Checklist
To help determine compliance with *The Health Information Protection Act*

The Health Information Protection Act (HIPA) legislates rights of individuals and obligations of the "trustees" in the health system with respect to personal health information. The Act applies to personal health information in the health system in any form, including traditional paper records and electronic records.

The basic goal of the legislation is to protect privacy of personal health information, while at the same time ensuring that information is available as needed to provide services and to monitor, evaluate and improve the health system in Saskatchewan for the benefit of individuals and the province.

The Act applies to "trustees" throughout the province that collect, use and disclose personal health information.

This checklist is designed to assist trustees evaluate the level of preparedness for compliance with the Act. Completing this checklist will help identify where policy or procedure may need to be developed and/or changed to ensure compliance with key parts of the Act.

> ***NOTE:*** ***The purpose of this checklist is to highlight some of the key HIPA compliance steps that must be taken. It is not intended to be an exhaustive list, nor is it intended to provide a complete statement of your organization's legal obligations. Reference should always be made to the official text of HIPA and the HIPA Regulations for a complete statement of the law.***

1. Are you a "trustee" as defined by HIPA?

The following definition from *The Health Information Protection Act* is necessary to identify whether you or your organization is a trustee that has custody and control of personal health information under the Act. This definition is taken from Section 2 of the Act.

> 2(t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> (i) a government institution;
>
> (ii) a regional health authority or a health care organization;
>
> (iii) a person who operates a special-care home as defined in *The Housing and Special-care Homes Act*;
>
> (iv) a licensee as defined in *The Personal Care Homes Act*;
>
> (v) a person who operates a facility as defined in *The Mental Health*

www.manaraa.com

Services Act;

(vi) a licensee as defined in *The Health Facilities Licensing Act*;

(vii) an operator as defined in *The Ambulance Act*;

(viii) a licensee as defined in *The Medical Laboratory Licensing Act, 1994*;

(ix) a proprietor as defined in *The Pharmacy Act, 1996*;

(x) a community clinic:

(A) as defined in section 263 of *The Co-operatives Act, 1996*;

(B) within the meaning of section 9 of *The Mutual Medical and Hospital Benefit Associations Act*; or

(C) incorporated or continued pursuant to *The Non-profit Corporations Act, 1995*;

(xi) the Saskatchewan Cancer Foundation;

(xii) a person, other than an employee of a trustee, who is:

(A) a health professional licensed or registered pursuant to an Act for which the minister is responsible; or

(B) a member of a class of persons designated as health professionals in the regulations;

(xiii) a health professional body that regulates members of a health profession pursuant to an Act;

(xiv) a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee;

(xv) any other prescribed person, body or class of persons or bodies; (*The Health Information Protection Regulations*, Chapter H-0.021 Reg 1, have prescribed the following individuals or organizations as trustees under the Act:

(a) the Health Quality Council;

(b) hearing aid dealers within the meaning of *The Hearing Aid Sales and Services Act*.)

Yes	No	
O	O	Are you (or is your organization) a trustee as defined above?

If YES, continue to Part 2 of the checklist.

2. Do you have information that is captured by HIPA?

The following two definitions from *The Health Information Protection Act* are necessary to identify the records that fall under the Act. Theses definitions are taken from Section 2 of the Act.

www.manaraa.com

2(m) **"personal health information"** means, with respect to an individual, whether living or deceased:

(i) information with respect to the physical or mental health of the individual;

(ii) information with respect to any health service provided to the individual;

(iii) 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;

(iv) information that is collected:

(A) in the course of providing health services to the individual; or

(B) incidentally to the provision of health services to the individual; or

(v) registration information;

(p) **"record"** 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;

In other words, the Act applies to any records (including paper, electronic, microfilm, x-rays, etc.) that hold personal health information as defined above.

Yes	No	
O	O	Do you have records containing personal health information as defined above?

If YES, continue down the checklist. If NO, you are complete.

3. Does HIPA prevail as the authority regarding personal health information in your custody or control?

Yes	No	
O	O	Was/is the personal health information in your custody or control obtained for the purposes of one of the following?

- *The Adoption Act* or *The Adoption Act, 1998*;
- Part VIII of *The Automobile Accident Insurance Act*;
- Section 16 of *The Cancer Foundation Act*;
- *The Child and Family Services Act*;
- *The Mental Health Services Act*;
- *The Public Disclosure Act*;
- *The Public Health Act, 1994*;
- *The Vital Statistics Act, 1995* or any former *Vital Statistics Act*;
- *The Workers' Compensation Act, 1979*;
- An Act or regulation prescribed in HIPA regulations as exempt from HIPA in accordance with Subsection 4(4).

www.manaraa.com

Personal health information obtained for the purposes of the above is exempt from certain parts of HIPA dealing with collection, use and disclosure.

However, the following parts and sections of HIPA still apply to these statutes:

- Part I; Section 8 and Section 11; Parts III, VI, VII, and VIII.

If you answered NO to the above, go to Part 4, *Rights of the Individual*.

If you answered YES, complete questions 4.2 and 4.5 in *Rights of the Individual*, then move to Part 5, *Protection of Personal Health Information*.

(See Section 4 of HIPA for more details on how the Act prevails over other statutes.)

4. Rights of the Individual

HIPA identifies a number of rights that individuals have in regard to their personal health information. Trustees must take all reasonable steps to ensure those rights are respected.

By answering the questions here and in other parts of this checklist, trustees will be able to determine if they are complying with HIPA in support of these rights.

4.1. Consent

Consent is required for use and disclosure of personal health information in many circumstances for which it is collected (Please see questions 6.4 and 6.5 for a discussion of deemed consent for the provision of services by a trustee). Where consent (not deemed) is required by the Act, it must satisfy the rules in Section 6.

Yes	No	
O	O	Except in circumstances where consent is deemed to exist, consent of individuals is usually required before their information can be used or disclosed. Is consent collected from the individuals at the time information is collected?
O	O	Is the consent related to the purpose for which the information is required?
O	O	Is the consent voluntary? Consent cannot be obtained through misrepresentation, fraud or coercion.
O	O	Is the consent informed? Ask yourself the following: Is the individual provided with information about the intended use and disclosure of the information? Is enough information provided to enable the individual to make an informed decision about consent?
O	O	While collecting information directly from an individual, do you provide information about why the information is being collected and what are the anticipated uses and disclosures?

www.manaraa.com

You must answer YES to all of the above in circumstances where consent is required by the Act.

Note:

* *In certain circumstances a trustee will disclose personal health information to another trustee so that a service can be performed. In such circumstances the trustee receiving the information may act on the consent gathered by the first trustee and may use or disclose the information for the purpose it was received or for a consistent purpose, without the need to get consent a second time.*

** *Consent does not have to be in writing, although a record of consent given may be a good record keeping practice.*

*** *The requirements for consent do not need to be met where consent is already deemed to exist (subsection 27(2) of the Act) in limited circumstances primarily related to the provision of direct care to the individual.*

(See Sections 5 & 6 of HIPA for more details on consent.)

4.2. Revoking Consent

An individual may revoke his or her expressed or implied 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. Consent may be revoked at any time, but no revocation shall have retroactive effect.

Yes	No	
O	O	Are there reasonable procedures in place to comply with a revocation of consent promptly after receiving the revocation?

(See Section 7 of HIPA for more details on the right to revoke consent.)

4.3. Comprehensive Health Records on SHIN

Individuals have the right to prevent access to a comprehensive health record that is created and controlled by the Saskatchewan Health Information Network (SHIN) or by a person prescribed in the regulations under the Act.

- This right applies to a comprehensive health record of an individual's personal health information. A comprehensive health record consists of records containing the individual's personal health information from one trustee that are then combined with records containing the individual's personal health information from another trustee(s). This comprehensive health record is created and controlled by SHIN or a prescribed person for the purpose of maintaining a comprehensive health history of an individual that would be available to any trustee.

- The individual may require that their comprehensive health record not be disclosed to trustees by giving a written direction to SHIN or the prescribed person. Upon receipt of such a written direction, SHIN or the prescribed person must comply.

www.manaraa.com

- The right does not apply to other services that may be offered by SHIN or the prescribed person such as office automation (e.g. e-mail, word processing, spreadsheets), program specific applications, or other services not part of the comprehensive health record.

Yes	No	
O	O	Do you use SHIN or a prescribed person for the purpose of combining an individual's personal health information with the individual's personal health information from another trustee(s) for the purpose of creating a comprehensive health record of that individual? • If yes, please answer the next question. • If no, please move to the next section, *Right to be Informed*.
O	O	Do you have a process in place to inform individuals how they can exercise their right to prevent access to their personal health information contained in a comprehensive health record (i.e. contact SHIN if so desired)?

(See Sections 2(c.1), 8 and 18.1 of HIPA for details on the right to prevent access to a comprehensive health record on SHIN or by a prescribed person.)

4.4. Right to be informed

HIPA requires that trustees take steps to inform individuals of the anticipated uses and disclosures of their personal health information and to establish policies and procedures to promote knowledge and awareness of the rights extended to individuals by the Act.

Yes	No	
O	O	Are individuals informed of anticipated uses and disclosures of the information you are collecting? (This applies only when you are collecting the information directly from them.)
O	O	Do you have policy and procedures to promote the rights under this Act to individuals from whom you are collecting personal health information? (Informing can take the form of pamphlets, brochures, verbal briefings, etc.)

The answers must be YES.

(See Section 9 of HIPA for details on the right to be informed.)

www.manaraa.com

4.5. Tracking disclosures without consent

All trustees must be able to inform individuals about disclosures of their personal health information made without their consent. This does not apply to disclosures where the consent is deemed to exist. Trustees should keep records of all such disclosures to ensure compliance with the Act. Trustees are required to "take reasonable steps" to enable this to happen. Examples include:

- an audit trail built into an electronic system that tracks and records who accesses the records;
- good record keeping practices, such as making a note to file about disclosures or retaining a file copy of a letter disclosing information;
- standard written policy and procedures that can demonstrate that certain disclosures routinely happen when certain circumstances exist;
- a manual log which tracks all disclosures.

Yes	No	
O	O	Are you able through practice, procedure or policy to tell someone about disclosures of their personal health information?

The answer must be YES. If you answered NO, you will need to ensure that steps are taken to allow compliance.

(See Section 10 of HIPA for details on the right to information about disclosures without consent.)

4.6. Collecting the Health Services Number (HSN)

HIPA places certain restrictions on the collection of the Health Services Number (the number on the Saskatchewan Health Services card) from individuals. Collection by a trustee for a health service or program of trustee is not restricted. However, if you collect the HSN for other reasons, it must be in accordance with HIPA.

Yes	No	
O	O	Do you require individuals to produce their Health Services Number for reasons not connected to health services?
O	O	If you require the Health Services Number for non-health purposes, is the collection authorized by an Act or regulation? If not, collection can be voluntary, but cannot be made as a condition of receiving a service. Individuals must have the option of using other identification.

(See Section 11 of HIPA for details on the right to limit production of the HSN.)

www.manaraa.com

4.7. Individual's request to review or appeal an action/decision of a trustee

HIPA gives individuals the right to apply to the Information and Privacy Commissioner to request a review of an action taken or a decision made by a trustee with respect to the individual's personal health information. Individuals also have the right to appeal to a court the decision of a trustee regarding whether the trustee will or will not comply with the recommendation of the Commissioner.

Yes	No	
O	O	Do you take steps to inform individuals of this right, in the event that you cannot resolve a concern of an individual regarding his/her personal health information?
O	O	Do you have procedures in place to review and respond to a recommendation that may be made by the Commissioner regarding a request for review made by an individual?

(See Sections 14 and Part VI of HIPA for details on the right and the rules of an individual to request a review or appeal.)

4.8. Individual's ability to designate to another person

HIPA gives individuals the right to designate another person to act on their behalf regarding any of the individual's rights with respect to their personal health information.

Yes	No	
O	O	Do you have procedures in place to comply with an individual's written direction that someone else has been designated to act on their behalf regarding the rights pertaining to their personal health information?

(See Sections 15 and 56 of HIPA for details on the right of an individual to designate to another person their rights with respect to their personal health information.)

5. Protection of personal health information

5.1. Duty to protect

A trustee must have policies and procedures that result in administrative, technical and physical safeguards that protect the integrity, accuracy and confidentiality of personal health information.

Yes	No	
O	O	Do you have written policies and procedures in place to protect the personal health information in your custody or control. The policies should ensure that the personal health information is and remains accurate, that the integrity of the information remains sound (i.e. you can prove they are the records they purport to be) and that confidentiality of the information is protected.

www.manaraa.com

Yes	No	
O	O	Do you have policy and procedure to protect information against threats to security or integrity?
O	O	Do you have policy and procedure to protect against loss of information?
O	O	Do you have policy and procedure to protect against unauthorized use, disclosure or modification of personal health information?
O	O	If you have the above policy, is it designed to protect information in all forms including, but not limited to: • paper records; • computer records including database, e-mail, electronic forms, etc.; • microfilm/fiche?

You should answer YES to each of the above questions. If you answered NO, update or create policy as necessary.

(See Section 16 of HIPA for specifics on protection of information.)

5.2. Retention and destruction

HIPA requires that all trustees have a written policy concerning the retention and destruction of personal health information. The policy must meet the requirements set out in regulations.

Yes	No	
O	O	Do you have written retention and destruction policies for the personal health information in your custody and/or control?
O	O	Do you comply with that policy?
O	O	Do you take steps to ensure that the information contained in your records is retrievable, readable and useable for as long as you require the records? Consider the following: • Are your paper records safely stored where they will not suffer damage from risks such as water? • Do you have plans in place to migrate electronic data (including imaged data) through successive versions of software and hardware? • Do you have a formal system to backup electronic data contained on all computer systems that store personal health information?

www.manaraa.com

Yes	No	
O	O	Do you take steps to ensure safe disposal of personal health information? Ask yourself if there is any risk of the information contained in the records becoming public because of the method of disposal. For example, records thrown in a garbage can or electronic records not completely removed from a hard drive sold for salvage may be at risk.

(See Section 17 of HIPA for details on retention and destruction policy.)

5.3. Information Management Service Provider agreements

If you use the services of a third party to process, store, archive, destroy, combine or otherwise manage personal health information for which you are the trustee, you must have a written agreement with that third party that meets the requirements of HIPA. The Act refers to the third parties as Information Management Service Providers (IMSP) and they include (for example) records storage facilities and information technology companies that store and process personal health information on your behalf.

Yes	No	
O	O	Do you have written agreements with all IMSPs that: • governs the access to and use, disclosure, storage, archiving, modification and destruction of any information provided to the IMSP; • provides for the protection of the information; • meets the requirements of any regulations under HIPA regarding the agreements; • ensures all your duties and responsibilities as a trustee are met by the IMSP?

<u>Note</u>*:*

* *This section of the Act is not yet proclaimed. Nevertheless, having an agreement in place is good practice.*

(See Section 18 of HIPA for details on using an IMSP.)

5.4. Duty to collect accurate information

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

Yes	No	
O	O	Do you take reasonable steps to ensure that the personal health information that you collect is accurate and complete?

(See Section 19 of HIPA for details on collecting accurate personal health information.)

www.manaraa.com

5.5. Duties when disclosing information to others

Any time personal health information is disclosed, the trustee must know the identity of the person that is receiving the information. If the person is not a trustee, the Act requires the trustee to take reasonable steps to inform the recipient that the information must not be used for any purpose other than the reason it was disclosed.

Yes	No	
O	O	Do you confirm to your satisfaction the identity of any individual to whom you disclose personal health information?
O	O	Do you inform non-trustees that they can only use the information for the purpose you are disclosing it to them and for no other reason, except where provided in this Act?

(See Sections 20 & 21 of HIPA for details on disclosing to others.)

5.6. Continuing duty of trustees

HIPA requires that if a trustee ceases to be a trustee (e.g. retires, leaves the province, or dies), the personal health information must still be cared for in accordance with the Act.

Yes	No	
O	O	Should you cease to be a trustee, do you have arrangements in place to transfer the personal health information in your custody and control to another trustee or to an information management service provider that is a designated archive?
O	O	In preparation for the possibility of an untimely death, do you have a personal representative that will assume the duties imposed by HIPA until such time that the personal representative can transfer custody and control of the personal health information to another trustee or to an information management service provider that is a designated archive?

(See Sections 22 of HIPA for details on the continuing duty of trustees.)

6. Collection, use and disclosure

6.1. Collect, use or disclose on a Need-to-Know basis

The Act requires that personal health information is collected, used or disclosed only on a need-to-know basis. This means that only information that is required for an acceptable purpose should be collected, used or disclosed. It also means that only those individuals who need to know the information for legitimate purposes under the Act should have access to the records.

www.manaraa.com

Yes	No	
O	O	Do you take steps to limit the personal health information that is collected, used or disclosed only to what is necessary to satisfy the purpose of the collection, use or disclosure?
O	O	Do you have policy and procedures to restrict access to an individual's personal health information by employees, volunteers and others who do not need to know the information to perform their jobs?
O	O	Do you use or disclose de-identified personal health information if it will serve the purpose?

(See Section 23 of HIPA for details on need-to-know.)

6.2. Restrictions on Collection

The collection of personal health information should be primarily for the benefit of the individual the information is about. Secondary collection is acceptable in the limited circumstances described in the Act or where authorized by law or with consent.

Yes	No	
O	O	Do you collect personal health information only for the benefit of the person the information is about?
O	O	If not, is the collection for a purpose described in Section 27, 28 or 29 of HIPA or authorized by another statute or regulation?

(See Section 24 of HIPA for details about the obligations to limit collection of personal health information.)

6.3. Manner of Collection

Personal health information should only be collected from the individual the information is about unless other circumstances prescribed in HIPA exist.

Yes	No	
O	O	Do you only collect personal health information directly from the individual the information is about?

www.manaraa.com

Yes	No	
O	O	If you collect personal health information from other sources does it meet one of the following criteria? • The individual has consented to collection by other means. • The individual is unable to provide the information. • Collection from the individual would prejudice the mental or physical health or the safety of any person. • The information is collected to determine the eligibility of an individual to participate in a program or service of the trustee, in the course of processing an application made by or on behalf of that individual. • The information is collected to verify the eligibility of an individual who is participating in a program of the trustee or receiving a service from the trustee. • The information is available to the public. • The information is collected from another trustee pursuant to Section 27, 28 or 29 of HIPA. • The information is collected for the purpose of assembling a family health history.
O	O	When collecting personal health information from other sources, do you take reasonable steps to verify the accuracy of the information?

(See Section 25 of HIPA for details on the manner of collection.)

6.4. Restrictions on Use

An individual's personal health information may only be used for purposes consistent with the Act. In most cases if deemed consent does not apply, then consent of the individual should be obtained prior to using personal health information. Exceptions are provided in detail in Section 26 of HIPA.

Yes	No	
O	O	Do you have consent from individuals for every use of their personal health information?
O	O	If you do not always have consent to use an individual's personal health information, does the use meet one of the following criteria? • The use is for a purpose for which the information may be disclosed pursuant to section 27, 28 or 29 of HIPA. • The information is being de-identified. • The use is for a purpose that will primarily benefit the individual. • The use without consent is provided for in regulations.

www.manaraa.com

HIPA explicitly prevents a trustee from using an employee's personal health information for employment purposes, without the consent of the employee.

Yes	No	
O	O	Do you get consent (expressed or implied) before using personal health information for employment purposes?

HIPA requires that access to records of personal health information is limited to those who need-to-know and to information that is needed to know.

Yes	No	
O	O	Is access to personal health information in your custody or control limited to those persons who need to know the information to perform their jobs?

(See Section 26 of HIPA for details about the use of personal health information.)

6.5. Disclosure

Disclosure of personal health information will in most cases require consent from the individual the information is about.

For the specific purposes of providing services to an individual, the Act states that consent is not required to use or disclose personal health information if it is required to provide a service to an individual. This includes using or disclosing personal health information to:

- arrange for a service;
- assess the need for a service;
- provide a service;
- continue provision of a service; or
- support the provision of a service.

An individual's **consent is deemed to exist** where personal health information is required for these purposes. The service must be one which is requested or required by the individual.

Where an individual's consent is deemed to exist, it must be for the purpose for which the trustee collected the information or for a purpose that is consistent with that purpose. In addition to service delivery, consent can also be deemed to exist for the purpose of disclosing personal health information of an individual to that individual's next of kin or someone with whom the individual has a close personal relationship if the disclosure relates to health services currently being provided to the individual and the individual has not expressly stated that they do not want their information to be disclosed.

www.manaraa.com

In circumstances where a trustee determines that an individual's consent is deemed to exist for service delivery, use or disclosure of the individual's personal health information by the trustee can only take place where:

- the use or disclosure is in accordance with established privacy and security policies and procedures; and
- if the use or disclosure is being made by a health professional, such access, use or disclosure must be in accordance with the ethical guidelines applicable to the health professional.

The Act also provides limited circumstances where personal health information can be disclosed without consent.

Yes	No	
O	O	Do you take steps to ensure that consent is received prior to disclosing personal health information?
O	O	Where the consent of an individual is deemed to exist, is the disclosure of personal health information: • for the purpose for which the information was collected or for a purpose that is consistent with that purpose; • for the purpose of arranging, assessing the need for, providing, continuing , or supporting the provision of, a service required by the individual; • to the individual's next of kin or someone with whom the individual has a close personal relationship if the disclosure relates to health services currently being provided to the individual and the individual has not expressed a contrary intention to a disclosure of that type?
O	O	In the case of a trustee who is someone other than a health professional, for those disclosures of personal health information where consent is deemed to exist, do you have policies and procedures that restrict the disclosure of personal health information to those persons who need to know the information to perform their jobs?
O	O	In the case of a trustee who is a health professional, for those disclosures of personal health information where consent is deemed to exist, is the disclosure in accordance with the ethical practices of your profession?
O	O	If consent does not exist, is the reason for disclosure one of the circumstances identified in Sections 27(4), 28 or 29 of the Act? (These sections allow limited disclosure without consent.)

(See Sections 27, 28 & 29 of HIPA for details about disclosing personal health information.)

www.manaraa.com

6.6. Use or Disclosure for Research

The Act sets out some rules that must be considered prior to using or disclosing personal health information for research purposes.

Yes	No	
O	O	If personal health information is to be used or disclosed for research purposes, is a process in place to ensure that the requirements identified in Section 29 of *The Health Information Protection Act* are met?

Note:

* *Refer to the Saskatchewan Health website (www.health.gov.sk.ca) for a list of "approved" Research Ethics Committees required by Section 29.*

(See Section 29 of HIPA for more details about using or disclosing personal health information for research.)

7. Requests to Access or Amend personal health information by individuals

7.1. Accessing personal health information

HIPA requires that individuals be given access to records containing their own personal health information. This is almost an unconditional right of access. There are a few exceptions listed in the Act, which are generally limited to a belief by the trustee that providing access may endanger the mental or physical health or the safety of the applicant or another person, or the information is about someone else.

Yes	No	
O	O	Do you provide access to records containing personal health information when requested by the individual the information is about? If no, you must establish procedures to provide access to records containing personal health information when requested.
O	O	Do you charge for providing access? If so, is it consistent with the regulations under HIPA (not yet proclaimed)?

(See Section 12 and Part V of HIPA for details on the right and rules of an individual to access their personal health information.)

7.2. Amending personal health information

An individual has the right to request an amendment to records of their personal health information. A trustee must amend the record by adding to the record. A trustee cannot make changes (except to registration information) that destroy or obliterate existing information.

www.manaraa.com

Yes	No	
O	O	Do you amend records of personal health information when required by the individuals the information is about? If no, you must establish procedures to amend records of personal health information when requested.

(See Section 13 and Part V of HIPA for details on the right and rules of an individual to amend their personal health information.)

8. General

8.1. Exercise of rights by other persons

In most cases the rights and powers conferred on individuals by HIPA will be exercised by those individuals (or in the case of minors, by their legal guardians). However, the Act provides for a number of circumstances where others may exercise the right or power.

Yes	No	
O	O	If an individual is not able to act on their own behalf, do you ensure that the other person meets one of the circumstances identified in Section 56 of HIPA?

(See Section 56 of HIPA for details on the exercising of rights by other persons.)

8.2. Education of staff

HIPA applies to all trustees and to their staff. In many cases, it will be staff who will be performing the actions regulated by HIPA (collecting, using, disclosing personal health information). Trustees will need to ensure that staff are aware of the policies and procedures of the trustee that ensure compliance with the Act.

Yes	No	
O	O	Do you have written policy and procedure that ensures compliance with the Act?
O	O	Is your staff familiar with the policy and are they periodically reminded of the policy?

www.manaraa.com

9. Other Things to Consider when Determining Compliance with HIPA

9.1. Designating one or more individuals within your organization who will be responsible for implementing and overseeing privacy compliance

O Although not formally required under HIPA, your organization may want to consider designating one or more individuals who will be responsible for implementing and overseeing privacy compliance. If an individual(s) is assigned with this responsibility, it is important to ensure that the individual(s) is well trained and has adequate managerial support and resources for doing the job.

9.2. Inventory your information holdings and identify the various purposes for which your organization collects, uses and discloses personal health information

O It is important to distinguish between primary purposes and any secondary purposes for which the personal health information is being used. Your organization must ensure that each of the purposes for which it is collecting, using or disclosing personal health information is properly authorized.

9.3. Develop an external communications plan that will provide patients with reasonable notice of your organization's privacy practices

O Communicating your organization's privacy practices can be done in a number of ways including the use of privacy brochures, website policies, posters, etc.

9.4. Develop, document and implement privacy policies and procedures for your organization

O There are a number of areas in HIPA which specifically require that privacy policies and procedures be developed and implemented. Areas to be treated as a priority from a policy development perspective might include:

- Security;
- Individual access to their personal health information;
- Disclosure of personal health information;
- Consent (when it is required, what it consists of, how it is recorded, etc.).

www.manaraa.com

9.5. Implement privacy awareness training for your personnel

o Privacy breaches are frequently caused by human error. To help prevent this, personnel should be trained on, and regularly reminded of, their obligations under HIPA. Training could start with a discussion or notice to employees reminding them of their obligations under HIPA including:

- that employees will only access personal health information on a need-to-know basis for performing services on behalf of the organization;
- that employees will keep all personal health information in their possession in the strictest of confidence and only use the information for the purposes of performing services on behalf of the organization;
- that upon no longer requiring the personal health information for the purposes of providing services on behalf of the Organization, the employees will return or destroy all copies of the personal health information in their possession as instructed by the Organization; and
- that employees will follow all applicable security and confidentiality policies, procedures and practices of the Organization.

9.6. Review existing safeguards to ensure personal health information under the control of your organization is properly protected.

o The law now requires an organization to have proper security in place to protect personal health information. This should include implementing proper document retention and destruction policies. On this point, it is very important to remember that all documents must be retained for any minimum periods prescribed by law.

9.7. Develop policy and procedures for dealing with requests by individual for access to their personal health information

o HIPA contains detailed rules and procedures for allowing individuals to access their personal health information. Your organization must be prepared to respond to such requests.

9.8. Develop policies and procedures for dealing with privacy related complaints and privacy breaches.

o A good complaint handling process can help prevent privacy related problems from escalating.

o Also, despite your organization's best efforts, privacy breaches may occur. In the event that a privacy breach does occur, your organization may want to develop a privacy incident response policy to manage the breach.

www.manaraa.com