Freedom of Information and Privacy

Training Refresh

Outline

Professional Recordkeeping

Disclosure and Use of Personal Information

Security of Personal Information

FIPPA Principles

The public has a right to request/access most records

But, FIPPA sets out specific and limited exemptions/exclusions

Protect the privacy of individuals' personal information (P.I.)

Oversight by the Information and Privacy Commission (IPC)

(FIPPA brought refinements and specific requirements to established University values and long-standing practices)

Coverage

FIPPA covers

all recorded information

in the custody or

under the control

of the University.

INCLUDES

everything, e.g. drafts, post it notes, computer files, e-mails, blackberry files, agendas etc. – everything!

VERBAL DISCLOSURES of personal information also covered

Some Reasons For Professional Recordkeeping

- No exemption for embarrassment
- Disclosure could occur for many reasons, **such as**:
- FIPPA, lawsuit, disgruntled individual, accident, data breach, evolving transparency expectations … etc. etc.
- Consider possible disclosure as you create records
- Today's e-mail could be tomorrow's headline
- What would be the effect on the University?
- How would you feel?

Professional Recordkeeping What to do …

- Create all operationally necessary records
- Official records are needed to demonstrate due diligence
- Write in a professional manner
- Always create excellent records
- Eliminate unnecessary copies, drafts/earlier versions
- Delete/shred transitory records on an on-going basis
- When appropriate, a phone call can be faster, clearer

Language and Tone

- Use gender neutral language
- Include informative, helpful, kind comments
- Beware expressions of prejudice, racism, sexism, etc
- Carefully consider comments with possible legal repercussions
- Don’t prejudge issues
- Avoid cruel or sarcastic language
- Omit unnecessary opinions, comments

E-mail

- E-mail is a record under FIPPA – treat like any other record
- Access rights and privacy protections apply
- UTOR to UTOR mail is considered secure
- E-mail outside UTOR is not secure – must encrypt if P.I.
- Assume e-mails are copied, printed, forwarded, archived etc.
- Same rules apply to voicemail
- Use caution when leaving voicemail messages outside U of T
  Consider who might access it, how it might be used, etc…

Personal Information Is…

- **Recorded** information about an **identifiable** individual
- e.g. student numbers, grades, work, address, email, photos, videos of identifiable individuals, situational information

- …but be careful because **verbal disclosures** matter too
- Take care with possible contextual identification
- Consider all sources, directories, articles, community &c
- Small cell principle; one in five-**plus** (for one attribute)

- Information in business/professional capacity **not** P.I.
  - e.g. name, position, routine work actions/information
  - **But** errors, omissions, misconduct, offenses usually are

Personal Information Use and Disclosure

- Emergency situations: **Never Hesitate** in emergencies!!
- Compelling circumstances affecting health or safety **Emergency disclosure** (health and safety trumps privacy)
- For the purposes for which it was collected
- With the individual's consent
- Internally on a **need-to-know** basis
- Very limited other circumstances

Need To-Know Information Sharing

- P.I. may be disclosed to a…
- University officer, employee, consultant* or agent* who…
- needs the record in the performance of their duties and…
- is necessary in the discharge of the University's functions.
- **Both the provider and the recipient of information are responsible for following the need-to-know rule**

* Only with a confidentiality agreement, reviewed by University legal counsel, to protect personal information kept offsite or shared with consultants and agents acting on the University's behalf

Emergency Disclosure

- P.I. may be disclosed in compelling circumstances to protect health or safety
- E.g. disclose to health care providers and/or family to help a distressed individual or to prevent a suicide
- Try to consult with your manager or appropriate University officials, but act if you can't contact them
- Immediately contact emergency response services or police if imminent injury, threat, danger or violence

  * Safety always takes precedence

Security

Protect P.I. and confidential* information **At all times!!**

Electronic records:

Keep in secure University server with restricted user rights (password, timed lockouts etc.) Outside secure server –only with permission– and use properly implemented encryption at all times, e.g. personal computer, laptop, portable hard drive, memory stick, mobile device. Access P.I. from outside University premises by using an encrypted secure means such as a virtual private network or encrypted remote desktop connection. Encrypt P.I. in emails sent externally.

Hard copy records:

Keep in secure institutional environment; locked file cabinets when unattended, locked office doors to where personal information is kept when not in use, outer locking door, including after hours. Outside secure institutional environment –only with permission– and use strong, effective security, e.g. do not leave records unattended in a vehicle, lock up when at home, etc

* Records/information are confidential unless **designated** public

Retention, Disposal

Maintain P.I. for at least **a year** after its **last** use

Do not destroy requested records

Dispose of P.I. securely - render information irretrievable, e.g. crosscut shred paper records, destroy or overwrite with “junk” data, consult IT department for computer drives

Privacy Risks

Privacy breach can happen in an instant, even when not at work

Most common breach is disclosing PI to unauthorized individual(s)

- e-mailing P.I. to wrong people
- not preventing unauthorized people from accessing data bases
- lost or stolen laptop or USB key, etc.

Be cautious about e-mailing to groups or “Reply to All”

The more sensitive the information, the higher the risk

Whenever dealing with PI - err on the side of privacy.

Privacy Event Response

Possible privacy breach?

- e.g. inappropriate disclosure of personal information

Immediately notify manager and FOIL. FIPP Office will;

- Stop problem
- Remedy harm
- Notify affected individuals
- Educate staff, fix processes
- Involve/notify IPC

If in doubt, always notify! – including requests for personal information by law enforcement agencies

Practices

- **FIPPA - Guideline Regarding Security for Personal and Other Confidential Information**
- www.provost.utoronto.ca/policy/FIPPA_-_Guideline_Regarding_Security_for_Personal_and_Other_Confidential_Information.htm
- **FIPPA–General, Administrative Access & Privacy Practices**

- Use or disclosure of personal information
- Privacy Event Responses
- Records management
- Secure destruction, etc.

- www.provost.utoronto.ca/Assets/Provost+Digital+Assets/Provost/fippa.pdf

Summary

Professional Record Keeping

Disclosure and Use of Personal Information

Security of Personal Information

Contact us!

Rafael Eskenazi
FIPP Director
(416) 946-5835
rafael.eskenazi@utoronto.ca

Howard Jones
FIPP Coordinator
(416) 946-7303
howard.jones@utoronto.ca

FIPP Office
McMurrich Building
Room 104
www.fippa.utoronto.ca