January 2015

CAUT LegalAdvisory

Personal Health Information Protection

Privacy is recognized in Canada as a value that deserves protection. In the workplace context, arbitrators and courts have often expressed the view that employees are entitled to protection of their privacy, but the principles applied by arbitrators are often subject to individualized application, and laws may be repealed or amended by unfriendly governments. Accordingly, laws may be an unpredictable basis upon which to rely in protecting employees' rights. The most effective way to protect your members' personal health information is to bargain clear collective agreement language.

Even within the scope of acknowledged rights of privacy, health information has been recognized as a particularly sensitive form of personal information which warrants especially strong protection. Because of its sensitivity, arbitrators and courts have consistently rejected employers' demands for random drug and alcohol testing. Arbitrators have also established principles which limit employers' rights to demand medical information from employees. For more information on these kinds of limitations, please see CAUT Legal Advisory *Protecting the Privacy of Personal Health Information, and Limiting the Employer's Right to Disclosure*.

Many jurisdictions in Canada now have laws which specifically protect "personal health information." The purpose of this advisory is to identify current and emerging issues related to protection of health information in the employment context, and to provide an overview of the status of current health information protection laws across Canada, and to identify policies which may form the basis for collective agreement language.

Relationship between General Health Laws and Collective Agreements

Although arbitrators have authority to interpret and apply statutes, they have demonstrated a reluctance to use privacy laws to support and enhance workers rights.† In any event, and apart from arbitrators' interpretations of privacy laws, employers are subject to many laws of general application which affect the rights of workers, including privacy legislation.

Issues Associated with Personal Health Information and Privacy

Personal health information is important and unlike other personal information, it is not easily ascertainable. Much personal information about you such as your family status and your home address can be discovered on the Internet, or through observation by others. Much of your health information is not so easily determined.

---

† Kate Hughes and Emily Dixon, *Ignored and Misunderstood—Privacy Rights and Medical Information in the Canadian Workplace*, Labour, Health, Pension & Benefits Law, November 1, 2013.

No one can tell your blood type by looking at your LinkedIn account, or by following you home. This sort of information was much easier to protect and secure when it was kept in a paper file in your family doctor's office. However, the delivery of health services has changed in recent years, and many of those changes affect the security of health information. Factors like increased patient involvement in their own health care; delivery of health care by a team of health professionals rather than by a single family doctor; storage of documents and communication of information electronically; and more focus on social determinants which affect health outcomes and therefore a wider range of professional involvement in health related issues all affect how health information is used and communicated, and to whom it is communicated.

The consequences of disclosure of health information are significant. Disclosure of personal health information can stigmatize individuals. It can result in prejudice, exclusion or denial of benefits. And with the increasing availability of genetic and genome based information, the potential for abuse and discrimination increases.

Electronic storage and the ability to easily share sensitive information with others raises the possibility of breaches of privacy through inadvertent leaks, or deliberate sharing of information beyond the purpose for which it was originally collected. Because information can be easily transmitted, policy makers must consider when and how that transmission should occur especially given the changes in delivery of medical services referred to above.

Policy makers have also had to consider the potential for aggregation and use of medical information for research purposes and other purposes which are in the public interest, like improving the delivery of health services generally. Policy makers must consider the implications of requiring anonymization of medical information for purposes like these, including the question of whether permanent de-identification is possible.

General Principles of Health Information Privacy Law (Relevant to Workplaces)

This section provides general guidance about most health information privacy laws, where they exist. However, there are variations from province to province, and laws may be amended from time to time. For the most current and comprehensive understanding of the principles that apply in your province, please refer to the law in your jurisdiction.

Health information privacy laws primarily regulate the conduct of custodians of health information. The terminology varies among jurisdictions, but the purpose of the laws is to regulate those who deal with health information. Custodians, generally, are members of the broad medical community who are involved in providing patient care. Custodians covered by the law can include dentists, chiropractors, midwives and optometrists. Often, medical entities providing services to primary caregivers (such as laboratories) are also covered by the laws.

Employers and insurance companies are not custodians bound by the primary obligations set out in health information privacy laws. But because they may receive health information in accordance with limits on disclosure which apply to custodians, they are covered by the laws as recipients of health information. However the duties and obligations imposed upon recipients of health information are limited, and sometimes, specific circumstances of receipt of health information by third parties (workers' compensation staff, for example) are governed by separate statutes.

Health information privacy laws regulate the collection, use and disclosure of medical information. Generally speaking, custodians must obtain informed consent from individuals before they collect health information; the information must only be used for the purposes for which it was obtained, and it can only be disclosed for the purposes for which it was collected. There are many exceptions or qualifications to these principles. For example, a doctor may be permitted without express consent to disclose health information to a specialist to whom a patient has been referred. In many jurisdictions, the patient is deemed to have impliedly consented to such

disclosure. In limited situations, information may be disclosed without consent, such as where an urgent safety concern to the patient or to the public is identified.

Health information privacy laws expressly contemplate that individuals should have control over their health information. This control is exercised in a number of ways. For example, consent, once granted, may always be revoked by a patient. In addition, and in certain circumstances, a patient may direct that his or her information which may have been provided to a custodian, not be disclosed, in a process known as "masking."

Individuals have rights to access and review their health information and to request changes to it, through the health information custodian.

In some jurisdictions, custodians are required to conduct audits and develop and implement plans for the custody of information, and privacy officials may have a role in ensuring compliance. Furthermore, in some jurisdictions, custodians are required to provide prompt notice of any breach of privacy and take immediate steps to address and remedy such breach.

Given that custodians (and not employers or insurers) are the primary target of health information laws, robust protection of your members' rights requires more than a promise to comply with the legislation. It requires protection written into your collective agreement. Collective agreement language, in turn, will be most effective if it draws on the statutory principles.

Highlights of Specific Issues: Use of Statutory Principles and Language for Collective Agreement Language

This section highlights some specific and important provisions in health information privacy laws, identifying those selected excerpts that provide the best modes for collective agreement language.

A. Definition of Personal Health Information

Collective agreement language which restricts an employer's right to collect, use and disclose personal health information should define the information which is subject to restriction as broadly as possible. The clearest and most comprehensive definition comes from *The Health Information Protection Act*, SS 1999, c H-0.021 in Saskatchewan, where "personal health information" is:

… with respect to an individual, whether living or deceased:

(i) information with respect to the physical or mental health of the individual;

(ii) information with respect to any health service provided to the individual;

(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

(iv) information that is collected:
(A) in the course of providing health services to the individual; or
(B) incidentally to the provision of health services to the individual; or

(v) registration information.

The definition contained in New Brunswick's *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05 defines "personal health information" to mean:

… identifying information about an individual in oral or recorded form if the information

(a) relates to the individual's physical or mental health, family history or health care history, including genetic information about the individual,

(b) is the individual's registration information, including the Medicare number of the individual,

(c) relates to the provision of health care to the individual,

(d) relates to information about payments or eligibility for health care in respect of the individual, or eligibility for coverage for health care in respect of the individual,

(e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any body part or bodily substance,

(f) identifies the individual's substitute decision-maker, or

(g) identifies an individual's health care provider.

While the New Brunswick definition is broader in some ways (it expressly includes genetic information and family history, for example), the Saskatchewan legislation *The Health Information Protection Act*, SS 1999, c H-0.021 has better introductory language because it is not limited to "identifying information" but rather is framed more broadly to encompass "information … with respect to an individual."

B. Alternatives/Limits

Health information protection laws restrict collection, use or disclosure of health information by custodians. The same obligations can be imposed on employers through collective agreement language. Set forth below are three examples of approaches related to an employer's collection, use or disclosure of health information:

Other Information — Ontario's *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A, excerpted below, requires custodians to consider whether other information would serve the purpose of health information and prohibits the use of health information if this is the case. Collective agreement language modelled on this would require employers to consider alternatives before requiring employees to disclose health information:

30.(1) A health information custodian shall not collect, use or disclose personal health information if other information will serve the purpose of the collection, use or disclosure.
— *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A

Extent of Information — If health information must be used (because there is no alternative), set forth below are three formulations which restrict the scope of what information can be required in a particular case:

Ontario's law provides as follows:

30.(2) A health information custodian shall not collect, use or disclose more personal health information than is reasonably necessary to meet the purpose of the collection, use or disclosure, as the case may be. — *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A

Alberta's language below, is more limiting than is Ontario's, because it restricts use to that which is "essential" for the purpose, which imposes a more stringent test than "reasonably necessary:"

Duty to collect, use or disclose health information in a limited manner
58(1) When collecting, using or disclosing health information, a custodian must, in addition to complying with section 57, collect, use or disclose only the amount of health information that is essential to enable the custodian or the recipient of the information, as the case may be, to carry out the intended purpose. — *Health Information Act*, RSA 2000, c H-5

Nova Scotia's language is probably the most restrictive, because it requires use of "the minimum amount necessary" to achieve the purpose. While it could be argued that this is synonymous with "essential" to the purpose, the language is better, because it suggests that the employer must actively consider minimizing the amount of information it is claiming:

Minimum amount
25(1) The collection, use and disclosure of personal health information must be limited to the minimum amount of personal health information necessary to achieve the purpose for which it is collected, used and disclosed.
— *Personal Health Information Act*, SNS 2010, c 41

C. Consent

All health privacy information laws contain a general requirement for express consent before health information is collected. Because the legislation is of general application, it contains exceptions to requirements for consent which are not relevant to the workplace. There is no need for an employer to obtain an employee's health information without his or her consent. Accordingly, collective agreements should contain language which confirms that the employer will not seek or obtain health information about an employee without his or her express consent.

D. Use

Once an employer has demonstrated that it is entitled to request production of health information in a particular case, it is important that the information be used only for purposes for which it was disclosed, and not for any other purpose. This is known in Ontario as the recipient rule, at s. 49 of the Act:

Restrictions on recipients

49.(1) Except as permitted or required by law and subject to the exceptions and additional requirements, if any, that are prescribed, a person who is not a health information custodian and to whom a health information custodian discloses personal health information, shall not use or disclose the information for any purpose other than,

(a) the purpose for which the custodian was authorized to disclose the information under this Act; or

(b) the purpose of carrying out a statutory or legal duty.

—*Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A

Collective agreement language should ensure that the employer will not use health information it has received in accordance with the collective agreement for any purpose other than the purpose for which it was disclosed.

E. Storage/Access by Others/Masking

Related to use, and very important in workplaces, are requirements for secure storage and limited access to personal health information. Most health information laws require custodians to have secure storage, archive and destruction systems, and to notify patients about their information practices. In addition, many health information privacy laws confer "masking" rights – individuals can request that some or all of their electronic records be protected from disclosure unless a more rigorous process of access is followed. In the Special Report prepared by the Office of the Information and Privacy Commissioner in BC, the Commissioner recommends a "role based access model" for its law, based on the principles of "need to know" and "least privilege."

In the workplace, these principles could be reflected in collective agreement language that provides as follows:

- Health information will be kept in files that are separate from personnel files;
- Health information will be accessed only by those who require the information, for example, individuals who must ensure that an accommodation plan for a returning employee is properly implemented;
- When health information is accessed, only that portion of the information which is relevant to the purpose for which it is being used will be disclosed to the individuals who need to know.

F. Access, Correction by Employee and Destruction or Return of Health Information

Health information privacy laws give individuals a right to access their health information and request that it be corrected, and to appeal to a privacy commissioner or a court if the information is not corrected. Typically, the individual must demonstrate that his or her record is inaccurate for the custodian to change the record. Similar provisions can be included in collective agreements. However, in all likelihood, if information produced to an employer by a health information custodian is inaccurate, the employee will likely invoke his or her right to have the information corrected under the applicable legislation in his or her jurisdiction, and the correction of information in the employer's files would follow from that.

The relevant Ontario language about correction is set out below:

55.(1) If a health information custodian has granted an individual access to a record of his or her personal health information and if the individual believes that the record is inaccurate or incomplete for the purposes for which the custodian has collected, uses or has used the information, the individual may request in writing that the custodian correct the record.

(8) The health information custodian shall grant a request for a correction under subsection (1) if the individual demonstrates, to the satisfaction of the custodian, that the record is incomplete or inaccurate for the purposes for which the custodian uses the information and gives the custodian the information necessary to enable the custodian to correct the record. — *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A

More relevant in the workplace context, is collective agreement language that requires timely removal from files and destruction of health information (or return to the employee of the health information) in certain circumstances, either:
a) automatically after a period of time has expired, or
b) when it is no longer required for the ongoing employment relationship, or
c) at the end of the employee's employment.

G. Privacy Management/Notification

Many health information privacy laws require that health information custodians designate an individual who is responsible for notifying patients about the custodian's health information systems, ensuring the systems comply with regulations, and for complying with notice and follow up requirements if information is disclosed contrary to the law, or if it is stolen or lost.

The policy underlying these statutory provisions is that custodians will likely be more accountable and compliant if they have privacy management programs in place and a designated individual who is responsible for compliance. Whether such a designated individual is appropriate in an academic workplace will depend on the individual circumstances of your academic institution.

By negotiating appropriate protections as set out in this document, the collective agreement will protect the health information of your members. But additional protection is achieved by requiring the employer to disclose to the academic staff association details of its information management and security systems that relate to health information. This disclosure should include a requirement to notify the association promptly if there is a security breach related to health information or an improper disclosure of same, so that the association is able to monitor compliance and enforce its members' privacy rights.

Privacy rights are important rights of employees and, while public policy recognizes and goes some distance to protect those rights through health information protection laws, employees cannot depend entirely on statutory protections. Negotiating strong collective agreement language, and vigilantly monitoring the employer's conduct and enforcing the terms of the agreement are necessary to ensure protection of health information in your workplaces.

Jurisdictions in Canada that Have Laws which Specifically Protect Personal Health Information

- *Health Information Act*, RSA 2000, c H-5 (Alberta)
- *Personal Health Information Act*, CCSM c P33.5 (Manitoba)
- *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05 (New Brunswick)
- *Personal Health Information Act*, SNL 2008, c P-7.01 (Newfoundland and Labrador)
- *Personal Health Information Act*, SNS 2010, c 41 (Nova Scotia)
- *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A (Ontario)
- *An Act Respecting the Sharing of Certain Health Information*, CQLR c P-9.0001 (Quebec)
- *The Health Information Protection Act*, SS 1999, c H-0.021 (Saskatchewan)
- *Health Information Privacy And Management Act*, SY 2013, c 16, [Not yet in force] (Yukon)