Blaney McMurtry LLP

PUBLICATION

Collecting and Disclosing Personal Information - Are You at Risk?

Date: December 17, 2013

Original Newsletter(s) this article was published in: Employment Update: December 2013

What is "Personal Information"?

Employers collect and store an enormous amount of data about their employees. This information is often required in order to properly process payroll and administer benefit programs. Any information about an identifiable individual is considered "personal information," namely, name, SIN, age, sex, marital status, address, phone number, medical information, performance data, etc. and may have privacy rights attached to it.

Risk Scenarios

1. You are contacted by a landlord, credit agency or mortgage broker asking you to confirm payroll information about a current or former employee.

2. Your Human Resources Manager is subpoenaed to court and asked to bring the personnel file of an employee.

3. A prospective employer requests a reference for a former employee in respect of whom you have negative comments.

In each of the above situations, personal information belonging to an employee may be disclosed. What are the restrictions on such disclosure and the risks if the restrictions are ignored?

4. An employee accesses the personal information of a colleague from the company's records and uses it against the interests of that employee.

In this fourth scenario, does the employer have any risk of liability?

Privacy Rights

If you are a federally regulated employer (bank, telecommunications' company, etc.) the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") requires you to

collect, store, use and disclose personal information solely in accordance with the employee's consent or as otherwise required at law. There are no equivalent statutory obligations governing the use of an employee's personal information by private Ontario employers.

While private Ontario employers are not subject to PIPEDA in respect of their employees, employers should nonetheless put in place appropriate policies and safeguards to protect employees' personal information. Common law obligations require employers to collect, use and disclose employee personal information solely in accordance with an employee's consent and to safeguard that information while it is in the employer's possession.

Medical information may present additional obligations.

It is the policy of the Ontario Human Rights Commission that in order to ensure the maximum degree of privacy and confidentiality of employee medical information, all health assessment information should remain with the examining physician and out of an employee's personnel file.[1]

Back to the Risk Scenarios

1. Without specific consent from the employee, disclosure of the requested information to a third party would constitute a breach and potentially subject the employer to damages.

2. The rules of court govern what information is compellable and at what stage of a judicial proceeding. The employer will require legal advice before responding to the subpoena for the personnel file.

3. While consent to disclosure can, in some instances, be implied, this is clearly not one of those situations. Without specific consent (perhaps provided at the time of the employee's termination), the employer subjects itself to a potential claim for damages if the information is released.

4. In Ontario, the court awarded damages where a bank employee accessed and misused the personal information of another bank employee.[2] It is easily foreseeable that there may be a case in the future where an employer is held vicariously liable for the actions of its employee where appropriate policies and protections were not put in place to prohibit and prevent such access and disclosure.

The Prudent Employer Addresses these Risks by Implementing these Best Practices

In order to avoid risk, employers should adopt policies and procedures which mirror the obligations set out in PIPEDA. Policies should include the following provisions:

1. Describe the personal information collected from employees, explain why the information is collected and how it is or will be used.

2. Use or disclose the personal information only for the purpose it was collected.

3. Provide access to personal information on a “need to know basis” only. In particular, make sure that sensitive medical information is kept separate from the general personnel file.

4. Permit employees to access their personal information, with the ability to challenge the accuracy and completeness of the information.

5. Include, as part of your Technology Use Policy, a specific provision prohibiting access, disclosure and/or use of the personal information of any other person.

6. Implement appropriate safeguards to prevent unauthorized access to personal information (locked cabinets, password protection, encryption, etc.).

7. Include in each employment application form a consent to the collection and use of personal information for purposes related to employment.

8. In the case of any doubt regarding consent to disclose, seek a specific written consent from the employee.

9. Adopt common sense procedures geared to your business to prevent the accidental disclosure of personal information, for example:

- avoid emailing sensitive information to groups;
- double check envelope address when mailing personal information;
- restrict requests for medical information to that which is only absolutely necessary;
- ensure data is wiped clean before discarding old computers; and
- shred all physical files when being disposed.

For any questions regarding privacy in the workplace and best practices, call one of the members of our Employment and Labour Group.

[1] Ontario Human Rights Commission, “Requesting Job-Related Sensitive Information”, Human Rights at Work 2008, 3rd Ed.
[2] *Jones v. Tsige*, 2012 ONCA 32 (CanLII).