



MedExtra Code for the Management of Personal Information Respecting Healthcare Clients

Based on the CSA Model for the Protection of Personal Information
CAN/CSA Q830-96

Code Last Revised:
September 2002

Responsibility:
Evan Savelson, Chief Privacy Officer

We hereby adopt the policies and procedures contained herein and confirm that the management is committed to ensuring that they are applied consistently across the Organization.

Jeffrey Brock, M.D.
President

Evan Savelson
Chief Privacy Officer

Controlled Copies Issued to the MedExtra Privacy Code Operating Committee:
Evan Savelson
Jeffrey Brock



1. Scope

This code is based on the CSA Model Code for the Protection of Personal Information (CAN/CSA-Q830-96). It describes how IcorpDigital.com Inc. dba MedExtra "MedExtra" subscribes to the principles of the CSA Model Code with respect to the Personal Information described in the Definitions below

1.1. Collection of Personal Information by MedExtra

MedExtra collects information concerning Clients and their various healthcare issues from the Clients themselves or Institutions or Healthcare Providers. The information may identify an individual Client; it may include the age and gender of a Client, office and home mailing addresses, and information concerning symptoms, diseases diagnosed or treated, treatments, Institutions/Healthcare Providers involved with the case.

1.2. Use of the Information by MedExtra

The information collected is used to help the Client identify a medically sound course of action and secure access to healthcare at preferred rates at/with Client-specified providers or facilities

1.3. Disclosure of the Information by MedExtra

MedExtra restricts access to its Client information to Healthcare Providers or Organizations involved in arranging the provision of healthcare for a specific Client.

2. Definitions

2.1. The following definitions apply in this code:

2.1.1. *Client* means an individual or Organization that enlists MedExtra to provide him/her/it care.

2.1.2. *Client Advocate* means someone engaged by MedExtra to provide non clinical assistance to Clients.

2.1.3. *Basic Information* refers to the MedExtra Patient Identification Form (attached).

2.1.4. *Case Information* means medical information pertaining to an individuals health.

2.1.5. *Case Manager* means someone engaged by MedExtra to provide clinical assistance to Clients.

- 2.1.6. *Collection* means the act of gathering, acquiring or obtaining personal information from any source, including third parties, by any means.
- 2.1.7. *Consent* means voluntary agreement with what is being done or proposed. Consent can be either express or implied. 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 Organization seeking Consent. Implied Consent arises where Consent may reasonably be inferred from the action or inaction of the individual.
- 2.1.8. *Disclosure* means taking Personal Information available to others outside the Organization.
- 2.1.9. *Healthcare Provider* means a professional in the field of medical care.
- 2.1.10. *Institution* means a facility at which Healthcare Providers provide medical care
- 2.1.11. *Organization* means any association, business, charitable Organization, club, government body, Institution, professional practice, union or other person or entity from which Personal Information is collected or to which Personal Information is disclosed.
- 2.1.12. *Personal Information* means information about an identifiable individual that is recorded in any form, including Basic Information and Case Information
- 2.1.13. *Use* means the treatment or handling of Personal Information within an Organization.

3. Principles

3.1. Principle 1 – Accountability

An Organization is responsible for Personal Information under its control and shall designate an individual or individuals who are accountable for the Organization's compliance with the following principles.

- 3.1.1. Accountability for MedExtra's compliance with the principles in this code rests with the Chief Privacy Officer of MedExtra, although other individuals within our Organization are responsible for the day-to-day Collection and processing of Personal Information. In addition, other individuals within our Organization, including members of the MedExtra Privacy Code Operating Committee, may be delegated to act on behalf of the Chief Privacy Officer of MedExtra.



3.1.2. The identity of the individuals designated by MedExtra to oversee our Organization's compliance with the principles will be made known upon request.

3.1.3. MedExtra is responsible for Personal Information in its possession or custody.

- a) MedExtra requires, as a condition of providing Personal Information to any Organization, that:
- b) such information shall not be transferred to any third party for processing, unless such third party has entered into an agreement with MedExtra with respect to the confidentiality and security of such information; and
- c) such information shall not be used for any purpose other than the purpose for which such information was provided.

3.1.4. MedExtra has implemented policies and practices to give effect to the principles, including:

- a) implementing procedures to protect Personal Information;
- b) establishing procedures to receive and respond to complaints and inquiries;
- c) training staff and communicating to staff information about our Organization's policies and practices; and
- d) developing information to explain our Organization's policies and procedures.

3.2. **Principle 2 – Identifying Purposes**

The purposes for which Personal Information is collected shall be identified by the Organization at or before the time the information is collected.

3.2.1. The purposes for which MedExtra collects Personal Information are documented in the following clause, and in our mandate and release forms, in order to comply with the Openness Principle 3.8 and the Individual Access Principle 3.9.

3.2.2. MedExtra collects Personal Information. This information is used to provide Case Management or Advocacy to secure access to healthcare at preferred rates at/with professionals or facilities.



- 3.2.3. Where MedExtra collects Basic Information; MedExtra specifies, in an oral agreement with the Client, the purposes for which such information is being collected. Where MedExtra collects Case Information; MedExtra specifies, in a written agreement with the Client, the purposes for which such information is being collected.
- 3.2.4. MedExtra will not use or disclose any Personal Information, for any purpose not previously identified, except as required or permitted by law. Should these purposes change, MedExtra will specify these changes in a written agreement with individual Clients.
- 3.2.5. Where MedExtra collects Basic Information; MedExtra's staff involved in the Collection is trained to explain to Client, at the time of the written agreement, the purposes for which the information is being collected.
- 3.2.6. This principle is closely linked to the Limiting Collection principle and the Limiting Use, Disclosure and Retention principle.

3.3. Principle 3 - Consent

The knowledge and Consent of the individual are required for the Collection, use or Disclosure of Personal Information, except where inappropriate. In certain circumstances Personal Information can be collected, used, or disclosed without the knowledge and Consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek Consent. Seeking Consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated.

- 3.3.1. MedExtra collects:
- a) Basic Information directly from the Client concerned;
 - b) Case Information from Clients, Healthcare Providers & Organizations currently or previously involved in the care of the Client.
- 3.3.2. MedExtra makes every reasonable effort to ensure that Clients are advised of the purposes for which their Personal Information will be used. Such purposes are stated in such a manner that a layperson can reasonably understand how the information will be used or disclosed.



3.3.3. MedExtra does not, as a condition of securing access to care, require a Client to Consent to the Collection, use, or Disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

3.3.4. The form of the Consent sought by MedExtra may vary, depending upon the circumstances and the type of information. In determining the form of Consent to use, MedExtra considers the sensitivity of the information.

a) Where MedExtra collects Basic Information; MedExtra considers that there is express Consent to the Collection, use and Disclosure of the information.

b) Where MedExtra collects Case Information; MedExtra requires Clients to express written Consent to the Collection, use or Disclosure of his or her Personal Information, prior to the Collection, use or Disclosure of said information.

i The written Consent may be of a form that permits MedExtra to collect Case Information from multiple sources identified by the Client orally or in writing.

3.3.5. MedExtra also considers that the purposes for which Personal Information collected directly from a Client or from a source other than the Client concerned is used and disclosed are consistent with the purposes for which such information was originally collected, and are not in conflict with the reasonable expectations of the Client.

3.3.6. The way in which MedExtra seeks Consent varies, depending on the circumstances and the type of information collected. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

a) Where MedExtra discloses a Client's file that identifies the individual, express Consent is solicited in the form of a Client Care Agreement is solicited

b) Where MedExtra collects medical files from Healthcare Providers or Organizations, the broad Consent of the "Release of Medical Information" is solicited

c) Where MedExtra discloses a summary or a Client's file where the individual is not identified, the broad Consent of the Client Care Mandate is solicited



3.3.7. Individuals can give Consent in many ways. For example: (a) an application form may be used to seek Consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving Consent to the Collection and the specified uses; (b) a check off box may be used to allow individuals to request that their names and addresses not be given to other Organizations. Individuals who do not check the box are assumed to Consent to the transfer of this information to third parties; (c) Consent may be given orally when information is collected over the telephone; or (d) Consent may be given at the time that individuals use a product or service.

3.3.8. A Client may withdraw Consent at any time, subject to legal or contractual restrictions and reasonable notice. MedExtra will inform the Client of the implications of such withdrawal.

3.4. Principle 4 - Limiting Collection

The Collection of Personal Information shall be limited to that which is necessary for the purposes identified by the Organization. Information shall be collected by fair and lawful means.

3.4.1. MedExtra collects only the amount and the type of Personal Information, which is necessary to fulfill the purposes previously identified, and specifies the type of information collected as part of its information-handling policies and practices, in accordance with the Openness principle.

3.4.2. The requirement that Personal Information be collected fairly and lawfully means that MedExtra will not mislead or deceive individuals about the purpose for which the information is being collected, or obtain Consent to collect the information through deception.

3.4.3. This principle is closely linked to the Identifying Purposes principle and the Consent principle.

3.5. Principle 5 - Limiting Use, Disclosure, and Retention

Personal Information shall 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 Information shall be



retained only as long as is necessary for the fulfillment of those purposes.

- 3.5.1. MedExtra will not use or disclose Personal Information, for any new purpose, except in accordance with previously stated clauses, and uses contractual means to ensure that any Organization to which it discloses Personal Information is similarly obligated.
- 3.5.2. MedExtra destroys, erases or renders anonymous any Personal Information that is no longer required to fulfill the purposes identified, and has developed guidelines and implemented procedures to govern the destruction, erasure or anonymizing of Personal Information, and uses contractual means to ensure that any Organization to which it discloses Personal Information is similarly obligated.
- 3.5.3. MedExtra will not disclose Personal Information except with the express Consent of the Client concerned or as required or permitted by law.
- 3.5.4. This principle is closely linked to the Consent principle, the Identifying Purposes principle and the Individual Access principle.

3.6. Principle 6 - Accuracy

Personal Information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

- 3.6.1. MedExtra uses its best efforts to ensure that Personal Information collected by it is accurate and complete and up to date.
- 3.6.2. MedExtra will not, as a matter of routine, update Client Case Information. MedExtra will update Case Information in the event that a Client's Case Information does not include documentation on care provided to the Client that is relevant to the current purpose.

3.7. Principle 7 - Safeguards

Personal Information shall be protected by security safeguards appropriate to the sensitivity of the information.



- 3.7.1. Where MedExtra collects Personal Information in recorded form directly from the Client concerned, or Healthcare Provider or Organization, such information is sent to MedExtra by mail, facsimile, courier or electronic transmission. Once received by MedExtra, MedExtra uses a variety of measures to ensure that the information is protected against loss or theft, as well as unauthorized access, Disclosure, copying, use or modification. All information collected by MedExtra is kept in the format received or in computer format. MedExtra transmits Clients files by mail, facsimile, courier or electronic transmission, with the identity of the Client encrypted.
- a) MedExtra uses contractual means to ensure that any Organization to which MedExtra discloses Personal Information is similarly obligated. All Personal Information disclosed by MedExtra to any Client or Healthcare Provider or Organization is sent in hard copy or computer format, or electronic transmission.
 - b) Where MedExtra transmits Personal Information electronically over a computer network the data is encrypted.
- 3.7.2. MedExtra affords the highest level of protection to all Personal Information, without distinction as to sensitivity.
- 3.7.3. The methods of protection used by MedExtra include:
- a) physical measures, such as a segregated computer system and restricted access to its premises and computer facilities;
 - b) Organizational measures, such as internal audits, security clearances, restricted access to the Personal Information and penalties for any breach of such measures; and;
 - c) technological measures, such as periodic testing of its computer security systems, confidential passwords and encryption.
- 3.7.4. All employees of MedExtra are made aware through regular, compulsory in-house seminars of the importance of maintaining the confidentiality of Personal Information, and are required to enter into confidentiality agreements prior to installation to a position.
- 3.7.5. MedExtra has developed guidelines and implemented procedures governing the disposal or destruction of Personal Information, to prevent unauthorized parties from gaining access to the information.



3.8. Principle 8 - Openness

An Organization shall make readily available to individuals specific information about its policies and practices relating to the management of Personal Information.

3.8.1. MedExtra is open about its policies and practices with respect to the management of Personal Information, and will provide to any Client, upon request, easily understandable information about its policies and practices, and a copy of this code.

3.8.2. The information about our policies and practices is contained in our policies and practices brochure, which includes:

- a) the name/title and address of the person who is accountable for our Organization's policies and practices and to whom complaints or inquiries can be forwarded;
- b) the means of gaining access to Personal Information held by our Organization;
- c) a description of the type of Personal Information held by our Organization, including a general account of its use;
- d) what Personal Information, if any, is made available to related Organizations; and
- e) an explanation of our Organization's policies and practices

3.8.3. More information can be obtained directly from MedExtra by mail; MedExtra, Corporate Communications Department, 4311 Frontenac, Montreal, Quebec H4H 2M4; upon request by email (to info@medextra.com); by fax (514) 526-4521 or telephone (1-877-37-EXTRA).

3.8.4. MedExtra reserves the right to modify this Privacy Code without notification to any Individuals or Organization with respect to which MedExtra has collected or will collect Personal Information

3.9. Principle 9 - Individual Access

Upon request, an individual shall be informed of the existence, use and Disclosure of his or her Personal Information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.



- 3.9.1. MedExtra will, upon request by any Client at any time, provide the Client with any identifiable Personal Information in MedExtra's possession concerning the Client, provided that the request is made at reasonable intervals. MedExtra reserves the right to make sensitive medical information available through a Case Manager. The Case Manager's time will be charged at the current hourly rate.
- 3.9.2. MedExtra requires only the name and evidence confirming the identity of the individual requesting the information, in order to provide the information referred to in the previous clause.
- 3.9.3. MedExtra will provide, as part of the information referred to in the previous clause, either a list of the third parties to which it has disclosed the information or to which it may have disclosed the information, depending upon the needs of the individual requesting the information.
- 3.9.4. MedExtra will respond to any request pursuant to the previous clause 3.9.1 as promptly as possible, and in any event within 30 days. The only costs to the Client would be for the time spent by the Case Manager, postage and any third-party costs for data retrieval authorized by the Client. The requested information will be provided or made available in an easily understandable form, together with any required explanation of abbreviations or codes.
- 3.9.5. Where an individual successfully demonstrates the inaccuracy or incompleteness of Personal Information concerning the individual, the information will be amended, immediately, by correcting or deleting information or adding information, as required. Where appropriate, MedExtra will promptly transmit the amended information to third parties to which MedExtra has previously provided the information in question.
- 3.9.6. Where a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved dispute will be recorded by MedExtra. Where appropriate, the existence of the unresolved dispute will be promptly transmitted by MedExtra to third parties to whom MedExtra has previously provided the information in question.



3.10. Principle 10 - Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the Organization's compliance.

3.10.1. The individual accountable for MedExtra's compliance is discussed in the first clause.

3.10.2. MedExtra has put procedures in place to receive and respond to complaints and inquiries about its policies and practices relating to the handling of Personal Information. The complaint procedures are easily accessible and simple to use.

3.10.3. MedExtra will, within a maximum of two weeks, inform individuals who make inquiries or lodge complaints, of the existence of the relevant complaint procedures.

3.10.4. MedExtra will promptly investigate all complaints. If a complaint is found to be justified through either the internal or external complaint review process, MedExtra will take prompt and appropriate measures, including if necessary, amending its policies and practices.