Information, Privacy and You

The primary pieces of access and privacy legislation that apply to the University of Manitoba are The Freedom of Information and Protection of Privacy Act (FIPPA) and The Personal Health Information Act (PHIA). FIPPA and PHIA provide the public the right of access to records in the custody or under the control of the University. The Acts also ensure privacy by placing restrictions on the collection, use and disclosure of personal information by public bodies and personal health information by trustees.

Frequently Asked Questions

How does access and privacy legislation affect me?

As an employee of the University of Manitoba, you are subject to restrictions on the collection, use, disclosure and destruction of personal information and personal health information during the performance of your duties. Furthermore, the records you create and maintain may be subject to access to information requests by the public.

Which records are covered by FIPPA and PHIA at the University of Manitoba?

FIPPA and PHIA applies to all recorded information in the custody or under the control of the University and its Colleges, including student records, human resource files, financial records, contracts, administrative records and employee email.

The Acts do not extend to information that may be considered exempt from disclosure, such as teaching or research materials.

What type of information would be considered “personal information” and “personal health information”?

Personal information is recorded information about an identifiable individual. This includes name, address, telephone or fax number, information about age, gender, ethnic origin, financial information, genetic information, or any identifying number such as the Social Insurance Number, student number, driver's license or credit card number, and so on.

Personal health information is information about an identifiable individual that relates to an individual's health and health care history including genetic information, the provision of health care to the individual, or payment for health care provided to the individual. This includes doctor’s notes, accommodation information, Personal Health Information Number (PHIN) assigned by Manitoba Health, as well as any identifying information collected in the course of providing health care services.

How do I post or return student assignments/grades/feedback while maintaining student privacy?

Reasonable security precautions must be employed when returning assignments and grades, as they are considered to be the student’s personal information. Avoid the use of student numbers on the front pages of tests and papers, and do not allow tests and papers to be left outside an office door or in a public area where students or passers-by can gain access to student numbers, grades and comments. Devise a method for receiving and returning tests and papers that will protect students’ personal information, such as returning them in class. Do not share or post lists of student grades electronically or physically post them in any location. Marks may only be shared with students on an individual basis, such as using the Gradebook function in Desire2Learn.
What are the restrictions for collecting students’ personal information?

Access and privacy legislation requires that we only collect the minimum amount of information necessary to carry out our duties. For the personal information we do collect, we must appropriately notify students of the specific purpose of that collection, and we must ensure the protection of that information.

Should I collect/copy doctor’s notes from students?

Students may be asked to produce a doctor’s note to verify or excuse an absence. It is recommended that documentation containing personal health information not be collected or copied by University faculty and staff unless it is necessary to do so for a specific authorized purpose. Rather than collecting this sensitive personal information, it is preferable to make a general note indicating the acceptance of a doctor’s note in the student’s file and then return the note to the student.

What can I do with the personal information and the personal health information I collect from students?

The personal information and personal health information collected from students should only be used for the authorized purposes for which it was originally collected, unless students provide informed and written consent about additional uses of their information. Personal information obtained for administrative purposes should not be used for faculty research or personal use without the express written consent of the students involved.

What student information can I share with others?

The personal information and personal health information of students should only be shared with those that need it to do their jobs at the University (administration, colleagues, etc.). Even then, only the minimum amount of information necessary for an authorized purpose should be shared with those that need to know. The personal information and personal health information of students should not be shared outside of the University (parents, family members or friends) without the prior written consent of the student.

How long should I keep student records/files/information?

The personal and personal health information collected from students should only be kept for the minimum amount of time necessary. This includes information relating to grades, marks, financial information (Social Insurance Numbers, remuneration, etc.), correspondence, illnesses, etc. Consult your University of Manitoba faculties and departments, or the Access and Privacy Office for approved retention periods (Records Authority Schedules) which meet your legal and operational needs.

Is it acceptable to use cloud-based services (e.g. Dropbox, Google Docs, Google Drive or SkyDrive) to collect and hold student data, such as images, names, student numbers, assignments or marks?

Data storage and file sharing services are growing in popularity because of the convenience they provide and the ease at which they allow for collaborative work. However, any records or data containing personal information or personal health information should not be posted to any data storage or file sharing services. Additionally, any records or data classified as confidential, restricted or protected, as outlined in the Data Classification Guidelines, should not be posted to any data storage or file sharing service.

Contact Us

Access and Privacy Office, 233 Elizabeth Dafoe Library, Fort Garry Campus, 204.474.9462, fippa@umanitoba.ca