DoctorCare Privacy Statement

Last updated: April 2015

Introduction:

This Policy applies to personal health information that is regulated by the *Personal Health Information Protection Act, 2004* (PHIPA). The Policy's purpose is to ensure that the manner in which DoctorCare collects, uses, discloses, retains and disposes of personal health information (PHI) is in accordance with the requirements of PHIPA.

Under PHIPA, DoctorCare is subject to privacy requirements as an "agent" that handles personal health information on behalf of physicians, who are health information custodians.

DoctorCare receives from referring physicians personal health information that includes a patient's name, contact information, and other eligibility criteria as required for each particular healthcare program offered by the physician and supported by DoctorCare.

Physicians contracting with DoctorCare are health information custodians governed by PHIPA. As such, they have the first responsibility for protection of their patients' personal health information. However, DoctorCare assumes responsibility for the protection of personal health information that is given to our custody and control for the purposes of supporting our physicians' programs.

Protection of Personal Information and Personal Health Information is very important. This policy has been developed to:

- Provide direction and help employees, consultants, students, affiliates and other individuals having cause to work at DoctorCare understand their roles and responsibilities under PHIPA and how to comply.
- Provide direction to DoctorCare employees on confidentiality and the treatment of personal health information.
- Create a workable framework for physicians and clinics using DoctorCare services to ensure the protection of personal health information.

Policy Statement:

DoctorCare employees, consultants, students, and other individuals having cause to work at DoctorCare will demonstrate their respect for individual privacy rights and their compliance to legislation by following the rules for the collection, use, disclosure, retention and disposal of personal health information in accordance with the *Personal Health Information Protection Act, 2004* (PHIPA) and by adhering to all privacy and security policies, procedures, and guidelines.

Most privacy legislation is based on 10 internationally recognized "privacy principles" or fair information practices. DoctorCare's Privacy Policy has been organized according to these privacy principles, as follows:

Principle 1 – Accountability for Personal Health Information

DoctorCare is responsible for personal health information received from health care professionals making referrals into DoctorCare programs.

Accountability for DoctorCare's compliance with PHIPA rests with DoctorCare's Managing Directors. Individuals with privacy expertise have been appointed to provide leadership, direction and problem-solving for DoctorCare's privacy management initiatives. Furthermore, a Privacy and Security Committee provides guidance and input into the development of policies, procedures, guidelines and privacy practices.

The contact information for DoctorCare's Privacy Officer is a matter of public record, and is published on DoctorCare's website.

DoctorCare is responsible for personal health information in its custody and control, including information that might be transferred to a third party for processing. DoctorCare uses contractual agreements and/or other authorized means to ensure a comparable level of protection and accountability whenever it is necessary for a third party to handle such information.

Principle 2 – Identifying Purposes for Collecting Personal Health Information

DoctorCare collects personal health information from physicians for the purposes of supporting the physician's programs.

DoctorCare documents and informs health information custodians and the public of the purposes for which it uses personal health information. DoctorCare receives from a referring health information custodian, personal health information including a patient's name, contact information, health card number, and program eligibility, so that a consultation with a health care professional may be arranged.

When DoctorCare contacts individuals directly to obtain additional personal health information required for the purposes outlined above, persons collecting the personal health information explain to individuals the purposes for which the information is being collected.

When personal health information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified and will be explained to the individual before it is used. Unless permitted by law, the consent of the individual will be obtained before the information is used for a new purpose.

When DoctorCare conducts quality improvement activities such as patient satisfaction surveys and call-recordings, express consent is sought and patients are informed they do not have to participate.

Principle 3 – Consent for the Collection, Use, and Disclosure of Personal Health Information

When a patient is referred to a DoctorCare supported program for a consultation, obtaining consent for providing personal health information to DoctorCare rests with the referring health information custodians. DoctorCare can assume the consent of a patient when it receives a referral.

PHIPA requires that consent to the collection, use and disclosure of personal health information be "knowledgeable". DoctorCare expects that patients will understand that the referring health information custodian will forward their personal health information to DoctorCare if a referral has been made into the program. At or before the time of the appointment, DoctorCare provides every patient with information that outlines the purposes of the DoctorCare program. At that point, patients can discuss the purposes for which DoctorCare collects, uses and discloses personal health information.

DoctorCare respects an individual's right to withdraw consent, subject to legal or contractual restrictions and reasonable notice. DoctorCare will inform the individual of the implication of such withdrawal, including the fact that the withdrawal will not have retroactive effect.

DoctorCare respects an individual's right to place conditions on the use and disclosure of personal information, unless such conditions, for example, prohibit or restrict any recording of personal health information by a health information custodian that is required by law or by established standards of professional or institutional practice.

Principle 4 – Limiting Collection of Personal Health Information

DoctorCare will limit the collection of personal health information to what is necessary for its purposes unless required by law to collect additional information.

DoctorCare will collect information by fair and lawful means and will not collect personal health information indiscriminately.

Principle 5 – Limiting Use, Disclosure, and Retention of Personal Health Information

Personal health information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal health information will be retained only as long as necessary for the fulfillment of these purposes.

Should DoctorCare propose to use personal health information for a new purpose, it will document this purpose.

Unless law permits the new purpose, the consent of the individual is required before information can be used for that new purpose.

DoctorCare's policy on retention and destruction of personal health information in DoctorCare's custody and control is compliant with PHIPA and consistent with industry best practices.

DoctorCare employees, consultants, students and other individuals who have cause to work with DoctorCare will follow established procedures that govern the destruction of personal health information.

Principle 6 – Accuracy of Personal Health Information

DoctorCare will take reasonable steps to ensure that the personal health information that it uses and discloses is as accurate, complete and up-to-date as is necessary for the purposes that are known at the time of the disclosure; otherwise, DoctorCare must clearly set out for the recipient of the disclosure the limitation if any on the accuracy, completeness or up-to-date character of the information.

DoctorCare will make every effort to ensure that personal health information in its custody and control is accurate and complete. DoctorCare will not routinely update personal health information unless such a process is necessary to fulfill the purposes for which the information was collected.

Principle 7 – Safeguards for Personal Health Information

DoctorCare has administrative, technical and physical safeguards to protect personal health information under its custody and control.

The security safeguards protect personal health information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. DoctorCare protects personal information regardless of the format in which it is held.

DoctorCare has established an organization-wide security policy that describes the administrative, technical and physical safeguards it employs to protect personal health information in DoctorCare's custody and control.

The methods of protection include, but are not limited to:

a) administrative safeguards, for examples privacy and security policies, limiting access to information on a "need-to-know" basis, and
b) physical safeguards, for examples, locked filing cabinets and restricted access to offices, and
c) technical safeguards, for example, the use of passwords and encryption

DoctorCare makes its employees aware of the importance of maintaining the confidentiality of personal health information through the use of internal policies, as well as internal training. All staff, consultants, students, and any other person working at DoctorCare are required to sign a confidentiality agreement.

Principle 8 – Openness

DoctorCare makes readily available to individuals a written public statement about its policies and practices relating to the management of personal health information.

Contact information for DoctorCare's Privacy Officer is published on DoctorCare's website.

DoctorCare's Privacy Policy is also posted on DoctorCare's website. A hard copy of the Privacy Policy is also available to members of the public on request to DoctorCare's Privacy Officer.

Principle 9 – Individual Access to Personal Health Information

Upon written request, and provided that DoctorCare is authorized to provide this by law, an individual will be informed of the existence, use, and disclosure of his or her personal health information in control of DoctorCare and will be given access to this information either directly or through a health custodian. An individual will be required to provide sufficient information to permit DoctorCare to provide an account of the existence, use, and disclosure of personal health information. The information provided will only be used for this purpose.

DoctorCare will respond to an individual's access request within the response time provided in PHIPA (usually within 30 days) and at minimal cost to the individual. The requested information will be provided or made available in a form that is generally understandable.

When an individual successfully demonstrates the inaccuracy or incompleteness of personal health information, DoctorCare will amend the information as required by law. Amendments may involve the correction, deletion or addition of information. Where appropriate, the amended information will be transmitted to third parties having access to the information in question.

Principle 10 – Challenging Compliance

Any individual who wishes to challenge DoctorCare's compliance with the above principles or with PHIPA may contact DoctorCare's Privacy Officer. Instructions for making complaints are posted on DoctorCare's website and may be obtained through DoctorCare's Privacy Officer.

DoctorCare will inform individuals who make inquiries or lodge complaints of relevant complaint procedures.

DoctorCare will investigate all complaints. If a complaint is found to be justified, DoctorCare will take appropriate measures, including correcting the issue and, if necessary, amending its policies and practices.

Definitions:

Health Information Custodian (HIC)

A person or organization who has custody or control of personal health information as a result of, or in connection with, the person's or organization's power or duties. Health information custodians listed under the Personal Health Information Protection Act, 2004 include, among others health care practitioners, hospitals, long-term care facilities, laboratories, pharmacies, community care access corporations, the MoLTC, medical officer of health or a board of health, and community or mental health centers whose primary purpose is the provision of health care (the *Personal Health Information Protection Act, 2004*, s.3 (1).)

Agent in relation to a health information custodian means;
A person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated (the *Personal Health Information Protection Act, 2004*, s.2)

Personal Health Information (PHI)

Identifying information about an individual in oral or recorded form, if the information, relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family, relates to the providing of health care to the individual, including the identification of a person as provider of health care to the individual, is a plan of service within the meaning of the Long Term Care Act, 1994 for the individual, relates to payment or eligibility for health care in respect of 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 such body part or bodily substance, is the individual's health number or identifies an individual's substitute decision-maker (the *Personal Health Information Protection Act, 2004*, s.4 (1).)

Identifying Information

Means 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 and individual (the *Personal Health Information Protection Act, 2004*, s.4 (2).)

Privacy

Privacy is the right of an individual to control the collection, use and disclosure of personal information about him or herself (Canadian Institute for Health Information, 2002).

Confidentiality

Confidentiality refers to the obligation of an individual or organization to safeguard entrusted information. The ethical duty of confidentiality includes obligations to protect information from unauthorized access, use, disclosure, modification, loss or theft. Fulfilling the ethical duty of

confidentiality is essential to the trust relationship between researcher and participant, and to the integrity of the research project. (Government of Canada Panel on Ethics, 2003).

Security

Security is the protection of personal health information from unauthorized or unintentional loss, theft, access, use, modification or disclose (Canadian Institute for Health Information, 2002). Security involves the protection of computer hardware and software from accidental or malicious access, use, modification, destruction or disclosure. Security also pertains to personnel, data, communications and the physical protection of computer installations. (IEEE Standard Dictionary of Electrical and Electronic Terms).

----------END OF POLICY----------