IPC
Practices
Number 21
Revised September 1998
PUTTING ONTARIO'S INFORMATION AND PRIVACY LEGISLATION TO WORK
INFORMATION AND PRIVACY COMMISSIONER/ONTARIO
ANN CAVOUKIAN, Ph.D., COMMISSIONER

Privacy of Personnel Files

Access to personnel files should be limited to authorized staff who need access to carry out their duties. In addition, because personnel files may include a variety of personal information, authorized staff should have access only to specific categories of personal information contained in the file. This IPC Practices *offers suggestions on how to control access to personnel files.*

The IPC has received privacy complaints from employees of institutions subject to the *Freedom of Information and Protection of Privacy Act* (the provincial *Act)* and the *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act)* regarding unauthorized access to personnel files and the disclosure of personal information to employees who did not need the record in the performance of their duties. Some complaints involved cases where staff who needed access to only a specific type of personal information were able to look at the entire contents of the file. Other complaints involved the absence of controls to prevent unauthorized access to personnel files in general. In these instances, the IPC found that the disclosure of personal information was not in compliance with the *Acts*.

The *Acts* set out circumstances where personal information may be disclosed. Sections 42(d) and 32(d) of the provincial and municipal *Acts* respectively permit the disclosure of personal information to officers or employees who need a record to carry out their duties. As well, section 4(2) of Regulation 460 under the provincial *Act* and section 3(2) of Regulation 823 under the municipal *Act* grant access only to those employees who need a record to perform their duties.

In addition, section 4(1) of Regulation 460 under the provincial *Act* and section 3(1) of Regulation 823 under the municipal *Act* require institutions to ensure that reasonable measures to prevent unauthorized access to records are defined, documented and put into place, taking into account the nature of the records to be protected.

Institutions should also note that other legislation such as the *Human Rights Code* and the *Occupational Health and Safety Act* may have specific requirements related to access to particular types of information.

The IPC recently reviewed Metropolitan Toronto's system for controlling access to employee-related personal information. The department found that Metro had developed a commendable system that assisted them in complying with the municipal *Act* and the Regulations. Some of the suggestions listed below were adopted from Metro's practices, with their consent.

Suggested Approach

General

Institutions should establish written policies and procedures to indicate which staff are authorized to access specific types of employee-related personal information. These policies should be communicated to all staff.

Filing system

Staff who need access to specific personal information do not need access to all personnel records, kept in a personnel file. They need access only to records required to perform their duties.

Suggestion: The Personnel department can create a filing system that distinguishes categories of records held in a personnel file. In this way, access to a specific category is limited to authorized staff. Employees dealing with a particular issue will only be given access to records related to that particular issue. Possible examples of categories include:

Corporate personnel category — The corporate file may include records such as résumés, a letter offering employment, salary information, group insurance information, emergency contact person, medical certificate, attendance records, reference checks, etc.

WCB claim category — WCB claims and related material.

Labour relations category — Grievances, legal opinions, and other information related to a labour matter.

With this type of system, someone working in payroll who needs access to an individual's monthly attendance reports and salary scale, will not have access to records filed under the category of labour relations since this personal information is not required by payroll. In this way, access is restricted only to individuals who need the personal information in order to perform their duties.

With regard to medical records, the best human resources practice is to maintain medical information separate from the main personnel file. If an institution has in-house health personnel, the IPC suggests that medical information be managed exclusively by the health personnel.

Routine and authorized access

Some staff are authorized to access personnel files on a regular basis while others may be authorized only in particular circumstances.

Suggestion: For staff who require access on a regular basis, institutions can create a list of people who are authorized to have routine access to specific categories of personnel files.

In cases where staff need access to specific personal information to perform a duty that is not routine, the staff member should obtain written authority from the person or department in charge of the records in question before access is granted.

Physical security — controls

Large organizations may have departments responsible for each category of paper record; smaller organizations may keep all records in one location. Depending on the size of an institution and the volume of records, institutions may have a central or separate file room or may need only a locked filing cabinet. Each institution requires a procedure suitable to its particular circumstance.

Suggestion: Physical access to a central file room may be restricted by locking the file room door and only allowing access to authorized staff. Entry by authorized staff may be controlled in various ways, such as through the use of a cipher lock which allows access only to staff who know the lock combination; through the use of access cards

which restrict entry to staff whose cards have been programmed; or a file room clerk may control access. Access to filing cabinets maybe restricted by keeping them locked and giving keys only to authorized staff.

Tracking system

The Personnel department should keep track of corporate personnel files that are removed from the file room or file cabinet.

Suggestion: Institutions may implement a procedure that requires employees to sign-out and sign-in files. In this type of system, employees record their names, the nature of the file and date of removal and replacement on a charge-out card.

Personnel records not maintained in the personnel file

Duplicate copies of some personnel records may be stored outside the Personnel department.

Suggestion: It is advisable to have one corporate personnel file maintained by the Personnel department in order to control access, track records and ensure security. However, supervisors or department heads may need to maintain a duplicate of certain employee records such as performance appraisals, attendance reports or internal memos. These employees should be responsible for maintaining the privacy and security of the duplicate records. Also, these duplicate records should be registered as a Personal Information Bank.

Electronic records

All of the suggestions listed above are applicable to paper records and may be applicable to electronic records. Some larger institutions have moved towards electronic methods of storing and retrieving personal information because it is easier to implement access controls through the use of passwords. Where personal information is stored electronically, paper records may be archived as an additional security measure.

Freedom of Information and Privacy Co-ordinators should ensure that staff in the Personnel department and any other related departments are aware of the information contained in this IPC Practices.

IPC
Practices

is published regularly by the **Office of the Information and Privacy Commissioner**.

If you have any comments regarding this publication, wish to advise of a change of address or be added to the mailing list, contact:

Communications Department
Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

30% recycled paper

ISSN 1188-7206