

Access & Privacy Workshop 2006

September 14-15, 2006 | Macdonald Block, Queen's Park, Toronto | Ontario



Navigating the Information Management Landscape

Sponsored by:

Office of the Chief Information and Privacy Officer

Co-Sponsors:

Canadian Association of Professional Access & Privacy Administrators (CAPAPA)

Association of Municipal Managers, Clerks & Treasurers of Ontario, (AMCTO)

Information Technology Education Council (ITEC),

Municipal Info Systems Association (MISA)

Ontario Association of School Business Officials (OASBO)



Register at www.governmentevents.ca or call 613-226-8317

Information Management is coming.

Access and Privacy are fundamental democratic rights whose delivery depends on strong support systems and processes.

This year's Workshop: Navigating the Information Management Landscape explores those support systems – the information management principles that support access and privacy and a wide range of other activities from communications, policy and information technology to program design.

Constant learning is key to building and maintaining strong information management as well as access and privacy programs to support the business objectives of institutions.

If you work with access, privacy, information technology, communications, policy, planning, records management or program design, join us for a great learning and networking opportunity in access and privacy.

Government Use Of Personal Information

The Municipal/Freedom of Information and Protection of Privacy Act (M/FIPPA) limits the ways in which an institution may use personal information that has been collected by it or another institution.

Legal Requirements

- M/FIPPA s.31/41 lists the three situations in which personal information that has been properly collected can be used:
- Where the person to whom the personal information relates has identified that information in particular and consented to its use;
- For the purpose for which the personal information was obtained or compiled or for a consistent purpose; or,
- For a purpose for which the personal information may be disclosed to the institution under s. 32/42 (see information tips on Disclosure of Personal Information).

Best Practices

- Only use personal information in accordance with law and policy.
- Only use personal information if:
 - The use is necessary for government activities, it is allowed by applicable policies, and at least one of the following conditions exists:
 - a. The person consented to the use of their personal information; or
 - b. The use is covered by, or consistent with, a notice of collection.
- Periodically check or audit uses of personal information for compliance with M/FIPPA and policy.
- Periodically review notices of collection, consents or other authorities to ensure they cover (and allow) all present and future necessary uses.

Government Notice of Collection

The Municipal/Freedom of Information and Protection of Privacy Act (M/FIPPA) requires that a “notice of collection” be provided to individuals whose personal information is collected.

Legal Requirements

- M/FIPPA s. 29(2)/39(2) lists the following three requirements to be included in a notice of collection:
 - The legal authority for the collection;
 - The principal purpose(s) for which the personal information is intended to be used;
 - The title, business address and telephone number of an official of the institution who can answer the individual’s questions about the collection.

Best Practices

- Establish legal authority for collections by or pursuant to statute.
- The notice of collection should reference any statutory provision that specifically permits the collection of personal information or, where no such section exists, the notice should refer to the statutory sections that establish the collecting program.
- A notice of collection should include enough detail on the purpose(s) that a person unfamiliar with the program can understand why the personal information is needed.
- The notice should, however, also be general enough in its description to allow new or unanticipated but related purposes to be adopted as the program evolves. Otherwise, a new notice and re-collection of the personal information may be required.
- Notices of collection should be placed on all forms used to collect personal information, such as registration forms for services or benefits for individuals.
- The requirements for a collection notice can also be satisfied by:
 - a) posting a collection notice where it will be clearly seen by anyone whose personal information is being collected; or,
 - b) providing a verbal collection notice at the point of collection - which should be specifically documented each time it is given for evidentiary purposes.
- An institution should ensure that its Directory of Records lists any changes to its personal information collection.

Government Collection of Personal Information

The Municipal/Freedom of Information and Protection of Privacy Act (M/FIPPA) allows direct and, in more limited circumstances, indirect collection of personal information where an institution has the legal authority to do so. Whenever an institution receives, acquires or otherwise obtains personal information from any source, it has “collected” it under M/FIPPA.

Legal Requirements

- M/FIPPA s. S. 28/38 (1): collection includes non-recorded as well as recorded personal information.
- M/FIPPA S. 28/38(2) prohibits collection of personal information unless it is legally authorized because it is:
 - expressly authorized by statute;
 - used for the purposes of law enforcement; or,
 - necessary to the proper administration of a lawfully authorized activity.
- M/FIPPA S. 29/39 permits collection of personal information only **directly** from the individual to whom it relates **unless** a condition in M/FIPPA ss .29/39(1) (a) through (h) authorizes indirect collection, i.e, from an individual other than the one to whom the personal information pertains.

Best Practices

- For all collections of personal information, record the date of collection and the details of the legal authority.
- When collecting personal information from other institutions, verify in writing that they complied with legal collection requirements.
- Collect only the personal information needed to complete your government activities.
- An individual authorizing the indirect collection of his or her own personal information should identify the personal information, its source and the collecting institution.
- Provide a notice of collection in accordance with the Government Notice of Collection information sheet.

Privacy Protection Across

The FIPPA View of Government

The Freedom of Information and Protection of Privacy Act (FIPPA) defines Government of Ontario ministries, agencies, boards, commissions and other bodies covered by the Act as legally distinct “institutions” for access and privacy purposes.

The Public View of Government

Nevertheless, the Government is, ultimately, one large organization with a complex network of shared responsibilities. This is particularly important when you consider that the public tends to see the Government as a single unit. They reasonably expect programs to work together to provide seamless, integrated, privacy-protective services.

A Focus on Co-ordination

The Freedom of Information and Privacy Directive sets out requirements for the management practices of ministries and other institutions for access and privacy. It cites “foster[ing] co-ordination among ministries and government agencies” as one of its purposes. It recognizes that a focus on co-ordination and consistency is key to managing privacy effectively.

Clearly, privacy tends to be at greatest risk where personal information flows across program boundaries. Ensuring privacy protection from the beginning to the end of the information “journey” is a challenge because the hand-off points for personal information management are particularly vulnerable to mismatches or omissions. Although it seems obvious, it is worth repeating that real cooperation requires open and frank communication between programs, particularly regarding the sharing of personal information.

See you in S
Register at www.governmente

Business Ministry Boundaries

“End-to-End” Accountability

Thus, as we create new business models for government-wide initiatives, we must ensure that there is end-to-end accountability for privacy protection. All public servants involved in projects with business partners must take “ownership” of privacy concerns, regardless of which side of the program line they reside on. This should lead to incorporating agreements for applying new risk mitigation strategies, security arrangements, shared policies and practices, etc., into Terms of Reference, Project Charters, Memoranda of Understanding, contracts, and other documents defining projects.

Best Practices

Provide privacy training at all staff and responsibility levels.

Define shared privacy responsibilities in documents such as Memoranda of Understanding, contracts and Project Charters, and review them regularly.

Establish and describe an accountability framework for all personal information flows, with a particular focus on hand-off points.

Include all partners, stakeholders, etc., in communication plans and discussions about program structures and procedures to ensure their knowledge and ownership of, and active participation in, program privacy design.

Your program’s boundaries should not mark the limit of your responsibility to protect the personal information that flows across them. Take the initiative yourself, or tell someone in authority who can address the situation. “Privacy – it’s your business.”

September!

events.ca or call 613-226-8317!

Government Disclosure of Personal Information

The Municipal/Freedom of Information and Protection of Privacy Act (M/FIPPA) sets out all situations in which personal information may be disclosed and prohibits any other disclosures of personal information.

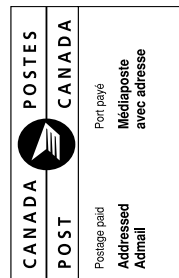
Legal Requirements

- M/FIPPA s. 32/42 lists the only situations in which an institution is permitted to disclose personal information. These include:
 - responses to FIPPA access requests;
 - with the specific, informed consent of the individual to whom it pertains;
 - where a notice of collection or other legal authority authorizes the disclosure;
 - to institution employees who need it for the performance of their duties;
 - to aid a law enforcement investigation;
 - specified health and safety purposes; and,
 - other limited circumstances.
- M/FIPPA s. 36/47(1) establishes an individual's right to access his or her own personal information.

Best Practices

- Since M/FIPPA s. 32/42 lists conditions where disclosure of personal information is permitted — but not necessarily required, institutions should establish policies detailing when and how such permitted disclosures take place, consistent with government and program goals and purposes.
- Always consult M/FIPPA for the particular requirements for specific disclosures.
- Disclosure of personal information to an institution other than the one that collected it should be supported by legislation and/or Service Level Agreements or contracts based on legislation.
- M/FIPPA limitations on personal information disclosure should be communicated to, and clearly understood by, employees.
- Personal information disclosure practices should be periodically reviewed to ensure continued compliance and currency with M/FIPPA, other statutes and policy.

Verney Conference Management
 20 Jamie Avenue, 2nd Floor
 Ottawa, ON K2E 6T6



REGISTRATION FORM
 Access & Privacy Workshop 2006
 Navigating the Information Management Landscape
 September 14-15, 2006, Toronto, Ontario

Registration fee: The early bird registration fee of \$175.00 (plus GST where applicable) covers all sessions, refreshments and luncheons for the two days. The registration fee increases to \$225 after July 31st. Cancellation with full refund allowable up to two weeks before the workshop, less \$25 administration fee, or a replacement delegate may be sent.

Confirmation: All registered delegates will receive a Confirmation email and Breakout Session Selection email before the workshop.

Program materials: An information kit will be available to all delegates upon registration at the workshop. It will include confirmation of Breakout Sessions selections, updated workshop information and an identification badge.

Delegate Name _____
 Delegate Title _____
 Organization _____
 Address _____
 City _____ Province _____ Postal Code _____
 Phone _____ Fax _____
 Email _____

3 Ways to Pay (please indicate one method):

- 1. Cheque to follow in mail (Payable to Verney Conference Management)
- 2. Invoice me
- 3. Visa / MC / Am Ex Card #: _____

Expiry Date: _____ Signature: _____

For further information: Call 613-226-8317 Fax: 613-226-8421
 Email: registration@verney.ca
 Web: www.governmentevents.ca/apw2006

Payment must be received on or by September 14, 2006. Send completed registration form with cheque or money order payable to :

VERNEY CONFERENCE MANAGEMENT
 20 JAMIE AVE., 2ND FLOOR, OTTAWA, ON K2E 6T6
 GST REGISTRATION # 865047062

To register, please make a photocopy of this page, complete and fax to 613-226-8421 or register online at www.governmentevents.ca