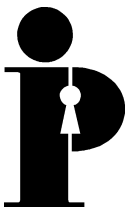
Information
and Privacy
Commissioner/
Ontario

Moving Information:
Privacy & Security Guidelines



Ann Cavoukian, Ph.D.
Commissioner
July 1997

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

The Information and Privacy Commissioner gratefully acknowledges the work of John Brans in preparing this report.

This publication is also available on the IPC website.

Table of Contents

Introduction **1**

Guidelines: How to Protect Privacy Before, During and After a Move **2**

Privacy Before the Move 2

Privacy During the Move 4

Privacy After the Move 6

Conclusion **8**

Appendix A **9**

Introduction

Moving an organization from one location to another requires keen logistical skills and a great deal of patience. Attention must be given to countless details and checklists in order to accomplish a successful move.

Part of the moving process inevitably entails the shipping of information, in both hard copy and electronically stored files. It is essential that personal information (such as a client's birth date, marital status, or financial information), and confidential information (such as strategic plans or reports), be packed, stored, shipped, unpacked and re-filed using secure measures that protect privacy. Taking all necessary security precautions will help to eliminate the unintended or inadvertent disclosure of personal or confidential information during a move.

As part of its mandate of educating organizations on how to protect privacy in a secure and efficient manner, the Office of the Information and Privacy Commissioner/Ontario (IPC) has developed guidelines on how to protect privacy before, during and after a move. Tips are provided on how to ensure that the privacy and security of personal and confidential information have been accounted for during all phases of a move.

In addition, one section deals with the obligations of government organizations under the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*).

Moving Information: Privacy & Security Guidelines could become an important resource. Consulting it at the preliminary stages of a move may help to ensure that all personal and confidential information remains secure throughout the move.

Guidelines: How to Protect Privacy Before, During and After a Move

Privacy Before the Move

Your Records, Your Responsibility

Organizations use a variety of services to co-ordinate the movement of records from one location to another. Some organizations may use their own facilities management staff, while others may employ the services of an external moving company.

Whichever method is used, it is extremely important that the organization which has custody or control of the records being moved recognizes that it is responsible for the secure shipment of the records, from start to finish. While the unit co-ordinating the move may be responsible for the "mechanics" of the move, the "custodian" of the records is ultimately responsible for ensuring that privacy remains intact.

Contract or Agreement with the Supplier

Organizations should sign a formal contract or agreement with all external suppliers hired for the purpose of moving records from one location to another, especially when those records contain personal or confidential information. This will ensure that all parties fully understand their respective roles and responsibilities.

The contract should also include tasks that may arise after the move has been completed. For instance, a moving company may be asked to cull and re-sort records or files containing personal/confidential information as the result of an organization centralizing its operations into one location. It is very important that all parties realize that the privacy and confidentiality provisions of the contract extend, in their entirety, to this final phase of the move.

Apart from the confidentiality and security requirements, government organizations should also include a specific reference to the privacy provisions of the *Acts* (see Appendix A).

Retention and Disposal

Prior to moving records from one location to another, most organizations dispose of any records that are no longer necessary.

Paper and other hard copy records should be shredded, pulped or burned rather than disposed of as garbage. Records should be destroyed by the organization's own staff or by acquiring the services of a credible vendor that utilizes specialized disposal methods and/or equipment. This phase of the movement of records from one location to another should be clearly communicated to all staff performing these functions. If this task is being provided by an outside agency, the contract should specify the method of disposal to be used. Culling of records should be done in a secure location, with limited access.

Records not identified for disposal and intended to be moved to another location should be packed in sturdy boxes. A log of each boxes' contents should be recorded and reconciled when placed on the truck, and checked again at their intended destination. Once the boxes have been packed and are ready for transport, they should be stored in a secure location until placed on the truck, with access to the files controlled.

Government organizations should refer to Appendix A for legislative requirements in this area.

Electronic Record Disposal

When disposing of personal computers or computer disks that once contained personal information, organizations should use a utility such as Norton Utilities or PC Tools, or use a recent version of the operating system that will "unconditionally format" or erase all data from the computer's hard drive, as well as any computer disks, in such a way that it cannot be reconstructed. Simply "reformatting" the hard drive or a computer disk is not adequate because commercial software can be used to reconstruct the information.

Once such a permanently-erasing utility has been used, it should be tested to ensure that it has performed the task properly — the hard drive and any computer disks should be completely erased, containing no personal or confidential information, prior to their disposal.

Adequate Storage Facilities

Any storage facilities used for long-term storage of records should have adequate security and climate-control standards. If the storage facilities of an outside agency are used, these requirements should be specified in the contract to ensure that these records will be not only be retrievable, but also in good condition in years to come. Organizations should ensure that any records of archival value are retained accordingly.

Log of Electronic Equipment & Records

Organizations should prepare a log of all equipment, storage media, and information stored on them. Once the move has been completed, the logs can be used to ensure that all the equipment and information were moved properly and that nothing was tampered with during or after the move.

Policy and Procedures for Training Staff

These Guidelines should be incorporated into a policy addressing the movement and disposal of paper and electronic records. The policy should have clearly defined roles and responsibilities for all individuals involved with the paper and electronic records disposal and movement process, and should be clearly communicated to those individuals. This policy can also be used to train all new staff, thereby providing a mechanism to ensure that records containing personal or confidential information are routinely protected.

Privacy During the Move

Know Where Your Records Are

Organizations should know where their records are at all times. While this may seem fairly obvious, it appears to bear repeating. When moving records from one location to another, files should be recorded on a log at each departure point (in the case of multi-office consolidation), and reconciled against this log twice: 1) when placed on the truck, and 2) when they arrive at their new destination. This will identify any files that may have been lost in transit. This will also allow the organization to quickly locate any files during the move, should the need arise. Someone should be assigned the responsibility of ensuring that files are kept secure at all times. This individual should conduct a 'walkabout' at both the old site and the new location to ensure that privacy has been maintained throughout.

Records Lost or Unauthorized Access

If the worst happens, and information becomes lost, stolen, or inadvertently disclosed to unauthorized parties, organizations should advise the individuals to whom the information relates of this breach of privacy. By doing so, it may divert a potentially embarrassing situation for the organization. It also enables the organization to begin assembling a new file or files. Consequently, if some files are found to be missing and cannot be located within a short time, the organization should consider contacting the individual to whom the personal information relates, to inform them of the situation. If this becomes impractical, in some cases due to the large numbers involved, some other means of notice than direct contact should be contemplated.

Secure Transportation

Records containing personal information (in paper or electronic form) should be transported in secure vehicles (i.e. locked trucks), and where possible, separately from other goods and materials (furniture, office supplies, etc.) that are also being transported — the former should be afforded a higher degree of security and should be treated accordingly.

Secure Location

Records should never be placed in an unsecured location. When records arrive at their intended destination, they should be moved directly to their new location. This location should be secure, and entry should only be permitted to pre-approved authorized personnel. When the records arrive at their new location, all entries and exits to the premises should be logged — consideration should be given to hiring a security guard(s) to monitor access to and from the premises, until such time that the organization is operational again.

If temporary premises are being used to store records on an interim basis, these must be secured at all times. Breaches of security and privacy often occur at such times, when sufficient attention has not been devoted to temporary facilities (even though considerable thought may have been given to the permanent storage facility). All persons involved in a move should be reminded of the need to ensure the seamless protection of information, from start to finish, including the use of any interim storage sites, no matter how temporary.

Equipment in Good Working Order

You may wish to ensure that all equipment intended to be used to store records at the new location are in good working order. Desks and file cabinets should be equipped with working locks and keys (lost keys are quite common). Keys, once linked to the right locks, should be tightly controlled. If keys are missing or locks are not working properly, they should be replaced or repaired prior to the storage of any personal or confidential information.

Electronic Security & Access

Large volumes of personal information are now routinely maintained in electronic form. Such media include personal computers equipped with hard drives, local area network file servers, diskettes, magnetic tapes and CD ROMs. When an office's operations move to another location, organizations must ensure that the information maintained on such media is kept secure from unauthorized access before, during and after the move. Thus, if any of the equipment or media contain personal or confidential information, appropriate security and access controls must also extend to that equipment.

Privacy After the Move

Controlling Access by Service Personnel

Once an organization's move has been completed and its records have arrived at the new location, various service personnel are required to perform numerous tasks at the new premises. Completion of services such as the installation of telephones, furniture assembly, computer installations, painting, etc. may not occur until after the records have been delivered to the new premises. These tasks are usually performed during regular business hours while the organizations' staff is present. However, in some cases, these tasks may have to be performed outside of regular business hours, or prior to the new location becoming fully operational. If this happens, it is extremely important that service personnel be supervised at all times to ensure that they do not access confidential or personal information.

It may be necessary to hire temporary security staff to supervise after-hours workers. Alternatively, the organization's own staff may be assigned this task. Whichever method is used, it is important that the supervisory staff be made aware of who is permitted to access records containing personal or confidential information. A list of authorized individuals should be compiled for this purpose.

Revise Policies and Procedures to Suit New Location

After an organization has moved its records to the new location, operational policies and procedures should be reviewed to ensure that they accurately reflect the new office configuration. Issues such as physical security of the premises, office access, file and records movement between floors or buildings, computer access protocols, facsimile transmission facilities, etc., should be addressed and updated accordingly.

These policies should also ensure that electronic records are protected at all times from unauthorized access.

Location of Fax Machines

Once an office has moved, careful consideration should be given to the location of the fax machine, ensuring that it is placed in a secure area. Ideally, it should be located such that:

- it is not placed in a public area;
- its use can be monitored by an authorized person; and
- only authorized staff have access to the information transmitted.

By restricting access to the fax machine to several authorized persons, the potential for unauthorized use and disclosure is considerably reduced.

Depending on volume, one central fax person and a backup should be responsible for all fax operations. In case of problems, technical or otherwise, staff will know who to contact. If new fax equipment is being considered, and will be used for transmission of personal or confidential information, encryption software should be considered.

Conclusion

It is to the advantage of every organization to ensure that personal and confidential information is protected during a move from one location to another. The Office of the Information and Privacy Commissioner/Ontario hopes that organizations will be able to use the guidelines outlined in this paper as a framework for developing and implementing their own policies when relocating information.

Appendix A

Compliance with the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*.

Government institutions must also follow the privacy and access provisions of the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*).

Records must be available should the government organization receive an access request under the *Acts*. Thus, government organizations have a legal obligation to know where their records are at all times and be able to retrieve them in a timely manner. By utilizing the logging procedure described in these guidelines, government organizations will know which records (files) are packed, in transit, unpacked, or awaiting re-filing should the need arise to access the files during the moving process.

Section 42 of the provincial *Act* and section 32 of the municipal *Act* require that personal information may only be disclosed under certain situations to authorized persons. Thus, while organizations should secure personal information, government organizations have a legal obligation under the *Acts* to provide privacy safeguards for personal information so that it is not accessible to unauthorized individuals.

The *Archives Act* and Management Board Directive 7-5 (*Management of Recorded Information*) require that no provincial government records may be destroyed or permanently removed from government custody except with the permission of the Archivist of Ontario.

While some records have only temporary value and may be destroyed once they are no longer useful, others should be preserved and transferred to the Archives of Ontario by provincial government organizations. Municipal organizations, while not required to follow these rules, should also ensure that a Records Management System that includes an archival process is in place.

To assist provincial organizations, the Archives of Ontario publishes fact sheets entitled RIM (Recorded Information Management). While these documents are aimed at organizations in the provincial government, they provide excellent tips on good records management practices that could be useful to all records and archives personnel. They are available from:

Office of the Archives of Ontario
77 Grenville Street, 6th floor
Toronto, Ontario
M5S 1B3
416-327-1600

Retention and Disposal

When government organizations cull records for retention and disposal purposes, they must ensure that the *Acts* as well as any records retention schedules are complied with. These retention schedules apply to both paper and electronic records.

Section 40(1) of the provincial *Act* and Section 5 of Regulation 823 under the municipal *Act* address the disposal of personal information. These sections require that personal information must be retained for at least one year after it was last used unless the individual to whom the information relates consents to an earlier disposal. Further, section 5 of Regulation 459 under the provincial *Act* requires that when personal information is destroyed, it is to be destroyed in such a way that it cannot be reconstructed or retrieved. While there is no equivalent to this requirement in the municipal *Act* or its regulations, it is our view that municipal organizations should also follow this practice. Similarly, non-government organizations should also follow this practice.

In addition, provincial organizations must also ensure that they comply with Management Board Directive 7-5 and the *Archives Act* when disposing of any records (general, exempt or personal) regardless of the medium. Provincial government organizations should consider contacting the Archives of Ontario to ensure that the requirements of the *Archives Act* are also met.

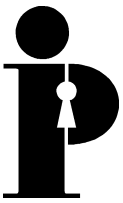
Electronic Personal Information

According to Management Board Secretariat's Directive 7-3, *Information Technology Security*, Ministries and Agencies must safeguard confidential information as well as ensure the integrity and availability of data while it is created, entered, processed, communicated, **transported**, disseminated, **stored or disposed** of through information technology [emphasis added]. It also defines the responsibility and mandatory requirements for developing, implementing and managing security measures for information technology resources during any office move having this type of equipment or termination of programs where it will be necessary to dispose of information of a personal nature.

If personal information must remain on the storage media (i.e. personal computers, hard drives, file servers, diskettes and magnetic tapes), during the organization's move, appropriate measures must be taken for the safe transfer of the information. Government organizations must prepare a log of the equipment etc.

If the information saved on the storage media is no longer required due to a program area being terminated, attention must be given to ensure that the *Acts* as well as any retention schedules are complied with. These retention schedules not only apply to electronic records but also to records maintained in paper form.

Provincial organizations must ensure that proper steps are taken to remove any information of a personal nature on all storage media and that the information is rendered unusable.



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca