MARCH OF DIMES CANADA LA MARCHE DES DIX SOUS DU CANADA

MODC Privacy Policy

Policy Name:	Program/Department:	Original Issue Date:	Last Revised:
MODC Privacy Policy	People and Culture/ Privacy Office	January 2022	June 2023

1. Introduction/Objective:

March of Dimes Canada (MODC) is committed to protecting the privacy and safeguarding the security of Personal Information, as defined below, under its control. This includes the personal information of MODC staff, clients and members of the public (e.g., donors or family members of clients) This Policy applies across all of MODC's operations in every province across Canada and applies to MODC's handling of personal information in any capacity.

MODC has adopted practices and procedures within this Policy, which give effect to the ten principles of fair information practices outlined in Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) and substantially similar provincial legislation in BC, Alberta and Quebec. Furthermore, the Personal Health Information, as defined below (PHI) of clients served by the MODC is recognized as highly sensitive information, and requires a high standard of privacy, confidentiality, and security. MODC recognizes that PHI belongs to the client to whom it relates and as custodians of that information, MODC is accountable for protecting the PHI of each client. MODC also recognizes that its collection, use and disclosure of PHI may be governed by applicable provincial legislation dealing with health information. In some cases, the obligations under these statutes (i.e., Ontario, Nova Scotia, New Brunswick and Manitoba) will supersede those found in PIPEDA where MODC is acting as a custodian (or its equivalent) for PHI in those provinces.

The purpose of the MODC Privacy Policy is to communicate responsible information handling expectations and provide guidance to the leadership, employees, and volunteers of MODC on matters concerning the protection of privacy in each jurisdiction in which MODC conducts activity.

2. Policy Statement:

MODC recognizes the privacy rights of individuals and the importance of maintaining confidentiality to protect and enhance public trust in MODC.

This policy applies to all personal information collected, used or disclosed by MODC with respect to clients, donors, fundraisers, event participants, individuals who use the services of MODC, employees and volunteers. All employees and volunteers including Directors of the Board and Board Committee members, students, contract workers, and all individuals who collect, use and disclose PI, including PHI or Confidential Information (CI) on behalf of MODC are bound by this Policy. For the purposes of this Policy, everyone included in the scope of this Policy will be referred to as "Covered Persons".

3. Definitions:

Covered Person means all employees, students, contract workers, volunteers and any individual who collects, uses, discloses personal information on behalf of MODC. For third parties contracted by MODC to provide a service, see Third Party with Custody of PI (below).

Confidential Information (CI) means all information (which can also include personal information) that is specifically identified as confidential, or is reasonably understood to be of a confidential nature that Covered Persons receive or have access to through MODC, and includes vendor arrangements and other proprietary information accessed or received by a third party. See **Third Party with Custody of Personal Information** (PI), below.

Data Incident is an event that can compromise the privacy, safeguarding, or availability of Confidential or Personal Information, whether physical or electronic. While not all data incidents are privacy breaches, for the purposes of this Policy, Data Incident or Privacy Breach shall be managed in a similar way, whether suspected or confirmed.

Managers and supervisors means any MODC employee in a manager or supervisory role. MODC executives, directors, managers and supervisors are responsible for and shall oversee the collection, use, disclosure, and safeguarding of confidential or personal information, including Personal Health Information, as defined in the MODC Privacy (PHI) in their program or functional area(s).

Privacy relates to the collection, use and disclosure of personal information in accordance with applicable law. **Data Protection** relates to the protection of such information.

Personal Information (PI) means any information that can be used, either alone or in combination with other information, to identify an individual. Examples of personal information include: name, address, e-mail address, gender, age, ID numbers, racial or ethnic origin, relationship status, income, employee files, , assessments, or evaluations, payment or medical/health records. An individual's name does not need to be attached to the information in order for it to qualify as personal information. Personal information does not include business contact information, such as a person's title, business telephone number, business email or address used to communicate with that individual in respect of their employment, business or profession.

Personal Health Information (PHI) is a type of personal information. PHI is information about an individual if the information: relates to the individual's physical or mental health, including family health history; relates to the provision of health care, including the identification of persons providing care; is a plan of service for individuals requiring long-term care; relates to payment or eligibility for health care; relates to an individual's entitlement to benefits under or participation in a health care program or service; is a drug, health care aid, device, product, equipment or other item provided to the individual under a prescription issued by a health care provider; relates to the donation of body parts or bodily substances or is derived from the testing or examination of such parts or substances; is genetic information about the individual; is the individual's provincial healthcare plan number; or identifies an individual's substitute decision-maker.

> **Note:** This PHI definition is taken from Ontario's Personal Health Information Protection Act (PHIPA). Other provinces (e.g., Nova Scotia, New Brunswick, Manitoba) in which MODC operates may have more expansive PHI definitions. Managers should contact the Privacy Office for more information and guidance on privacy laws in other provinces that may apply, and to determine and address any additional requirements to ensure ongoing privacy compliance within their program or functional area(s).

Privacy Regulator means any provincial or federal regulator with jurisdiction over PI.
Ten (10) Fair Information Principles form the ground rules enshrined in federal and provincial privacy law for the collection, use and disclosure of personal information, as well as for providing access to personal information.

Third Party with Custody of Personal Information (PI) means any outside individual or business that provides a service to, or acts on behalf of MODC, and may require the third party to collect PI on behalf of MODC or have access to PI collected by MODC. Examples of third parties include a consultant or advisor, or professional services provider such as external legal counsel, insurers, benefits provider, IT solution developer, etc. Whenever arranging access to or collection of PI by a third party, senior leaders and managers must ensure that contracts for the provision of services contain privacy and confidentiality provisions and other safeguards to protect privacy and confidential information. See **Privacy Safeguards** (sec. 6.7) for more information.

4. Legislative Context:

MODC will comply with all privacy and data protection laws, regulations, and rules in each jurisdiction where MODC conducts business or activity, that outline how organizations may collect, use, and disclose personal information. MODC may also be subject to provincial health information laws for certain services that it offers. Directors and Managers may contact the Privacy Office/Senior Manager, Privacy for more information about applicable federal and provincial privacy laws, and to review and address any additional requirements in order to ensure ongoing privacy compliance within their program or functional area(s).

5. Roles and Responsibilities:

All ‘Covered Persons’ that have access to or handle information on behalf of MODC shall follow the privacy protection procedures outlined below, which reflect the 10 Fair Information Principles adopted by MODC to ensure responsible handling of information in its custody.

MODC employees and volunteers are required to handle PI responsibly by following privacy protection procedures outlined in this policy, when collecting, using, disclosing, safeguarding PI on behalf MODC. Refer to Principle 1 (Accountability) in section 6.1 below, for detailed requirements pertaining to Covered Persons.

MODC managers and supervisors are responsible for the day-to-day collection, use, and safeguarding of PI under their control. Managers shall ensure that employees and any volunteers with access to personal information, are aware of and receive training on privacy procedures and practices established by MODC for the collection, use, disclosure and safeguarding of personal information including PHI. Refer to **Principle 1 (Accountability)** in section 6.1 below, for detailed requirements pertaining to MODC managers and supervisors. Managers and supervisors must adhere to their obligations under MODC’s **Data Incident and Privacy Breach Management Procedure**, which outlines requirements and steps to follow on discovering or being notified by a Covered Person of a suspected Data Incident or Breach.

The **Chief Privacy Officer** (Vice President, People & Culture) is accountable for and has

oversight of MODC's Privacy Program that includes establishing operating policies, procedures, and processes among other Program components outlined as follows, to support MODC's Privacy Policy:

- Development of operating policies, procedures, processes, and ongoing monitoring of evolving privacy laws and regulations, to support MODC's ongoing compliance
- Ensuring privacy and data protection awareness training for employees and volunteers and contractors of MODC
- Establishing requirements for Covered Persons who have access to PI held by MODC to sign a confidentiality agreement
- Publication of a Privacy Notice for stakeholders and the public
- Establishing and maintaining a process to receive, investigate and resolve questions, complaints or concerns from individuals, substitute decision makers and the public
- Ensuring investigation of reported privacy breaches, and recommendations for corrective action and enhancements to avoid similar breaches in the future
- Establishing a process to monitor and audit access to records of PHI to detect and prevent privacy breaches
- Ensuring procurement/contract templates include privacy provisions to protect PI, when MODC enters into arrangements with a third party for the provision of services (e.g., IT solution provider, software development or system upgrade provider, etc.), or for a third party required to collect information on behalf of MODC (e.g., insurance provider, pension provider, etc.).

6. Privacy Protection Procedures:

All Covered Persons must be aware of and follow the privacy protection procedures and requirements outlined below, which are based on the 10 Fair Information Principles articulated in PIPEDA.

6.1 Accountability – MODC is responsible for Personal Information (PI) including PHI under its control and custody.

The **Chief Privacy Officer** is appointed to oversee compliance with the 10 Fair Information Principles, and with the Privacy Office team shall lead the MODC's Privacy Program to continuously enhance MODC's commitment to privacy.

Managers and supervisors are responsible for overseeing compliance with this Policy by employees and volunteers in their area of responsibility, which includes responsibility for the following:

- Having oversight on the day-to-day collection, use, disclosure, and safeguarding of personal information under their control
- Ensuring staff, and any volunteers with access to PI (including PHI), are aware of and receive training on privacy protection procedures and practices established by MODC for the collection, use, disclosure, and safeguarding of personal information

- Ensuring established procedures are followed that ensure access to and disclosure of Personal Information is only made by or to authorized individuals. For more information, managers and supervisors may refer to **Responding to Individual Access Requests Procedure** available in MODC Management Practices, or contact the Privacy Office for further guidance
- Watching for and identifying opportunities to correct conditions that may threaten the confidentiality, integrity, or security of information
- When receiving a report or concern from staff about a suspected data incident or privacy breach, immediately contacting the Privacy Office – Chief Privacy Officer (VP P&C) or designate (Senior Manager, Privacy) to review the incident and determine appropriate response in adherence with the Data Incident and Privacy Breach Management Procedure. Managers must adhere to the Privacy Incident and Breach Management Procedure available in MODC Management Procedures, and contact the Privacy Office for further guidance.
- Before developing new or changing existing processes or systems, managers shall conduct a privacy impact assessment (PIA), which is a privacy risk management process and tool that helps organizations ensure that privacy requirements are met, and that any potential impacts on privacy have been identified and addressed in keeping with MODC's privacy commitment. Managers and supervisors may refer to the **Privacy Impact Assessment Procedure** and PIA tool available in MODC Management Procedures, or contact the Privacy Office for further guidance.
- When entering into an arrangement with a third party (e.g., supplier, service provider), managers and supervisors shall ensure that any contractual arrangements include appropriate privacy protection provisions to safeguard personal information in the custody of a third party. Managers may refer to established procurement/MODC contract templates that include privacy protection provisions, or refer to the **Third Parties with Custody of Personal Information Guidance** in MODC Management Procedures, or contact the Privacy Office, or Procurement Team for more information about MODC contract templates.
- Assisting the Chief Privacy Officer in performing the monitoring and audit activities described in the **Monitoring Privacy Compliance Guidance** in MODC Management Procedures.

Employees (and volunteers with access to personal information) are responsible for adhering to this Policy, and includes taking action by doing the following:

- Understanding and following all privacy and data security policies and procedures established by MODC, including security requirements developed for the use of electronic systems
- Safeguarding the privacy and confidentiality of PI including PHI collected, used and disclosed in the course of their duties by using safeguards appropriate to the sensitivity of the information – see 6.7 below for more details
- Protecting their passwords and other devices (e.g., keys, access cards, access tokens) that enable access to MODC information assets
- Acting in a timely and co-operative manner to prevent, detect and respond to data security

and privacy breaches or other incidents, to prevent or solve issues and implement improvements

- Reporting immediately to their manager or director, and to the Privacy Office any actual or suspected privacy incident or breach, and cooperate with any related investigation
- Attending and completing mandatory education and awareness training
- Reporting to the Privacy Office any concerns, problems or need for improvement to the management and security of confidential information according to MODC procedures
- Complying with MODC's privacy policy and procedures

Privacy Awareness Training

Employees (and any program volunteers with access to information) must complete mandatory privacy education as determined by MODC. Privacy education will be determined based on the employee or volunteer's role and responsibilities at MODC.

Confidentiality Agreement

To ensure accountability, all new hires, employees, volunteers, and agents of MODC are required to sign a "Confidentiality Agreement" at the beginning of their relationship with MODC, and then on an annual basis thereafter. The obligations for ensuring privacy and confidentiality set out in this policy continue after the employment, contract, or other affiliation between MODC and its employees or volunteers ends.

Failure to comply with this Policy or to uphold the confidentiality agreement may result in disciplinary or corrective action up to and including termination of MODC employment or volunteer assignment.

6.2 Identifying Purposes – MODC shall identify the purposes for collecting personal information before or at the time personal information is collected.

MODC needs to collect and use information about its clients, parents/guardians, donors, employees and volunteers, in order to conduct its activities and operations that include delivery of programs and services to communities served. The purposes for MODC collecting personal information include:

a) To establish and maintain responsible relationships with its clients, parents/guardians, donors, employees, volunteers
b) To manage, develop, and enhance MODC operations, programs and services
c) To acknowledge gifts, issue tax receipts, and address other administrative requirements
d) To process and collect fees for service
e) To assess client needs
f) To determine program, service, employment or volunteer eligibility
g) To provide safe and secure MODC environments
h) To meet legal, regulatory, and contractual requirements
i) To collect data for statistical, research purposes, to better understand community needs
j) To communicate a range of programs, services, philanthropic opportunities that benefit

people we serve.

Covered Persons may collect Personal Information for the purposes outlined above and any another specific purpose(s) identified for their program or functional area, in order to operate MODC programs and activities. Covered Persons must not collect more Personal Information than is required to fulfill these purposes.

6.3 Consent – The knowledge and consent of an individual is required for the collection, use, or disclosure of personal information, except where exceptions to consent are required or permitted by law, particularly with respect to PHI of MODC's clients where it delivers services that are covered by provincial health information legislation.

The purposes for collection and use of personal information shall be communicated in clear, accessible, and understandable language, so that individuals including children and vulnerable persons can understand why personal information is being collected, and how MODC uses the information, and may disclose information in certain circumstances if required. Privacy statements shall be established by MODC management in consultation with the Privacy Office explaining the purpose(s) for collection and use of personal information for each MODC program and service.

Employees shall speak with their supervisor or manager if there is a request or concern from a client or other individual regarding how consent is obtained, or the collection, use or disclosure of personal information by MODC. Supervisors and Managers have more information available in, and are required to follow, the **Consent Guidance** available in MODC Management Procedures or contact the Privacy Office. The Guidance document outlines the various ways established by MODC to communicate the purpose(s) for collection and use of information, and how to obtain consent including when express consent (in writing) is required instead of implied consent, as well as the **exceptions** to consent required or permitted by law, particularly those where MODC is acting as a custodian of PHI.

6.4 Limiting Collection – MODC shall limit the collection of personal information to that which is needed for the purposes identified by the organization, and all information shall be collected by fair and lawful means.

For any questions or concerns regarding limiting collection, employees may speak with their supervisor or manager. Supervisors and managers have more information available in the **Limiting Collection Guidance** available in MODC Management Procedures or contact the Privacy Office, and may contact the Privacy Office for more information.

6.5 Limiting Use, Disclosure, and Retention – MODC shall not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required or permitted by law. Personal information shall be retained only as long as necessary to serve those purposes.

For any questions or concerns regarding the use, disclosure, or retention of information, employees may speak with their supervisor or manager. Supervisors and managers have more information available in and are required to follow and ensure that staff in their area of responsibility follow, the **Disclosure of Personal Information Guidance** as well as the

Records Retention Guidance documents available in MODC Management Procedures. Managers may also contact the Privacy Office at any time for further guidance.

6.6 Accuracy - Personal information shall be as accurate, complete, and up to date as possible, in order to properly satisfy the purposes for which it is to be used. MODC and its employees shall take all reasonable steps to ensure the accuracy and completeness of any Personal Information they collect or record, to minimize the possibility that inaccurate information is being used to make a decision about an individual. Where employees are unclear about whether a record contains accurate information, they should clarify with the individual concerned.

6.7 Safeguards – MODC shall protect Personal Information using security safeguards appropriate to the sensitivity of the information.

Covered Persons must follow established security safeguards to ensure that all Personal Information and Confidential Information is protected against unauthorized access, collection, use, disclosure, or disposal, as well as loss or theft. Employees and volunteers are expected to be familiar with, maintain and enforce the physical, administrative, and technical security measures applicable to their own program or functional areas and must be aware of and adhere to applicable policies, including IT Policies as well as any guidelines for protection of personal information determined by the Chief Privacy Officer. Safeguards include but are not limited to:

- Firewalls, intrusion-detection, anti-virus, strong passwords, mandatory PDA access control and other software solutions for technical security.
- Confidentiality sign-off by all employees and volunteers.
- Orientation, familiarizing and training employees and volunteers on MODC Privacy Policy and practices, and an ongoing emphasis on the importance of safeguarding any personal information to which employees are privy.

Employees and volunteers may speak with their manager or supervisor for more information about safeguards established to protect personal information collected and used in their program or functional area.

Senior leaders and managers entering into an arrangement with a third party (service provider, supplier or consultant), which may involve the third party accessing or collecting or processing information on behalf of MODC, shall ensure contractual agreements contain requirements for confidentiality and privacy protection safeguards. For more information, managers may refer to established MODC contract templates that include privacy provisions, or refer to the **Third Parties with Custody of Personal Information Guidance** in MODC Management Procedures, or contact the Privacy Office for further guidance.

6.8 Openness - MODC shall make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

MODC's Privacy Statement is available to the public on MODC's website and in its applications, which provide specific information about its policies and practices relating to its handling of PI, including PHI.

6.9 Individual Access - Upon request, and to the extent required by applicable legislation, MODC shall inform an individual of the existence, use, and disclosure of their personal information, and shall provide an individual access to that information, subject to 'exceptions to access' that might apply in certain circumstances permitted by law. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. Staff shall refer any requests for access to and/or correction of personal information held about an individual to their manager or supervisor for further guidance or handling.

Managers and supervisors shall respond to a request for access to information within a reasonable time, and at minimal or no cost, and shall ensure that personal information is provided in an accessible format that is understandable. Supervisors and Managers have more information available in, and are required to follow, the **Responding to Individual Access Requests Procedure** in MODC Management Procedures. This procedure and guidance outlines the key steps for responsible handling by managers and supervisors of requests that include how to respond to access requests involving separated spouses, or 'exceptions to access' in certain circumstances when MODC may not provide access to information (e.g. to protect the safety or security of another individual), as well as a sample response template letter, and other important information for supervisors to consider when reviewing an information access request from an individual. Managers may also contact the Privacy Office for further guidance when responding to an information access request from an individual.

6.10 Challenging Compliance – An individual shall be able to challenge MODC's compliance with the above principles. Individuals with a challenge or concern about MODC's privacy practices may contact MODC's Privacy Office:

- by email: privacy@marchofdimes.ca; or by phone at 416-425-3463; or
- by mail at: Attn: Chief Privacy Officer, March of Dimes Canada
  National Office, 202-885 Don Mills Road Toronto, ON, M3C 1V9

Employees and volunteers shall refer any inquiries or complaints about MODC's handling of personal information, to their manager or director who may consult with the Privacy Office for further guidance. Supervisors and managers have more information available in, and are required to follow, the **Monitoring Privacy Compliance Guidance** in MODC Management Procedures or contact the Privacy Office for more information.

7. Reporting a Privacy Incident or Breach

Any Covered Person that suspects a privacy incident or potential or actual breach, must immediately report the suspected incident or breach, including theft or loss of Personal Information, or device, or paper or electronic records, or alleged non-compliance with this Privacy Policy, to the Privacy Office. Employees are also required to contact their manager or director, who will consult with the Privacy Office – Chief Privacy Officer or Senior Manager, Privacy for further guidance to determine appropriate response, which may include fulfilling any mandatory notification requirements.

For more information, directors, managers and supervisors may refer to MODC's **Data Incident and Privacy Breach Management Procedure** available in MODC Management Procedures. MODC's Privacy Office shall maintain in a secure location all incident documentation involving privacy incidents or breaches reported by Covered Persons.

8. MODC Related Procedures and Reference Documents

The following are related procedures and reference documents and resources that provide additional information available online in the Corporate Documents Library. Managers and supervisors may also contact the Privacy Office for more information about MODC procedures and guidance.

- **Data Incident and Privacy Breach Management Procedure**
- **Consent Guidance** – to follow
- **Limiting Collection Guidance** – to follow
- **Disclosure of Personal Information Guidance** – to follow
- **Responding to Individual Access Requests Procedure** – to follow
- **Privacy Impact Assessment Procedure –** to follow
- **Third Parties with Custody of Personal Information Guidance –** to follow
- **Records Retention Guidance**
- **Monitoring Privacy Compliance Guidance**

9. Contacts and Other Resources:

For more information about MODC's Privacy Policy, employees and volunteers may speak with their supervisor or staff contact, or alternatively contact the **Chief Privacy Officer** (VP People & Culture) or designate (Senior Manager, Privacy) regarding a privacy question or concern. For any data/system security questions or concerns, supervisors may contact the **VP IT** or designate for further guidance.