

CMA POLICY SUMMARY

HEALTH INFORMATION PRIVACY CODE

This Code articulates principles for protecting the privacy of patients, the confidentiality and security of their health information and the trust and integrity of the therapeutic relationship. Its provisions are more exacting than those currently in place in the Canadian health care system. Although a patchwork of laws across Canada permit or require health information collection, use, disclosure and access without patient consent, or even knowledge, this Code would require that all of these laws and any proposed laws be reviewed for consistency with its provisions. Moreover, existing practices and initiatives concerning health information collection, use, disclosure and access, including health information systems or networks, may be contrary to patient expectations and the physician's duty of confidentiality. These practices and initiatives must also be reviewed for consistency with this Code. Many laws, practices and initiatives may not withstand the kind of scrutiny deemed necessary and reasonable for the protection of privacy and the trust and integrity of the therapeutic relationship.

CMA issues this Code in recognition that its implementation raises numerous issues and challenges, and that the changes it envisions will require time and the expenditure of resources. CMA appreciates that, given the complexity of the health care system, agreement and cooperation among a wide range of users and collectors of health information will be essential to the successful implementation of this Code. In view of these challenges, CMA issues this Code to the Canadian health care community at this time as an ideal to strive for, to guide and coordinate the efforts that need to be made to protect the privacy of patients, the confidentiality and security of their health information, and the trust and integrity of the therapeutic relationship. Moreover, this Code is issued in the understanding that those to whom it applies will not be able to achieve full compliance with its provisions until such time as numerous implementation issues have been clarified and resolved through cooperation and the coordinated efforts of many different stakeholders. Consequently, companion implementation documents are being developed that provide for a gradual implementation of the Code's provisions over a 5-year span and outline work that needs to be done to achieve the ideal it envisions.

Section A: Scope

This Health Information Privacy Code ("Code") has been produced by physicians to protect the privacy of their patients, the confidentiality and security of their health information, and the trust and integrity of the therapeutic relationship. This Code is based on the Canadian Standards Association's Model Code for the Protection of Personal Information ("CSA Code") as a sectoral code of the CSA Code. This Code provides instruction and guidance respecting health information collection, use, disclosure and access.

1. This Code describes the minimum requirements to pro-

tect the privacy of patients and the security and confidentiality of their health information.

2. This Code has been developed by physicians in their capacity as clinicians and in recognition of their principal obligation to patients.
3. This Code recognizes the potential benefits of the use of health information for secondary purposes, including teaching, research and system planning, and contains provisions to permit such use under clearly defined terms and conditions.
4. This Code has been developed as a sectoral code of the Canadian Standards Association's Model Code for the Protection of Personal Information and consequently

© 1998 Canadian Medical Association. Up to 10 copies of the full text of this policy summary may be made for noncommercial personal use, provided that credit is given to the original source. Any other use, including republishing or redistributing in any form or manner, in whole or in part, requires explicit permission from CMA.

Correspondence, requests for permission to republish or redistribute, and requests for additional copies should be addressed to the Member Service Centre, Canadian Medical Association, 1867 Alta Vista Dr., Ottawa ON K1G 3Y6; tel 888 855-2555 or 613 731-8610 x2307; fax 613 731-9102; cmamsc@cma.ca

All policy summaries of the CMA are also available electronically through CMA Online (www.cma.ca/policybase).

adopts the minimum standards contained in the CSA Code and augments them to meet the special circumstances of health information.

5. The development of this Code has been inspired by the report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, entitled *Privacy: Where Do We Draw The Line?*
6. The Code applies to all health information and to all individuals, groups or organizations that collect, use, disclose or access such information. Its objective is to instruct in the development and implementation of policies, practices, health information systems or networks, and legislation.
7. The principles that make up this Code are interrelated. Health information custodians adopting this Code shall adhere to these principles as a whole.
8. Health information custodians must subscribe to the principles contained in this Code and agree to uphold them, but may tailor this Code by modifying or adding principles, provided the changes afford no less protection to the privacy of patients and the confidentiality and security of their health information.
9. Statements containing “shall” or “must” indicate requirements that must be met by any health information custodian who wishes to adopt this Code and be recognized for having done so. The use of “should” indicates a recommendation or aspiration.

Section B: Definitions

The following definitions apply in this Code:

“Access” means the ability to acquire or possess health information in any information format.

“Accountability” means having clearly defined and understood responsibilities in connection with health information, agreeing to accept those responsibilities and being subject to appropriate sanctions for failing to fulfil accepted responsibilities.

“Authorized” means that which occurs with patient consent or within the provisions of this Code and applies to purposes, collection, use and disclosure of, or access to, health information.

“Authorized user” is someone permitted to collect, use, disclose or access health information under the provisions of this Code, who is properly instructed on his or her limits and responsibilities, and who can be held accountable for his or her compliance.

“Collection” means the act of accessing, receiving, compiling, gathering, acquiring or obtaining health information from any source, including third parties, and by any means. It includes information collected from the patient, as well as

secondary collection of this information in whole or in part by another provider or user.

“Confide” and “confided” mean the revelation of information by a patient within the therapeutic context.

“Confidentiality” and “confidential” mean that health information that is confided by a patient is to be kept secret and not disclosed or made accessible to others unless authorized by patient consent. A breach of confidentiality occurs whenever a health professional discloses or makes health information available to others without or inconsistent with the patient’s consent.

“Consent” means a patient’s informed and voluntary agreement to confide or permit access to or the collection, use or disclosure of his or her health information for specific purposes. “Express consent” is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the provider seeking consent. “Implied consent” arises where agreement may reasonably be inferred from the action or inaction of the individual and there is good reason to believe that the patient has knowledge relevant to this agreement and would give express consent were it sought.

“Disclosure” means the provision of health information to a third party for any reason, or making health information available for a third party to collect. It includes any transfer or migration of health information from one provider or user to another.

“Duty of confidentiality” means the duty of physicians and other health professionals in a fiduciary relationship with patients to ensure that health information is kept secret and not disclosed or made accessible to others unless authorized by patient consent.

“Emergency situations” means those instances when health care must be provided to preserve life or prevent severe harm to a patient who is unable, owing to the circumstances, to be cognizant of the context and whose surrogate is not immediately available to make decisions on the patient’s behalf.

“Fiduciary duty” means the obligation to act with the utmost good faith for the benefit of another.

“Health information” means any information about a patient that is confided or collected in the therapeutic context, including information created or generated from this information and information that is not directly or indirectly linked to the provision of health care. It includes all information formats.

“Health information custodian” means any organization or

institution that has custody, care or control of health information, and includes hospitals, regional boards, governments, corporations, and solo or group medical practices.

“Information format” means any form containing or recording health information, including:

- (a) a form that identifies or could identify a specific patient, either directly or indirectly;
- (b) a form that removes the link between the patient and information about him or her and which could, either directly or indirectly, be manipulated to reconnect the link between the patient and information about him or her (“deidentified–relinkable”);
- (c) a form that removes the link between the patient and information about him or her with the intent of preventing any reconnection of the link between the patient and information about him or her in accordance with recognized standards (“anonymous”); or
- (d) the composite form produced when health information is linked to any information about the patient from any other source, whether or not it is also health information.

“Integrity of health information” means the preservation of its content throughout storage, use, transfer and retrieval so that there is confidence that the information has not been tampered with or modified other than as authorized.

“Health professional” is any person having a fiduciary duty to patients who is registered and entitled by provincial or territorial law to practise or provide health care in that province or territory.

“Knowledge” means the patient’s awareness of what can or must happen with the health information he or she confides or permits to be collected.

“Linkage” is the joining together of health information with information from any other source or database, in whatever form. When health information is linked to any other information, the composite is also health information.

“Nonconsensual” collection, use, disclosure or access, whether justified or not, occurs without a patient’s consent and contravenes the patient’s right of privacy.

“Patient” means the person about whom health information is collected and, for the purposes of this Code, may also mean a surrogate or guardian acting on behalf of this person.

“Physician” means a person who is registered and entitled under the laws of a province or territory to practise medicine in that province or territory.

“Primary” means that which occurs for the therapeutic benefit of a particular patient. “Secondary” means not directly related to the therapeutic benefit of the particular patient from whom the information has originated.

“Purpose” means an end or aim for which health information is collected, used, disclosed or accessed. A description of purpose can be general enough to incorporate a range of like information uses provided that the generic description is sufficiently narrow and limited so as to communicate to the ordinary person a clear understanding of the potential information uses that could reasonably be expected to be relevant to their consent. The “primary therapeutic purpose” is the delivery of health care to a particular patient with respect to a particular and immediate health need or problem. It encompasses consultation with and referral to other providers on a need-to-know basis. A “primary longitudinal purpose” concerns developing composite health information about a particular patient, such as a detailed medical history, beyond direct application to any particular and immediate health need or problem, in order to enhance ongoing care to that person. “Secondary legislated purposes” have been subjected to the legislative test specified in this Code and have subsequently been written in law. “Secondary nonlegislated purposes” are any other purposes, such as education or research not governed by legislation, that meet the provisions of this Code and the secondary nonlegislative test provided by this Code.

“Provider” means a health professional or institution that delivers health care services or products in the therapeutic context.

“Right of privacy” includes a patient’s right to determine with whom he or she will share information and to know of and exercise control over use, disclosure and access concerning any information collected about him or her; it entails the right of consent. Nonconsensual collection, use, disclosure or access violates the right of privacy, even if it is justified.

“Security” means reasonable precautions, including physical and technical protocols, to protect health information from unauthorized collection, use, disclosure and access, and to ensure that the integrity of the information is properly safeguarded. A breach of security occurs whenever health information is collected, used, disclosed or accessed other than as authorized, or its integrity compromised.

“Sensitivity of health information” refers to the patient’s interest in keeping the information secret. It varies according to the nature of the information, its form, and the potential negative repercussions of its collection, use or disclosure on the patient’s interests.

“Therapeutic context” means a setting in which information

is confided by or collected from, about or on behalf of a patient who:

- (a) is in a therapeutic relationship with or under the care of a physician or health professional;
- (b) is resident in or seeking health care within a facility or institution whose principal purpose is the provision of health care, including physicians' offices, hospitals and other health care facilities;
- (c) confides information within a fiduciary relationship to a health care professional and with the belief that the health care professional will maintain its confidentiality, subject to very limited exceptions; or
- (d) confides information in the belief that it is necessary for the safe, timely and effective delivery of health care.

"Transparency and openness" are the characteristics of policies, procedures and practices that seek to ensure that patients know what can or must happen with the health information they confide or permit to be collected, used, accessed or disclosed.

"Use of health information" means any processing of health information including storage, retention, retrieval, manipulation, connection or linkage to other sources of information in any format.

Section C: Principles

Principle 1: The right of privacy

The right of privacy is fundamental in a free and democratic society. It includes a patient's right to determine with whom he or she will share information and to know of and exercise control over use, disclosure and access concerning any information collected about him or her. The right of privacy and consent are essential to the trust and integrity of the patient-physician relationship. Nonconsensual collection, use, access or disclosure violates the patient's right of privacy. The right of privacy is important and worthy of protection not just for the good of individuals in society but also for the good of society as a whole.

- 1.1 Canadians are entitled to expect and enjoy fundamental privacy rights and guarantees, which include:
 - (a) physical, bodily and psychological integrity and privacy;
 - (b) privacy of personal information;
 - (c) freedom from surveillance;
 - (d) privacy of personal communications; and
 - (e) privacy of personal space.
- 1.2 The basic duties owed to others to ensure that their privacy rights are adequately respected include:
 - (a) the duty to ensure consent;
 - (b) the duty to take all the steps necessary to respect ad-

equately others' privacy rights or, if their rights must be infringed, to interfere with privacy as little as possible;

- (c) the duty to be accountable;
 - (d) the duty to be transparent; and
 - (e) the duty to build privacy protection features into technological systems and designs.
- 1.3 The specific duties related to the protection of the patient's right of privacy in health information include:
 - (a) the duty to hold health care information in trust;
 - (b) the duty to limit information collection to what is necessary and justifiable for the benefit of the patient;
 - (c) the duty to ensure that patients are informed by reasonable means about purposes for collection, use, disclosure or access at or before the time of collection, including the potential for such to occur non-consensually;
 - (d) the duty to ensure that the information is accurately recorded;
 - (e) the duty to ensure consent by reasonable means, except in limited circumstances where the right of privacy and of consent are justifiably infringed by some compelling right, good or duty;
 - (f) the duty to ensure that the right of privacy and the right to consent are infringed no more than is necessary by the compelling right, good or duty;
 - (g) the duty to use and disclose health information only as consistent with the purposes identified at or before the time it was collected;
 - (h) the duty to keep health information only for as long as necessary to fulfil identified purposes;
 - (i) the duty not to disadvantage people because they elect to exercise their right of privacy; and
 - (j) the duty of physicians and other health professionals to hold information in confidence.
 - 1.4 Although the patient's interests and concerns about health information may vary depending on the sensitivity of the information, the right of privacy extends to all health information in whatever format.

Principle 2: Special nature of health information

Governing principles and rules for health information must recognize the patient's right of privacy in health information, its highly sensitive nature, the circumstances of vulnerability and trust under which it is confided or collected, and the fiduciary duties of health professionals in relation to this information. The patient-physician relationship as defined by trust and a professional promise of confidentiality is a societal good worthy of protection.

- 2.1 Principles and rules governing health information must recognize:
 - (a) its high level of sensitivity and protect the patient's right of privacy accordingly;

- (b) that the principal purpose for confiding and collecting this information is to benefit the patient;
 - (c) that in the therapeutic context patients may be vulnerable and under duress, and must not be subjected to manipulation, coercion or exploitation;
 - (d) that patients confide information to physicians and other health professionals under a very special trust, and that physicians and other health professionals have fiduciary duties to patients, including a duty to hold information in confidence.
- 2.2 Principles and rules governing health information must ensure that physicians and other health professionals can discharge their fiduciary duties and therefore shall take into account that:
- (a) patients may be in a situation of vulnerability owing to infirmity or incapacity, urgent need, lack of knowledge and power, or simply because they have needs and have to rely or depend upon providers to meet those needs;
 - (b) patients confide information that is ordinarily considered by them to be private because they have certain needs that require the care of a provider and believe the information is required by the provider to help meet those needs;
 - (c) were it not for those needs, and the expectation that the provider can help patients meet them, the occasion for the collection of the health information would not exist and the information would remain private;
 - (d) were it not for the reputation of health professionals for trustworthiness and the expectation that information disclosed to them will be held in confidence, patients would be less willing to confide health information fully and truthfully in the therapeutic context; and
 - (e) to the extent that provisions for health information inhibit patients from confiding health information fully and truthfully, their health care will be adversely affected.

Principle 3: Constraints on purposes and limitation on collection, use, disclosure and access

The principal purpose for the collection of health information is to benefit the patient who confides or permits information to be collected for a therapeutic purpose. Secondary purposes for the use of the information shall not be pursued if they inhibit patients from confiding information for the primary purpose, exploit patients' vulnerability, compromise the ability of physicians to discharge their fiduciary duties to patients or borrow on the trust patients invest in physicians for the primary therapeutic purpose. Collection, use, disclosure or access for secondary purposes shall be restricted to what is necessary for those purposes and shall not impede the confiding or collection of information for primary purposes.

Nonconsensual access to and collection, use or disclosure of health information is a violation of a patient's right of privacy, compromises the physician's duty of confidentiality and is potentially disruptive of the trust and integrity of the therapeutic relationship. Therefore, it must only occur in very limited circumstances — namely emergency situations, in accordance with legislation that meets the requirements of this Code, or in response to a court decision or order. Even consensual collection, use, disclosure or access may erode the right of privacy and the trust and integrity of the therapeutic relationship. Therefore, it must only occur with due consideration of possible negative impacts and with measures designed to maximize privacy protection.

- 3.1 Provided that the principles contained in this Code are adhered to, and in particular that the principles related to patient consent are rigorously applied, health information may be collected, used, disclosed or accessed for the following purposes:
- (a) Primary purposes:
 - (i) Primary therapeutic purpose is the initial reason for a patient seeking or receiving care in the therapeutic context, and pertains to the delivery of health care to a particular patient with respect to the presenting health need or problem. It encompasses consultation with and referral to other providers on a need-to-know basis.
 - (ii) Primary longitudinal purpose concerns developing composite health information about a particular patient, such as a detailed medical history, beyond direct application to the presenting health need or problem, in order to enhance ongoing care to that person.
 - (b) Secondary purposes:
 - (i) Secondary legislated purpose refers to health information collection, use, disclosure or access required or permitted by legislation or regulation that meets the provisions of this Code and the legislative test provided by this Code.
 - (ii) Secondary nonlegislated purpose is any other purpose, such as education or research not governed by legislation, that meets the provisions of this Code and the secondary nonlegislative test provided by this Code.
- 3.2 Health information collection, use, disclosure or access for the primary therapeutic and longitudinal purposes may be as extensive as necessary to fulfil these purposes and reflect the high level of trustworthiness and accountability of health professionals in the therapeutic context.
- 3.3 Health information collection, use, disclosure or access for any secondary purposes shall be as minimal as necessary in recognition of the need to protect the patient's right of privacy in the therapeutic context.
- 3.4 Health information collection, use, disclosure or access without patient consent shall only occur in the limited

circumstances provided by this clause. Nonconsensual health information collection, use, disclosure or access, including the conversion of health information from one information format to another, is a violation of a patient's right of privacy, may compromise the physician's duty of confidentiality, and is potentially disruptive of the trust and integrity of the therapeutic relationship. Therefore, it must only occur under strict conditions and in these very limited circumstances:

- (a) when permitted or required by legislation or regulation that meets the requirements of this Code; or
- (b) when ordered or decided by a court of law.

3.5 Any existing or proposed secondary purpose for health information collection, use, disclosure or access, including health information systems or networks, shall be subjected to a patient privacy impact analysis that shall include an evaluation of:

- (a) the likely impact of the proposed measures on the right of privacy of patients;
- (b) the likely impact of the proposed measures on the relationship between patients and their physicians, and in particular on the duty of confidentiality and the trust within this relationship;
- (c) the likely impact of the proposed measures on the willingness of patients to disclose health information;
- (d) the likely impact of the proposed measures on the ability of patients to receive health care; and
- (e) compelling evidence to demonstrate broad public support for the proposed measures.

3.6 Any proposed or existing legislation or regulation made under legislative authority that permits or requires health information collection, use, disclosure or access shall be subjected to the following legislative test:

- (a) There must be demonstration that:
 - (i) a patient privacy impact assessment has been conducted, the analysis has been made public and has been duly considered prior to the introduction of legislation;
 - (ii) collection, use, disclosure and access will be limited to the greatest degree possible to ensure that
 - the collection of health information by persons external to the therapeutic context will neither trade on nor compromise the trust of the patient-physician relationship;
 - patients are not likely to be inhibited from confiding information for primary purposes;
 - the ability of physicians to discharge their fiduciary duties to patients will not be compromised; and
 - patient vulnerability will not be exploited;
 - (iii) collection, use, disclosure and access will be restricted to what is necessary for the identified purpose(s) and will not impede the confiding or collection of information for primary purposes;
 - (iv) provisions exist for ensuring that patients are

provided with knowledge about the purpose(s) and that, subject to 3.6(b), patient consent is clearly voluntary;

- (v) the means used are proportionate and the collection will be limited to purposes consented to or made known to the patient;
- (vi) the patient's privacy will be intruded upon to the most limited degree possible in light of the purpose(s) consented to or made known to the patient;
- (vii) linkage of the health information will be limited; and
- (viii) unless clear and compelling reasons exist,
 - all reasonable steps will be taken to make health information anonymous; and
 - if it has been demonstrated that making health information anonymous would render it inadequate for legitimate uses, the information will be collected and stored in a deidentified-relinkable format.

(b) When nonconsensual collection, use, disclosure or access is permitted or required by legislation or regulation that meets the requirements of this Code, the following conditions must also be met:

- (i) the right of privacy has to be violated because the purpose(s) could not be met adequately if patient consent is required; and
- (ii) the importance of the purpose(s) must be demonstrated to justify the infringement of the patient's right of privacy in a free and democratic society.

(c) Any legislative provision or regulation that permits or requires health information collection, use, disclosure or access nonconsensually shall not, without compelling reasons, be applied retroactively to existing health information.

3.7 Any proposed or existing secondary nonlegislated purpose shall be subjected to the following nonlegislative test:

- (a) Before a health information custodian uses health information in its custody for secondary nonlegislated purposes, or before it releases or makes health information accessible to an external third party for secondary nonlegislated purposes, it must demonstrate or require the third party to demonstrate that:
 - (i) a patient privacy impact assessment has been conducted, the analysis has been made public, the results have been duly considered and uses for that purpose will not be pursued if there is an adverse effect on privacy;
 - (ii) collection of health information by persons beyond the therapeutic context will not exploit or compromise the trust of the patient-physician relationship;
 - (iii) patients are not likely to be inhibited from confiding information for primary purposes;

- (iv) the ability of physicians to discharge their fiduciary duties to patients will not be compromised;
 - (v) patient vulnerability will not be exploited;
 - (vi) collection will be restricted to what is necessary for the identified purpose(s) and will not intrude upon primary purposes;
 - (vii) patients will be fully informed of the purpose(s) and patient consent will be clearly voluntary;
 - (viii) patient privacy will be intruded upon to the most limited degree possible in light of the purpose(s) consented to;
 - (ix) linkage of health information will be restricted and consented to by the patient;
 - (x) unless clear and compelling reasons exist,
 - all reasonable steps will be taken to make health information anonymous;
 - if it has been demonstrated that making health information anonymous will render it inadequate for legitimate uses, then the information will be collected and stored in a de-identified–relinkable format;
 - (xi) any third party to whom health information is released has adopted this Code or has equivalent provisions in place; and
 - (xii) the purpose(s) will not be applied retroactively to existing health information unless patient consent is given.
- 3.8 Health information shall not be collected by means that are unlawful, unfair or exploit the patient's vulnerability, nor shall any of the patient's beliefs or potentially false expectations about subsequent collection, use, disclosure or access be exploited.
- 3.9 Courts of law should respect the provisions of this Code when issuing orders or decisions.
- 3.10 Health information shall be retained only as long as it is necessary to fulfil authorized purposes. Once the authorized purposes are fulfilled it shall be securely destroyed, unless some issue or decision related to the patient and pertinent to the patient's health information is pending.

Principle 4: Knowledge and specification of purpose, collection, use, disclosure and access

In the therapeutic context, health information is confided by or collected from patients under the patient's presumption that it is necessary to meet his or her therapeutic needs. The potential that health information, in whole or in part, may be subsequently collected, used, disclosed or accessed for other purposes without their consent, and what those purposes might be, must be made known to the patient by reasonable means before it is confided or collected for primary purposes. It is not acceptable to withhold such knowledge from patients deliberately out of concern that knowledge could inhibit them from confiding important information fully and truthfully.

- 4.1 A health information custodian must have documentation that lists all purposes for which it uses or discloses the health information it collects, including to whom it permits access to what information, in what format and whether consent is required.
- 4.2 Within the therapeutic context health information is confided or provided by patients in the knowledge or with the belief that it is necessary to achieve therapeutic purposes. Patients must be explicitly informed about any other purposes.
- 4.3 Health information must not be used for purposes not identified to the patient at or before the time it is confided or collected, unless patient consent is subsequently sought and obtained.
- 4.4 Patients must either have, or by reasonable means be provided with, knowledge about what can or must happen with their health information. The degree of detail or specificity of this knowledge is what could be presumed germane to the decision of a reasonable person in the circumstances of the patient.
- 4.5 Unless a particular patient has given indication to the contrary, the conveyance of generic information is a reasonable means of providing knowledge. When the preferences of a particular patient for being informed are known or can be reasonably inferred given his or her circumstances, the provision of knowledge should as much as possible be tailored to these known preferences.
- 4.6 The goal of providing knowledge to patients is to ensure that before they confide information or permit information to be collected they actually understand what can or must subsequently happen with their information, particularly without their consent.

Principle 5: Consent

The patient's ability to decide with whom he or she will share information is crucial for the protection of the right of privacy and for the preservation of trust in the therapeutic context. Only the patient's consent to health information collection, use, disclosure and access for the primary therapeutic purpose can be inferred. Except for the very limited nonconsensual purposes addressed in this Code, any other collection, use, disclosure or access requires express consent. Non-consensual collection, use, disclosure or access infringes the right of privacy and compromises the trust of the fiduciary relationship. To satisfy the requirement that consent be informed, the patient must have, or by reasonable means be provided with, knowledge about the potential for subsequent nonconsensual collection, use, disclosure or access before he or she confides any information.

- 5.1 Except for the very limited conditions set out in 3.4 concerning nonconsensual collection, use, disclosure or access, consent is required for health information collection, use, disclosure or access for any purpose.

- 5.2 For the purposes of this Code, consent for health information collection, use, disclosure or access in emergency situations is deemed to have been given to the extent necessary to allay the emergency as consistent with legal principles governing emergency medical care. The protection accorded this information shall be consistent with the provisions of this Code.
- 5.3 Consent to health information collection, use, disclosure and access for the primary therapeutic purpose may be inferred. Consent to subsequent collection, use, disclosure and access on a need-to-know basis by or to other physicians or health providers for this purpose, and for this purpose alone, may be inferred, as long as there is no evidence that the patient would not give express consent to share the information.
- 5.4 Interpretation of "need-to-know" shall be guided by consideration of what the reasonable person in similar circumstances would expect, or otherwise authorize by his or her consent. If expectations are unclear or ambiguous, care should be taken to ascertain those expectations and to make the flow of information among providers in the therapeutic context consistent with those expectations.
- 5.5 Consent to collection, use, disclosure and access for longitudinal primary purposes must be express unless the provider has good reason to infer consent.
- 5.6 For the purposes of this Code, disclosure of health information to the patient's relatives or significant others is recognized as assisting in primary purposes. Consent to this disclosure must be express unless the provider has good reason to infer patient consent.
- 5.7 Consent can only be inferred in the case of primary purposes, and for primary purposes alone; collection, use, disclosure or access thus authorized must be limited either to the known expectations of a particular patient or to what the reasonable person in similar circumstances would likely believe necessary to receive health care.
- 5.8 Implied consent does not deprive the patient of the right to refuse consent or the right to challenge the provider's finding of implied consent.
- 5.9 Patient consent for secondary nonlegislated purposes shall be express, voluntary and fully informed.
- 5.10 Where express consent is required, patients must be informed of their right to refuse consent. It is not acceptable to compromise care deliberately as a consequence of the patient's refusal to provide express consent or to exploit any fear the patient might have that this could occur.
- 5.11 Consent shall not be obtained by coercion, deception or manipulation. Failure to inform the patient by reasonable means of relevant information pertinent to consent invalidates this consent.
- 5.12 Although all health information is sensitive and should be treated as such, the more sensitive the health information is likely to be, given what is known about the

circumstances or preferences of the patient, the more important it is to ensure that consent is voluntary and informed.

Principle 6: Individual access

Patients have the right of access to their health information. In rare and limited circumstances, health information may be withheld from a patient if there is a significant likelihood of a substantial adverse effect on the physical, mental or emotional health of the patient or substantial harm to a third party. The onus lies on the provider to justify a denial of access.

- 6.1 The patient is entitled to know about, and subject to 6.5 to have access to, any information about himself or herself under the custody of the health information custodian.
- 6.2 Patients should be informed that they have the right to access their health information, to read it and to have copies of it.
- 6.3 Patients who wish to access their information should be given the opportunity to do so with explanation from a health professional who is knowledgeable about this information and capable of interpreting it for the patient.
- 6.4 Patients must be able to receive copies of their health information at a reasonable cost that does not exceed the cost of providing the information.
- 6.5 Providers may, in rare and limited circumstances, withhold health information from a patient if there is a significant likelihood of a substantial adverse effect on the physical, mental or emotional health of the patient or substantial harm to a third party. The onus is on the provider to justify a denial of access.
- 6.6 Patients are entitled to know who has gained access to their health information and for what purposes.

Principle 7: Accurate recording of information

Accurate recording is important to protect the patient's right of privacy and to meet the purposes for its collection, use, disclosure or access.

- 7.1 Health information shall be recorded as accurately as possible, and shall be as complete and current as necessary for authorized purposes.
- 7.2 The recording of statements of fact, clinical judgements and determinations or assessments should reflect as nearly as possible what has been confided by the patient and what has been ascertained, hypothesized or determined to be true using professional judgement.
- 7.3 Patients who have reviewed their information and believe it to be inaccurately recorded or false have the right to suggest amendments and to have their amendments appended to the health information.
- 7.4 Whenever possible, health information should be

recorded in a form that allows for authorized secondary purposes consented to by the patient. Any standardization of recording requirements relevant to subsequent secondary purposes shall not impede recording of information for primary purposes.

Principle 8: Security

Security safeguards must be in place to ensure that only authorized collection, use, disclosure or access occurs. Such safeguards must also assure the integrity of the available information.

- 8.1 Health information, regardless of the information format, shall be protected by security safeguards to ensure compliance with the provisions of this Code.
- 8.2 The development of security safeguards with respect to levels of access for various users shall recognize the differences in the sensitivity of health information and permit access accordingly.
- 8.3 Security safeguards shall impede as little as possible health information collection, use, access and disclosure for primary purposes.
- 8.4 A health information custodian shall ensure that persons are able to collect, use, disclose or access health information in its control only as authorized. Persons thus authorized must have a clear understanding of the authority, parameters, purposes and responsibilities of their access, and of the consequences of failing to fulfil their responsibilities.
- 8.5 An authorized person's access to health information, including persons or groups external to the health information custodian, shall be limited to only the information needed for the authorized purpose(s), in the least intrusive format.
- 8.6 Security safeguards shall include both physical and human resource safeguards to prevent unauthorized health information collection, use, disclosure and access. Physical security measures include such safeguards as locked filing cabinets, restricted access to certain offices or areas, and the use of passwords, encryption and lock-boxes. Human resource security measures include security clearances, sanctions, training and contracts.
- 8.7 Health information custodians must protect health information in their custody so as to ensure its integrity and have assurance that the integrity of information received from other health information custodians has been similarly safeguarded.
- 8.8 Security safeguards should incorporate identification, authentication, information integrity/availability and non-repudiation, as appropriate.

Principle 9: Accountability

Accountability is owed first and foremost to the patient.

Health information custodians must have in place policies and procedures that recognize this principal accountability and health professionals' duty of confidentiality to the patient. Anyone a health information custodian authorizes to have access to health information must be capable of being held accountable for his or her actions. In addition, health information custodians must designate a qualified person responsible and accountable for monitoring and ensuring internal compliance with this Code.

- 9.1 Health information custodians are responsible for the security of health information they collect, use, disclose or permit access to.
- 9.2 Health information custodians must ensure that persons, including administrative and technical support staff, receive authorization to access health information only as necessary to fulfil authorized purposes.
- 9.3 A health information custodian must ensure that anyone permitted to have access to health information has clearly defined and understood responsibilities in connection with health information, agrees to accept those responsibilities, and is subject to appropriate sanctions for failing to fulfil the accepted responsibilities.
- 9.4 Health information custodians must designate a qualified person responsible and accountable for monitoring and ensuring internal compliance with this Code. The designated accountable person shall have the autonomy, authority and resources necessary to ensure the health information custodian's adherence to the Code. In the case of small private practices, practitioners may designate themselves.
- 9.5 Policies and procedures to ensure compliance with this Code must consider the special, direct accountability of health professionals to their patients. The high level of trust vested in health professionals is crucial to the initial confiding of health information for the therapeutic purpose.
- 9.6 Health information custodians must ensure that third parties privy to health information have adopted this Code or are bound by equivalent provisions. Provided that this has been determined before health information is disclosed or made accessible, health information custodians are not accountable for the actions of third parties or for what subsequently happens to the information.
- 9.7 Although it is the responsibility of the health information custodian to ensure that patients are appropriately informed, secondary users whose information requirements impose a burden upon the health information custodian are responsible for covering their share of any related costs or resource requirements (e.g., preparation of brochures). Health information custodians may reasonably require secondary users to cover their own costs as a condition of making health information available to them as authorized.

Principle 10: Transparency and openness

Policies, procedures and practices relating to health information must be transparent so that patients can clearly understand the extent and circumstances of health information collection, use, disclosure and access. They must be explicit enough that patients are adequately informed and able to acquire knowledge germane to their confiding of information, and must be open to scrutiny and challenge.

- 10.1 Health information custodians must have transparent, explicit and open policies, procedures and practices, tailored to their practice setting, that seek to ensure that patients are provided with information about what can or must happen with their health information without their consent.
- 10.2 Policies, procedures and practices shall be as explicit as necessary to ensure that patients are aware of any considerations that could be relevant to deciding what information they elect to freely confide or consent to be collected, used, disclosed or accessed. Nothing must be left implicit that, if made explicit, could reasonably be expected to alter a patient's decision to freely confide information. Information about nonconsensual collection, use, disclosure and access must be made explicit.
- 10.3 Patients should be able to discuss the health information custodian's policies, procedures and practices concerning health information with a knowledgeable person and have specific questions about their own health information answered in a timely fashion.
- 10.4 A health information custodian's policies, procedures and practices shall ensure that patients can understand what might, can or must happen to their health information, that consent is sought as required by this Code and that nothing is left implicit or unknown to patients that if known or made explicit could reasonably be expected to alter a patient's decision to freely confide information.
- 10.5 Patients shall be able to challenge the health information custodian's compliance with the provisions of this Code by addressing their concerns to the designated accountable person.
- 10.6 Procedures shall be in place to receive and respond to complaints or inquiries about policies, procedures and practices relating to health information collection, use, disclosure and access. The complaint process must be easily accessible and simple to use.
- 10.7 Patients who make inquiries or lodge complaints shall be informed of the existence of relevant complaint mechanisms.
- 10.8 All complaints shall be investigated. If a complaint is found to be justified, appropriate remedial measures shall be taken such as amending policies, procedures or practices.

Section D: Health information policies

Health information custodians must have in place and implement policies, procedures and practices that give effect to the principles of this Code.

- 1.1 Health information policies, procedures and practices should be tailored to the specific health care setting of the custodian and shall address and provide for:
 - (a) complying with and giving effect to the principles of this Code;
 - (b) protecting the security of health information;
 - (c) ensuring the accurate recording and integrity of health information;
 - (d) documentation of all purposes for which the health information custodian uses or discloses the health information it collects, including to whom it permits access to what information, in what format and whether consent is required;
 - (e) documentation of what health information may be linked to other pieces of information;
 - (f) documentation of what health information is made available to third parties;
 - (g) allowing access only to authorized users in the appropriate format and for the limited purposes for which they are authorized;
 - (h) identification of the person who is accountable for the policies, procedures and practices and to whom complaints or inquiries can be made;
 - (i) receiving and responding to complaints and inquiries;
 - (j) ensuring that persons who collect, use, disclose or access health information can be held accountable and are under an enforceable duty to keep information secure;
 - (k) ensuring that persons who work for or in the health institution know and receive sufficient training about this Code and related institutional policies, procedures and practices to ensure accountability;
 - (l) the means of gaining access to one's own health information held by the health institution;
 - (m) making available information that a particular patient specifically requests or reasonably can be presumed to wish to know;
 - (n) ensuring that patients have, or by reasonable means are provided with, knowledge about their health information and that consent is sought and obtained as appropriate; and
 - (o) specification of minimum and maximum retention periods and rules for the succession, transfer and destruction of health information.
- 1.2 The health information custodian's policies must be readily available to patients and should include information about practices and procedures.