Privacy with Your Wearable Devices and Your Friends: Alexa, Siri, and Google

Brian Beamish

Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

BORN Ontario

November 7, 2019

Privacy 101

Our Office

- Provides independent review of government decisions and practices on access and privacy
- Commissioner is appointed by, and reports to, the Legislative Assembly to ensure impartiality
- Oversees Ontario's access and privacy laws
- These laws establish the public's right to access government-held information and protect their personal privacy rights

IPC's Mandate

- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - Covers 300 provincial institutions
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - Covers 1,200 municipal organizations
- *Personal Health Information Protection Act* (*PHIPA*)
  - Covers individuals and organizations involved in the delivery of health care services
- Expanded Mandate: *Child, Youth and Family Services Act*

Federal Privacy Legislation - *PIPEDA*

- The collection, use and disclosure of personal information in the commercial sector is regulated by federal privacy legislation under the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)
  - *PIPEDA* applies to all commercial activities, including those involving phi

PHIPA Protects PHI

Some of the features of PHIPA include:

- Consent-based
- Limits on collection, use and disclosure
- Requires data minimization
- Firm restrictions on secondary use
- Responsibility for data security

What is Consent?

- Consent must be:
  - Given by the individual
  - Knowledgeable
  - Relate to the information
  - No deception/coercion

- The collection, use and disclosure of PHI for purposes other than health care requires **express consent**

Privacy and Wearable Devices

Disruptive Technology

- A product or technology that displaces established technology or fundamentally changes, or creates, an industry
  - online banking, robotics and WiFi are forms of disruptive technologies that have changed the way we live, work and even receive health care.
  - Wearable technology – can monitor fitness, sleep patterns, vital signs.
  - Data can be transmitted to wearer or to a server.

Benefits of Wearable Technologies

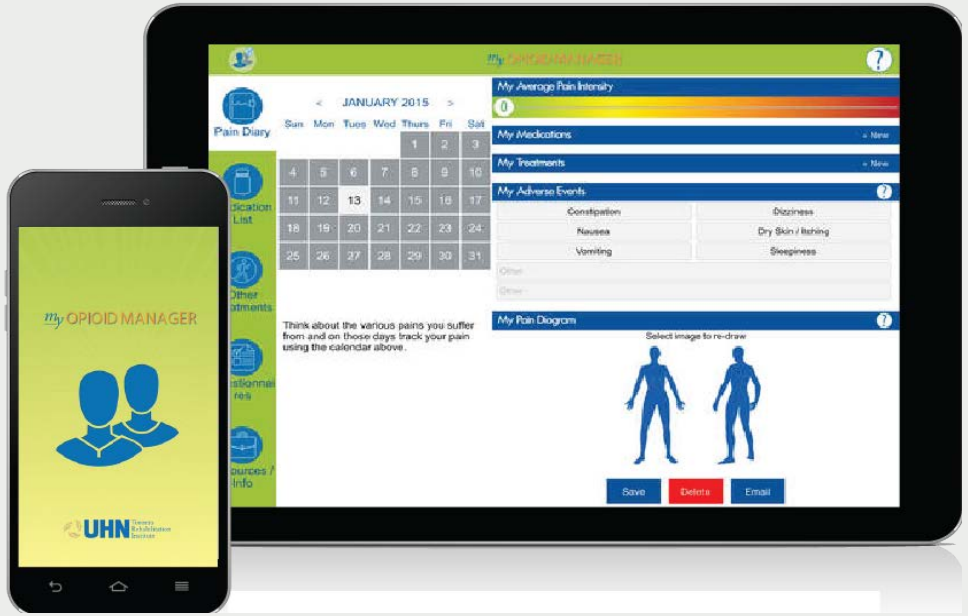
- The benefits of wearable devices are undeniable and constantly expanding:
  - store health and wellness data (i.e.: heart rate, blood pressure, respiratory rates, blood glucose levels and body temperature)
  - track disease management and log symptoms or side effects
  - provide educational information
  - set reminders to take medication or keep appointments

There are Privacy Risks!

- Wearables and apps collect and store highly sensitive data including:
  - PHI
  - personal information
  - location
  - lifestyle and spending habits
- Data is highly valuable to data brokers, product developers, retailers, and insurance companies
- Clinical and social researchers are also interested in health and lifestyle data
- Law enforcement has used Fitbit data to locate individuals
- Hackers constantly seek access to personal information

Legislative Oversight

- Custodians that develop wearables or apps must ensure they comply with Ontario's health privacy law
- Custodians that use commercial wearables or apps for health care must also ensure *PHIPA* compliance
- *PHIPA* also applies to the use of non-health care related apps, such as when a custodian transmits information via What's App



Legislative Oversight

- Commercial development of health apps by corporations is subject to federal privacy law, *PIPEDA*
- American *HIPAA* compliant apps and devices may not comply with *PHIPA* or *PIPEDA*

Commercialization of Data

- Concerns about consent to use and disclose PHI arise from companies selling the data.
- Data aggregators and data brokers buy and sell PHI or mass aggregate data sets
- Insurance companies, for example, may wish to raise premiums or refuse coverage based upon data that they use to re-identify an individual
- Whether users are expressly and knowingly consenting to these “data for sale” transactions is a fundamental privacy concern

Consent

- Many users are not aware, or do not read the company policies, on how their data could be used or disclosed, including whether it is sold to third parties
- Options for withdrawing or modifying consent on some commercial apps can be limited and difficult for average users to understand
- Is consent for secondary uses real?

Data collected by HICs

- Under *PHIPA*, HICs must not collect or disclose more information than is necessary, for the purpose of the collection (data minimization)
- Custodians are often asked to provide PHI to third party app developers for health care related purposes – is consent required even if de-identified?
- Health care providers can ‘repurpose’ data collected and tracked on a wearable device for non-medical reasons such as diet or exercise
  - Under *PHIPA* data acquired through third party software or app becomes PHI

Security Practices

- Strong privacy protection and security practices are crucial for protecting data
- Use strong security preferences and passwords
- Data encryption and secure storage
- Who has access to data?
- HICs need to ensure data sharing agreements are in place when using wearables or apps
- HICs should urge caution when recommending the use of wearables or apps to their patients – due diligence is required

In Case of Breach - Duty to Notify

Notification of individual

- A HIC must notify the individual at the first reasonable opportunity if personal health information is stolen, lost or used or disclosed without authority
- In the provincial electronic health record, the HIC must also notify the individual at the first reasonable opportunity if it is collected without authority

Notification of the IPC

- A HIC must also notify the IPC of a theft, loss or unauthorized collection, use or disclosure in most circumstances

Considerations for Commercial Wearables and Apps

- When selecting a commercial wearable or app consider:
  - is data encrypted during all stages of transmission and storage?
  - Who has access to the data, and is access being monitored to ensure only authorized access?
  - Are security measures reviewed, tested and updated?
  - Are there data agreements in place between companies that contain sufficient privacy protection requirements?
  - Has the information been properly anonymized to prevent individual identification?
  - If the data is destroyed, what processes are used to ensure it is safely destroyed to prevent reconstruction?
  - Is consent informed/knowledgeable to support sale/disclosure to third parties?

This is truly an exciting time to be in healthcare. The possibilities of digital tools to improve patient wellness and healthcare are extraordinary. We should not let the promise go unfulfilled, but we must also take care.

Eric Parakslis, Harvard Medical School

Questions?

CONTACT US

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965