Practice Tool for Exercising Discretion:

Emergency Disclosure of Personal Information by Universities, Colleges and other Educational Institutions

October 2008

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER — for — British Columbia

David Loukidelis
Commissioner

Information and Privacy Commissioner of Ontario

Ann Cavoukian, Ph.D.
Commissioner

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

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038, Stn. Prov. Govt.
Victoria, BC V8W 9A4
CANADA
250-387-5629
1-800-663-7867
Fax: 250-387-1696
Website: www.oipc.bc.ca

Practice Tool for Exercising Discretion:

Emergency Disclosure of Personal Information by Universities, Colleges and other Educational Institutions

In emergency situations, privacy laws in Ontario and British Columbia[1] **do not** prohibit universities, colleges or other educational institutions from responsibly disclosing a student's personal information, including information about their mental, emotional or other health conditions, to parents or others who may be able to help in a crisis.

Ontario's *Freedom of Information and Protection of Privacy Act* (Ontario *FIPPA*) and *Municipal Freedom of Information and Protection of Privacy Act* (Ontario *MFIPPA*) permit the disclosure of personal information "in compelling circumstances affecting the health or safety of an individual." They also allow for disclosure "in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased."[2]

Ontario's *Personal Health Information Protection Act* (Ontario *PHIPA*) also allows for the disclosure of personal health information if the health information custodian[3] "believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons." Ontario *PHIPA* also permits disclosure "for the purpose of contacting a relative, friend or potential substitute decision-maker of the individual, if the individual is injured, incapacitated or ill and unable to give consent personally."[4]

Similarly, BC's *Freedom of Information and Protection of Privacy Act* (BC *FIPPA*) allows for the disclosure of personal information if "compelling circumstances exist that affect anyone's health or safety." BC's *FIPPA* also allows disclosure "so that the next of kin or a friend of an injured, ill or deceased individual may be contacted."[5] BC's *Personal Information Protection Act* (BC *PIPA*), which applies to the private sector, contains similar provisions.[6]

In other words, ***life trumps privacy***, and our laws reflect that reality.

Tragedies should not occur as a result of a misunderstanding of privacy legislation.[7] There is no question that the decision to disclose a student's personal information without consent is extremely difficult and requires a reasoned judgment call.[8] The decision rests, on a case-by-case basis, with whoever is responsible, be that a doctor, student counsellor, residence advisor or the head[9] of an institution. A great deal of deliberation and discretion must be exercised, often very quickly. The decision must be made very carefully and sensitively, but privacy laws do not stand in the way of an educational institution's ability to make this decision, where appropriate.[10]

Disclosure of Personal Health Information

Example: Significant Risk of Serious Bodily Harm

A student has been receiving psychological treatment at the university's counselling centre. The student's psychologist has noted that the student is severely depressed and also suspects a dependency on prescription drugs. The psychologist believes that there is a risk of suicide and would like to involve the student's family physician, immediate family member, or another emergency contact, in the student's therapy. However, the student has specifically instructed the psychologist not to disclose any personal health information to anyone. Over a week-long break in the academic year, the student calls the psychologist from out of town. The student's speech is slurred and he is threatening to end his own life. Our privacy laws would allow the psychologist to disclose the student's personal health information to a third party if the disclosure was believed to be necessary to reduce the significant risk of serious bodily harm, such as suicide.

The approach taken in these laws to the disclosure of personal health information in emergency circumstances reflects the current approach taken by the courts in both the United States and Canada.[11] The disclosure of personal health information allowed by BC and Ontario privacy laws is also consistent with disclosure permitted by the rules governing medical professionals such as physicians, nurses and psychologists.[12] For example, the College of Physicians and Surgeons of Ontario's Policy – Confidentiality of Personal Health Information, says that a "physician may disclose personal health information about an individual if the physician believes, on reasonable grounds, that the disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm to a person or group of persons." The situation is similar in BC. For example, the code of conduct for professional psychologists allows disclosure without consent "to protect against a clear and substantial risk of imminent and serious harm to the client" or others. And even if there is a conflict between these laws and other requirements, including professional codes of conduct, each of these privacy statutes prevails unless another statute explicitly overrides it.[13]

Disclosure of Personal Information in the Public Interest

The above example applies to a health information custodian working for a university or college. As noted above, Ontario *FIPPA*, Ontario *MFIPPA* and BC *FIPPA* contain similar emergency disclosure provisions that allow student residence advisors, school counsellors, and other personnel to disclose a student's information, without consent, where they become aware of compelling circumstances affecting the health or safety of an individual or others. This includes serious mental health concerns or threats of violence.

In addition, BC *FIPPA*, Ontario *FIPPA*, and Ontario *MFIPPA* all allow – and actually require – disclosure of a student's personal information if there is a risk of significant harm to their health or safety or that of another individual. In Ontario, an institution's head must, "as soon as practicable, disclose any record to the public or persons affected if the head has reasonable and probable grounds to believe that it is in the public interest to do so and that the record

reveals a grave… health or safety hazard to the public."[14] In BC, an institution must, "without delay, disclose to the public, [or] to an affected group of people…information about a risk of significant harm to the…health or safety of the public or a group of people."[15]

Example: Significant Risk of Harm to the Public

A school counsellor has observed that one of her student patients is very angry and has been expressing feelings of deep despair and hopelessness. He blames others for his misfortunes and has expressed ideas of "getting even." The student has no known friends. The counsellor has read essays written by the student that are violent, graphic and very disturbing. Having mentioned his blog, the counsellor read a number of the student's postings that were also disturbing and self-aggrandizing. One blog posting included a photo of the student with what appears to be an improvised explosive device. The counsellor's professional opinion is that the student is on the verge of a breakdown and she is concerned that he will harm himself or others. She recognizes her duty to respect the student's privacy, but believes there is a significant risk that the student may act out his desire for revenge. She determines that it may be necessary to disclose the student's personal information in order to prevent significant harm to the student, fellow students, or to the public.

Several other urgent situations are described in the Fact Sheet, Disclosure of Information Permitted in Emergency or other Urgent Circumstances, available on the Ontario IPC's website, **www.ipc.on.ca**.

Notification of Disclosure

If a student's personal information is disclosed, you may be required to give notice of the disclosure to the student. Different *Acts* have different notification requirements. In compelling circumstances affecting the health or safety of an individual, Ontario *FIPPA* and *MFIPPA* require that upon disclosure, notification be mailed to the last known address of the individual to whom the information relates.[16] BC *FIPPA* allows for postponing notification if "the head of the public body considers that giving this notice could harm someone's health or safety."[17]

If personal health information is disclosed pursuant to Ontario *PHIPA*, it requires, subject to certain exceptions, that notification be given to the individual at the "first reasonable opportunity."[18] BC *PIPA* requires notice under the *Act* to be mailed to the last known address of the individual whose personal information is being disclosed.[19]

In Ontario, before disclosing personal information for reasons of public health and safety, notice must be given to any person to whom the information in the record relates, if it is practicable to do so.[20] In BC, before disclosing personal information for reasons of public health and safety, the head must notify, if practicable, any third party to whom the information relates, and the BC Information and Privacy Commissioner. If notice is not practicable, the head must mail a notice to the last known address of the third party, and to the BC Information and Privacy Commissioner.[21]

Be Prepared – Have a Clear Policy & Procedure

Educational institutions must balance many factors when responding to situations that involve health and safety. The key is to ensure that relevant staff understand the privacy rules and are able to move quickly to make good decisions. Institutions should have clear policy and procedures in place well in advance, to provide guidance on how to respond. These will be invaluable in making a timely decision and rapidly communicating that decision to affected individuals.[22] It is equally important to regularly educate and train all staff on relevant policy and procedures and on the basics of what privacy laws permit in emergency situations.

1. Notice to Students

Provide an explanation to all students (and parents, if applicable) about the possible disclosure of personal information without consent in emergency situations, for example:

- when emergency contact information is collected;
- in orientation packages or at orientation sessions, especially if parents participate;
- at the point of professional counselling.

The notice could also include information detailing how the institution will notify students, parents or emergency contacts of an emergency situation such as a lockdown, e.g. by use of a phone tree, text message system, or notification on the institution's website.

2. Accurate Emergency Alert Information

In situations where there is an immediate threat to students and staff, notification of the threat or an emergency alert should be readily available to all members of a college or university community, whether it is:

- posted prominently at every public phone;
- sent by text message;
- through one click on the home page of an institution's website;
- at every common-use computer monitor, or other communication device.

It is also important to have up-to-date emergency contact information for all students. In an urgent situation, there is no time to hunt for the new phone number of a student's parent or emergency contact. The information should be regularly confirmed with students, perhaps by requiring that it be reviewed and confirmed through a check-off box (online or in person) before registration is permitted for a new school year.

3. Clear Decision-Making Roles and Responsibilities

Deciding to disclose personal information without consent is extremely difficult, requiring a very sound judgment call; nonetheless, the decision must be made. A great deal of deliberation and discretion must be exercised, yet the time for deliberation may be extremely limited. In consultation with mental health professionals, establish decision-making processes, assign roles, designate who is to maintain them and communicate this information to all involved. You must ensure that these include risk-assessment criteria to guide decisions in a prudent yet timely fashion.

Emergency Disclosure Contact

You must also be able to activate a pre-established communication method among relevant colleagues at a moment's notice. Immediate consultation supports both decision-making and initial steps in implementing the action plan.

4. Constant Effort – Educate, Train, Practice, Evaluate

Educate all stakeholders broadly and repeatedly. Train your staff on all relevant policies and practice using your protocols. Coordinating people from different areas and systems will require a well-communicated structure and procedure. Setting up scenarios and role-playing situations may assist in ensuring that when a rapid response is actually needed, it will be forthcoming.

Example: A Well-Prepared Protocol

Continuing from our second example, a counsellor has observed disturbing behaviour on the part of one of her student patients that leads her to believe that the student is on the verge of a breakdown. Concerned that the student will harm himself or others, she thinks that it may be necessary to disclose the student's personal information in order to prevent significant harm to the student or to the public. The counsellor calls the pre-established Emergency Disclosure Contact, who is immediately available to provide advice on the situation. After consultation with the Contact, the counsellor decides whether and how to disclose the student's personal information. The Contact also assists the counsellor in deciding whether to contact the police or security persons and/or take other appropriate action. If disclosure occurs and notification is required, the counsellor would notify the student of the disclosure, and prepare a written report. If the disclosure occurs, the Contact would then debrief and evaluate the protocol, with the goal of implementing appropriate adjustments.

Tips for Developing Policies – Taking Action in Emergencies

No matter who first becomes aware of an urgent situation, or under what circumstances, if the decision is made to disclose without consent, the course of action to be taken should be clear. The following are points to consider in creating a policy:

1. Know Who to Call

All faculty and staff must know the phone number or email address of the Emergency Disclosure Contact. They have to know that their call will be answered immediately.

2. Discuss How to Proceed

Immediately establish communication between the Emergency Disclosure Contact and the individual who initiated the emergency call, to obtain advice on how to proceed. The Emergency Disclosure Contact may be available in an advisory capacity, or may be the designated decision-maker.

The Emergency Disclosure Contact should:

- be available on a standby basis to provide advice;
- have expertise in what is permissible under privacy laws regarding emergency disclosures (this person could be, for example, the institution's FOIP coordinator);
- have a reliable backup available during periods of absence or vacation;
- be able to coordinate quickly, through a pre-established plan, with other relevant individuals such as colleagues, staff, security and police, if necessary.

3. Decide Manner and Scope of Disclosure

Decide whether any information should be disclosed, exactly what information must be disclosed and to whom. If the decision is made to disclose, the time and manner of the disclosure should be decided. Also decide whether the police or security persons should be notified, and other appropriate actions to be taken.

4. Notify and Document

If personal information or personal health information is disclosed, notify the individual whose information is disclosed, if necessary, and document that notification. (See above section on "Notification of Disclosure").

After disclosure, the Emergency Disclosure Contact should debrief and evaluate, with the goal of implementing any appropriate adjustments and training of staff.

More information

This fact sheet does not offer solutions for decision-making in individual cases under our privacy laws or other laws. It is intended to offer general information to those working in educational institutions about what our privacy laws actually provide for in this area. The most important point is that privacy laws **permit** the disclosure of personal information and personal health information, without consent, in emergency or urgent situations.

For further information about privacy legislation, visit our websites:

Office of the Information & Privacy Commissioner of Ontario: **www.ipc.on.ca**

Office of the Information & Privacy Commissioner for British Columbia: **www.oipc.bc.ca**

Endnotes

1. The relevant statutes in Ontario are the *Freedom of Information and Protection of Privacy Act* (Ontario *FIPPA*), the *Municipal Freedom of Information and Protection of Privacy Act* (Ontario *MFIPPA*) and the *Personal Health Information Protection Act, 2004* (Ontario *PHIPA*). Please see **http://www.e-laws.gov.on.ca/**. The relevant statutes in British Columbia are the *Freedom of Information and Protection of Privacy Act* (BC *FIPPA*) and the *Personal Information Protection Act* (BC *PIPA*). Please see **http://www.oipc.bc.ca/legislation.htm**.

2. Please see sections 42(1)(h) and (i) of Ontario *FIPPA* and sections 32(h) and (i) of Ontario *MFIPPA*.

3. "Health information custodian" and "personal health information" are defined terms in Ontario *PHIPA*. Please see sections 3 and 4 of Ontario *PHIPA*.

4. Please see sections 38(1)(c) and 40(1) of Ontario *PHIPA*.

5. Please see sections 33.1(m) and (n) of BC *FIPPA*.

6. BC's *Personal Information Protection Act* (BC *PIPA*), which applies to the private sector—including healthcare professionals in private practice—allows disclosure without consent where there are reasonable grounds to believe that compelling circumstances exist that affect the health or safety of any individual. It also allows disclosure without consent where it is clearly in the interests of the individual and consent cannot be obtained in a timely way. And it permits disclosure to the next-of-kin or a friend of an injured, ill or deceased individual.

7. This was similarly noted by the Virginia Tech Review Panel (discussing misperceptions regarding US privacy law) in its report on the shooting that occurred on its campus on April 16, 2007. For more information, please see the Virginia Tech Review Panel Report at **http://www.governor.virginia.gov/TempContent/techPanelReport-docs/FullReport.pdf**. Please also see Letter from Ontario Commissioner Dr. Ann Cavoukian to Governor Tom Ridge, dated August 31, 2007.

8. Please see Letter from Ontario Commissioner Dr. Ann Cavoukian to Ontario colleges and universities, dated April 28, 2008.

9. "Head" and "personal information" are defined terms in Ontario *FIPPA* and Ontario *MFIPPA*. Please see section 2 of Ontario *FIPPA* and section 2 of Ontario *MFIPPA*.

10. Privacy laws in Ontario and BC protect individuals who disclose a student's personal information, as long as they acted in good faith and reasonably under the circumstances, from legal actions or proceedings. This protection includes, among other things, the disclosure of information or failure to disclose information, and the failure to give a required notice, if reasonable care is taken to give the required notice. Please see section 62(2) of Ontario *FIPPA*, section 49(2) of Ontario *MFIPPA*, section 71 of Ontario *PHIPA* and section 73 of BC *FIPPA*.

11. Please see *Smith v. Jones*, [1999] 1 S.C.R. 455, where the Supreme Court of Canada found that the safety of the public is of such importance that, where there is an imminent risk of serious bodily harm or death to an identifiable person or group, solicitor-client privilege may be set aside (paras. 35 and 78). Please also see the US case of *Tarasoff v. Regents of the University of California*, 131 Cal. Rptr. 14 (1976, S.C.).

12. Statutes and policies that govern confidentiality of personal health information in Ontario include: Regulation 856/93 to the *Medicine Act, 1991* and Policy – Confidentiality of Personal Health Information (for physicians); Regulation 799/93 to the *Nursing Act, 1991* and Policy – Personal Health Information (for nurses); and Regulation 801/93 to the *Psychology Act, 1991* and Canadian Code of Ethics (for psychologists).

13. Please see section 67 of Ontario *FIPPA*, section 53 of Ontario *MFIPPA*, section 7(2) of Ontario *PHIPA*, section 79 of BC *FIPPA*, and section 3(5) of BC *PIPA*.

14. Please see section 11 of Ontario *FIPPA* and section 5 of Ontario *MFIPPA*.

15. Please see section 25 of BC *FIPPA*.

16. Please see section 42(1)(h) of Ontario *FIPPA* and section 32(h) of Ontario *MFIPPA*.

17. Please see section 33.1 (m) (ii) of BC *FIPPA*.

18. Please see section 16(2) of Ontario *PHIPA*.

19. Please see section 18(1)(k) of BC *PIPA*.

20. Please see section 11(2) of Ontario *FIPPA* and section 5(2) of Ontario *MFIPPA*.

21. Please see section 25 (3) and (4) of BC *FIPPA*.

22. The Virginia Tech Review Panel Report, published in August 2007, recommends the development of accurate guidelines and adoption of best practices to assist institutions to employ their discretion in appropriate ways. A report of the September 13, 2006 Dawson College shooting published by the Quebec coroner's office on September 5, 2008, also recommends that public institutions have emergency plans in place to deal with catastrophic events.

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

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038, Stn. Prov. Govt.
Victoria, BC V8W 9A4
CANADA
250-387-5629
1-800-663-7867
Fax: 250-387-1696
Website: www.oipc.bc.ca