PRIVACY REFERENCE GUIDE FOR PHYSICIANS

MARCH 6, 2017

RÉSEAU DE SANTÉ Horizon HEALTH NETWORK

Notice

privacy reference guide for physicians

This guide is intended to provide clarity, build awareness and increase the level of confidence on the part of New Brunswick physicians working within the Horizon Health Network (Horizon) in their handling of personal health information under the New Brunswick *Personal Health Information and Privacy and Access Act (PHIPAA)*. Physicians working within Horizon include individuals employed by Horizon (salaried professionals) as well as fee-for-service professionals who have obligations as 'agents' when working within and on behalf of Horizon, a custodian under *PHIPAA*. Physicians may also have their own independent obligations as 'custodians' under *PHIPAA* when working within their own practices.

This document is intended to be a general reference guide; it is an overview document only. It is not intended to provide a complete statement of physicians' legal obligations and as such it should not be construed as legal advice. It should be used in conjunction with the official text of *PHIPAA* and its Regulations. If there is any discrepancy between references in this document to the official text of *PHIPAA* and its Regulations, the official text should be considered the authoritative document.

Horizon's Chief Privacy Officer is responsible for overseeing privacy matters within Horizon and should be consulted for further guidance in interpreting or applying the scenarios in this guide and for specific questions about privacy management.

Acknowledgement

The Horizon Privacy Management Project Team and Steering Committee would like to thank all those who participated as members of the Physician Privacy Advisory Committee for their input into the development of this guide and for their ongoing commitment to patient care.

This guide was produced in collaboration with Mara Consulting.

What's included in the guide

Introduction

The Horizon Health Network's vision for the Privacy Management Program is to create a sustained culture of privacy throughout Horizon characterized by an environment in which all employees and physicians are knowledgeable and accountable for complying with privacy policies and principles and protecting personal health information in their roles.

Horizon is committed to achieving this vision to ensure the protection of patient and client personal health information through strong and effective privacy management practices. Strengthening leadership and accountability for privacy management within Horizon, increasing transparency in privacy practices, engaging in meaningful collaboration, and improving education and communication with respect to privacy matters are key focus areas.

It is very important for your protection and for protecting the privacy of your patients that as physicians working within Horizon, you fully understand your legal responsibilities related to handling and protecting personal health information (in addition to your existing professional obligations). This is an important component of sustaining patient and client trust.

This 'Privacy Reference Guide for Physicians' has been developed using real life examples provided by the members of the Horizon Physician Privacy Advisory Group (PPAG) and the Horizon Privacy Management Steering Committee, from Professional Physician Associations and from jurisdictional research. We hope it will give you some practical guidance on how to identify common causes of privacy breaches and how to prevent privacy breaches when handling personal health information.

I encourage you to contact me at any time with questions or concerns about any of the content in this guide, or with respect to any other privacy matters for which I can offer support.

Kelly Chase, Chief Privacy Officer
Horizon Health Network
Phone: 506-870-2824
Toll free: 1-877-422-8717
Email: Kelly.Chase@HorizonNB.ca

Privacy definitions and basics

Privacy basics

Some of the fundamental privacy concepts and principles physicians should be aware of whenever they are handling patients' personal health information are described in this section. These concepts and principles should be read in conjunction with the case studies beginning on page 17 of this guide.

Physicians are encouraged to consult with Horizon's Chief Privacy Officer regarding any questions they may have about the propriety of accessing, collecting, using and disclosing personal health information in any given circumstance – i.e., if in doubt, ask!

It should be noted that professional obligations, including medical record keeping requirements identified under the *Hospital Act,* its regulations, as well as other legislative and regulatory obligations must still be accommodated; privacy obligations under New Brunswick legislation and the guidance provided throughout this document are not intended to replace those obligations.

The principle of **confidentiality** is a cornerstone of the ethical practice of medicine. Confidentiality refers to the commitment to protect a patient's personal health information that he/she has disclosed in a relationship of trust from being disclosed to others without the patient's consent. Patients share sensitive, often intimate information with their doctors, and physicians, in turn, have long recognized the obligation to keep that information confidential.

Privacy is the right of individuals to decide/control to what extent information about themselves is shared with or accessed by others. Privacy is broader than confidentiality, as conventionally understood; upholding the confidentiality of patient information does not necessarily equal compliance with privacy legislation. For example, under privacy legislation, access to patient information is restricted to those individuals who are involved in providing or supporting the provision of health care to patients within Horizon; allowing access to other employees and agents within Horizon would violate a patient's right to privacy. In addition, once a patient has consented to a health care provider accessing his/her personal health information to provide health care, the patient has a right to withdraw or limit that consent at any time.

The Horizon Health Network is defined as a '**custodian**' under the *Personal Health Information Privacy and Access Act (PHIPAA). PHIPAA* authorizes a custodian to collect, maintain and use personal health information for 1) providing or assisting in the provision of health care or 2) planning and managing the health care system or 3) providing a government service. A physician operating his or her own practice/clinic is a custodian under the Act when collecting, maintaining or using personal health information in that context.

Horizon staff and physicians (including fee-for-service physicians) working in Horizon are considered '**agents**' whenever they act for or on behalf of Horizon (the custodian) with respect to personal health information and not for their own purposes. As agents of Horizon they are obligated to comply with Horizon's legal obligations under *PHIPAA* and its privacy policies when working within Horizon.

For this document, references to 'custodian' should be read and interpreted as references to both custodians and agents. Physicians acting as agents of Horizon Health Network are bound by the same privacy obligations imposed upon Horizon Health Network as the custodian.

Consent

Privacy legislation requires Horizon to obtain consent of the individual before collecting, using or disclosing his or her personal health information, except in circumstances specified in the Act. Consent may be 'express (written) consent' [1] or 'implied knowledgeable consent'.

In either case, for consent to be valid it must:

- be granted by the individual about whom the information relates if the individual is capable of granting consent, or be the consent of the individual's substitute decision-maker;
- be knowledgeable;
- relate to the personal health information;
- be granted freely and not obtained through deception or coercion; and
- be able to be withdrawn or withheld.

In addition to consent being withdrawn or withheld, consent may also be subject to limits imposed by the patient. For example, a patient could request that certain personal health information not be disclosed to certain health care providers. Additionally, a patient has the right to amend a previously provided consent, expanding or restricting previously agreed upon use.

PHIPAA permits Horizon, as a custodian, to collect, use and disclose personal health information without consent, in certain circumstances including, but not limited to:

- Billing provincial health plans
- Responding to a court order
- Conducting quality improvement and risk management activities, e.g. patient safety reporting, morbidity or mortality reviews
- Enabling the Department of Health to plan and manage the health care system

Before using or disclosing personal health information without patient consent, physicians should ensure the practice is authorized under *PHIPAA* by reviewing appropriate Horizon policies and seeking guidance from Horizon's Chief Privacy Officer.

Implied Knowledgeable Consent

Physicians of Horizon who are providing health care services within a patient's 'circle of care' may generally rely on implied knowledgeable consent for the collection, use or disclosure of personal health information. The legislation allows a physician working in Horizon to assume, unless it is not reasonable in the circumstances to assume, that he/she

[1] Proposed amendments to *PHIPAA* may permit express consent to be obtained verbally or in writing. However, at the time of writing this guide, *PHIPAA* requires that express consent be obtained in writing.

has the individual's implied consent, and to assume the consent is knowledgeable, to collect or use the individual's personal health information or to disclose that information to another custodian or person for the purpose of providing health care to that individual.[2]

Knowledgeable Consent

The consent to the collection, use or disclosure of an individual's personal health information is knowledgeable if it is reasonable to believe that the individual:

- knows the purpose of the collection, use or disclosure, as the case may be;
- may give or withhold consent; and
- understands that the information can only be collected used or disclosed without his/her consent in accordance with the provisions of the *PHIPAA*.

If it comes to a Horizon staff member or physician's attention that an individual has a disability or limited ability to read or understand the notice or the language it is written in, staff must make reasonable efforts to assist in explaining the information or obtain help in doing so, to ensure consent is knowledgeable.

Circle of Care

The 'circle of care' is not a defined term under *PHIPAA.* It is an educational model intended to assist the health care community in understanding the sharing and use of patient information within the provisions of privacy legislation among custodians and individuals. The circle of care supports the care and treatment of individuals by allowing personal health information to be accessed, used and disclosed amongst custodians and individuals based on implied knowledgeable consent for providing health care to those individuals.

Persons within an individual's circle of care will include health care professionals such as physicians, nurses and clinicians providing patient care, specialists or other health care providers to which the patient has been referred by the physician; persons who support the provision of health care through laboratory and diagnostic services, as well as a range of individuals providing professional consultation services. The individuals within the circle of care should be obvious to the patient and reflect common practices.

The collection, use or disclosure of personal health information by a custodian can occur under an implied knowledgeable consent model within the patient's circle of care when[3]:

1. The personal health information that is being collected, used or disclosed has been received from the patient or his/her substitute decision maker or another custodian.
2. The personal health information that is being collected or used has been received for the original purpose of providing or assisting in providing health care to the patient. If the personal health information initially collected is to be

---

[2] *PHIPAA* S. 18(1), 18(2)

[3] Adapted from: Circle of Care (Ontario Privacy Commissioner) - healthcareathome.ca/ww/en/news/Documents/Circle%20of%20Care%20-%20Ontario%20Privacy%20Commissioner.pdf

used for other purposes, such as research, express consent must be obtained from the patient to use the information for the new purpose.

3. The personal health information is being collected, used, or disclosed for the sole purpose of providing or assisting in the provision of health care to the individual. Note that a health care provider not currently providing or assisting in providing health care to the patient would be considered outside the circle of care construct. As such, former and prospective health care providers with no demonstrated patient/provider relationship would be excluded under this model. The "circle of care" concept is relative to each specific patient episode of care. Thus, a physician may be within the circle of care for one event or admission of a patient but not another.
4. The sharing of personal health information must be to another health care provider who is providing or assisting in providing health care to the patient. Horizon physicians may not assume an individual's implied knowledgeable consent in disclosing personal health information to a person or organization that is not involved in providing health care to the patient, regardless of the purpose of the disclosure (e.g. a disclosure of personal health information to a family member is not considered to be within the circle of care).
5. The patient must not have expressly withheld or withdrawn his/her consent to the collection, use or disclosure of his/her personal health information. *PHIPAA* permits a patient or his/her substitute decision maker to withhold or withdraw consent to the collection, use or disclosure of personal health information, unless the collection, use or disclosure is permitted or required by law.

Note: There are other circumstances that do not fall within the circle of care, but for which physicians may be permitted to access, use and possibly disclose personal health information under the law and without consent. For example:

- Section 34(1)(h) of *PHIPAA* permits personal health information to be used for risk management and quality improvement activities. This would include, for example, a physician's ability to revisit provided care after a period, for reassessing the care provided and/or influencing future care to be provided (i.e. Quality Improvement).
- Section 39(1) of *PHIPAA* permits a health care provider to disclose personal health information without the consent of the individual to whom the information relates if he/she reasonably believes that disclosure is required to prevent or reduce a risk of serious harm to the mental or physical health or safety of the individual to whom the information relates or another individual. Consider a situation, for example, in which a physician must make a referral to a social worker regarding a concern about the environment that a mother will bring her baby home to, such as when there is evidence of substance abuse. In this circumstance, Section 42 of *PHIPAA* may also apply. This section requires a custodian to disclose personal health information without the consent of the individual to whom the information relates if it is required under another law. The physician would be obligated to make a referral to Child Protection under the NB *Family Services Act* if the physician has reason to believe a child has been physically or emotionally neglected.

Physicians should consult *PHIPAA* or the Chief Privacy Officer for more information if in doubt about whether access, use or disclosure of personal health information may occur without the consent of the patient.

When the Circle of Care does not Apply – Express Consent

If a physician has not satisfied the above conditions, he/she cannot assume that he/she has a patient's implied knowledgeable consent to collect, use or disclose his/her personal health information. Physicians who need or want to collect, use or disclose the patient's personal health information will need another form of authorization to do so.

Express consent of an individual is required for collecting, using or disclosing personal health information outside of the circle of care, except where otherwise permitted by *PHIPAA*.

Examples of when express consent will be required include:

- Disclosing personal health information to the media, fundraising bodies, or marketers;
- Disclosing personal health information to non-custodians, such as insurance companies, employers or the individual's legal counsel, unless required by law;
- Using or disclosing personal health information as part of research studies. Note: Some research studies which meet the specific requirements outlined in *PHIPAA* (subject also to Research Ethics Board review and approval) do not require express consent. Physicians should not attempt to determine when a proposed use of personal information is research, and when consent will or will not be required. *PHIPAA* contains very specific requirements that must be followed when personal health information will be used for research purposes. Inquiries regarding the proposed use and disclosure of personal health information as part of research activities should be directed to the Department of Research Services and/or Horizon's Chief Privacy Officer; and
- Disclosing an individual's personal health information to another health care provider for a purpose other than providing health care to that individual, or disclosing personal health information to a health care provider who is outside the individual's circle of care. When the circle of care does not apply, physicians must obtain express written consent from the patient prior to disclosing personal health information or verify that the disclosure is authorized to occur without consent under the law, to ensure that they comply with *PHIPAA*.

Consent is considered 'express' if[4]:

- the custodian requests the individual to provide the personal health information, and he/she complies;
- the individual knows the purpose of the collection, use or disclosure of the information, (consent is knowledgeable); and
- the individual grants the custodian permission in writing to collect, use or disclose the information.

[4] *PHIPAA* S. 19

Rule of Minimums

Physicians are required by privacy legislation to limit the collection, use and disclosure of personal health information to the minimum amount necessary to accomplish the purpose for which the personal health information is to be used or disclosed[5]. In all cases, professional discretion should be employed, and only relevant and necessary personal health information may be collected, used and disclosed, even when the collection, use or disclosure of that personal health information occurs with the consent of the individual or is otherwise authorized under the Act. Similarly, physicians are not permitted to collect personal health information if other information would suffice and may only collect the minimum amount of information needed to meet their clinical and record-keeping obligations[6]. Physicians must be conscious of this principle when sharing or obtaining information about patients with/from other care providers.

Need to Know Principle

'Need to know' is understood to mean that access to personal health information is necessary to conduct one's professional duties.

While sharing personal health information within the circle of care is permitted under *PHIPAA*, the Act also requires Horizon to limit the use and disclosure of personal health information to only those employees and agents, including physicians, who need to know the information to carry out the purpose for which the information was collected or received or to carry out a purpose authorized by the Act[7]. This generally includes members of the patient's health care team where it is reasonable to believe that the client/patient or his/her substitute decision maker is aware of the purpose of the collection, use or disclosure of his/her personal health information and knows that they can either give or withhold consent. For example: using privileges in the Meditech system to search for health records of friends is contrary to the need to know principle.

Although Horizon has implemented certain controls, the onus is also placed on physicians to ensure that they do not access or search for patient records without patient consent or without first ensuring that they are otherwise authorized by the legislation to do so without obtaining the patient's consent.

---

[5] *PHIPAA* S. 32(2); S. 35(2)

[6] *PHIPAA* S. 29

[7] *PHIPAA* S. 32(3); S. 35(3).

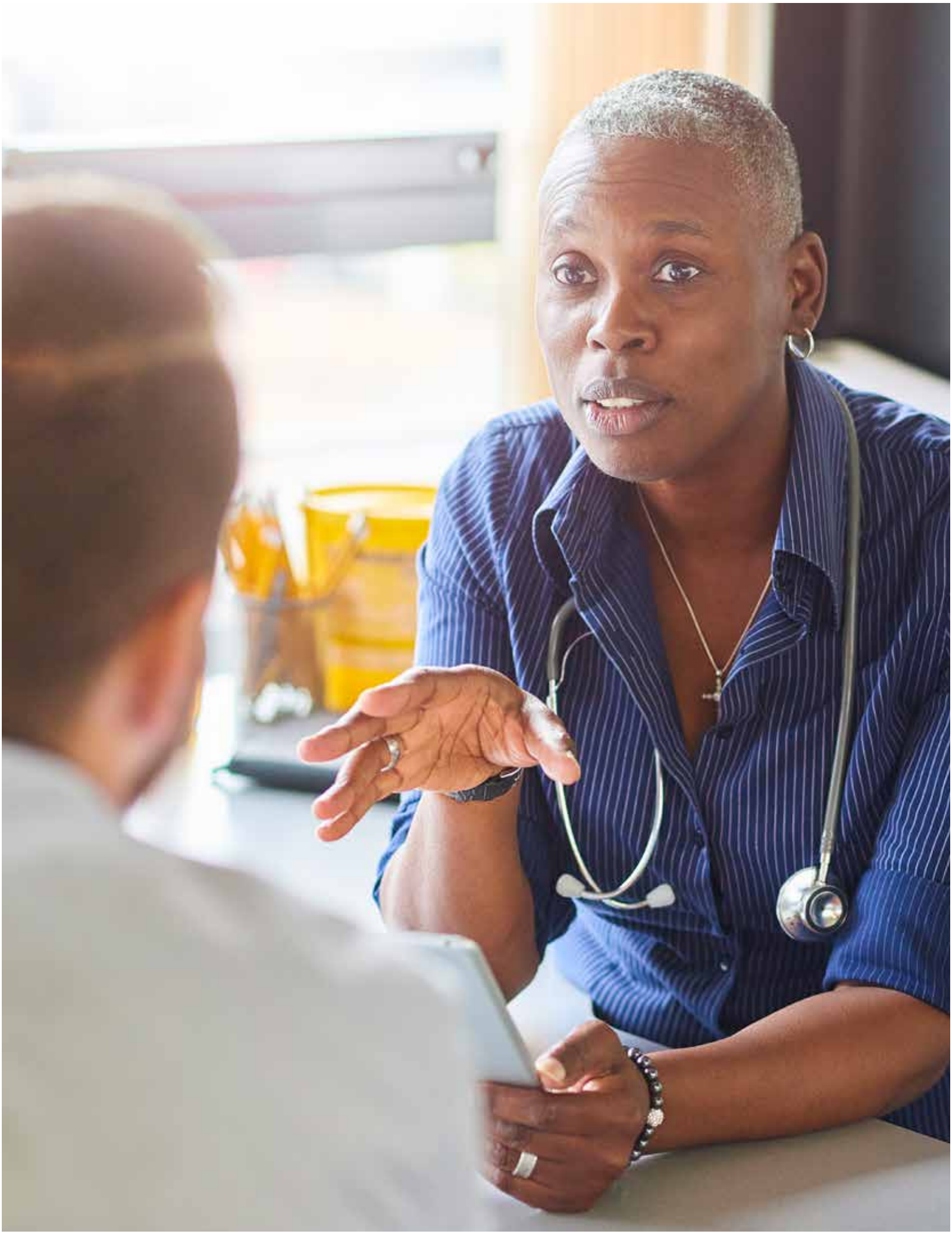
Privacy definitions

Term	Description
Agent	An individual or organization that acts for or on behalf of the custodian in respect to personal health information only for the custodian's purposes. 'Fee-for-service' physicians are considered agents of Horizon and are bound by Horizon's legal obligations under *PHIPAA* and its privacy policies when working within Horizon. A fee-for-service physician, when working in his/her medical clinic, would be considered a custodian with respect to personal health information he/she collects, uses or discloses in that context.
Commissioner	The Access to Information and Privacy Commissioner for New Brunswick, who is appointed under provincial legislation. Any individual may make a complaint to the Commissioner alleging that Horizon has collected, used or disclosed his or her personal health information contrary to *PHIPAA*, or has failed to protect his or her personal health information in a secure manner as required by this Act. On receiving a complaint under *PHIPAA*, the Commissioner is required to investigate the complaint or take steps to resolve the complaint informally to the satisfaction of the parties. The Commissioner may also initiate her own investigations to monitor Horizon's compliance with the Act. For example, the Commissioner may decide to investigate a privacy breach that has occurred within Horizon, which has been reported to the Commissioner. Horizon is required to report privacy breaches that meet certain specific criteria (outlined in the legislation) to the Commissioner.
Confidentiality	The commitment to keep a patient's personal health information private; to protect the information from being disclosed to others without the patient's consent.
Custodian	An individual or organization that collects, maintains or uses personal health information for providing or assisting in the provision of health care or treatment or the planning and management of the health care system or delivering a government program or service. The Horizon Health Network is a custodian under *PHIPAA*. In the health care context, custodians also include health care providers, health care facilities, researchers handling personal health information as part of an approved research project, research data centres, nursing homes, Ambulance NB and other persons or organizations designated under the Act and the Regulations. A health care provider may be a custodian in one context (e.g. a physician when working in his/her medical clinic) and an agent of a custodian in another (e.g. a fee-for-service physician with privileges working within a Horizon health care facility).

Term	Description
Health Care	Any observation, examination, assessment, care, service or procedure that is carried out or provided for a health-related purpose and: • to diagnose, treat or maintain an individual's physical or mental condition; • to prevent disease or injury or to promote health; or • as part of rehabilitative or palliative care. Health care also includes: • the compounding of a drug, for the use of an individual, pursuant to a prescription; • the dispensing or selling of a drug, a device, equipment or any other item to an individual, or for the use of an individual, pursuant to a prescription; and • a health care service prescribed by regulation, which includes the donation of blood, tissue or organs.
Health Care Provider	A person who is registered or licensed to provide health care under an Act of the Legislature or who is a member of a class of persons designated as a health care provider in the *PHIPAA* Regulations.
Personal Health Information (PHI)	Identifying information about an individual in oral or recorded form if the information: • relates to the individual's physical or mental health, family history or health care history, including genetic information about the individual; • is the individual's registration information, including his/her Medicare number; • relates to the provision of health care to the individual; • relates to information about payments or eligibility for health care in respect to the individual, or eligibility for coverage for health care in respect to the individual; • relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any body part or bodily substance; • identifies the individual's substitute decision-maker; or • identifies an individual's health care provider.
Privacy	The right of individuals to decide/control to what extent information about themselves is shared with or accessed by others. The privacy rights of individuals extend beyond the expectation that their information will be kept confidential.

Term	Description
Privacy Breach	A confirmed inappropriate access to, collection of, use of, disclosure of, or disposal of personal information or personal health information in contravention of the *Personal Health Information Privacy and Access Act (PHIPAA)* or the *Right to Information and Protection of Privacy Act (RTIPPA).* Privacy breaches can take many forms including but not limited to: • Sending an email or document to the wrong recipient • An employee of a physician accessing records without a 'need to know' • Disclosure of personal health information to someone other than the patient without proper authorization, whether in verbal or written form • Lost or stolen equipment containing personal health information • Disposing of equipment without properly erasing the personal health information Privacy legislation (*PHIPAA*) requires that certain privacy breaches (meeting specific criteria) be reported to the affected individuals and to the Access to Information and Privacy Commissioner for NB.
Privacy Complaint	Includes a concern or challenge brought forward by any individual relating to the privacy policies, procedures and practices implemented by Horizon or relating to Horizon's compliance with its policies or with privacy legislation.
Privacy Incident	Includes any actual or suspected inappropriate access to, collection of, use of, disclosure of, or disposal of personal information or personal health information in contravention of the *Personal Health Information Privacy and Access Act (PHIPAA)* or the *Right to Information and Protection of Privacy Act (RTIPPA).* All suspected privacy breaches and all privacy complaints will initially be identified as privacy incidents unless and until they have been confirmed as privacy breaches.

Term	Description
Substitute Decision Maker	In relation to an individual, means a person who is authorized under *PHIPAA* to give, withhold or withdraw consent on behalf and in the place of the individual with respect to the collection, use or disclosure of the individual's personal health information. For example, if the patient lacks capacity and the patient's substitute decision maker requests access to his/her personal health information, it can be shared. Otherwise, the patient must expressly consent (in writing) to the other person (such as a family member) receiving this health information. An exception to this is when Horizon shares confirmation a patient is in hospital, his/her room and telephone extension, and general condition (e.g. good, fair) with family members on the day they ask, unless the patient has objected. In the case of children and young people, physicians must assess if it is reasonable in the circumstances to believe that the minor is capable of deciding whether or not to consent to the collection, use or disclosure of personal health information and to appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing the consent. For example, in certain cases, a physician may conclude that a 15-year-old child is capable of consenting, in which case a physician would only be able to share the child's personal health information if the child provided written consent.
Third Party	In the context of disclosing personal information, any person, group of persons, or organization, other than the person or organization who directly collected the personal information or personal health information, or the individual him or herself.



Case studies

Examples related to privacy and 'circle of care'

This section of the guide is intended to illustrate the application of the implied knowledgeable consent provisions of the *Personal Health Information Privacy and Access Act* (*PHIPAA)* using a variety of health care scenarios. It should be noted that the implied knowledgeable consent provisions of *PHIPAA* apply equally to paper-based and electronic records of personal health information. It is also important to note that scenarios that vary even slightly from those presented in this section of the guide may result in a different application of *PHIPAA* and in those scenarios guidance may differ from what's provided in this guide. Physicians are encouraged to consult Horizon's Privacy Office for further guidance.

Refer to page 47 for information about the Legislative and policy considerations supporting the guidance provided under each of the following scenarios:

Case 1 - Informal ('curbside') consult

Situation

Physician A sees Physician B in the hallway and asks Physician B for advice about a patient; this is not a formal referral or consult and Physician B is not currently providing care to Physician A's patient. Physician B reviews the patient's electronic health record and provides requested verbal advice to Physician A.

Privacy issues to consider

1. Can Physician A share information about his patient with Physician B under an implied knowledgeable consent model for seeking advice (is Physician B considered within the patient's circle of care in this scenario)?
2. Does Physician B have the patient's implied knowledgeable consent to access the patient's electronic health record in this scenario?

Guidance for Physicians

Issue #1:
Can Physician A share information about his patient with Physician B under an implied knowledgeable consent model for seeking advice?

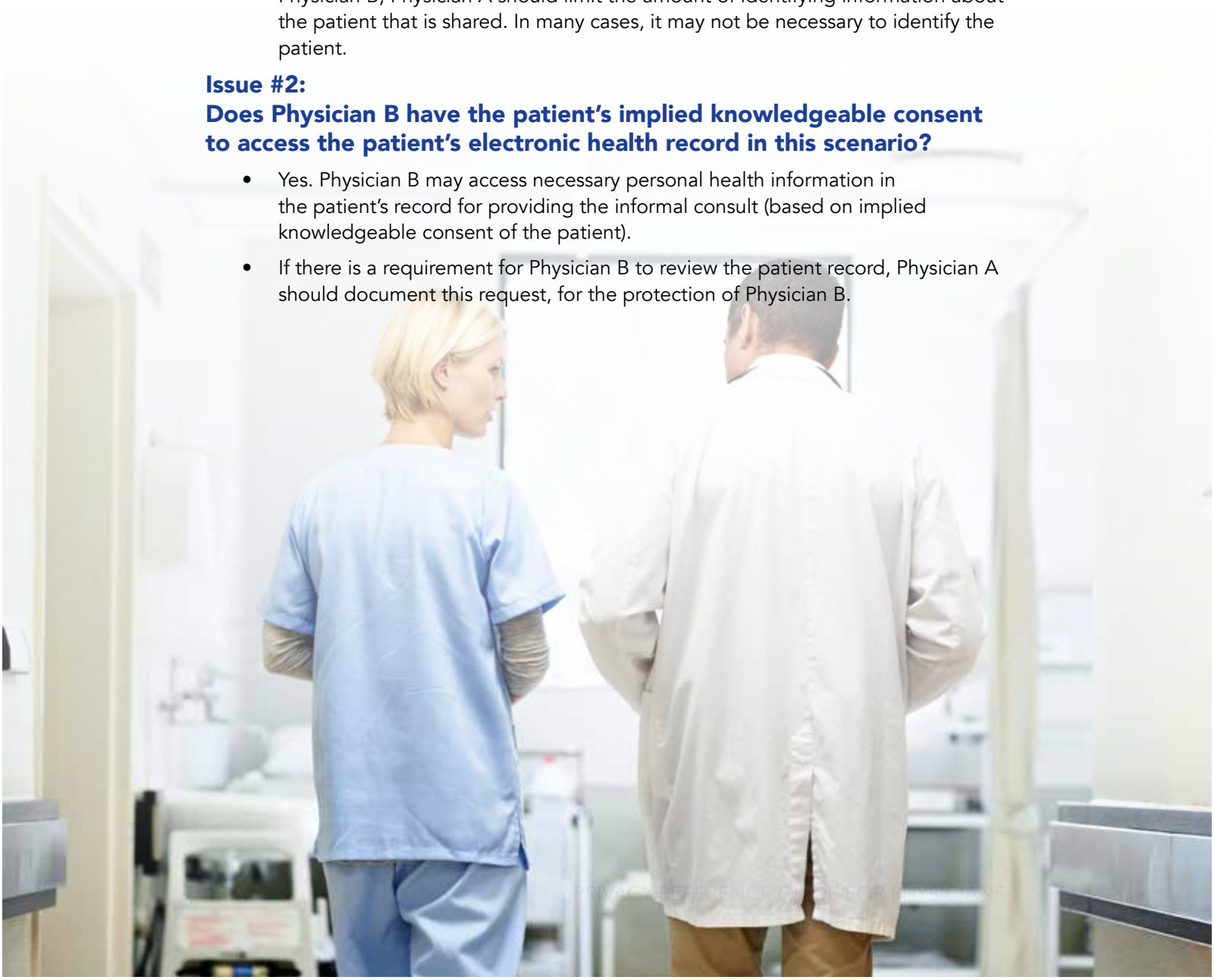
- Yes. Physician A can share necessary personal health information with Physician B to seek advice on the care of the patient, if the consultation is for the sole purpose of improving the patient's quality of care.
- Note: As a custodian, Horizon has an obligation to ensure patients are informed about the purpose of collecting their personal health information and how it may

be used and shared. This case assumes that patients are knowledgeable about, and would therefore reasonably expect their personal health information to be shared among health care providers for providing care to them. Physicians may generally make this assumption if Horizon has posted or made readily available a notice describing the purpose for collecting personal health information where it is likely to come to the individual's attention, such as in admitting areas.

- In some circumstances, patients may not consent to their physician consulting with another health care provider. Patients have a right to limit or withdraw their consent to a physician accessing or sharing their personal health information at any time.
- The 'need to know' principle is relevant here; it must be considered whether Physician B needed to know the patient's personal health information in this situation.
- The 'rule of minimums' must also be considered – physicians should ensure that only the minimum amount of personal health information is shared and accessed in the case of an informal consult. When seeking an informal consult from Physician B, Physician A should limit the amount of identifying information about the patient that is shared. In many cases, it may not be necessary to identify the patient.

Issue #2:
Does Physician B have the patient's implied knowledgeable consent to access the patient's electronic health record in this scenario?

- Yes. Physician B may access necessary personal health information in the patient's record for providing the informal consult (based on implied knowledgeable consent of the patient).
- If there is a requirement for Physician B to review the patient record, Physician A should document this request, for the protection of Physician B.



Case 2 – Physician on call

Situation

An 'on-call' physician prepares for her shift by reviewing the electronic health record of the patients on the unit to which she has been assigned to cover for another physician. When on call, she reviews the X-rays applicable to John Doe's situation and reviews his chart in more detail to obtain a better understanding of his health situation and health history. She treats John Doe for a broken hip while covering for another physician. She has no further contact with John Doe after the end of her shift.

After a couple of weeks, the physician is no longer on call, and she learns that John Doe has died. The physician checks the patient's electronic health record to see if she may have missed anything and to learn from any mistakes.

Privacy issues to consider

1. Can the on-call physician rely on the implied knowledgeable consent of all patients on the unit to review their charts before her shift begins? (When does the circle of care begin?)
2. Is the physician part of John Doe's Circle of Care and entitled to access John Doe's personal health information while on call? Are there any limits to the amount of information in the patient's file the on-call physician may access?
3. Is the on-call physician still within the Circle of Care when she accesses the patient's electronic health record after care has been provided, when she is no longer on call? Would this answer differ if the patient were not deceased?

Guidance for Physicians

Issue #1:
Can the on-call physician rely on the implied knowledgeable consent of all patients on the unit to review their charts before her shift begins? (When does the circle of care begin?)

- Yes. Once the physician has confirmed that she is responsible for providing health care to the patients on the unit, she may access individual patients' personal health information in anticipation of providing health care; but should adhere to the rule of minimums by only accessing the minimum amount of personal health information necessary for that purpose.
- Physicians should use good judgment and only access personal health information when it is reasonable in the circumstances to do so. If individual patients have not been assigned to the physician's care and access to personal health information is based only on a possible future requirement to provide care, it may not be viewed as reasonably necessary 'for the purpose of providing health care to the individual'. The on-call physician will not be considered to be in the circle of care for patients with whom she has no care relationship.

Issue #2:
Is the physician part of John Doe's Circle of Care and entitled to access John Doe's personal health information while on call? Are there any limits to the amount of information in the patient's file the on-call physician may access?

- Yes. The physician would be considered within John Doe's Circle of Care when she is on call; she may access the personal health information she requires to provide health care to John Doe. *PHIPAA* is not intended to interfere with the provision of good patient care. The use of personal health information may occur under an implied knowledgeable consent model, if the patient has not exercised his right to withdraw his consent to this use of his personal health information. Physicians should always adhere to the 'need to know' principle, and only access as much personal health information about the patient as is needed to provide health care in each instance.

Issue #3:
Is the physician still considered to be within the Circle of Care if she accesses the deceased patient's electronic health record?

- The physician would not be considered in the circle of care; however, *PHIPAA* permits physicians to access the records of patients without their consent if it is for the purpose of reassessing the care provided and/or influencing future care to be provided i.e., Quality Improvement. This would include for example, a physician's ability to revisit previously provided care.
- Health care professionals who were most recently involved in treating John Doe prior to his death, including the on-call physician, would be permitted to review the deceased patient's file from a quality management perspective to prevent future errors (if applicable) from occurring.
- Documenting that the access is for quality improvement purposes is good practice.
- Rule of minimums, the physician should limit her access to those portions of the record that are necessary for the specific quality improvement purpose.

Would this answer differ if the patient were living (not deceased) when the record was accessed?

- The on-call physician would be considered outside of the circle of care once she is no longer treating the patient and has no continuing care relationship with the patient. Access to a patient's record would be permitted under an implied knowledgeable consent model only if the physician must access the personal health information to provide health care to the patient (e.g. follow-up care).
- If the physician wishes to access John Doe's file once he is no longer treating him for a quality improvement purpose, she should consult with, and obtain approval of the appropriate Chief of Staff prior to accessing the patient record and document the purpose for the access. The on-call physician should not access the record independently for this purpose.

Case 3 – Pathologist accesses records

Situation

A pathologist accesses many patient records to make accurate diagnoses during her laboratory work. In addition to those records to which she has been assigned, she is often asked through an informal consult to review a slide, sample or patient chart and provide an opinion or diagnosis.

She may not always remember the circumstances of why she was looking in certain patient records months later. She is concerned that her access to such a large volume of patient records may be questioned.

Privacy issues to consider

1. Will the pathologist be considered within the patient's Circle of Care when she accesses the patient's records?
2. Are there any limits to what she may access (e.g., only the diagnostic images; partial health record, entire health record)?

Guidance for Physicians

Issue #1:
Will the pathologist be considered within the patient's Circle of Care when she accesses the patient's records?

- The pathologist is a critical member of the patient care team and would be considered part of the circle of care for the patients to which she has been

assigned. She can assume she has a patient's implied knowledgeable consent to access the patient's health care record and to use the personal health information for carrying out the health care activities needed to provide a proper diagnosis, unless the patient has expressly withdrawn his or her consent.

- As a specialist, the pathologist may also be consulted informally by another physician to confirm or provide a diagnosis. Pathologists or similar specialists should document the purpose and outcome of these types of informal consultations in the patient file, to the extent possible. In this way, it is clear that the pathologist is part of the circle of care.
- An unusually large number of records accessed over a period of time might be flagged as part of an audit and investigated further if there is reason to believe that the pathologist accessed records without a clear 'need to know'.

Issue #2:
Are there any limits to what personal health information the pathologist may access (e.g., only the diagnostic images; partial health record, entire health record)?

- The pathologist may view any personal health information in an individual's electronic record that is pertinent to her work in providing health care to the patient.
- The pathologist must ensure that she accesses only those patient files to which she has been assigned or for whom a consult has been requested and documented.
- If the pathologist inadvertently accesses an incorrect patient record (e.g., perhaps the pathologist has searched incorrectly, opens the record and realizes this is the incorrect patient's record), she should close the patient record right away. The pathologist is encouraged to make a note of the error for her records in the event this access is questioned in the future, as part of an audit.

Case 4 – Physician checking on former patient

Situation

A surgeon hears that a former patient is in the hospital for oncology treatments. The surgeon operated on her once about a year ago, and knows her from church.

The surgeon is currently not assigned to the patient's care and does not work in the oncology unit; however, he is concerned about her health situation. Having treated her in the past, he decides to check the patient's record to learn more and understand how her health situation may have changed.

Privacy issues to consider

1. Can the physician assume that it is acceptable to review a former patient's electronic health record based on the patient's implied knowledgeable consent?

Guidance for Physicians

- No. The physician cannot access the record based on a patient's implied knowledgeable consent if he has no care relationship with the patient, or out of personal curiosity.

Things to consider:

- **If** the treating physician has requested the surgeon to access the patient's record to provide advice or input to benefit the care of the patient, the physician may rely on implied knowledgeable consent to access the record.
- **If** the purpose for accessing the former patient file is for a quality management activity (i.e. to improve the quality of future care, learn from any mistakes related to his diagnosis and treatment), access may occur without patient consent under *PHIPAA*.
    - Physicians wishing to access records of patients who they have not treated for a prolonged period, or who they are not currently treating for a quality improvement purpose should obtain approval of the appropriate Chief of Staff prior to accessing the patient record.
    - The physician should document the reason for the access, so that in the event of an audit he can explain it.
- **If** either of the above applies, the physician should still only access those portions of the record that are necessary (rule of minimums).

Case 5 – Physician checking patient's drug use with pharmacy

Situation

A physician suspects a patient of inappropriately obtaining prescription drugs from many physicians and pharmacies. The patient's physician is concerned for the patient's health and feels there may be a risk of significant harmful side effects from the combination of drugs the patient may have been prescribed. The physician calls a pharmacy to request a list of medications for this patient. The physician did not obtain written consent from the patient to contact the pharmacy and the pharmacy doesn't request written consent from the patient before releasing the information to the physician.

In addition, the physician decides to contact the psychiatrist assigned to the individual to check on the patient's condition. There was no consent from the patient for the physician to do this.

Privacy issues to consider

1. Did the physician need the patient's consent to obtain the list of medications from the pharmacy or can he rely on the patient's implied knowledgeable consent?
2. Can the physician and the psychiatrist rely on implied knowledgeable consent to share information about the patient's condition?

Guidance for Physicians

Issue #1:
Did the physician need the patient's consent to obtain the list of medications from the pharmacy or can he rely on the patient's implied knowledgeable consent?

- The physician may assume implied knowledgeable consent of the patient to collect the personal health information from the pharmacy if it is for the purpose of providing health care to a patient the physician is currently treating, unless the patient has expressly withdrawn his/her consent. If the purpose for the physician's collection of the personal health information from the pharmacy is for the care/safety of the patient and prevention of side effects, this would be considered to be a valid health care purpose and the physician can rely on the patient's original consent to collect the personal health information from the pharmacy.

Issue #2:
Can the physician and the psychiatrist rely on implied knowledgeable consent to collect and use the personal health information as part of the patient's circle of care?

- The physician may collect and the psychiatrist may disclose the patient's personal health information if doing so is for the purpose of providing health care to the patient he is currently treating.
- If the patient has revoked his/her knowledgeable implied consent, the custodian cannot collect personal health information from another custodian.

Case 6 – Physician accesses her own record in the system

Situation

A physician recently had a blood test at the hospital where she works. She decides to use her Meditech system access to look up her test results and takes the opportunity to review the other aspects of her file.

Privacy issues to consider

1. Since the physician has access in the Meditech system, is it acceptable for her to review her own record?

Guidance for Physicians

Horizon's Confidentiality Declaration of Understanding signed by all physicians requires all employees to agree to 'access my own health information only through Health Records or the designated custodian of my information.'

- Personal health information in the physician's own medical record, like that of other patients, is collected for the purpose of providing health care and may be accessed, used and disclosed only for that same purpose unless the Act permits otherwise. The privilege of access is not given for any other purpose. Having access rights to an electronic medical records system does not infer you have a right of unrestricted access to all information contained in the system, including your health record or the health record of family members.
- Although not considered a privacy breach, it is a violation of Horizon Policy for physicians to access their own health record or the health record of family members without following appropriate protocols. Physicians wishing access to their own medical record within Horizon may make a request to the hospital's health records department using the hospital's stated procedure, which is based on the access provisions set out in *PHIPAA*.
- The physician may request another physician who is within her circle of care to access her medical record if the other physician uses his or her credentials to log into the system to access the physician patient's medical record.
- Ethical considerations and hospital protocols related to physicians treating themselves or family members should also be considered.

Case 7 – Helpful neighbour

Situation

A physician is outside in his yard and witnesses an elderly neighbour fall. The physician calls the hospital and orders an X-ray right away. The physician is not the elderly neighbour's family physician. Since it has been a week and the neighbour is anxious to hear the outcome, the physician uses his privileges to view the results of the X-ray.

Privacy issues to consider

1. Is the physician part of the neighbour's circle of care?
2. Can the physician access the neighbour's health record because he ordered the X-ray?

Guidance for Physicians

Issue #1:
Is the physician part of the neighbour's circle of care?

- Yes. If the neighbour has sought medical advice and care from the physician and the physician orders the X-ray results, he or she is providing health care to the neighbour and considered to be within the circle of care.

Issue #2:
Can the physician access the neighbour's health record because he ordered the X-ray?

- There is a clinical requirement for an ordering physician to follow up on the X-ray. On this basis, the physician may access the health record to review the X-ray results. The neighbour's personal health information, including diagnostic imaging results and other information in his electronic health record within Horizon, is collected for the purpose of providing health care to the individual (neighbour) and may be accessed by the physician if it is for that same purpose (providing health care).
- The physician should only access relevant aspects of the health record needed to provide care.
- Once the X-ray follow-up has been completed and there is no continuing care relationship with the neighbour, the physician would require express consent of the neighbour before further accessing personal health information.

Examples related to privacy and technology

Changes in technology continue to provide physicians and patients with a more efficient way of maintaining and communicating personal health information. There are, however, several ways in which a physician may inadvertently breach patient privacy when using technology. This section of the guide reviews some of those typical scenarios and offers guidance for physicians on how to avoid these risks.

Case 8 – Texting to communicate patient information

Situation

A physician regularly uses his personal smart phone to text a description of a patient's symptoms and suspected diagnosis, etc. to another physician to obtain a quick consult or response.

Privacy issues to consider

1. Is personal health information being exchanged?
2. Are both physicians within the patient's circle of care?
3. Is personal health information being protected in the manner required by *PHIPAA*?

Guidance for Physicians

Issue #1: Is personal health information being exchanged?

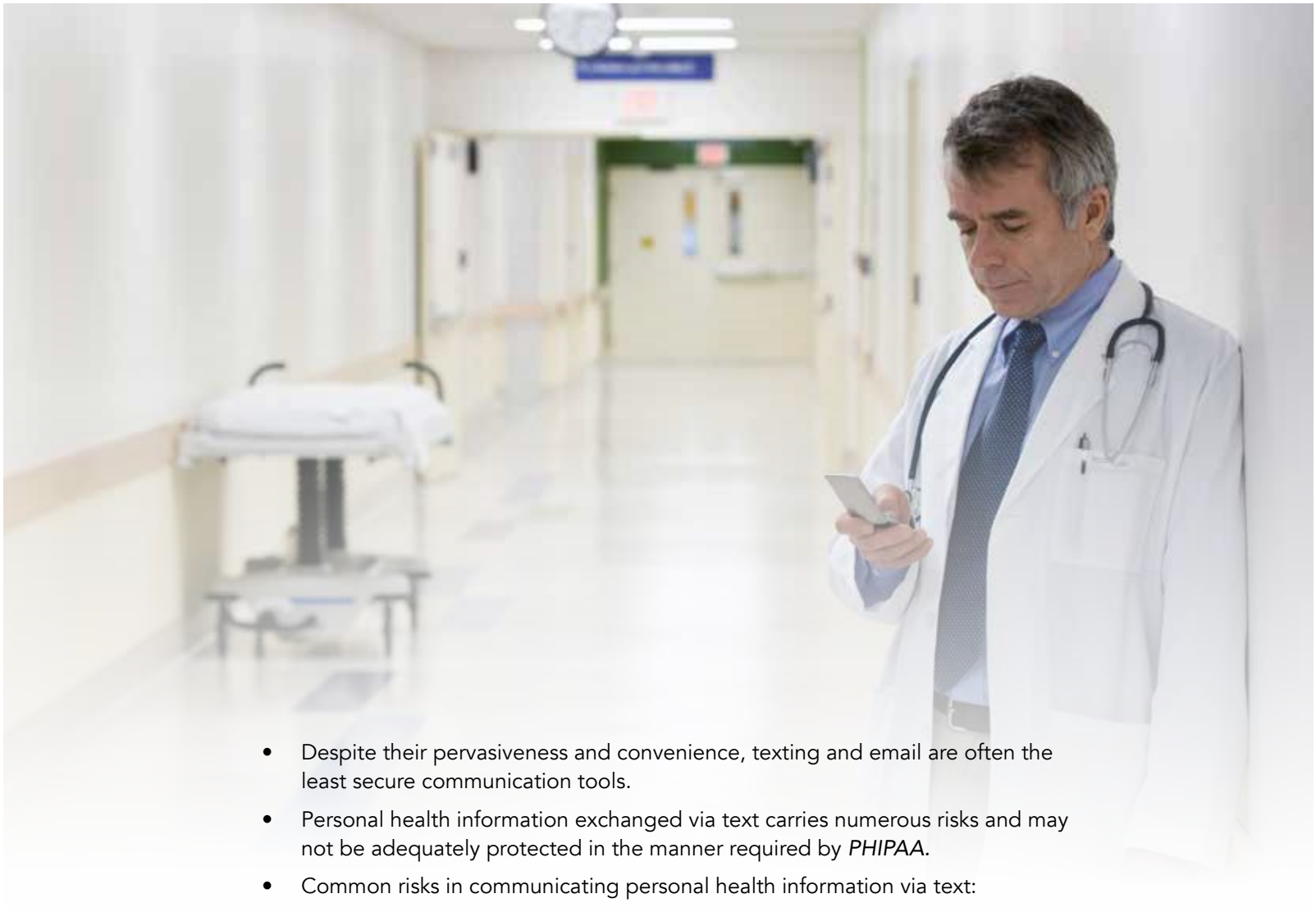
- Yes. A description of the patient and symptoms or suspected diagnosis may be enough to identify the patient and therefore is considered personal health information.

Issue #2: Are both physicians within the patient's circle of care?

- Yes. A physician can share necessary personal health information with another physician for obtaining advice related to the provision of health care, based on implied knowledgeable consent of the patient. Both physicians will be in the patient's circle of care.
- Refer to case #1 – curbside consult for details.

Issue #3: Is personal health information being protected in the manner required by *PHIPAA*?

- Physicians have a professional and legal obligation to protect the privacy of patients' personal health information; this includes safeguarding that information whenever it is transferred or communicated within Horizon using reasonable safeguards to prevent such risks as unauthorized access or disclosure of personal health information.



- Despite their pervasiveness and convenience, texting and email are often the least secure communication tools.
- Personal health information exchanged via text carries numerous risks and may not be adequately protected in the manner required by *PHIPAA*.
- Common risks in communicating personal health information via text:
  - Potential loss or theft of the mobile device, leading to inappropriate access or disclosure of personal health information.
  - Text messages could be stored without the knowledge or permission of the patient or could be misdirected.
  - Text messages are easily accessed by anyone who has access to the mobile device without the need to enter a password.
  - Text messages are subject to retention requirements and patient rights of access under *PHIPAA* if they are used to make decisions about patient care.
- Due to the numerous risks involved, texting <u>is not</u> currently an approved method of communicating personal health information within Horizon. An exception can be made when there is an imminent risk to the patient or clinician's safety and no other accepted form of communication is available.
- In response to these risks, and in recognition of the convenience and utility of using mobile devices within the workplace, Horizon is updating its policies to address the use of physician-owned mobile devices, including the use of texting, in order to provide additional guidance to physicians.
- Physicians should consult Horizon's Privacy Office if they have further questions about texting or secure methods of communicating personal health information.

Case 9 – Patient photos/images taken using a personal wireless device

Situation

A surgeon finds an unexpected mass during the operation on a patient and takes a photo of it with his personal phone to quickly send to another surgeon seeking her advice/expertise. The surgeon believes the use of the phone for snapping a quick picture in the middle of an operation is the most efficient way of consulting with the other surgeon for a quick response, as physicians always carry their phones. He feels that patient care has been greatly improved and no harm has been done because he deleted the photo.

Privacy issues to consider

1. Did the physician obtain valid consent to take and share the photo?
2. Is personal health information being protected in the manner required by *PHIPAA*?

Guidance for Physicians

Issue #1: Did the physician obtain valid consent to take and share the photo?

- Consent is required for collecting and sharing personal health information. In this instance, as in many other instances of collecting and sharing photographs, it must be considered whether the photographs could reasonably be expected to identify the individual, i.e. whether it meets the definition of personal health information and would be subject to *PHIPAA*. If the individual can be identified from the photo directly, or together with other information such as a name, then the photo would be considered personal health information.
- If considered personal health information, taking and sharing the photo for providing health care to the patient may occur with the patient's implied consent. To ensure consent is knowledgeable, Horizon will be adding a statement to the surgery consent form that can be used to obtain patients' consent to photographs being taken if required for providing patient care in the operating room.

Issue #2: Is personal health information being protected in the manner required by *PHIPAA*?

- Personal health information collected and stored using personal phones may not be adequately protected in the manner required by *PHIPAA*. For example, personal health information initially stored on both physicians' phones may be replicated in numerous storage locations - i.e., backed up to 'iCloud'. In addition, such devices are subject to loss or theft.
- To meet its obligations to protect personal health information, Horizon's current position is that photos in the Operating Room must be taken with 'OR cameras' only.
- If there is a requirement for a physician to take and send a photo quickly (such as in an emergency) using a physician's personal device, the device must be encrypted and password protected as per Horizon policy.

Case 10 – Social Media: Patient requests to 'friend' his/her physician

Situation

A physician creates a Facebook account to stay in touch with her children and grandchildren. After a few weeks, the physician begins to receive friend requests from several patients. Not wanting to offend her patients, she accepts the requests. The physician notices some patients' messages include health-related questions and others post information about their health issues. In both instances, wanting to be helpful, the physician adds a comment.

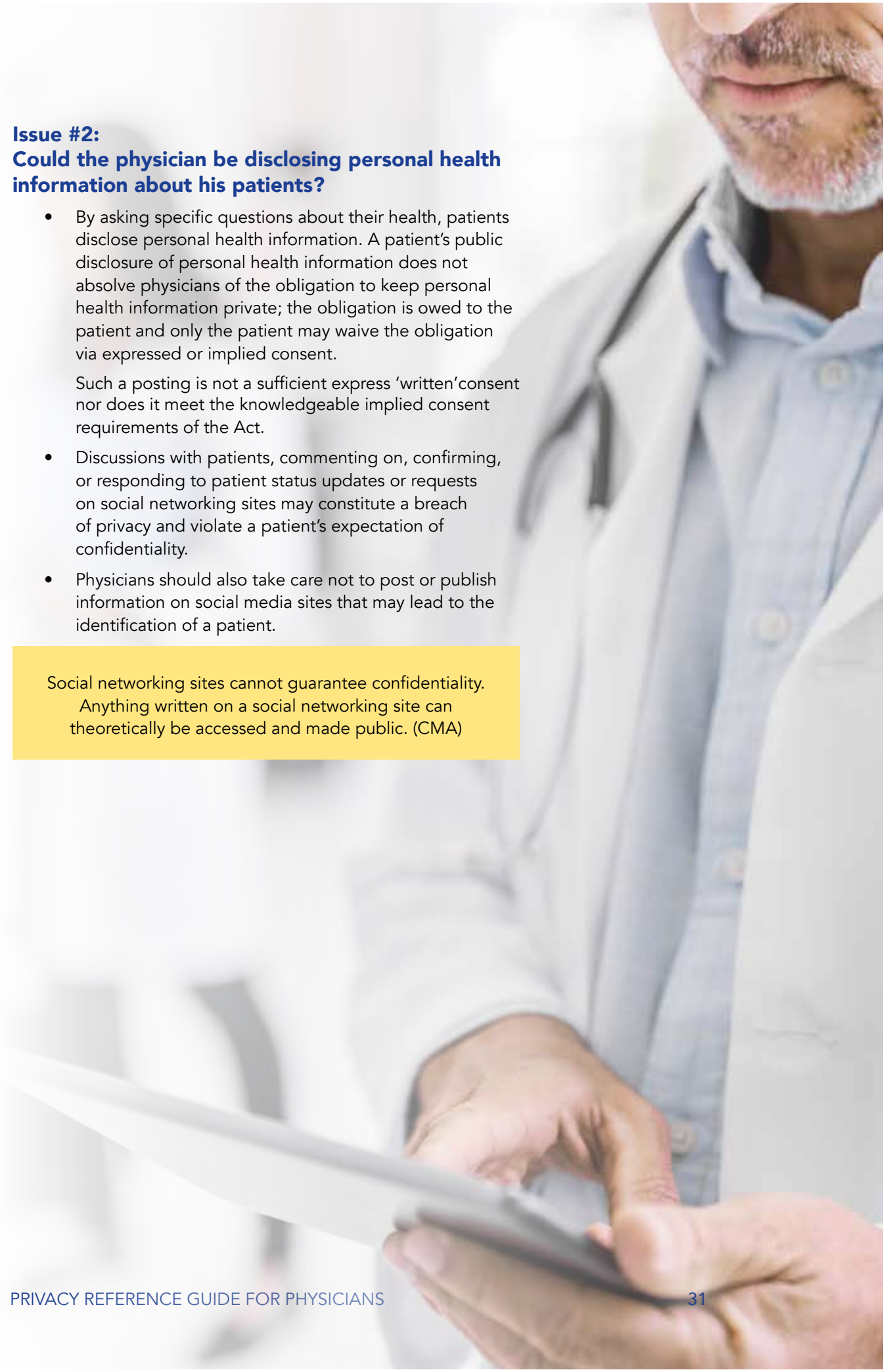
Privacy issues to consider

1. What policy and ethical obligations arise?
2. Could the physician be disclosing personal health information about his patients?

Guidance for Physicians

Issue #1: What policy and ethical obligations arise?

- Physicians should remember to separate personal and professional lives when using social networking sites and should respect and enforce professional boundaries.
- Electronically "friending" or communicating with patients through social media sites may extend the scope of professional responsibility. Physicians should maintain professional boundaries in the use of electronic media by refraining from accepting a friend request from a patient on Facebook or making a comment on a patient's Facebook post or group.
- When communicating through social media, physicians should recognize ethical and legal obligations to maintain patient privacy and confidentiality at all times. The Canadian Medical Association's Code of Ethics suggests that physicians should avoid public discussions or comments about patients that could reasonably be seen as revealing confidential or identifying information.
- Physicians should assume that all content on the Internet is public and accessible to all. Remember that words written on social networking sites have the potential to live on forever.
- Horizon's Social Media Policy discourages 'friending' of patients on social media sites. Staff in patient care roles generally should not initiate or accept friend requests except in unusual circumstances where a friendship may pre-date a treatment relationship.



Issue #2:
Could the physician be disclosing personal health information about his patients?

- By asking specific questions about their health, patients disclose personal health information. A patient's public disclosure of personal health information does not absolve physicians of the obligation to keep personal health information private; the obligation is owed to the patient and only the patient may waive the obligation via expressed or implied consent.

  Such a posting is not a sufficient express 'written'consent nor does it meet the knowledgeable implied consent requirements of the Act.
- Discussions with patients, commenting on, confirming, or responding to patient status updates or requests on social networking sites may constitute a breach of privacy and violate a patient's expectation of confidentiality.
- Physicians should also take care not to post or publish information on social media sites that may lead to the identification of a patient.

Social networking sites cannot guarantee confidentiality. Anything written on a social networking site can theoretically be accessed and made public. (CMA)

Examples related to privacy and environment

Case 11 – Private conversations with patients

Situation

A physician is having a private conversation with the mother of a patient who has just been admitted to hospital. The conversation occurs in the waiting area of the Emergency Department and although he describes the patient's condition to the mother in a fair degree of detail, the physician is careful not to mention the patient's name. He is heard saying "he's only 16 years old, these types of skull fractures heal quickly, but it may be a few months before he's back in nets".

The next day, the headline in the paper is "rookie Wildcats' hockey goalie suffers head injury; out for the season". The mother makes a complaint to the hospital alleging a breach of privacy.

Privacy issues to consider

1. Did a privacy breach occur?
2. If so, what could have been done to prevent the breach?

Guidance for Physicians

Issue #1: Did a privacy breach occur?

- Yes. A privacy breach occurred in this situation because personal health information was disclosed (in this case overheard) by a third party.

Issue #2: What could have been done to prevent the privacy breach?

- In this case, there may be steps that both Horizon and the physician could have taken to prevent the privacy breach. It will be important to review the factors that contributed to the breach and put constructive measures in place to prevent recurrence.
- Physicians and all staff are responsible to take reasonable precautions to ensure that conversations regarding patient information are not inadvertently overheard by others within hearing distance. For example, physicians should be cautious if discussing matters of personal health with patients in emergency room areas, or if a conversation is taking place with staff close to a reception area. If possible, the physician should try to find a private area to discuss the patient's health information. If it is necessary to communicate information about a patient in an

open area where others may overhear, physicians should make sure that they convey only the least amount of information needed, to reduce the likelihood that others may identify the patient.

- Physicians may identify potential deficiencies or limitations in the physical environment that may pose the risk of a privacy breach occurring when they are discussing personal health information with patients or colleagues. In these cases, they are encouraged to discuss their concerns with Medical Staff Administration and/or the Chief Privacy Officer to identify measures that could be taken to reduce the risk of privacy breaches.

Case 12 – Communicating urgent diagnosis

Situation

A physician needs to communicate a diagnosis and the need for an emergency procedure to a patient as quickly as possible and has been unable to reach the patient by phone. The physician would like to leave a voice mail message at the patient's home, or at least leave a message with the patient's spouse if she answers the phone.

Privacy issues to consider

1. Will leaving a voice mail in this situation result in a privacy breach?
2. Is the patient's spouse a member of the patient's circle of care?
3. Is the patient's spouse a substitute decision maker?
4. What other options might be available to the physician for contacting the patient?

Guidance for Physicians

Issue #1: Will leaving a voice mail message in this situation result in a privacy breach?

- Physicians should be aware that when leaving voice messages for patients, more than one person in a home or an office may access messages.
- Conveying a patient's diagnosis and need for a medical procedure to the patient's spouse or another individual in the home who may have access to the answering machine or telephone voice messaging system constitutes a disclosure of the patient's personal health information, for which consent is generally required under the legislation.
- If the physician does not have consent for this disclosure, and personal health information is retrieved from the voice mail message by a spouse or another person in the home, this would normally constitute an unauthorized disclosure of personal health information.
- In exceptional circumstances, where the physician reasonably believes that disclosing personal health information to the spouse by leaving a message is necessary to prevent or reduce a risk of serious harm to the health or safety of the patient, the Act provides an exception and allows the physician to communicate the urgent need for the emergency procedure to the spouse or other family member without the patient's consent. Even when the Act allows for this disclosure to occur without consent, the physician is still obligated to ensure he discloses only the minimum amount of personal health information needed to urgently convey the need for the patient to receive emergency medical attention.

Issue #2:
Is the patient's spouse a member of the patient's circle of care?

- No. The patient's spouse is not part of the circle of care. The physician may not rely on implied knowledgeable consent to disclose personal health information to the spouse; disclosure of personal health information to the spouse is not required for providing health care to the individual.

Issue #3:
Is the patient's spouse a substitute decision maker?

- If the patient is capable of granting, withholding or withdrawing consent to the collection, use or disclosure of personal health information, then the spouse is not a substitute decision maker unless the spouse has been granted authority in writing to act on behalf of the patient in this regard.

Issue #4:
What other options might be available to the physician for contacting the patient?

- Physicians wishing to communicate with patients by telephone should consider obtaining written consent to use this method of communication with patients, including leaving messages.
- Even with this consent, physicians are advised to exercise caution regarding the content of any messages left for patients. It is acceptable for messages to contain the name and contact information of the physician or the physician's office. However, messages should not contain any personal health information of the patient, such as details about the patient's medical condition, test results or other personal matters, because it is unclear who may be checking the voice mail messages.

Case 13 – Police inquiry in Emergency Department

Situation

A patient with a stab wound arrives at the Emergency Department after midnight. The patient is immediately admitted and treated by the physician on call. An hour later police arrive at the Emergency Department inquiring if anyone has been treated for stab wounds during the shift. The police officers do not have a subpoena or search warrant.

Privacy issues to consider

1. Under what circumstances, if any, may the identity of the stab wound victim be disclosed to police?

Guidance for Physicians

- In the Emergency Department, if the Law Enforcement Agency does not have the patient's name but is seeking a patient based on a description of injury, date or time, staff are not able to release information without a search warrant or production order.
- Inquiries from law enforcement agencies requesting contact with any patient, access to patient information or access to staff for any purpose (i.e., delivery of subpoenas, arrest warrants, and/or collection of evidence) are directed to Security Services (where available) or the facility duty officer.
- Reporting a gunshot or stabbing wound is not mandatory in New Brunswick. If the physician assesses that disclosure is required to prevent or reduce a risk of serious harm to the mental or physical health or safety of the individual or to another individual, or to prevent or reduce the risk of significant harm to the health or safety of the public or a group of people, the law enforcement agency may be contacted to reduce the risk of harm.
- If the above conditions are not present, then a signed Authorization for Release of Health Information, a court order/search warrant or production order is required for the release of personal health information.

Examples related to secondary uses of personal health information - research, education, quality management

PHIPAA permits custodians to use personal health information for the purpose for which it was collected or created, with the consent of the individual, or for other uses specifically permitted by the Act. These other uses are examples of 'secondary uses' and include research, education/teaching and quality improvement. Common scenarios involving secondary uses of personal health information are discussed in this section of the guide.

Case 14 – Accessing patient records for clinical trial

Situation

A physician has been approached by a pharmaceutical company to conduct a clinical trial of an experimental treatment drug for dementia. The physician would like to trial the new drug with 30 patients with dementia. He asks a member of the health records/decision support team within Horizon to construct a report to identify potential candidates for the new drug based on specific criteria. He reviews the list, and pulls up the Meditech patient files for the potential candidates to confirm that they would be eligible. Several patients on the list are already patients he is treating. He updates the list and instructs his assistant to pass the names of potential participants to the study's research assistant (RA), who will contact patients to assess interest in participating in the trial.

Privacy issues to consider

1. Will the physician be considered part of the circle of care for the patients' records he accesses for the purpose of confirming who would benefit from the clinical trial of the experimental drug?
2. Is patient consent required before the physician may access the patients' personal health information for the purpose of confirming whether they would benefit from the new experimental drug?
3. Would providing the names of potential patients who might benefit from the experimental drug to the Research Assistant constitute a breach of privacy? What if the physician hires a nurse on contract to play the same role as the research assistant?
4. What process could be followed that would allow patient contact information to be shared with the Research Assistant?
5. What other approvals must the physician obtain before accessing and using the patient files for this clinical trial?

Guidance for Physicians

Issue #1:
Will the physician be considered part of the circle of care for the patients' records he accesses for the purpose of conducting the clinical trial of the experimental drug?

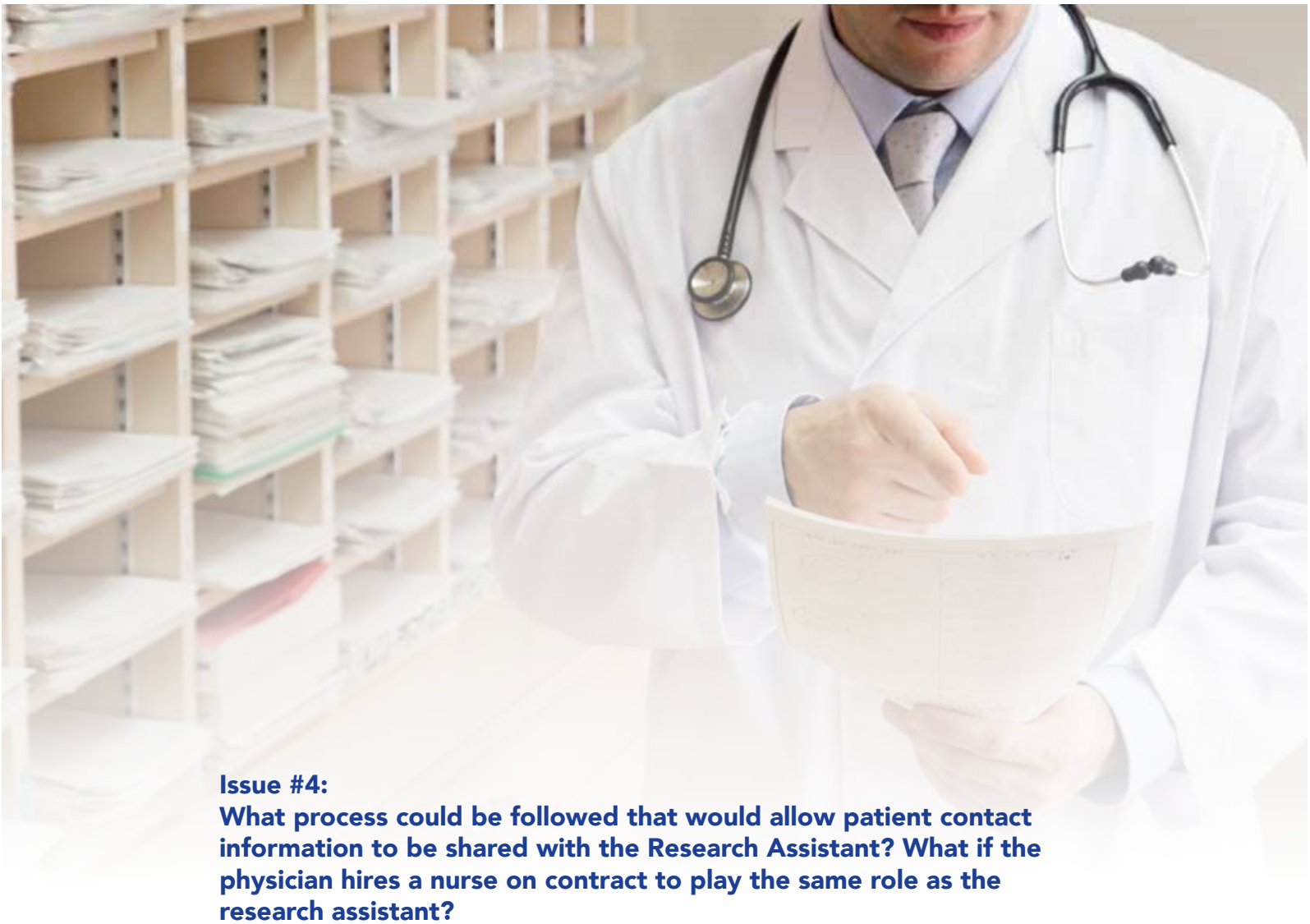
- If the physician accesses the records of patients with whom he has an existing care relationship for the purpose of determining whether they would benefit from the new drug, this access would be considered a continuation of the care and treatment he is providing to those patients. The physician would be in the circle of care for those patients.
- The physician is not acting as a member of the circle of care for the other patients with whom he has no existing care relationship, as he is accessing these patients' records for the primary purpose of conducting research, and not for providing health care. Therefore, the physician cannot rely on these patients' implied knowledgeable consent to access their health records for the purpose of identifying whether they would benefit from the clinical trial.

Issue #2:
Is patient consent required before the physician may access the patients' personal health information for determining whether they would benefit from the new experimental drug?

- The physician conducting the clinical trial can rely on the implied knowledgeable consent of only those patients with whom he has an existing care relationship to access their personal health information. On this basis, he may access basic diagnostic information necessary to determine if the patients would benefit from participating in the trial.
- The physician is not permitted to access the health record of prospective study participants (patients) with whom he has no existing care relationship, unless these patients have provided express (written) consent for the physician to access their record.

Issue #3:
Would providing the names of potential patients who might benefit from the experimental drug to the Research Assistant constitute a breach of privacy?

- Yes. The physician cannot disclose the patient's personal health information (a diagnosis of dementia) to the drug company's research assistant without first obtaining these patients' express (written) consent to do so. The research assistant is not in the patients' circle of care and the personal health information is being disclosed for a purpose unrelated to the patients' health care or treatment (conducting research). Note that if the physician hired a nurse on contract to be the research assistant for this study as opposed to the research assistant from the drug company, the same rule applies because the disclosure of the personal health information is primarily for research purposes. In summary, the disclosure of personal health information (contact information and diagnosis) must be to another custodian (or an agent of the custodian) and it must be for primarily for providing health care.



Issue #4:
What process could be followed that would allow patient contact information to be shared with the Research Assistant? What if the physician hires a nurse on contract to play the same role as the research assistant?

- The physician conducting the trial may contact his own patients, introduce the clinical trial and obtain express (written) consent to share their contact information with the research assistant for participating in the trial. Alternatively, after introducing the trial, if the patient is interested in participating, the patient could be given the research assistant's contact information to follow up directly.
- For other prospective patients, participation in the study would have to be initiated by these patients' treating physicians, using the same process.

Issue #5:
What other approvals must the physician obtain before using or disclosing information in the patient files for this clinical trial?

- Physicians are not permitted to use or disclose personal health information for research purposes without first consulting with Horizon's Department of Research Services and/or the Horizon Chief Privacy Officer, who will advise on the specific legal requirements that must be met before undertaking any proposed research activities using patient information. Each proposed research project within Horizon must meet strict requirements outlined in *PHIPAA* respecting the use and disclosure of personal health information for research purposes, including (but not limited to) approval of the proposed research project by Horizon's Research Ethics Committee, compliance with Horizon privacy policies and with the Tri-Council Policy.

Case 15 – Communicating research findings containing personal health information

Situation

A physician has recently acted as a researcher in a clinical trial within Horizon for patients with advanced multiple sclerosis. The trial has gone well and the research team, led by the physician, wishes to communicate the research findings hospital wide, and potentially publish the study. The study's screening criteria included age, gender, geographic area, physical symptoms, and medications. The researcher is preparing to communicate and publish his research findings and wants to know what to keep in mind.

Privacy issues to consider

1. Given these screening criteria, is there a risk that study participants could be identified from the research results? What should be done to prevent this?

Guidance for Physicians

- Physicians must ensure that personal health information of study participants who have provided their consent to participate in the study is protected and not disclosed outside of the research team.
- 'Identifying information' is information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual. Individuals may be able to be identified without disclosing their actual names. For example, it is reasonable to expect that a single individual or even a very small group of individuals with certain characteristics (e.g. advanced multiple sclerosis, female, of a certain age or geographic location) may be able to be identified.
- Research findings should be published in de-identified form. De-identified, when referring to personal health information, means personal health information from which all identifying information has been removed.
- To reduce the risk of inadvertent disclosure of personal health information, best practices dictate that data sub-sets or table cells with five or fewer individuals should not be published due to the risk that individuals may be able to be re-identified.
- Physicians acting as researchers for approved research projects within Horizon should document the plan for publication of research findings. This plan should be reviewed and approved by the Research Ethics Committee, in consultation with the Department of Research Services to ensure compliance with Horizon's privacy policies and with the Tri-Council Policy and to ensure that risks related to unauthorized disclosure are appropriately mitigated. Failure to do so may result in a privacy breach.

Case 16 – Rounds with medical students

Situation

A physician completes his rounds each day with a group of medical students. During this time, the medical students watch the physician treat the assigned patients and review the corresponding charts. Afterwards, the physician decides to search for and review several other charts for patients with similar health issues as one of the patients on his rounds. He intends to use the charts for educating the medical students.

Privacy issues to consider

1. Are the medical students considered to be in the circle of care for the patients on the physician's rounds?
2. Is the physician authorized to access the charts of the additional patients that are not on his rounds for the purpose of educating the medical students?

Guidance for Physicians

Issue #1:
Are the medical students considered to be in the circle of care for the patients on the physician's rounds?

- Physicians providing health care to patients on their rounds are within the patients' circle of care, and are entitled to access these patients' personal health information for the purpose of providing health care. Medical students working under the direction of physicians are in turn permitted to access personal health information of those patients for whom they are providing care on the rounds.

- Medical students may only access the patient files needed for the purpose of providing health care, under the guidance of physicians; they should not independently access patient files without authorization.
- Physicians may access the charts of patients that are on their rounds for the purpose of educating the medical students; for example, reviewing a patient chart with medical students who are simply observing the provision of care to the patient, as opposed to providing direct care.

Issue #2:
Is the physician authorized to access the charts of the additional patients that are not on his rounds for the purpose of educating the medical students?

- The physician does not have these patients' implied knowledgeable consent to access these charts as he is not doing so for the purpose of providing health care to these patients. If a physician intends to access the personal health information of other patients for educating the medical students, this should be done as part of a recognized Horizon continuing education/professional development program and it should be clear that access to the charts was required for this purpose.
- Consistent with the rule of minimums, physicians must ensure that only the minimum amount of patient information is accessed for the specific educational purpose identified and should, wherever possible, conduct these teaching activities without identifying individual patients.
- Physicians wishing to access personal health information of patients to which they are not actively providing care in any other circumstance should consult with the Chief Privacy Officer for Horizon to determine if such access is authorized under *PHIPAA*. Access to and use of personal health information under other circumstances may constitute a privacy breach.

Case 17 – Accessing patient health records for teaching purposes

Situation

Two surgeons are discussing a particularly unusual/interesting case with two new physicians as a teaching/mentoring opportunity and the patient's X-rays are reviewed. At one point, one of the treating surgeons mentions in passing, that 'Mrs. Jones' case is extremely unusual'.

Afterwards, one of the young physicians decides to conduct a search for Mrs. Jones' electronic health record to review the issues in more detail. This search returns many patients' records with the last name Jones. The physician reviews several of the records before finding the proper 'Mrs. Jones' and reviewing the case in detail.

Privacy issues to consider

1. Did a privacy breach occur when the two surgeons discussed the case with the two physicians?
2. Are the new physicians permitted to review the X-rays even though they are not treating Mrs. Jones?
3. Can the new physician access Mrs. Jones' records for strictly learning purposes?
4. Did a privacy breach occur when the young physician searched for the file? When he reviewed it?

Guidance for Physicians

Issue #1:
Did a privacy breach occur when the two surgeons discussed the case with the two physicians?

- It is not clear whether the new physicians have a role in providing health care to Mrs. Jones. If the new physicians are not providing health care to Mrs. Jones, then they do not 'need to know' the identity of Mrs. Jones in this scenario.
- To avoid a privacy breach, the surgeons should attempt to discuss the case for educational purposes without disclosing the identity of Mrs. Jones.

Issue #2:
Are the new physicians permitted to review the X-rays even though they are not treating Mrs. Jones?

- The surgeons are permitted to review the X-rays with the new physicians if this is part of the surgeons' role in educating the new physicians on providing health care. *PHIPAA* allows personal health information to be used in this manner if the use is limited to the minimum amount of information necessary to satisfy the educational purpose.

Issue #3:
Can the new physician access Mrs. Jones' records for strictly learning purposes?

- No. If the new physician is not involved in the care or treatment of Mrs. Jones, she cannot take it upon herself to search for or access Mrs. Jones' records for 'learning purposes'. This would constitute a privacy breach.

Issue #4:
Did a privacy breach occur when the young physician searched for the file? When he reviewed it?

- Yes. The process of searching for Mrs. Jones' record in the system for 'learning purposes' represents a privacy breach because the new physician a) was not authorized to access Mrs. Jones' file; and b) accessed the files of other patients for whom she had no care relationship in the process.
- Physicians should only search for the health records of patients with whom they have an existing care relationship.
- Wherever possible, physicians should use more granular search criteria such as Medicare Number to prevent many patients' records from being returned in the search. Best practice from the Meditech Training guide for identifying the correct patient suggests:
    - To identify the patient, the Medicare number should always be used as the first identifier if available.
    - If not available, then a combination of unit number and the full legal name of the patient should be used.
    - The exact date of birth and sex is required when using the legal name. The date of birth is entered as day/month/year.
    - When using the Medicare number or full legal name, select the patient from the Master Patient Index.

Case 18 – Physican researcher reviewing patient charts

Situation

A physician researcher is interested in understanding the impact of telehealth technology as a mechanism to conduct follow-up assessments for patients who have had coronary artery bypass grafting (CABG) surgery between January 2014 and January 2015. The study sample size is estimated at 80 patient charts. The researcher wants to compare outcomes of patients managed using telehealth technology with those seen through follow-up in the office. The outcomes are rate and type of post-operative complications and number and type of emergency room visits during the 60-day post-operative period.

The researcher states that it is impracticable to obtain consent from the patients to whom the information relates as it would involve too many resources to contact 80 patients and would place undue hardship on the physician researcher, which could jeopardize the research being undertaken. He has requested that Horizon Health Records/Decision Support compile a list of patients who fit the criteria, and plans to access the records of those patients directly to conduct the research. The data fields to be collected are: gender, age, date of surgery, complications pre-, peri- and post-operatively (up to 60 days), date of discharge, discharge disposition, type of follow-up (telehealth office) and number of emergency room visits. The researcher wishes to present his findings at an international cardiology conference in San Diego.

Privacy issues to consider

1. Can the researcher access and use personal health information of the 80 patients without their consent, for the purpose of conducting the research study?
2. What process must the physician researcher follow?
3. What must the researcher keep in mind when presenting his findings?

Guidance for Physicians

Issue #1:
Can the researcher access and use personal health information of the 80 patients without their consent, for the purpose of conducting the research study?

- The physician may only use personal health information collected for providing health care for a research purpose if the research project meets the specific criteria outlined in the PHIPAA. It is important to understand that *PHIPAA* requires that:
    - The research project be reviewed and approved by the Horizon Research Ethics Committee, in accordance with the Tri-Council Policy on Research; AND all the following criteria:
        - the research must be of sufficient importance to outweigh the intrusion into privacy that would result from the disclosure of the personal health information;

- the research purpose cannot reasonably be accomplished unless the personal health information is provided in a form that identifies or may identify individuals;
- the individuals to whom the information relates have consented to its use and disclosure or it is unreasonable or impractical for the person proposing the research to obtain consent from the individuals to whom the information relates; and
- the research project contains (i) reasonable safeguards to protect the privacy and security of the personal health information, and (ii) procedures to destroy the information or de-identify the information at the earliest opportunity, consistent with the purposes of the project.

- It is unclear from the information presented in this case whether:
  - the research is of sufficient importance to outweigh the intrusion into privacy that would result from the disclosure of the personal health information;
  - it is necessary to identify individuals to conduct the research;
  - it is unreasonable or impractical for the physician (or the physician's office) to obtain consent from the patients who may be impacted; and/or
  - adequate safeguards have or will be implemented by the physician to protect the privacy and security of the personal health information.

Issue #2: What process must the researcher follow?

- The physician researcher must prepare a written proposal and present the proposal for the Horizon Department of Research Services.
- The proposal must then be reviewed by the Horizon Research Ethics Board, who must determine if it meets the ethical requirements set out in the Tri-Council Policy Statement and the specific privacy and safeguard requirements set out in *PHIPAA*.
- The physician, in his capacity as a researcher (and not as care provider), is required to enter into an agreement with Horizon:
  - not to publish the personal health information requested in a form that could reasonably be expected to identify the individuals to whom the information relates;
  - to use the personal health information requested solely for the purposes of the approved research project; and
  - to ensure that the research project complies with the safeguards and procedures described in paragraph (3)(d).

Issue #3: What must the researcher keep in mind to present his findings?

- The physician is not permitted to publish personal health information in a form that could reasonably be expected to identify the individuals whose personal health information is included in the study.
- See the response to Case 16 on dissemination of research findings for more information.

Legislative and policy assessment

Legislative & policy considerations related to each case

For reference purposes, this section provides the legislative and policy considerations related to each case.

Case 1 – Informal 'curbside' consult

- *PHIPAA* S. 17(3) - Unless it is not reasonable in the circumstances to make the assumption, a custodian is entitled to assume that an individual knows the purpose of the collection, use or disclosure of the individual's personal health information by a custodian if the custodian posts or makes readily available a notice describing the purpose where it is likely to come to the individual's attention or provides the individual with such a notice.
- *PHIPAA* S. 18(1) - Implied knowledgeable consent - The physician is entitled to assume that she has the individual's implied consent, and to assume the consent is knowledgeable, to access the individual's personal health information for the purpose of providing health care to that individual.
- *PHIPAA* S. 32(3) - Need to know principle - requires Horizon to limit the use of personal health information it maintains to those employees and agents of the custodian who need to know the information to carry out the purpose for which the information was collected or received (for the provision of health care in this case) or to carry out any of the permitted uses authorized under Section 34.
- *PHIPAA* S. 32(2) - Rule of minimums - Every use by a custodian of personal health information must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used.

Case 2 – Physician on call

- *PHIPAA* S. 18(1) - Implied knowledgeable consent
- *PHIPAA* S. 34(1) - (Permitted uses of personal health information) - A custodian may use personal health information in its custody or under its control for one or more of the following purposes:
    - (a) for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, unless the individual expressly instructs otherwise;
    - (f) for the purpose of risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the custodian.
- *PHIPAA* S. 32(2) - Rule of minimums

- *PHIPAA* S. 3(2)(ii) - personal health information of deceased individuals is included in the scope of *PHIPAA*. The personal health information of deceased persons is only excluded from the Act if the individual has been deceased for 50 years.

Case 3 – Pathologist accesses records

- *PHIPAA* S. 18(1) - Implied knowledgeable consent
- *PHIPAA* S. 32(2) - Rule of minimums
- *PHIPAA* S. 32(3) - Need to know principle

Case 4 – Physician checking on former patient

- *PHIPAA* S. 18(1) - Implied knowledgeable consent
- *PHIPAA* S. 34 - Express consent is required when accessing personal health information for a purpose other than providing health care, unless the other use is specifically permitted under the Act.

Case 5 – Physician checking patient's drug use with a pharmacy

- *PHIPAA* S. 18(1) - The physician, the psychiatrist, and the pharmacist are all custodians or agents of custodians under *PHIPAA*. Unless it is clear from the circumstances that it is no longer reasonable to rely on the patient's continuing knowledgeable implied consent, a custodian is permitted to collect, use and disclose personal health information from another custodian or person if it is for the purpose of providing health care to an individual the custodian is currently treating.
- *PHIPAA* S. 18(2) - If it is clear that the patient has revoked their knowledgeable implied consent, the custodian cannot collect personal health information from another custodian.

Case 6 – Physician accesses her own record in the system

- *PHIPAA* S. 7(1) provides a legislated right of access on the part of an individual upon making a request to the custodian, to examine or receive a copy of his/her personal health information maintained by a custodian.
- Horizon's Access to and Release of Personal Health Information Policy outlines the accepted procedure for release of records within Horizon.
- *PHIPAA* S. 50 requires Horizon, as a custodian, to implement reasonable safeguards to protect personal health information from unauthorized access. Unauthorized access occurs whenever personal health information is accessed for a reason that is not permitted by *PHIPAA*.

Case 7 – Helpful neighbour

- *PHIPAA* S. 18(1) - Implied knowledgeable consent
- *PHIPAA* S. 32(3) - Need to know principle

Case 8 – Texting to communicate patient information

- *PHIPAA* S. 18(1) - Implied knowledgeable consent
- *PHIPAA* S. 32(3) - Need to know principle
- *PHIPAA* S. 50(1), 50(2) - Horizon is required, as a custodian, to protect personal health information against risks such as unauthorized access to or use or disclosure, secure destruction or alteration of the information, by ensuring nationally or jurisdictionally recognized information technology security standards and processes are in place, that are appropriate for the level of sensitivity of the personal health information to be protected.
- Horizon's Confidential Information Sharing Policy does not support this method of communication when confidential information is involved.
- Horizon's Appropriate Use of Wireless Communication Devices Policy restricts the use of personal wireless devices (i.e. smartphone) to locations within Horizon facilities that do not have local operational restrictions such as an Intensive Care Unit.
- Horizon is currently updating its policies on this topic.

Case 9 – Patient photos/images taken using a personal wireless device

- *PHIPAA* S. 1 – Definition of personal health information - includes identifying information about an individual related to the individual's physical or mental health, or related to the provision of health care to the individual.
- *PHIPAA* S. 1 – Definition of identifying information - Photos associated with a patient's health condition are considered personal health information of the patient if the photo identifies the individual or if it is reasonable to foresee that the photo could be utilized, either alone or with other information, to identify the individual.
- *PHIPAA* S. 27 - Even if they are later deleted, taking photos is a collection of the patient's personal health information. Horizon, a custodian under *PHIPAA*, is required to obtain patient consent prior to collecting a patient's personal health information and this consent must be knowledgeable.
- *PHIPAA* S. 50 - (safeguards) - Once collected, Horizon has an obligation to protect personal health information to the level required by legislation.

Case 10 – Social Media: Patient requests to 'friend' their physician

- *PHIPAA* S.1 - The identity of an individual's health care provider constitutes his or her personal health information.
- By acknowledging that he or she is the patient's physician online or by providing advice, the physician could be disclosing personal health information about the patient.
- Horizon's Social Media Policy
- *PHIPAA* S. 18; S. 19 – (Implied knowledgeable consent and Express Consent) - By asking specific questions about their health, patients disclose personal health information. A patient's public disclosure of personal health information does not absolve physicians of the obligation to keep personal health information private; the obligation is owed to the patient and only the patient may waive the obligation via expressed or implied consent. Such a posting is not sufficient express 'written' consent nor does it meet the knowledgeable implied consent requirements of the Act.

Case 11 – Private conversations with patients

- *PHIPAA* S. 1 – Personal Health Information includes 'identifying information' in both oral and recorded form.
- *PHIPAA* S. 1 - 'Identifying information' is 'information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual'. The fact that the physician described the patient as a 16 year old goalie with a skull fracture in a crowded waiting room, has likely contributed to identifying the individual, since someone in the waiting room may have had other information available to them – e.g. maybe they attended the hockey game and witnessed the accident.
- *PHIPAA* S. 19(1) requires express (written) consent for the disclosure of the individual's personal health information including when the custodian discloses information to

  (c) a visitor to a health care facility

Case 12 – Communicating urgent diagnosis

- Horizon's Confidential Information Sharing Policy
- Conveying a patient's diagnosis and need for a medical procedure to the patient's spouse or another individual in the home who may have access to the answering machine or telephone voice messaging system constitutes a disclosure of the patient's personal health information.
- *PHIPAA* S. 37(1) - Physicians may disclose an individual's personal health information if:

  (a) The individual or his/her substitute decision-maker is the recipient of the disclosure, or

(b) The individual or his/her substitute decision-maker consents to the disclosure.

- *PHIPAA S.* 39(1) - A custodian may disclose personal health information without the consent of the individual to whom the information relates if the custodian reasonably believes that the disclosure is required:

  (a) To prevent or reduce a risk of serious harm to the mental or physical health or safety of the individual to whom the information relates or another individual.

- *PHIPAA* S. 18(1) - Implied knowledgeable consent
- *PHIPAA* S. 19(1) requires express (written) consent – for disclosure of personal health information outside the circle of care.
- *PHIPAA* S. 1 - "Substitute decision-maker", in relation to an individual, means, unless the context requires otherwise, a person who is authorized under this Act to give, withhold or to withdraw consent on behalf and in the place of the individual with respect to the collection, use or disclosure of the individual's personal health information.

Case 13 – Police inquiry in Emergency Department

- *PHIPAA* S 39(1) - a custodian may disclose personal health information without the consent of the individual to whom the information relates if the custodian reasonably believes that the disclosure is required:

  (a) to prevent or reduce a risk of serious harm to the mental or physical health or safety of the individual to whom the information relates or another individual, or

  (b) to prevent or reduce a risk of significant harm to the health or safety of the public or a group of people, the disclosure of which is clearly in the public interest.

- *PHIPAA* S 40(1)(b) - A custodian shall disclose personal health information without the consent of the individual to whom the information relates (b) for the purpose of complying with a summons, subpoena, warrant, order or similar requirement issued by a court, person or entity with jurisdiction to compel the production of personal health information or for the purpose of complying with the Rules of Court concerning the production of personal health information in a proceeding.
- Horizon Draft Policy - Release of personal health information to Law Enforcement Agencies.

Case 14 – Accessing patient records for clinical trial

- *PHIPAA* S. 19 (1) - Unless otherwise provided in this Act, express consent of an individual is required in relation to the collection, use or disclosure of

his/her personal health information by a custodian, including when the custodian discloses information to:

(e) a person for the purpose of research.

- *PHIPAA* S. 34(1)(m) - A custodian may use personal health information for a research project, but only if the project has been approved by a research review body (research ethics committee);
- *PHIPAA* S. 43 - A custodian may disclose personal health information to a person conducting a research project only if the research review body has approved the project as having met the specific requirements outlined in the Act. These include but are not limited to ensuring that there are specific security safeguards in place to protect the personal health information that is the subject of the research project.
  *Must also comply with the Tri-Council Policy

Case 15 – Communicating research findings containing personal health information

- *PHIPAA* S. 43 requires custodians to ensure that research project adheres to reasonable safeguards to protect the privacy and security of the personal health information. This would include measures to ensure that study participants' privacy is protected, such that they are not able to be identified from within the published results.
- *PHIPAA* S. 35(1) prohibits disclosure of personal health information except as specifically authorized by *PHIPAA*.
- *PHIPAA* S. 36 allows a custodian to disclose personal health information that has been de-identified for any purpose.

Case 16 – Rounds with medical students

- *PHIPAA* S. 34(1) (g) allows a custodian to use personal health information for educating agents of the custodian to provide health care.
- *PHIPAA* S. 32(2) – Rule of minimums
- *PHIPAA S. 32(3)* – Need to know principle
- *PHIPAA* S. 18(1) – Implied knowledgeable

Case 17 – Accessing patient health records for teaching purposes

- *PHIPAA* S. 34(1) - A custodian may use personal health information in its custody or under its control for (g) educating agents of the custodian to provide health care.
- *PHIPAA* S. 32(2) - Every use by a custodian of personal health information shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is used.

- *PHIPAA* S. 32(3) - A custodian shall limit the use of personal health information it maintains to those employees and agents of the custodian who need to know the information to carry out the purpose for which the information was collected or received or to carry out any of the permitted uses authorized under Section 34.

Case 18 – Physician researcher reviewing patient charts

- *PHIPAA* S. 34(1)(m) - A custodian may use personal health information for a research project, but only if the project has been approved by a research review body (research ethics committee).
- *PHIPAA* S. 43 - A custodian may disclose personal health information to a person conducting a research project only if the research review body has approved the project as having met the specific requirements outlined in the Act, including:
    - the research project must be reviewed and approved by the Horizon Research Ethics Committee, in accordance with the Tri-Council Policy on Research;
    - the research must be of sufficient importance to outweigh the intrusion into privacy that would result from the disclosure of the personal health information;
    - the research purpose cannot reasonably be accomplished unless the personal health information is provided in a form that identifies or may identify individuals;
    - the individuals to whom the information relates have consented to its use and disclosure or it is unreasonable or impractical for the person proposing the research to obtain consent from the individuals to whom the information relates; and
    - the research project contains (i) reasonable safeguards to protect the privacy and security of the personal health information, and (ii) procedures to destroy the information or de-identify the information at the earliest opportunity, consistent with the purposes of the project.
- The physician, in his capacity as a researcher (and not as care provider), is required to enter into an agreement with Horizon:
    - not to publish the personal health information requested in a form that could reasonably be expected to identify the individuals to whom the information relates;
    - to use the personal health information requested solely for the purposes of the approved research project; and
    - to ensure that the research project complies with the safeguards and procedures described in paragraph (3)(d).

References

Horizon Policies

- Confidentiality (HHN-BD-007)
- Access to and Release of Personal Health Information (HHN-IM-004)
- Social Media (HHN-CO-006)
- Appropriate Use of Wireless Communication Devices (HHN-GA-011)
- Confidential Information Sharing (HHN-IM-003)
- Privacy Incident and Breach Management Policy *New

Horizon Health Network (Regional Health Authority) Bylaws, October 2013

Province of New Brunswick *Personal Health Information Protection and Access Act (PHIPAA)*,

http://laws.gnb.ca/en/showfulldoc/cs/P-7.05//20160929

Canadian Medical Association Code of Ethics (Privacy and Confidentiality Sections 31-37)

https://www.cma.ca/Assets/assets-library/document/en/advocacy/policy-research/CMA_Policy_Code_of_ethics_of_the_Canadian_Medical_Association_Update_2004_PD04-06-e.pdf

CMPA Good Practices Guide- Privacy and Confidentiality

https://www.cmpa-cpm.ca/serve/docs/ela/goodpracticesguide/pages/communication/Privacy_and_Confidentiality/privacy_and_confidentiality-e.html

Information and Privacy Commissioner of Ontario, Circle of Care- Sharing Personal Health Information for Health-Care Purposes, August 2015

https://www.ipc.on.ca/wp-content/uploads/Resources/circle-of-care.pdf

Canadian Nurses Protective Society

(https://www.cnps.ca/upload-files/pdf_english/mobile_devices.pdf)

CMPA reference: Using Email Communication with Your Patients: Legal Risks, revised May 2015 (Case 11)

(https://www.cmpa-acpm.ca/-/using-email-communication-with-your-patients-legal-ris-1)

CMA- Social Media and Canadian Physicians: Issues and Rules of Engagement (Case 10)

(https://www.cma.ca/Assets/assets-library/document/en/advocacy/CMA_Policy_Social_Media_Canadian_Physicians_Rules_Engagement_PD12-03-e.pdf)

CMPA template consent form (Case 11)

https://www.cmpa-acpm.ca/documents/10179/301287261/com_16_consent_to_use_electronic_communication_form-e.pdf

CMA Clinical vignettes re: Social Media and Canadian Physicians

(https://www.cma.ca/Assets/assets-library/document/en/advocacy/CMA_Social_Media-e.pdf)


RÉSEAU DE SANTÉ
Horizon
HEALTH NETWORK