by a government institution and one or more of the following:

- another government institution;
- a local authority;
- a trustee as defined in The Health Information Protection Act;
- a First Nation;
- a police service or regional police service as defined in The Police Act, 1990;
- the Royal Canadian Mounted Police;
- a non-profit organization that provides a service of the type to be included in the common or integrated service;
- any other agency or organization that the Minister of Health determines is appropriate.

Complainant refers to an individual who makes a formal privacy complaint to a trustee or to the Commissioner.

Comprehensive health record means a comprehensive health record described in subsection 18.1(2) of HIPA (See section 2(c.1) of HIPA).

Confidentiality implies a trust relationship between the person supplying information and the individual or organization collecting it.

Consent means informed, voluntary agreement with what is being done or proposed with respect to the collection, use of disclosure personal health information. HIPA provides trustees with three different options. See section 6 of this Guide for more information.

Express consent is the highest standard and can be written (e.g. form or letter) or verbal. It must be informed and meet all the following conditions:

- The specific personal health information to be collected, used or disclosed;
- Anticipated uses and/or disclosures;
- To whom the personal health information may be disclosed;
- The date the consent is effective and the date on which the consent expires; and
- Any potential risks associated with the collection, use or disclosure.

Implied consent must first meet a number of conditions. The consent to the collection, use or disclosure of personal health information by a trustee may only be implied if:

- In all circumstances, the purpose of the collection, use or disclosure is or will become reasonably obvious to the individual.
- It is reasonable to expect that the individual would consent to the collection use or disclosure.
- The trustee is not aware that the individual withdrew consent.
• The trustee uses or discloses the information for no other purpose other than the purpose for which it was collected.
• The individual has the right to “opt out”.

_Deemed consent_ means a trustee can forgo express or implied consent in certain circumstances, such as when an individual is unable to give consent, is unconscious or in emergent circumstances. See subsection 27(2) of HIPA.

_Consent to fundraising statement_ means a brief statement to the effect that, unless a client opts out, client information may be used by the designated trustee for fundraising purposes or disclosed to a fundraising agency for fundraising purposes as authorized by section 7.1 of the HIPA Regulations.

_Control_ connotes authority. A record is under the control of a trustee when the trustee has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. Custody is not a requirement for control.

_Custody_ is the physical possession of a record by a trustee.

_Data minimization principle_ means that a trustee should collect, use or disclose the least amount of identifying information necessary for the purpose.

_Deemed refusal_ means that a trustee has not responded to an access request within 30 days and it will be interpreted that the trustee will not provide the applicant with the requested personal health information pursuant to subsection 36(3) of HIPA.

_De-identified personal health information_ means personal health information from which any information that may reasonably be expected to identify an individual has been removed (See HIPA s.2(d)).

_Designated archive_ means an archive designated in the regulations for the purposes of section 22 (See HIPA s.2(e)). _Section 4 of the HIPA Regulations_ designates several archives.

_Designated trustee_, with respect to section 7.1 of the HIPA Regulations, means a regional health authority, an affiliate or the Athabasca Health Authority.

_Disclosure_ is the exposure of personal health information to a separate entity, not a division or branch of the trustee in custody or control of that information.

_Drug_, for the purposes of sections 6.1, 6.2 and 6.3 of the HIPA Regulations, means a drug that is listed in section 18.1 of the college’s bylaws and is approved by the Minister of Health.

_Duty to Assist_ means responding openly, accurately and completely to an individual requesting access to his/her own personal health information in accordance with section 35 of HIPA.

_Eligible client_ means a client who meets the criteria set out in subsection 7.1(5) of the HIPA Regulations.

_Endanger_ means the act of putting someone or something in danger; exposure to peril or harm.
Error means a mistake or something wrong or incorrect.

Fiscal year means the period commencing on April 1 in one year and ending on March 31 in the following year (See section 2(g) of HIPA).

Frivolous is typically associated with matters that are trivial or without merit, lacking a legal or factual basis or legal or factual merit; not serious; not reasonably purposeful; of little weight or importance.

Fundraising activity means a fundraising activity for a health-related charitable purpose.

Fundraising agency means a registered charity as defined in the Income Tax Act (Canada) that:

- is incorporated in Saskatchewan for the sole purpose of carrying out fundraising activities for the benefit of a designated trustee; and
- has entered into a fundraising agreement with a designated trustee.

Fundraising agreement means an agreement between a designated trustee and a fundraising agency by which the fundraising agency is authorized to carry out fundraising activities on behalf of the designated trustee.

Government institution means a government institution as defined in The Freedom of Information and Protection of Privacy Act. It includes (See section 2(h) of HIPA):

- the office of Executive Council or any department, secretariat or other similar agency of the executive government of Saskatchewan; or
- any prescribed board, commission, Crown corporation or other body, or any prescribed portion of a board, commission, Crown corporation or other body, whose members or directors are appointed, in whole or in part:
  - by the Lieutenant Governor in Council;
  - by a member of the Executive Council; or
  - in the case of:
    - a board, commission or other body, by a Crown corporation; or
    - a Crown corporation, by another Crown corporation;

It does not include:

- a corporation the share capital of which is owned in whole or in part by a person other than the Government of Saskatchewan or an agency of it;
- the Legislative Assembly Service or offices of members of the Assembly or members of the Executive Council; or the Court of Appeal, Her Majesty’s Court of Queen’s Bench for Saskatchewan or the Provincial Court of Saskatchewan.

Guardian means someone who has the authority to make decisions for an adult. A personal guardian makes decisions about an adult’s personal welfare and a property guardian makes decisions about an adult’s finances and property.

Hazard means a risk, peril or danger.
**Health care organization** means a health care organization as defined in *The Regional Health Services Act* (See section 2(h.1) of HIPA).

**Health professional** means a person who is licensed pursuant to an Act for which the minister is responsible and is authorized by *The Drug Schedules Regulations, 1997* to prescribe or dispense a drug.

**Health professional body** is a body that regulates the members of a health profession or health discipline pursuant to an Act. Examples of these bodies include the College of Physicians and Surgeons of Saskatchewan, Saskatchewan Registered Nurses Association, Chiropractors' Association of Saskatchewan, etc.

**Health Quality Council** is the council described in section 3 of *The Health Quality Council Act*.

**Health region** means a health region as defined in *The Regional Health Services Act* (See section 2(h.2) of HIPA).

**Health related charitable purpose**, for the purpose of section 7.1 of the HIPA Regulations, means a charitable purpose related to a health services facility situated in Saskatchewan or to the provision in Saskatchewan of a health service or program.

**Health service**, as defined by subsection 2.2 of *The Regional Health Services Administration Regulations*, means services as follows:

- alcohol, drug or substance abuse or addiction assessment, education and treatment services;
- chronic disease management services;
- community health services;
- convalescent care and palliative care services;
- counselling services;
- diagnostic imaging services;
- disability management services;
- disease and injury prevention services;
- emergency medical response services;
- emergency stabilization services;
- health assessment and screening services;
- health education services;
- health promotion services;
- home care services;
- hospital services;
- laboratory services;
- long-term care services;
- medical services;
• mental health services;
• nursing services;
• personal care services;
• physician services;
• provision of drugs, medical supplies and surgical supplies;
• public health services;
• registered nurse or nurse practitioner services;
• rehabilitation services;
• specialty and subspecialty medical services and surgical services;
• therapy services;
• any other goods and services ancillary or incidental to health promotion and protection or respecting the care, treatment or transportation of sick, infirm or injured individuals.

**Health services number** means a unique number assigned to an individual who is or was registered as a beneficiary to receive insured services within the meaning of *The Saskatchewan Medical Care Insurance Act* (See section 2(i) of HIPA).

**Hospital**, for the purpose of section 7.1 of the HIPA Regulations, means a facility designated as a hospital pursuant to *The Facility Designation Regulations*, and includes a hospital operated by the Athabasca Health Authority.

**Immediate family** – the IPC recommends that Trustees in Saskatchewan adopt the list for “nearest relative” provided by subsection 15(1) of *The Health Care Directives and Substitute Health Care Decision Makers Act* for the definition of immediate family. The list is as follows:

- the spouse or person with whom the person requiring treatment cohabits and has cohabited as a spouse in a relationship of some permanence;
- an adult son or daughter;
- a parent or legal custodian;
- an adult brother or sister;
- a grandparent;
- an adult grandchild;
- an adult uncle or aunt;
- an adult nephew or niece.

**Information management service provider** means a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf (See section 2(j) of HIPA).
**Information sharing agreement** is an agreement that governs the collection, use disclosure and safeguarding of personal health information by the parties. For the purposes of [section 5.2 of the HIPA Regulations](https://example.com/hipa), the information sharing agreement must meet the requirements set out in subsection 5.2(2) of the HIPA Regulations.

**Integrity** refers to the condition of information being whole or complete; not modified, deleted or corrupted.

**Local Authority**, pursuant to The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP), means:
- a municipality;
- a committee of a council of a municipality;
- any board, commission or other body that is appointed pursuant to The Cities Act, The Municipalities Act or The Northern Municipalities Act, 2010 and is prescribed;
- the board of a public library within the meaning of The Public Libraries Act, 1984;
- the Northern Library Office established pursuant to The Public Libraries Act, 1984;
- any board of education or conseil scolaire within the meaning of The Education Act;
- a regional college within the meaning of The Regional Colleges Act, other than the Saskatchewan Indian Community College;
- the Saskatchewan Polytechnic;
- the University of Saskatchewan, including Saint Thomas More College;
- the University of Regina, including Campion College and Luther College with respect to its post-secondary level activities;
- a regional health authority or an affiliate, as defined in The Regional Health Services Act;
- any board, commission or other body that receives more than 50% of its annual budget from the Government of Saskatchewan or a government institution; and is prescribed.

**Mental health** refers to the functioning of a person's mind in a normal state.

**Minister** means the member of the Executive Council to whom for the time being the administration of HIPA is assigned (See section 2(k) of HIPA).

**Need-to-know principle** is the principle that trustees and their staff should only collect, use or disclose personal health information needed for the diagnosis, treatment or care of an individual or other authorized purposes. Personal health information should only be available to those employees in an organization that have a legitimate need-to-know that information for the purpose of delivering their mandated services. A trustee should limit collection and use of personal health information to what he/she needs-to-know to do his/her job, not collect or use information that is nice to know.

**Next of kin** – it is the Commissioners view that “next of kin” be interpreted the same as immediate family in the context of HIPA. (See immediate family.)
**Notation** is a note made on the individual’s personal health information or in a electronic medical record indicating that the individual has requested an amendment to the personal health information. A notation should include the date, who requested the amendment, what the requested amendment was and a signature of the decision maker.

**Not reasonably practicable** refers to something that is not feasible or possible from a realistic or practical standpoint.

**Office of the Information and Privacy Commissioner** means the individuals employed to assist the Information and Privacy Commissioner. The acronym IPC is used for this term. See also *Information and Privacy Commissioner*.

**Omission** means that something is missing, left out or overlooked.

**Opt out**, for the purpose of section 7.1 of the HIPA Regulations, means to inform a designated trustee or a fundraising agency, in accordance with subsection 7.1(10) of the HIPA Regulations, that a client does not consent to the use or disclosure of his or her client information by the designated trustee or the fundraising agency for the purposes of a fundraising activity.

**Opting-out procedure**, for the purpose of section 7.1 of the HIPA Regulations, means a procedure by which a client may inform a designated trustee or a fundraising agency, as the case may be, that the client wishes to opt out.

**Personal health information** means, with respect to an individual, whether living or deceased (See section 2(m) of HIPA):

- information with respect to the physical or mental health of the individual;
- information with respect to any health service provided to the individual;
- information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
- information that is collected:
  - in the course of providing health services to the individual; or
  - incidentally to the provision of health services to the individual; or
- registration information.

**Personal representative** means an executor under a will or an administrator appointed by the court as Executor Administrator of an estate.

**Person in a personal relationship close** could include a common-law spouse, a close friend or other person who can demonstrate that he or she has such a relationship with the individual who is the subject of the information.

**Physical Health** refers to the well-being of an individual’s physical body.

**Physical safeguards** are physical measures, policies, and procedures to protect personal health information and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.
**Preparation date**, for the purpose of section 7.1 of the HIPA Regulations, means the date on which a client list is prepared.

**Prescribed** means prescribed in the regulations. See regulations (See section 2(n) of HIPA).

**Primary purpose** means the purpose for which personal health information was originally collected, and includes any purpose that is consistent with that purpose (See section 2(o) of HIPA).

**Privacy** is the “general right of the individual to be left alone, to be free from interference, from surveillance and from intrusions.” In the context of health information protection, it is the right of an individual to be able to control access to as well as the collection, use and disclosure of his or her information.

**Privacy breach** happens when there is an unauthorized collection, use or disclosure of personal health information, regardless of whether the personal health information ends up in a third party's possession. See Appendix C for more details.

**Readable** means that the personal health information is able to be read or legible.

**Record**, as defined in subsection 2(p) of HIPA, means a record of information in any form and includes information that is written, photographed, recorded, digitized or stored in any manner, but does not include computer programs or other mechanisms that produce records.

**Regional health authority** means a regional health authority as defined in *The Regional Health Services Act* (See section 2(p.1) of HIPA).

**Registration information** means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations (See section 2(q) of HIPA).

**Regulations** mean *The Health Information Protection Act Regulations*. See section on the HIPA Regulations for more details.

**Request for review** means an application for a review by the Commissioner pursuant to section 42 of HIPA. See also Review and Application for Review.

**Retrievable** means that the trustee must be able to access personal health information with reasonable ease when required to do so.

**Review** is the process by which the Saskatchewan Information and Privacy Commissioner considers a decision of a trustee regarding granting access to an individual’s own personal health information or the failure to respond to a request.

**Right of Access** is the right of an individual to view or obtain copies of records in the custody or control of a trustee granted by section 32 of HIPA.

**Safety** implies relative freedom from danger or risks.
**Secondary purpose** refers to the use or disclosure of personal health information for a purpose other than that for which it was originally collected (e.g. research, use for health system planning, fundraising, etc.).

**Security** means a condition of safety or freedom from fear or danger.

**Severing** is the exercise by which portions of a document are removed before that document is provided to an applicant. The portions that are removed must be subject to subsection 38(1) of HIPA. See subsection 38(2) of this Guide for more detail.

**Successor** would be the person or organization that obtains ownership of or title to a trustee’s facility or practice when the trustee ceases to be a trustee. A successor could be an individual, a partnership, corporation or other unincorporated organization or sole proprietorship.

**Subject individual** means the individual to whom personal health information relates (See HIPA s.2(s)).

**Technical safeguards** are the technology and the policy and procedures for its use that protect personal health information and control access to it.

**Threat** means a sign or cause of possible harm.

**Trivial matter** is something insignificant, unimportant or without merit. See also *frivolous.*

**Trustee** means any of the following that have custody or control of personal health information (See section 2(t) of HIPA):

- a government institution;
- a regional health authority or a health care organization;
- a licensee as defined in *The Personal Care Homes Act*;
- a person who operates a facility as defined in *The Mental Health Services Act*;
- a licensee as defined in *The Health Facilities Licensing Act*;
- a licensee as defined in *The MRI Facilities Licensing Act*;
- an operator as defined in *The Ambulance Act*;
- a licensee as defined in *The Medical Laboratory Licensing Act, 1994*;
- a proprietor as defined in *The Pharmacy and Pharmacy Disciplines Act*;
- a community clinic:
  - as defined in section 263 of *The Co-operatives Act, 1996*; or
  - incorporated or continued pursuant to *The Non-profit Corporations Act, 1995*;
- the Saskatchewan Cancer Foundation;
- a person, other than an employee of a trustee, who is:
  - a health professional licensed or registered pursuant to an Act for which the minister is responsible; or
a member of a class of persons designated as health professionals in the regulations;

- a health professional body that regulates members of a health profession pursuant to an Act;
- a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee;
- any other prescribed person, body or class of persons or bodies;

Currently, subsection 3(a) of the HIPA Regulations prescribes the Saskatchewan Health Quality Council as a trustee.

**Unauthorized access** occurs when individuals have access to personal health information that they do not need-to-know, either by accident or on purpose. This would also qualify as either an unauthorized use or unauthorized disclosure.

**Unauthorized collection** occurs when personal health information is collected, acquired, received or obtained by any means for purposes that are not allowed under sections 23, 24 or 25 of HIPA.

**Unauthorized use** refers to the use of personal health information for a purpose that is not authorized under sections 23 and 26 of HIPA.

**Unauthorized disclosure** refers to the act of revealing, showing, providing copies, selling, giving or relaying the content of personal health information in ways that are not permitted under sections 23, 27, 28, 29 and 30 of HIPA.

**Use** includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee. For example, in a regional health authority and its facilities, the sharing of information between employees constitutes ‘use’ of the personal health information since the sharing happens under the control of the regional health authority (See section 2(u) of HIPA).

**Vexatious** means without reasonable or probable cause or excuse.

**Written request for access** means a request made pursuant to section 34 of HIPA (See section 31(b) of HIPA).
APPENDIX B – DETAILED EXAMPLES OF SAFEGUARDS

The following tables describe examples common of administrative, technical and physical safeguards that a trustee should have in place.

Administrative safeguards

Administrative safeguards are controls that focus on internal organization, policies, procedures and maintenance of security measures that protect personal health information.

A Concise Written Set of Security Rules

Privacy Policy:

COACH recommends the following:

Develop a privacy policy based on the requirements of your applicable privacy legislation as they pertain to collecting, using and disclosing personal and/or personal health information, including consent requirements, individual access to information and correction and security safeguards.

If you do not have a documented policy, it will be difficult for you to communicate your privacy and security practices to patients, the public and external stakeholders or partners. On the other hand, if you do have a policy in place, you are clearly demonstrating that you have done your due diligence with respect to privacy and security. This is crucial if your practice is ever subject to a privacy audit, complaint, and privacy breach or security incident.

Policies must be tailored specifically for the unique circumstances of each organization. The IPC has said that the privacy policy of every Trustee should address:

- Accountability for personal health information;
- Purpose for collecting personal health information;
- Consent for collecting, using and disclosing personal health information;
- Accuracy and correction of personal health information;
- Retention and destruction of personal health information (written records retention and disposition schedule);
- Privacy breach management;
- Use and disclosure audits;
- Use and disclosure control;
- Individual access to information;
- Privacy complaint management; and
- Enforcement mechanisms
### Privacy Procedures:

Establish [privacy](#) procedures to serve as an extension of your privacy policy. This assists in informing colleagues and staff about their role in protecting and working with [personal health information](#). Procedures should provide you and your staff with consistent steps for managing:

- complaints, breaches of privacy and [security](#) incidents
- individual access to and correction of personal health information
- [consent](#)
- right to be informed
- right to information about disclosures without consent
- administrative, technical and physical safeguards

[Collection](#), [use](#) and [disclosure](#) of personal health information on a need-to-know basis

### Appointment of a Staff Member with Overall Responsibility for the Protection of Personal Health Information

The College of Physicians and Surgeons of Saskatchewan (CPSS) recommends a [privacy](#) officer in its [CPSS Checklist for Compliance with HIPA](#) as follows:

- The office must designate an individual (ideally a physician) to act as Privacy Officer to oversee management of [personal health information](#).
- The Privacy Officer should be familiar with the obligations under HIPA.
- This individual should develop and implement the privacy policies for the clinic and provide clinic staff with advice regarding HIPA compliance.
- All employees should know who this person is.
- The privacy officer would also handle privacy inquiries and complaints.

### Staff Training

[Trustees](#) must educate their employees about HIPA, the trustee’s duties under HIPA, safeguards the trustee has established, the need-to-know and consequences for violating HIPA.

**Staff should get refresher training each year.**

### Security Clearances

Security clearances may include asking employees for background checks.

### Access Restrictions

Employee access to [personal health information](#) must be restricted. This includes personal health information in electronic or other form. Employees should be instructed who are authorized to use, modify, transform, disclose or dispose of personal health information to perform their assigned duties. Authorization for each information user should be based on the ‘need-to-know’ of that individual pursuant to section 23 of HIPA.

Procedures should be in place to revoke or restrict access when employees leave or are away for extended periods (e.g. parental leave).
Regular Audits

Trustees should schedule regular audits of actual practices for compliance with security policies.

Confidentiality Agreements/Information Sharing Agreements

COACH advises the following:

Enter into agreements before sharing any personal health information with a third party. Agreements protects you and your practice by establishing the terms and conditions of providing personal health information that you may receive from or share with others, including centralized databases and other healthcare providers. Agreements can also establish accountability between you and electronic service providers, including network providers.

See Appendix H – on Information Sharing Agreements located in this Guide.

Communications with Patients

COACH states:

Identify the consent requirements that apply in your jurisdiction. (Your professional college can help you with this matter.) While implied consent allows the collection, use and disclosure of personal health information in healthcare delivery within the circle of care, best practice suggests, and in some cases, legislation requires, that you make your patients aware of your privacy practices. Therefore, you should provide patients with the following information:

- The purposes for which you collect their personal health information
- How the information will be used
- With whom the information will be shared
- When the consent of patients will be sought
- How patients can request access to and correction of their personal health information
- How you manage privacy breaches and security incidents

The best method for information your patients is by posting a patient privacy notice or providing a handout.

See section 9(3) of HIPA

Records Retention and Disposition Schedule

Section 17 of HIPA places duties on trustees to store (or retain) and destroy personal health information in secure ways.

Subsection 17(1) is not yet proclaimed by the legislature. However, the intent of this clause is to provide trustees with guidance on how long personal health information is to be kept.

Even though subsection 17(1) is not proclaimed, trustees should still have a written records retention and disposition schedule. This outlines all the types of personal health information that a trustee possesses and how long it will be retained. Trustees should consult with their respective regulatory body for guidance when setting these timelines.

Further the trustee should have had destruction policies and procedures that explicitly describe all
steps that the trustee and staff must take to prepare records for destruction. A trustee should keep records of what has been destroyed, such as destruction certificates.

When an IMSP is used for the destruction of personal health information proper agreements should be in place.

See section 18 of HIPA.

The Hospital Standards Regulations 1980 is a source of guidance regarding retention periods for personal health information and it reads as follows:

Health record to be retained

15(1) Subject to subsection (2), the patient’s health record shall be retained by the hospital for a minimum period of ten years from the date of last discharge or until age nineteen if the patient is a minor, whichever period is the longer or for such further period as may be deemed necessary by the hospital after consultation with the medical staff.

(2) Where microfilming is employed, the health record must be retained in its original form for a minimum period of six complete years, and the microfilm must be retained for the remainder of the retention period mentioned in subsection (1).

The Saskatchewan Medical Association’s website recommends the following:

- The College of Physician and Surgeons requires that records be held for six years after the patient was last seen. Records of pediatric patients shall be retained until two years past the age of majority or six years after the date last seen, whichever may be the later date.
- The Canadian Medical Protective Association recommends that members keep medical records for at least 10 years from the date of last entry or, in the case of minors, 10 years from when the age of majority is reached or 10 years from the last entry, whichever is greater.

The trustee needs to ensure that they have a policy and procedure in place that establishes the retention period and the process for destruction and storage of the medical records.

**Technical Safeguards**

*Technical Safeguards* are the technology and the policy and procedures for its use that protect personal health information and control access to it.

See Appendix E – for more information on Faxing Personal Health Information.

**Technical Safeguards for Electronic Personal Health Information**

- User IDs and passwords on digital systems
- Encryption for storage and transmission
- Firewalls, virus scanners
- Identification and authentication controls

**Other Technical Safeguards**

Technical safeguards also include measures taken to ensure personal health information is protected while it is being communicated. Examples include eavesdropping, and interception while e-mailing or
faxing personal health information.

- **Eavesdropping** occurs when unauthorized individuals inadvertently or through the use of deceptive techniques gain access to personal health information. Examples include patients in a waiting room overhearing the receptionist discussing personal health information over the telephone.

- **Interception** occurs when unauthorized individuals inadvertently or through the use of deceptive techniques gain access to personal health information. An example would be a fax containing personal health information being sent by mistake to a wrong number.

### Physical Safeguards

*Physical Safeguards* are physical measures, policies, and procedures to protect personal health information and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.

See the Appendix E – for Faxing Personal Health Information

<table>
<thead>
<tr>
<th>Examples of Physical Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Locked filing cabinets</td>
</tr>
<tr>
<td>• Restricted office access</td>
</tr>
<tr>
<td>• Alarm systems</td>
</tr>
<tr>
<td>• Securing electronic hardware</td>
</tr>
<tr>
<td>• Clean desk approach</td>
</tr>
</tbody>
</table>
APPENDIX C – PRIVACY BREACH GUIDELINES

What is a Privacy Breach?

When does a Privacy Breach Occur?

A privacy breach is often thought of as inappropriate sharing of personal health information. However, a privacy breach can occur in a number of different ways:

**Collection:** A privacy breach could occur if a trustee asks for or collects more personal health information needed for the purpose for which it is being collected (e.g. a health services number is required for a non-health related service, personal health information is not collected directly from the individual, etc.). The rules for collection are found in section 23, 24 and 25 of HIPA.

**Use:** A privacy breach could occur when personal health information already in the possession or control of the trustee is used for reasons that are not consistent with the purpose for which they were collected (e.g. personal health information is collected to provide one service and then used to promote a different service). The rules for use are found in sections 23, 26, 29 and 30 of HIPA.

**Disclosure:** A privacy breach could occur when an unauthorized disclosure of personal health information transpires (e.g. when personal health information is missing, when an employee accesses personal health information without a need-to-know, when a trustee shares personal health information with another organization, etc.). Note: if personal health information in the possession or control of a trustee is missing, even if there is no evidence that someone has viewed the personal health information, it qualifies as a disclosure. The rules for disclosure are found in section 23, 27, 28, 29 and 30 of HIPA.

**Accuracy:** Trustees have a duty to ensure personal health information is as accurate and complete as possible. A privacy breach may occur when personal health information is inaccurate. See section 19 of HIPA.

**Other sub-issues:** Other issues that might arise during a privacy breach investigation could include need-to-know, data minimization and consent. However, they would likely be tied to one of the other major issues.

What is Privacy?

“Privacy” can have many different meanings. However, in HIPA the focus is on personal health information privacy; the right of an individual to determine for him/herself when, how and to what extent his/her personal health information will be shared. The definition of personal health information is found in section 2(m) of HIPA.
There’s been a Privacy Breach – Now What?

If you have discovered a privacy breach, contact your organization’s Privacy Officer immediately. Write down all of the information related to the discovery of the breach.

If you have been tasked with dealing with the breach, consider the following guidelines.

Contain the Breach

It is important to contain the breach immediately. In other words, ensure that personal health information is no longer at risk. This may involve:

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that was breached.
- Revoking access to personal health information.
- Correcting weaknesses in physical security.

Notification

The following is a list of individuals or organizations that may need to be notified in the event of a privacy breach:

- Contact your organization’s privacy officer immediately.
- Proactively report the breach to the IPC. For more information see the specific section on proactively reporting breaches later in this document.
- If criminal activity is suspected (e.g. burglary), contact police.
- Contact the affected individual unless there are compelling reasons why this should not occur.

How to Notify Affected Individuals

Notification of individuals affected by the breach should occur as soon as possible after key facts about the breach have been established.

It is best to contact affected individuals directly, such as by telephone, letter or in person. However, there may be circumstances where it is not possible and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include a notice on a website, posted notices, media advisories, and advertisements. Ensure the breach is not compounded when using indirect notification.

Notifications should include the following:

- A description of the breach (a general description of what happened).
- A detailed description of the personal health information involved (e.g. name, medical records, etc.).
- Steps taken and planned to mitigate the harm and to prevent future breaches.
• If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g. how to change a health services number).
• Contact information of an individual within your organization who can answer questions and provide further information.
• A notice that individuals have a right to complain to the IPC. Provide contact information.
• Recognition of the impacts of the breach on affected individuals and an apology.

Investigate the Breach
Once a breach has been contained the next step is to investigate the breach. Here are some key questions to ask during a privacy breach investigation:

When and how did your organization learn of the privacy breach?
• Has the privacy breach been contained?
• What efforts has your organization made to contain the breach?

What occurred?
• What type of breach occurred (e.g. collection, use, disclosure, accuracy, etc.)?
• What personal health information was involved in the privacy breach?
• When did the privacy breach occur? What are the timelines?
• Where did the privacy breach occur?

How did the privacy breach occur?
• Who was involved?
• What employees, if any, were involved with the privacy breach? What privacy training have they received?
• Who witnessed the privacy breach?
• What factors or circumstances contributed to the privacy breach?
• What is the root cause of the breach?

What is the applicable legislation and what specific sections are engaged?

What safeguards, policies and procedures were in place at the time of the privacy breach?
• Were these safeguards, policies and procedures followed?
• If no safeguards, policies or procedures were in place, why not?
• Were the individuals involved aware of the safeguards, policies and procedures?

Who are the affected individuals?
• How many are there?
• What are the risks associated to a privacy breach involving this information?
• Have affected individuals been notified of the privacy breach?

Prevent Future Breaches
The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring.

What steps can be taken to prevent a similar privacy breach?
• Can your organization create or make changes to policies and procedures relevant to this privacy breach?
• Are additional safeguards needed?
• Is additional training needed?
• Should a practice be stopped?

Privacy Breach Report
Once the necessary information has been collected, it is a good idea to prepare a privacy breach investigation report. The report should include the following:

• A summary of the incident and immediate steps taken to contain the breach.
• Background of the incident. Timelines and a chronology of events.
• Description of the personal health information involved and affected individuals.
• A description of the investigative process.
• The root and contributing causes of the incident.
• A review of applicable legislation, safeguards, policies and procedures.
• A summary of possible solutions and recommendations for preventing future breaches. This should include specific timelines and responsibility for implementation of each action.

When Employee Snooping is Suspected
Sometimes the privacy breach involves an employee or contractor who purposely accessed personal health information of individuals without a need-to-know. The following are steps or items to consider when investigating this type of breach:

• Record details of how the breach came to light. Gather relevant materials.
• Suspend employee’s access to the personal health information.
• Retrieve log information if available.
• Interview the employee in question. Establish if the employee may have shared their user account and identification and routinely logs out of account.
• Identify and interview any witnesses.
• Review the privacy training the employee in question has received. Have warnings of routine audits been given?
• Review any relevant contracts.
• Consider who needs to be notified (e.g. supervisor, union, police, e-Health Saskatchewan, etc.)
• Decide if the identity of the employee in question will be disclosed to the affected individual when providing notification.
• Proactively report to the IPC for further advice.

The IPC recommends that a trustee share any discipline measures taken against an employee who has snooped (without revealing the identity of the individual) to the rest of the
employees in the organization and the affected individuals. Please also include any details of employee discipline in your Investigation Report to the IPC.

**What Can I Expect if the IPC is involved?**

The [IPC](#) can learn of a privacy breach and begin an investigation in several different ways. Some of them include:

- The trustee can proactively report a breach to the IPC.
- A citizen could come to the IPC with a complaint about a trustee’s actions or practices.
- A third party in possession of personal health information could notify the IPC.
- Employees of a trustee could inform the IPC of inappropriate practices within the organization.
- The IPC could act on media reports.

**What are the advantages of proactively reporting a breach to the IPC?**

While not mandatory, the [IPC](#) does encourage organizations to proactively report. Some of the benefits include:

- Timely, expert advice.
- The IPC will monitor the situation and if satisfied with your organization’s internal investigation report may close the file rather than conducting a formal investigation.
- Should affected individuals contact the IPC, it can assure the individuals that it is working with your organization to address the breach which may prevent a formal investigation by the IPC.
- Should the media get wind of the privacy breach, your organization can assure the public that they are working with the IPC to address the matter.

**Summary of Investigation Process**

Our goal is to complete review and investigation files on average within 35 days, 80% of the time.

1. A privacy complaint or proactively reported breach is received at the [Office of the Information and Privacy Commissioner](#) (IPC). It will be assigned to an Early Resolution Officer (ERO).

2. ERO will ensure all necessary information has been received from the complainant and will attempt informal resolution between the parties.

3. If early resolution is not possible, the ERO will send out a notification e-mail to all parties. It will request that all submissions and materials be provided in 14 days. File will be assigned to an Analyst.
4. Analyst will ensure materials arrive in 14 days.
   a) If materials are not received in 14 days, or an agreed upon deadline, the escalation guidelines are as follows:
      i) Analyst will follow up and attempt to receive materials
      ii) Analyst will escalate to Director of Compliance (DOC) – DOC will attempt to get materials within a week before moving it on;
      iii) DOC will escalate to Commissioner – Commissioner will contact the ‘head’

5. Analyst will review materials received – do some initial analysis to determine direction of investigation.

6. Analyst will meet with Commissioner and DOC to discuss direction of investigation. Analyst will prepare the draft report.

7. Analyst will send PDF of Draft Report to the Privacy Officer of the trustee (password protected) and request response in one week. The trustee can contact Analyst within the one week timeframe to discuss the findings and recommendations. This has the potential to change a finding or recommendation.

8. Analyst will put draft Report into final format and send to Commissioner for final approval.

9. Analyst will e-mail Final to complainant and trustee.
   a) One e-mail will go to the complainant.
   b) Another e-mail should go to the trustee:
      i) E-mail will be sent to the Head;
      ii) E-mails will be copied to the Privacy Officer, the Deputy Minister of Justice and Executive Director of the Access and Privacy Branch;
      iii) The Deputy Minister of Health should be copied on HIPA related Reports.
   c) Another e-mail should go to relevant third parties if applicable.
   d) Report is now issued.

10. All reports will be posted to the website after 7 days of issuance.

11. If no response is received from the trustee within 30 days of issuing the final report, Analyst will provide the trustee with one reminder of its duty to respond. No response is tracked as no compliance.

**Informal Resolution**

Where possible, the IPC will aim to achieve informal resolution for investigation files. Informal resolution is beneficial to all parties involved as it can expedite resolution for the Complainant and reduce the amount of work for both the trustee and IPC.

When a privacy complaint is first received by the IPC, it will receive a file number and be assigned to an ERO. The ERO will first verify that the IPC had received all the necessary
information and documents from the Complainant. The ERO will then contact both the Complainant and the trustee in order to facilitate a possible informal resolution.

Some of the ways an ERO might facilitate an informal resolution are as follows:

- Dispel any misunderstandings.
- Clarify the applicant’s objectives with the trustee.
- Facilitate negotiations between the Complainant and trustee.
- Clarify the role of the IPC.
- Identify the possible outcomes of an investigation.

If an ERO is not able to reach an informal resolution within a week, notification letters will be sent and the file will be assigned to an Analyst. However, the IPC will be open to reaching informal resolution at any stage of the investigation process.

If the IPC is satisfied with a trustee’s internal investigation report, we may close the file rather than conducting a formal investigation.

When informal resolution is achieved, the Commissioner will not issue a Report.

What will be the IPC’s focus?
The IPC will look at all of the elements of the breach. However, focus will be on the following areas:

- Compliance with the applicable legislation.
- Safeguards, policies and procedures in place at the time of the breach. Were they followed? Were they effective?
- Training of the employees involved.
- Potential employee snooping (if applicable).

The key questions for a privacy breach investigation found in this document capture most issues the IPC routinely considers during our investigation. However, every investigation is unique. It is not unusual for an Analyst to ask further questions of a trustee during the process.

It is important to also provide the IPC with relevant documentation such as policies and procedures, training materials, copies of the personal health information in question, etc.

Draft Report
Once finished, the Analyst will present a draft report to the trustee which includes analysis of the file, findings and recommendations.

The trustee can respond to the draft report indicating if it agrees with the findings and whether it will follow the recommendations. Please provide any final information at this time.
Again, in order to meet our goal of resolving investigation files in 35 days, 80% of the time, we ask for a response from trustees within one week. If you cannot do it in one week, please call the Analyst to discuss. If there is no response, the Analyst will move the investigation forward to a final report.

Please note that the Commissioner may paraphrase or quote from a trustee or complainant’s submission, letter or e-mails in the draft or final report.

**Commissioner’s Report**
Once an Analyst has received the response to the draft report from the trustee, he/she will make final changes to the report and pass it to the Commissioner for his final approval.

The Commissioner will issue a report for every investigation file that is not resolved informally. A copy of the report will also be sent to the Ministry of Justice and Ministry of Health.

All reports will be posted on the IPC website after three days from issuance.

We ask that the trustee provide a response to the report and recommendations within 30 days to the relevant parties.

**The IPC is Paperless**
The IPC has gone paperless. As such we prefer to receive correspondence, internal investigation reports and other documentation electronically. Any documentation could be sent by e-mail or by mail on a CD or USB key.

Please password protect any sensitive PDF or Word documents, especially if they contain personal health information. Please do not hesitate to contact us if you require support. Finally, please do not transmit the password in the same e-mail as the documents. Please send it in a separate e-mail or call the IPC.
APPENDIX D – WHAT TO EXPECT DURING A REVIEW WITH THE IPC

The Information and Privacy Commissioner’s office (IPC) has set the goal of resolving all files review files within 35 days, 80% of the time. We also aim to build the best process in Canada.

Summary of Review Process
1. An application for review is received at the Office of the Information and Privacy Commissioner (IPC). It will be assigned to an Early Resolution Officer (ERO).

2. ERO will ensure all necessary information has been received from the applicant and will attempt informal resolution between the parties.

3. If early resolution is not possible, the ERO will send out a notification e-mail to all parties. It will request that all submissions and materials be provided in 14 days. File will be assigned to an Analyst.

4. Analyst will ensure materials arrive in 14 days.
   a) If there is permission to share submissions and index – analyst will share. If there is nothing said about sharing, Analyst will make one phone call or send one email to trustee to inquire. No response means not willing to share – carry on with next steps.
   b) If materials are not received in 14 days, or an agreed upon deadline, the escalation guidelines are as follows:
      i) Analyst will follow up and attempt to receive materials
      ii) Analyst will escalate to Director of Compliance (DOC) – DOC will attempt to get materials within a week before moving it on;
      iii) DOC will escalate to Commissioner – Commissioner will contact the trustee

5. Analyst will review materials received – do some initial analysis to determine direction of review.

6. Analyst will meet with Commissioner and DOC to discuss direction of review. Analyst will prepare the draft report.

7. Analyst will send PDF of Draft Report to the trustee and request response in one week. The trustee can contact Analyst within the one week timeframe to discuss the findings and recommendations. This has the potential to change a finding or recommendation.

8. Analyst will put draft Report into final format and send to Commissioner for final approval.

9. Analyst will e-mail Final to applicant and trustee.
   a) One e-mail will go to the applicant.
   b) Another e-mail should go to the trustee:
i) E-mails will be copied to the Privacy Officer, the Deputy Minister of Justice, Deputy Minister of Health and Executive Director of the Access and Privacy Branch;

c) Another e-mail should go to relevant third parties if applicable.

d) Report is now issued.

e) IPC will delete copies of “the record” in its possession.

10. All reports will be posted to the website after 3 days of issuance.

11. If no response is received from the trustee within 30 days of issuing the final report, Analyst will provide the trustee with one reminder of its duty to respond. No response is tracked as no compliance.

Informal Resolution

Where possible, the IPC will aim to achieve informal resolution for review files. Informal resolution is beneficial to all parties involved as it can expedite resolution for the applicant and reduce the amount of work for both the trustee and IPC.

When an application for review is first received by the IPC, it will receive a file number and be assigned to an ERO. The ERO will first verify that the IPC had received all the necessary information from the applicant and documents. The ERO will then contact both the applicant and the trustee in order to facilitate a possible informal resolution. Some of the ways an ERO might facilitate an informal resolution are as follows:

- Ensure all possible records have been provided to the applicant.
- Clarify what kind of records the applicant is seeking.
- Clarify the applicant’s objectives with the trustee.
- Facilitate negotiations between the applicant and trustee.
- Clarify the role of the IPC.
- Identify the possible outcomes of a review.
- Narrow the scope of a review if informal resolution is not successful.

If an ERO is not able to reach an informal resolution within a week, notification letters will be sent and the file will be assigned to an Analyst. However, the IPC will be open to reaching informal resolution at any stage of the review process.

Preliminary Objections

In the event that the trustee has reason to believe that either the Commissioner does not have jurisdiction to deal with an application for review or that the application for review is frivolous, vexatious, not made in good faith or concerns a trivial matter, the trustee should raise a preliminary objection to the review and notify the Commissioner accordingly. The trustee should provide particulars and any relevant information in support of the preliminary objection. Normally, the Commissioner will make a decision pursuant to section 43 of HIPA with respect to that preliminary objection before proceeding further with the review. He will advise both the applicant and the trustee of his decision.
If at any time during a review the trustee decides to release new responsive records to the applicant, please do so as soon as possible and let the ERO or Analyst know.

When informal resolution is achieved, the Commissioner will not issue a Report.

Note: In most cases, informal resolution is achieved at the discretion of the applicant.

**Notification of the Review**
When the IPC issues a formal notification letter to the trustee, it will advise that a review is underway, ask for preliminary objections and advise that the IPC requires a copy of the record at issue and a submission. The submission is the trustee's arguments supporting its decision to withhold records.

Once the contact information is received, the IPC will notify the third party if applicable. Providing notice to third parties allows them the opportunity to make representations on whether or not access should be allowed to records that contain its information.

**Preparing the Record/Index of Records**
The IPC requires a copy of any responsive records to conduct the review.

The trustee must provide the Commissioner's office with a copy of the entire package of withheld records responsive to the applicant's access request. The records that have been provided to the IPC will NOT be released to the applicant.

There is no need to send the IPC records that have already been released to the applicant. If any information has been withheld from the applicant, the trustee must provide a copy of the record to the IPC with:

- the withheld information outlined or highlighted, and
- the relevant section number(s) of the applicable Act clearly indicated beside or near the withheld information.

All the pages should be numbered in sequence. However, this may not always be practical. In facilitating the review, it is very helpful if the trustee prepares an “index of record(s)” in table form. That index usually includes the following:

1. The page number(s) on which information has been withheld or disclosed. The index should account for every single page of the record.
2. A title or description of the record.
3. For each page upon which information has been withheld, identification of the section numbers of the applicable Act under which any information has been withheld is required.
A sample index appears below:

<table>
<thead>
<tr>
<th>Page Number(s)</th>
<th>Title / Description</th>
<th>Section(s)</th>
<th>Withheld in full or part?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lab results from 01/04/2016</td>
<td>38(1)(f)</td>
<td>Full</td>
</tr>
<tr>
<td>2-4</td>
<td>Letter of referral to psychologist</td>
<td>38(1)(a)</td>
<td>Part</td>
</tr>
<tr>
<td>5-10</td>
<td>Notes from marital counselling session</td>
<td>Pages 5-9 disclosed to applicant</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Page 10 – 38(1)(b)</td>
<td>Part</td>
</tr>
</tbody>
</table>

Finally, once the review has concluded, the IPC will shred physical copies of the record or delete electronic copies as soon as the report is issued.

**Preparation the Submission**

The purpose of the submission is to inform the Commissioner about the main arguments of the case and to present supporting information.

See section 38 of this Guide which provides some tests that have been used in the past. These tests can be used by trustees as a guide in preparing submissions. Trustees will also need to provide any supporting information to meet the relevant tests.

The Commissioner will use this information and material to base his decision. The amount or type of material required in order convince the Commissioner will vary dependent on the particular facts, issues and circumstances. If a trustee fails to convince the Commissioner, he will recommend the release of the record at issue.

A submission can contain the following:

- Table of Contents;
- Relevant tests and arguments in support of your position;
- Supporting documents, authorities and other relevant information; and
- Appendices (e.g. Affidavits) if necessary.

Do not hesitate to contact an Analyst if you require assistance in identifying the relevant tests and types of supporting documentation required to complete a submission.

A typical submission is about 10 pages (excluding the record). We ask that both trustees and applicants limit submissions to 40 pages or less, if possible. We discourage extensive discussion of philosophy or principles in the submission. It is best if trustees focus their submissions on the relevant sections, and criteria and tests contained in the exemptions guide.
Timelines and Escalation Policy
In order to achieve the goal of resolving review files in 35 days, 80% of the time, the IPC requires the index of records, record and submission from the trustee within two weeks of the date of the notification letters.

On a case by case basis, please notify us as soon as possible if this timeline is not achievable. Small extensions are negotiable.

If the index of records, record and submission are not forthcoming, the IPC has an escalation policy in place as follows:

1. First, the Analyst will attempt to receive materials within 2 weeks or a negotiated timeframe.
2. The Analyst will escalate to the DOC – DOC will attempt to get materials within a week before escalating it to the Commissioner;
3. If escalated to the Commissioner – the Commissioner will contact the ‘head’.

Sharing of Submissions
The review may be better facilitated by sharing the index of records and submission with the Applicant which can assist with informal resolution. Please note that the index of records and submission is separate and distinct from the record. Only the index of records and submission will be shared with the trustee’s permission. The record will not.

Some benefits of sharing the index of records are as follows:

- The applicant may only be interested in getting access to a portion of the responsive record and narrow the scope of the review.
- The applicant may gain a better understanding of the trustee’s arguments which may lead to a narrowing of the scope or end the review.

Some benefits of sharing the submission are as follows:

- The applicant may gain a better understanding of the trustee’s arguments which may lead to a narrowing of the scope or end the review.
- The applicant may feel there is increased procedural fairness.

Please indicate clearly if we may share the index of records and/or submission as follows:

“Submission can be shared”

OR

“Submission cannot be shared”

Please note that the exchange of submissions will not impede the IPC timeline. The Analyst will proceed with the analysis while waiting for a response from the applicant if the index of records and/or submission has been shared. The analysis may be changed at a later stage in the process once a response is received.
Draft Report
Once finished, the Analyst will present a draft report to the trustee which includes analysis of the file, findings and recommendations.

The trustee can respond to the draft report indicating if it agrees with the findings and whether it will follow the recommendations. Please provide any final arguments at this time.

Again, in order to meet our goal of resolving reviews in 35 days, 80% of the time, we ask for a response from trustees within one week. If you cannot do it in two weeks, please call the Analyst to discuss. If there is no response, the Analyst will move the review forward to a final report.

Please note that the Commissioner may paraphrase or quote from a trustee or Applicant’s submission, letter or e-mails in the draft or final report.

Commissioner’s Report
Once an Analyst has received the response to the draft report from the trustee, he/she will make final changes to the report and pass it to the Commissioner for his final approval.

The Commissioner will issue a report for every review file that is not resolved informally. All parties involved in the Review will receive a copy of this report (e.g. trustee, applicant, third parties, etc.). A copy of the report will also be sent to the Ministry of Justice and/or Ministry of Health.

All reports will be posted on the IPC website after three days from issuance.

As set out in the legislation, the trustee then has 30 days to provide a response to the relevant parties.

The IPC is Paperless
The IPC has gone paperless. As such we prefer to receive correspondence, submissions, copies of the record and other documentation electronically. Any documentation could be sent by e-mail or by mail on a CD or USB key.

Please password protect any sensitive PDF or Word documents, especially if they contain personal information or personal health information. Please do not hesitate to contact us if you require support.

Finally, please do not transmit the password in the same e-mail as the documents. Please send it in a separate e-mail or call the IPC.

Making Your Case
As noted above, the trustee’s submission is its opportunity to convince the Commissioner that certain exemptions apply to the records at issue. In legal terms, this is sometimes called meeting the “burden of proof”.
A trustee has the burden of proof pursuant to section 47 of HIPA if it claims that access to records should or must be refused. In other words, the trustee must convince the Commissioner that exemptions apply. The burden is not on the applicant to establish that an exemption does not apply.

For example, if a trustee applies section 47 of HIPA to refuse access to certain records, it falls to the trustee to bring forward arguments that disclosure could reasonably be expected to endanger the mental or physical health or the safety of the applicant or another person. If the trustee is able to convince the Commissioner of this, the trustee will have met the burden of proof.

To assist trustees to meet the burden of proof, see section 38 of this Guide which identifies definitions, tests, criteria and factors to consider when arguing the application of each exemption.

Other information that would be useful in meeting the burden of proof:

- Arguments in support of the relevant tests for an exemption.
- Excerpts from relevant legislation or regulations that apply to the operations of the trustee and that relate to the issues under review.
- Excerpts from policy manuals that set out practices or policies followed by the trustee that relate to the issues under review.
- Relevant court decisions or past Reports of the IPC. The IPC publishes on its website some reports and recommendations issued when it concludes a review of a decision of a trustee that is not informally resolved.
- Decisions made by Information and Privacy Commissioners in other jurisdictions that may be of assistance to the Commissioner in his consideration of the issues.

In some instances, an affidavit can strengthen a trustee’s arguments. This is especially helpful when establishing records were obtained in confidence and showing that a proper search has been performed. For more information on affidavits please see the IPC resource Using Affidavits in a Review with the IPC.
APPENDIX E – FAXING PERSONAL HEALTH INFORMATION

Why are Safeguards for Faxing Necessary?
Faxing personal health information increases the risk of an unauthorized collection, use or disclosure of this information. Some reasons for these risks include:

- Human error: we can easily make an error when entering a 10 digit fax number into the fax machine, or using auto-suggest functions, sending personal health information to the wrong number resulting in it being received by an unintended recipient without a legitimate need-to-know.

- Lack of control: even when a fax is sent to the correct number, without proper safeguards on the receiving end, personal health information could be viewed by an unintended recipient (ex. the faxed information is left unattended or the fax machine is located in an area where multiple people have access to it).

- Out-of-date contact information: many trustees rely on pre-programmed fax machines or fax numbers from electronic health records or directories that may be out of date causing a fax to be directed to someone without a need-to-know.

What is a Misdirected Fax?
A “misdirected fax” is a fax containing personal health information that is received by an individual without a need-to-know. This would result in an unauthorized disclosure of personal health information. Even if a misdirected fax is received by another trustee, without a need-to-know it qualifies as a privacy breach.

Safeguards for Faxing Personal Health Information
The following are suggestions for safeguards that trustees incorporate into their written policies and procedures.

Policies and Procedures

- Adopt a written policy on faxing personal health information and ensure that employees, including all new employees, are trained and regularly reminded of the policy.

- Policies and procedures should include specific references to applicable privacy legislation and the types of information that can be faxed by or to your organization.

- Post reminders about key points near fax machines.

- If possible, designate one employee to be responsible for sending and receiving personal health information by fax. Train that employee in proper procedures and ensure they are aware of the legal duty to protect the information.

Ensure all employees receive training and regular reminders about faxing safeguards, policies and procedures.
Sending Faxes

- Determine if there is an immediate time requirement that necessitates faxing the personal health information. Is there a quick and more secure way to forward the information to the recipient?

- If the subject individual requests that their personal health information be faxed, first explain the risk of accidental disclosure or the possibility that the information may be deliberately intercepted by people other than the intended recipient and seek their consent before faxing.

- Remove all personal identifiers and confidential information before faxing the information, wherever possible.

- Before faxing personal health information, confirm that you have the correct fax number for the intended recipient and confirm with the recipient (or another employee in the office) the right number before sending.

- When faxing personal health information, confirm that the recipient has taken appropriate precautions to prevent those without the requisite need-to-know from viewing the faxed document.

- Always use a fax cover sheet clearly identifying the sender, the contact information for the sender, the intended recipient, the recipient’s fax number and the total number of pages sent. Include a confidentiality clause that specifies that the faxed material is confidential, is intended only for the stated recipient, and is not to be used or disclosed by any other individual. The confidentiality clause should ask the individual in receipt of a fax received in error to immediately notify the sender and then return or securely destroy the personal health information (as requested by the sender).

- After the fax number has been entered carefully check the number before hitting “send”.

- Check the fax confirmation report to be certain that the fax went to the right place – check the number on the report against the confirmed recipient’s number. Also check the number of pages actually transmitted and received. If you have designated one employee for faxing, that individual should check each day’s fax history reports for errors or unauthorized faxes.

- When faxing personal health information, stay by the machine to ensure that all materials were transmitted correctly.
Receiving faxes

- Retrieve all materials that have been faxed from the fax machine immediately and deliver to the individual with a ‘need-to-know’. Do not leave faxes sitting on or near the fax machine.

- Security precautions should be taken for faxes received after normal business hours such as ensuring that no one without a need-to-know will have access to the fax machine if it is unattended.

Fax Equipment

- Ensure that your fax machine prints a fax header at the top of the page which includes the fax number and date and time.

- If you have a need to continually fax personal health information, look into acquiring a fax machine that has enhanced security features such as encryption or other heightened security measures.

- Fax machines should be physically located in an area of the office that prevents unauthorized individuals from viewing/retrieving faxed personal health information. Make sure to control access to the machine.

- Be aware that your fax number likely will be reassigned to another individual or company once you have given up the number. If you require the number not to be used while you advise clients that the organization is moving or closing, check with your telephone service provider about options to rent the number for a period of time to ensure all clients have been contacted and have had the opportunity to update their contact information.

- Be aware that fax machines now have hard drive and/or memories that store and retain information. When disposing of or selling a fax machine, ensure that the hard drive has been properly scrubbed to remove all information that was stored on the hard drive or memory. Alternatively, ensure the machine is destroyed properly so no personal health information can be retrieved from it.

- Only pre-program commonly used fax numbers and be sure to check those numbers regularly to ensure accuracy.

- If you have pre-programmed a fax header into your fax machine that automatically prints the fax number on the recipient copy, update that information if your fax number or office contact information changes.

- Safeguarding faxes not only applies to fax equipment. If you re-locate or if your contact information is changed, ensure that you update your fax number with all of your contacts and directories that included the previous number. Don’t forget to destroy pre-printed forms, fax cover sheets and correspondence that refer to your previous number. This would include such items as letterhead, business cards, prescription forms, etc. – all of which need to be replaced with updated information.
Checklists: What to do When You’ve Sent or Received a Misdirected Fax

What to do if you receive a misdirected fax

✔ Recognize that this is a significant matter with the need for some urgency to address both privacy implications and possibly continuity of care for the subject individual.

✔ Determine if you have a need-to-know.

✔ Notify your privacy officer.

✔ Use the fax cover sheet or fax header to determine who the sender is.

✔ Contact the sender to advise of the breach so they become aware of the breach.

✔ When possible, speak to the organization’s privacy officer so that the incident can be logged and investigated and safeguards implemented if necessary to prevent similar occurrences.

✔ Discuss with the sender how to contain the breach and what do with the misdirected fax (ex. return by mail, secure destruction, etc.) When possible, give the sender confirmation once the agreed upon action has been performed.
  - Do not keep a copy of the misdirected fax.
  - Do not attempt to forward the misdirected fax to the intended recipient as this could compound the breach. Leave that to the sender.

✔ Consider notifying the IPC who has a legislated mandate to investigate privacy breaches and ensure they are properly managed. Factors to consider include:
  - Is the sender identifiable?
  - Is the personal health information particularly sensitive?
  - Are there multiple faxes with apparent multiple senders?
  - Is the problem recurring after proper steps have been taken to contain past occurrences?

✔ The IPC will ask if you have first made attempts to contact the sender and then ask that you mail in the misdirected fax with any relevant details to our office.
What to do if you have sent a misdirected fax

✔ Contact your organization’s privacy officer for guidance and support. Also consult the IPC resource Helpful Tips: Privacy Breach Guidelines.

✔ Contain the breach: Immediately contact the organization(s) to which the misdirected fax(es) has been sent.
  o Confirm that the fax has been received.
  o Explain that the fax contains personal health information and has been sent in error.
  o If you have the original fax, ask the recipient if they have the capability to destroy the personal health information securely (ex. capability to shred in a cross-cut shredder). Ask for confirmation that destruction has occurred.
  o Otherwise, ask that the recipient return the personal health information by mail or send a courier for pick up.
  o Request that the recipient not keep any copies of the personal health information. Ask for confirmation.
  o Inform the recipient of the mandate and role of the IPC should they have further concerns or questions.
  o Document the conversation.

✔ Ensure the personal health information reaches the intended recipient.

✔ Once the breach has been contained investigate.
  o Determine root cause of the breach.
  o Review written policies and procedures on faxing personal health information to ensure that best practices were followed.
  o Determine if the employees involved in the breach were aware of the policies and procedures and had received training.
  o Begin writing internal investigation report.

✔ Analyse the breach and consider the associated risks to both the organization and affected individuals.

✔ Notify the affected individuals. Contact the IPC if unsure that this step is warranted.

✔ Notify the IPC as soon as possible. When privacy breaches are proactively reported to the IPC, depending on the scale and severity of the breach, it will open a file to monitor the response of the trustee and ensure best practices are being followed. The file is then closed once the trustee’s internal investigation has satisfactorily come to a close. If the breach is covered by the media, the trustee will have the benefit of assuring the public it is working with the IPC.

✔ Complete an internal investigation report. Report should focus on ways to prevent future occurrences.
What can be expected in an IPC Investigation

✓ If the IPC is made aware of a privacy breach involving misdirected faxes by an affected individual or third party, the trustee will be informed of a formal investigation by a written notification letter. If the breach is proactively reported by the trustee, the IPC will open a file and monitor the response of the trustee.

✓ In either case, the IPC will request the trustee’s internal investigation report. The report should contain, but is not limited to, the following:
  o Number of faxes, affected individuals and recipients. Times and dates of misdirected faxes. Data elements contained in the faxes.
  o Details of the trustee’s efforts to contain the breach.
  o A determination if there was a need-to-know or if there was an unauthorized disclosure of personal health information.
  o Specific details of the circumstances leading to the misdirected fax(es).
  o Trustee’s determination of the root cause of the breach.
  o Trustee’s review of its policies and procedures on faxing personal health information and training of staff.
  o Whether the trustee has notified affected individuals. Why or why not?
  o Trustee’s steps to prevent further occurrences.

✓ See Appendix C – Privacy Breach Guidelines for more information of the IPC’s breach of privacy investigation process.
# APPENDIX F – WHEN TO DISCLOSE PERSONAL HEALTH INFORMATION TO FAMILY AND FRIENDS

## When to Disclose Personal Health Information to Family and Friends

<table>
<thead>
<tr>
<th>To Who</th>
<th>What</th>
<th>Consent</th>
<th>Subsection of HIPA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In General</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Someone with a written delegation pursuant to section 15 of HIPA</td>
<td>Personal health information as described in the written delegation</td>
<td>Express Consent</td>
<td>15, 56(f)</td>
</tr>
<tr>
<td>Personal Guardian or person designated by The Residential Services Act, The Rehabilitation Act or The Health Care Directives and Substitute Health Care Decision Makers Act.</td>
<td>All personal health information</td>
<td>Express Consent</td>
<td>56(b), 56(e)</td>
</tr>
<tr>
<td>Parent or legal guardian</td>
<td>All personal health information • If the individual is less than 18 years of age, if in the opinion of the trustee, the disclosure would not constitute an unreasonable invasion of the privacy of the individual</td>
<td>Implied Consent</td>
<td>56(d)</td>
</tr>
<tr>
<td><strong>In An Emergent Situation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Immediate Family or *Person in a close personal relationship</td>
<td>Individual's location, presence, condition, diagnosis, progress and prognosis • Only if care is being/has been provided that day</td>
<td>Deemed Consent or No Consent: Should not be contrary to the express wishes of the individual</td>
<td>27(2)(c)</td>
</tr>
<tr>
<td><strong>When the Individual is Deceased</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Personal representative of the individual</td>
<td>Personal health information related to the administration of the individual's estate</td>
<td>Deemed Consent or No Consent: Should not be contrary to the express wishes of the individual</td>
<td>27(4)(e)(i), 56(a)</td>
</tr>
<tr>
<td>Immediate Family or Person in a close personal relationship</td>
<td>Personal health information related to circumstances surrounding the death of the subject individual or services recently received by the subject individual • If in accordance with the trustee's policies, procedures and ethical practices</td>
<td>Deemed Consent or No Consent: Should not be contrary to the express wishes of the individual</td>
<td>27(4)(e)(ii)</td>
</tr>
<tr>
<td>Someone with a written delegation pursuant to section 15 of HIPA – if the delegation specifically extends into death</td>
<td>Personal health information as described in the written delegation</td>
<td>Express Consent</td>
<td>15, 56(f)</td>
</tr>
</tbody>
</table>

*Immediate Family* – the IPC recommends that Trustees in Saskatchewan adopt the list for “nearest relative” provided by subsection 15(1) of The Health Care Directives and Substitute Health Care Decision Makers Act for the definition of immediate family. The list is as follows:
- the spouse or person with whom the person requiring treatment cohabits and has cohabited as a spouse in a relationship of some permanence;
- an adult son or daughter;
- a parent or legal custodian;
- an adult brother or sister;
- a grandparent;

*Person in a close personal relationship* could include a common-law spouse, a close friend or other person who can demonstrate that he or she has such a relationship with the individual who is the subject of the information.

*Personal representative* is someone appointed by the court as Executor Administrator of an estate.

This relates to The Health Information Protection Act (HIPA).
APPENDIX G – DE-IDENTIFIED PERSONAL HEALTH INFORMATION

Pursuant to subsection 2(d) of HIPA, “de-identified personal health information” means personal health information from which any information that may reasonably be expected to identify an individual has been removed.

Personal health information has not been properly de-identified if:

- the identity of the individual can be determined by combining available data or information within the same or in several different records held by those who have access to the information; or
- the identity of the individual can be determined by comparing information representing distinguishing characteristics with other information sources having both the distinguishing characteristics and the names or other identifiers of individuals.

Some techniques to de-identify personal health information include:

**Anonymity transformation** refers to the process of taking individually identifying personal health information and rendering it non-identifying.

**Stripping** refers to the technique or process of removing names and personal identifiers from records that were identifiable. The resulting records are essentially anonymous when viewed in isolation from other contextual information. However, information representing distinguishing characteristics may be sufficient to re-identify the individual when compared with other information sources which have both the distinguishing characteristics and the names.

**Encrypting** refers to the technique or process of transforming information from human readable form to a meaningless form using a computational algorithm. Encryption can be used for an entire record of information, in which case it must be decrypted before it can be used at all. Secure applications decrypt the information prior to providing access to authorized individuals performing specific activities.

Encryption can be used to transform a personal identifier to a unique, but anonymous identifier. Anonymous identifiers allow processing of discrete person level records to analyze information across time, data sources or geographical areas for such purposes as measuring utilization, health system performance, and health outcomes or program evaluation.

**Re-coding** refers to the technique or process of transforming a very specific value for a data element to one which is meaningful but less precise. An example would be to transform a birth date to an age at a point in time. Re-coding is useful when the purpose for which information is desired does not require the same degree of specificity as the purpose for which the information was first recorded.

**Abstracting** refers to the technique or process of transforming information by selecting only the relevant aspects from a complete set of information. This process is useful when the
purpose for which the information is desired does not require the full set available and meets the principle of minimum amount of information used for each specific purpose.

*Aggregating* refers to the technique or process of transforming information about individuals into information about groups of individuals with common characteristics. An example would be statistical tables that count the number of individuals falling into specific groups. However, if there are only a small number of individuals within a certain category, they may be able to be identified by context.

*Deriving* refers to the technique or process of transforming specific elements of information into a new piece of information through a mathematical calculation. The derived element of information may be more meaningful to a particular purpose and also less likely to reveal identity than the specific elements from which it was derived. An example would be the length of stay in a facility that can be derived from the difference between the date of admission and the date of discharge. Both the admission date and the discharge date can be used to identify a *record* of an individual even though the identity had been encrypted or stripped if compared to a source of information which contained both dates and names.
APPENDIX H – INFORMATION SHARING AGREEMENTS

An information sharing agreement is an agreement that governs the collection, use disclosure and safeguarding of personal health information by the parties.

It is essential for trustees to have detailed written agreements in place when engaging an IMSP. This includes:

- identifying the objectives of the agreement and the principles to guide the agreement;
- whether the IMSP is permitted to collect personal health information and if so, a description of that information and the purposes for which it may be collected;
- whether the IMSP may use personal health information provided to it by the trustee and if so, a description of that information and the purposes for which it may be used;
- whether the IMSP may disclose personal health information provided to it by the trustee and if so, a description of that information and the purpose for which it may be disclosed;
- the process for the IMSP to respond to access requests or requests to amend or correct personal health information or for the IMSP to refer access requests to the trustee;
- where applicable, how the IMSP should address an individual's express wish relating to the disclosure of personal health information; and
- how personal health information is to be protected, managed, returned, or destroyed by the IMSP in accordance with HIPA.

Information sharing agreements should have the following components:

- Define what personal health information means.
- Describe the purpose for information sharing.
- Reference all applicable legislation that provides the legal authority for collection.
- Establish an understanding of who has custody and control.
- Identify the type of information that each party will share with each other.
- Identify the uses for the information and limitations on the uses to the specified purpose.
- Describe who will have access and under what conditions.
- Describe how the information will be exchanged.
- Describe the process for ensuring accuracy.
- Describe the process for managing privacy breaches, complaints, and incidents.
- Identify retention periods.
- Identify secure destruction methods when retention expires.
- Describe the security safeguards in place to protect information.
- Describe termination of the agreement procedures.

Also see the IPC’s resource Best Practices for Information Sharing Agreements.

COACH advises the following:

Enter into agreements before sharing any personal health information with a third party. Agreements protect you and your practice by establishing the terms and
conditions of providing personal health information that you may receive from or share with others, including centralized databases and other healthcare providers. Agreements can also establish accountability between you and electronic service providers, including network providers.
APPENDIX I – SAMPLE REQUEST FOR DISCLOSURE TO POLICE FORMS
Without Consent

DO NOT ADDRESSOGRAPH

REQUEST FOR DISCLOSURE OF PERSONAL HEALTH INFORMATION TO POLICE SERVICES WITHOUT CONSENT

I advise (facility) ___________________________ on (date) _______________ that personal health information on (Patient/Client/Resident name) ___________________________ born ___________________________ (dd/mm/yyyy), is required for the following reason(s):

☐ Avoiding or minimizing a serious and immediate threat to an identifiable individual(s).
☐ Assisting in the identification of a patient/client or locating a relative/friend of the patient/client/resident.
☐ The information is required to enforce or carry out a lawful investigation pursuant to the Criminal Code or the Controlled Drugs and Substances Act and/or the Patient/Client/Resident received or was offered health services as a direct result of an incident that is the subject of a lawful investigation pursuant to the Criminal Code or the Controlled Drugs and Substances Act.

The following information is being requested:

☐ Name, address, date of birth, and telephone number
☐ Information regarding the nature and severity of an injury connected to the enforcement of the lawful investigation
☐ Factual circumstances surrounding an incident that is subject to the lawful investigation.
☐ Factual circumstances surrounding the provision of health services offered as a direct result of an incident that is the subject of the lawful investigation.

The above information is needed to assist with the lawful investigation because:

I agree that the information disclosed pursuant to this request will only be used or disclosed by the Police Service for the purpose for which it was disclosed to the Police Service, and no other purpose, unless otherwise authorized pursuant to The Health Information Protection Act.

Police Service: ___________________________
Printed Name of Officer: ___________________________ Signature: ___________________________
Badge Number: ___________________________ Phone Number: ___________________________ Date: ___________________________
This request is: ☐ Urgent (within 24 hours) ☐ Non-Urgent (required within 72 hours)

Nurse in Charge or Facility Manager Designate releasing the requested information:
Name: ___________________________ Signature: ___________________________ Date: ___________________________

Note: Information cannot be released if the police officer is unable to produce proper identification, unable to provide a sufficient description of the individual in question or does not fill out the form correctly.
With Consent

REQUEST FOR DISCLOSURE OF
PERSONAL HEALTH INFORMATION
TO POLICE SERVICE

I request (trustee) ____________________________ for personal health information for
(name of individual) ________________________________

The following information is being requested:

- Information regarding the nature and severity of an injury to the individual.
- Factual circumstances surrounding the provision of health services provided to the individual.
- Information that would ensure the health and safety of the individual while in custody.

The above information is needed to ensure the health and safety of the individual while in the custody of the Police Service.

Police Service: ________________________________
Printed Name of Officer: ____________________ Signature: ____________________
Badge Number: ___________ Telephone Number: ____________ Date: ________________

CONSENT

I (name of individual) ___________________________ of (city/town) ___________________________

Consent to (hospital) __________________________ providing __________________ (Police service) with
information as requested by (peace officer) ________________________ for the purpose of ensuring my
health and safety while in custody.

Name_____________________________ Signature_____________________________

Date_____________________________
APPENDIX J – CHECKLIST FOR SEARCHING FOR PERSONAL HEALTH INFORMATION

Checklist for Searching for Personal Health Information

Build your search strategy by considering the following:

Types of information available
What type of personal health information is the individual seeking? For example:
- Patient chart
- Appointment information
- Laboratory results
- Medication information
- Immunization information
- Discharge summaries and medical imaging reports
- Clinical encounters
- Treatment plans
- Chronic disease information
- Consultation reports
- Independent medical evaluations
- Images, for example:
  - X-Ray
  - Ultrasound
  - CT
  - MRI

Time period
What is the period of time? For example:
- A single test or appointment
- Specific day, month, year
- Duration of a certain hospital stay

Record Type
Did you consider records in all different forms? For example:
- Paper
- Digital
- Microfiche
- Audio cassette
- Medical file
- Photographs
- Videotape

Location details
Did you consider records in different places?
- at facilities/locations/units/offices?
- records being temporarily retained:
  - on the unit

Page 1
Checklist for Searching for Personal Health Information

- in individual employee’s or physician’s offices
- vehicles or homes
- managed off-site by an information management service provider (IMSP)
- in the possession of a contractor, consultant, agent, lawyer
- stored on mobile electronic devices (i.e. laptops, smart phones, cell phones, tablets)
- contained within information systems (legacy, EMR, EHR)?
  - Did you use filtering tools to search?
  - Did you run any relevant reports (summary or detailed)?

Record organization
Did you consider how records are organized?
- How are records classified within the records management system? For example, are the records classified by:
  - Alphabet
  - Year
  - Function
  - Subject
- Did you search relevant folders on all drives within the records management system?
- Before searching, did you identify in advance key words to search?
- Do you need someone with different user rights to access restricted documents?

Record retention
Did you consider the record’s lifecycle?
- Did you find out where all active and non-active files are stored?
  - Storage on site?
  - Storage off-site?
- Consider disposal/destruction schedules?
- Review relevant destruction certificates?

Did you consult with Experts?
Did you talk to those ‘in the know’?
- Identify employee(s) “experienced in the subject matter”
- Records or information managers
- IT
- IMSP

Other types of records
Does the individual want to know who viewed his or her personal health information?
- If yes, did you refer him or her to eHealth Saskatchewan? eHR Viewer Audits - https://www.ehealthsask.ca/services/ehr-viewer/Pages/eHR-Viewer-Audits.aspx

Did the requestor also have interest in other kinds of information/records?
- His or her personal information?
- Administrative records?
- Other

Disclaimer
The above list is meant to be a guide. Providing the above details is not a guarantee that the IPC will find the search conducted was reasonable. Each case will require different search strategies and details depending on the records requested.