eQOL Inc. Corporate Privacy Policy: Our Commitment to the Protection and Security of Personal Health Information

Version 1.05

January 26, 2018

Approval History

Approved by	Title	Approved Date
Binh Nguyen	CEO	09/2014
Jonathan Tomkun	Product Development Manager	09/2014
Jonathan Tomkun	Product Development Manager	02/2016
Jonathan Tomkun	Product Development Manager	03/2016
Binh Nguyen	CEO	09/2016
Jonathan Tomkun	Product Development Manager	09/2016
Jonathan Tomkun	Product Development Manager	04/2017
Jonathan Tomkun	Product Development Manager	01/2018

Revision History

Version	Version Date	Modifications Summary	Modified by
1.01	Feb 16, 2016	Preliminary modifications for Canada Health Infoway & Ontario Telemedicine Network review	Jonathan Tomkun
1.02	Mar 14, 2016	Modifications based on Canada Health Infoway feedback	Jonathan Tomkun
1.03	Sep 12, 2016	Scheduled review and update	Jonathan Tomkun
1.04	Apr 5, 2017	Review and update	Jonathan Tomkun
1.05	Jan 26, 2018	Review and update	Jonathan Tomkun

eQOL's Corporate Privacy Policy will be reviewed biennially by eQOL's Product Development Manager (PDM) to ensure accuracy and completeness.

For further information regarding eQOL's Privacy Policy, contact eQOL's PDM. The PDM may be contacted by:

Telephone	647-479-4615
Email	support@eqol.ca
Mail	Product Development Manager, eQOL Inc. 2487 Bloor Street West, Suite 1 Toronto, ON M6S 1R5

Contents

1 Purpose

This document is intended to describe eQOL's Privacy Policy, including the requirements and responsibilities related to the protection of personal health information (PHI) that is collected, used or disclosed by eQOL.

eQOL provides services to health information custodians (HICs) that enable them to access and maintain a more accurate and up-to-date record of patient health. To carry out these services, eQOL collects, uses, retains and discloses PHI as part of its regular business operations.

PHI is defined as identifying information about an individual that relates to their physical or mental health. This might also include the health history of an individual's family, the individual's health card number, or any information that could link an individual to a particular health care provider. eQOL is committed to the protection of PHI, and strives to meet and exceed the requirements laid out in all applicable legislation for the protection of this important information.

2 Scope

This Policy applies to all eQOL employees and the agreements that eQOL establishes with HICs that it provides services to. The Policy pertains to all services and business activities that may impact the privacy and security of PHI that eQOL collects, uses or discloses, including electronic, written and verbal PHI. eQOL is bound by the regulations within the Personal Health Information Protection Act, 2004 (PHIPA) for use and disclosure. PHIPA is an Ontario health privacy law that establishes rules for the management and protection of PHI for health care service providers and HICs. eQOL is not a HIC with respect to the PHI handled through its services; eQOL may act as an "agent" for HICs, as defined in PHIPA. eQOL also adheres to regulations regarding the collection, use, and disclosure of personal information by private sector organizations as laid out at the federal level (*Personal Information Protection and Electronic Documents Act (PIPEDA)*) and by other provinces with laws deemed substantially similar to PIPEDA by Industry Canada (*Personal Information Protection Act (PIPA)* in British Columbia and Personal Health Information Act (PHIA) in Nova Scotia). eQOL also strives to comply with the International Organization for Standardization (ISO) and the International Electrotechnical Commission's (IEC) Information technology – Security techniques – Code of practice for information security management standard (ISO/IEC 27002). ISO 27002 establishes guidelines and general principles for information security management and is promoted as a practical guideline for developing organizational security practices.

HICs include health care practitioners, hospitals and other health institutions, pharmacies, laboratories, and any other person or organization that delivers health care services. Under PHIPA, HICs are authorized to collect, use, retain and disclose PHI in order to provide their services, but they have a responsibility to preserve the privacy and security of the PHI under their care. HICs have control of patients' health records through the ownership of the materials and

systems in which PHI is recorded; however, patients are the sole owners of their PHI.

3 Policy Statement

eQOL shall protect the confidentiality, integrity and availability of information in accordance with legal obligations and the reasonable requirements of the parties that control the information. eQOL shall also protect the integrity and availability of information technology-based services, and will hold individual users accountable for unauthorized or inappropriate access, disclosure, disposal, modification, or interference with sensitive information or services.

4 Privacy Principles

eQOL's Privacy Principles are centered on the *10 Fair Information Practices* of the Personal Information Protection and Electronics Documents Act (PIPEDA), Canada's private-sector privacy law. These principles are often used as the foundation for other PHI privacy regulations, including PHIPA. The definitions for each of the 10 principals were obtained from the Office of the Privacy Commissioner of Canada's website. Visit https://www.priv.gc.ca/en/ for more information.

4.1 Accountability

An organization is responsible for personal information under its control and shall designate an individual or group of individuals who are accountable for the organization's compliance with their privacy principles.

4.1.1 eQOL Inc. Accountability

eQOL is committed to the protection and privacy of PHI that is entrusted to it. eQOL has appointed the Product Development Manager (PDM) to implement and ensure compliance with eQOL's privacy policy. In particular, the PDM will be responsible for:

- Ensuring that eQOL personnel are informed of new services or business operations that involve PHI;
- Deciding when to perform additional privacy impact assessments (PIA) or threat and risk assessments (TRA) as new projects are acquired;
- Implementing any recommendations that result from the completion of a PIA or TRA;
- Ensuring that there is sufficient staff on hand to safely support business operations that involve the collection, use or disclosure of PHI.

In addition to the PDM's role in maintaining PHI security, privacy protection is instilled within company culture and involves all levels of eQOL personnel, including the CEO and board members. The PDM reports all relevant privacy and security information to upper management, who play an active role in the privacy policy at eQOL.

4.1.2 Employee Accountability & Management

In order to protect PHI and reduce the probability of inappropriate viewing and unauthorized use of sensitive data, authorized access to PHI is limited to employees that require access to carry out their employment duties. A description of the specified roles at eQOL and their varying levels of PHI access permissions may be found below:

- Product Development Manager – has access to patient information to oversee clinical operations; clinical operations and technical support staff report to the PDM and escalation of support may be handled by the PDM; the PDM also ensures compliance with privacy policy;
- Clinical Coordinator – has access to patient information in order to provide clinical support to patients and clinicians;
- Back End Administrator – has access to patient information in order to correct any service issues and verify that systems are properly sending and receiving PHI securely;
- eQOL Support Technician – has access to patient account information in order to provide technical support to patients and clinicians;
- Business Administrator – restricted access.

Prior to being approved for employment, candidates must pass verification checks overseen by the PDM to ensure that they are suitable for a position with eQOL. This may include character reference checks, a check for completeness and accuracy of their curriculum vitae, background checks, and confirmation of academic and professional qualifications. Part of the hiring process may include ensuring an understanding of the role of security/privacy in the position and eQOL's expectations. Once employment is confirmed, eQOL personnel receive appropriate training prior to taking part in any operations that involve the collection, use or disclosure of PHI. This training is overseen by the PDM and includes:

- An overview of PHIPA and other applicable legislation;
- A review of eQOL's Privacy Policy;
- A complete description of the employee's role with regard to privacy and security responsibilities and handling of PHI;
- The signing of confidentiality agreements prior to starting employment;
- Awareness training regarding the importance of maintaining confidentiality and for reporting privacy incidents.

Furthermore, the PDM will continuously review the training content and update personnel to ensure that there is an awareness of any new activities that may affect the various privacy/security roles at eQOL (see section 4.1.1 for details). As part of the training on eQOL's policies, all employees must be familiar with the communication channels and processes to receive security advice or to report potential security incidents.

The extent of privacy training and security review will vary depending on the particular role at eQOL. Employees that have access to PHI will be fully prepared prior to being granted access to such information. In addition, those

personnel must also sign confidentiality agreements and may be required to complete additional training to participate in special research projects.

The PDM maintains a record of employees that have received formal training and signed employee agreements on file by keeping a hard and soft copy.

In the event of internal privacy breach or employee misconduct with regards to PHI under eQOL's care, disciplinary actions will be enacted to deter future incidents and to provide additional awareness of the importance of PHI privacy and security. The severity of disciplinary actions will depend on the gravity of the offence; at a minimum, the employee will receive a formal reprimand from upper management and additional privacy retraining. Should it be warranted, the employee may have their PHI access privileges revoked or their employment with eQOL may be terminated.

eQOL has a formal process for the return of assets at end of employment that is modeled from the ISO/IEC 27002 standard for information security management. This process includes the return of all hardware and software issued to employees as part of their employment. This includes tablets, computers, laptops, peripheral components, mobile computing devices, and all electronic media that may be stored on these devices. In the event that an employee uses their own personal equipment during employment, all relevant information will be transferred from that device to an organization-owned device and will be securely erased from the personal equipment. Access rights to information and devices will be removed at the end of employment, including user accounts with access to PHI and keys or swipe cards that allow access to physically secure areas at the organization. In addition, any information that is important to ongoing operations will be documented by the employee and transferred to the organization prior to their departure.

4.1.3 eQOL Agreements

eQOL forms contractual agreements with all third party HICs to formally establish roles and responsibilities related to collection, use, retention, disclosure and protection of PHI. Contractual agreements formed with other non-HIC third parties may also establish roles and responsibilities related to collection, use, retention, disclosure and protection of PHI, dependent on the nature of the third party and the nature of their involvement with eQOL. These agreements are formally ratified by upper level management and decision makers prior to eQOL providing any services to the HIC or its end users. The agreements will address the following, if applicable:

- Legislative obligations;
- Privacy and security training for HIC staff and the patients under their care, and training in the use of eQOL's health care management solutions;
- Roles and responsibilities of each party, and the associated processes and safeguards to protect PHI including monitoring and compliance;
- Purposes for the collection, use and disclosure of PHI and the scope of the PHI each party may access;

- Roles and responsibilities relating to the management of privacy incidents and breaches;
- Procedures for the termination of contractual agreements, including the expected duration of the agreement and requirements for returning information or removing access to programs or information systems;
- Appointing a primary point of contact within each party to facilitate communication.

eQOL's agreements will also address the procedure for cross-referencing or linking with external parties' information systems, technologies, or programs as applicable. This will be carried out on a case-to-case basis with unique considerations for the systems that each HIC may employ at their organization. In all cases, eQOL will work with the HIC to establish a secure data transfer interface or application programming interface (API) where PHI may be shared.

In the event of a security or privacy breach, HICs that have contractual agreements with eQOL will be notified immediately and appropriate steps to contain and repair the issue will be taken in collaboration with those organizations. In addition, the PDM will take steps to ensure that all third parties comply with the conditions of eQOL's agreements.

4.1.4 Client Training

eQOL's client training program consists of two programs: patient training and staff training. Patient and staff training programs each involve two main foci: training for how to use eQOL health management products, such as eQ Connect™, and awareness training concerning good practice measures for the protection of PHI. Patient training may be carried out by an eQOL representative or by HIC staff; this determination will be formalized in contractual agreements with HICs.

4.1.4.1 Patient Training

All patients will be trained on how to use eQOL health management solutions prior to being sent home with the product. eQOL has a documented training program that outlines how this will be accomplished and established training materials for patients. Patients will have the opportunity to review the PHI that will be collected from them and that their clinicians will be able to view remotely. The usage of the solution by patients may be tracked by eQOL for product improvement purposes; all patients will be informed ahead of time of eQOL's intention and tracking procedures. It will be made clear to patients that eQOL health management solutions are not substitutes for acute/emergency care and patients will be instructed to always seek medical attention should they encounter any serious medical situations.

Good practice measures are also reviewed with patients prior to product deployment, and include all recommendations for how to properly use the system. Training will stress that the mobile component of the patient interface contains PHI and that this device can be easily lost or stolen. Mobile PHI is protected by encryption and strong passwords, which will prevent any PHI from

being compromised in the event of loss. Nonetheless, patients will be instructed to keep the device in their possession at all times, and to prevent others from logging into the system or using the medical equipment as any data inputted into the system will be considered part of their medical record. In the event that a patient loses or damages their device, they will be instructed to contact eQOL immediately to report the issue. As part of eQOL's security safeguards, all users must use a strong password to login to the system; patients will be instructed not to write down or share their passwords. Use of the device will be strictly limited to care related activities and patients will be encouraged to always log out of the software when they are finished. Patients may also choose to enable locking on the device; should this be the case the patient will receive instructions on how this can be achieved.

4.1.4.2 Staff Training

All client staff will be trained how to use eQOL health management solutions prior to deployment of the product. eQOL has a documented training program that outlines how this will be accomplished and established training materials. Part of this training will involve an explanation of the PHI that will be collected and how it is transferred and stored between patients and clinicians to promote understanding and awareness of the system. It will be stressed that data inputted into the system is completed by the patient and could be prone to human error. eQOL implements automatic error checking/input validation (e.g. checking if proper numbers/characters were inputted) and upper/lower limits that are defined by human physiological limits to prevent the majority of errors. Upon review of data, clinicians may notice an abnormal entry, either due to patient error or patient clinical issue. In the event that a questionable entry is noted, client staff should employ their usual care procedures and contact patients regarding the entry. Users will also be informed of eQOL's auditing procedures, which track all logins and operations on the care provider interface to ensure appropriate usage of the system.

Client staff logins will require strong passwords, and clinicians will be instructed to protect their passwords by not writing them down or sharing them with anyone. In addition, eQOL will enforce password changes, as agreed upon with the institution, to further protect PHI that is accessible on care provider interfaces. Client staff will also receive good practice measures training regarding logging out of the system and ensuring that the care provider interface is accessed only on hospital property and networks, unless otherwise specified by a HIC and eQOL agreement. Due to the sensitive nature of data stored on the care provider interface, clinicians will be instructed not to copy/transfer any data outside the eQOL interface, unless otherwise specified by an eQOL agreement. Furthermore, users are restricted from looking at PHI for patients for which they are not directly providing care.

4.1.5 Breach and Privacy Incident Management

eQOL's PDM will oversee privacy incident and breach management by developing and maintaining processes, practices and tools to manage,

investigate, and remediate any privacy incidents that may arise. These procedures are clearly communicated to all employees as part of their privacy and security awareness training (see section 4.1.2) and to all third parties in eQOL's agreements (see section 4.1.3). As part of these procedures, all personnel and third parties are to report any incidents or breaches to the PDM immediately.

These procedures also provide a framework for how privacy incidents are to be contained after they have been identified and protocol for notifying all affected stakeholders and individuals as soon as possible. This might include suspending unauthorized practices that resulted in the incident, recovering affected records, shutting down the system where the incident occurred, or revoking access to a system, depending on the details and severity of the breach.

Incidents will also be fully investigated in order to identify a cause and to determine which individuals or assets may be involved. After the incident has been assessed and fully understood, eQOL will carry out remediation efforts, both short and long term, to correct the issue and ensure that all affected parties have been notified and fully understand the implications of the incident. To simplify the notification process, eQOL has established primary points of contact within our third party HICs to facilitate communication (see section 4.1.3).

The PDM will maintain a record of all incidents to provide reports for management, which will contribute to the evaluation and revision of eQOL's privacy policy.

4.2 Identifying Purposes

The identifying purposes principle states that purposes for which personal information is collected must be identified by eQOL at or before the time the information is collected.

4.2.1 eQOL's Identifying Purposes Policy

eQOL collects, uses and discloses PHI in order to provide services to its clients. Prior to the collection of this PHI, eQOL will identify and explain to its clients the purposes for which the PHI will be used and will obtain consent to carry out any activities relating to PHI. To enhance transparency and simplify understanding of the purposes for PHI collection, eQOL has made available the *Listing of Personal Health Information Data and Purposes for Collection* document.

As part of our contractual agreements with health information custodians, eQOL will ensure that those organizations keep their patients informed of the purposes for which the PHI will be collected. eQOL's policy also states that patients may withdraw consent at any time and eQOL will immediately cease the collection of PHI. For further information regarding eQOL's purposes for the collection, use and disclosure of PHI, please refer to eQOL's *Listing of Personal Health Information Data and Purposes for Collection* document.

eQOL shall only use PHI for the purposes explicitly listed in the *Listing of Personal Health Information Data and Purposes for Collection* document and will

obtain consent before collecting, using or disclosing PHI for purposes other than those outlined in the aforementioned document, unless required by law.

4.3 Consent

The knowledge and consent of an individual must be obtained for the collection, use, or disclosure of PHI, except where inappropriate.

4.3.1 eQOL's Consent Policy

Prior to the collection, use or disclosure of PHI, eQOL will obtain consent from individuals. This consent will be obtained either by an eQOL representative or by the individual's health care provider, depending on eQOL's agreement with the third party HIC. eQOL will ensure that HICs are provided with documentation about eQOL's activities and policies to inform patients prior to consent, including eQOL's Privacy Policy and the *Listing of Personal Health Information Data and Purposes for Collection* document.

Consent obtained from clients and patients must be knowledgeable, clear and relevant to the information being collected, used or disclosed for specific and identified purposes. This consent will be obtained without deception or coercion, and a record of the consent will be maintained for client and patient reference.

4.4 Limiting Collection

The collection of PHI shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1 eQOL's PHI Collection Policy

eQOL will only collect information that is relevant and necessary for the provision of our services. Individuals will be made aware of all of the PHI that will be collected and the purposes for its collection. See section 4.1.4 for more details.

4.5 Limiting Use, Disclosure, and Retention

PHI shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the covered individual or as required by law. PHI shall be retained for an indefinite period of time to comply with PHIPA guidelines and other applicable legislation.

4.5.1 eQOL's PHI Use, Disclosure, and Retention Policy

eQOL will only collect PHI that is necessary for the identified and consented purposes outlined in section 4.4.1. eQOL collects PHI directly from patients and their approved health care providers. This data is used to create and maintain a comprehensive health record that facilitates the management of PHI between the health care team and the patient. As part of eQOL's third party agreements with HICs, PHI will only be disclosed upon request by authorized clinicians or administrative users through the care provider interface. Patients may access their recent PHI anytime through the secure patient interface, and may request access to their past PHI at any time.

This PHI data will be retained for the required period of time to comply with provincial guidelines, PHIPA, and other applicable legislation.

4.6 Accuracy

PHI shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1 Accuracy of PHI Entrusted to eQOL

The accuracy and completeness of PHI under eQOL's care is of utmost importance. eQOL receives PHI directly from individuals and their health care team and therefore the primary responsibility for the accuracy of information lies with the individuals and the HICs with which eQOL has made agreements. In addition, eQOL provides safeguards to protect the PHI from improper modification (both inadvertent or purposeful). For details on the mechanisms that eQOL provides for safeguarding the PHI under our care, see section 4.7.1.

Individuals have access to their PHI through our secure health management solutions and upon request. See section 4.9.1 for more details about our individual access policy. Individuals also have the right to amend any information that they find to be inaccurate or incomplete. See section 4.10.1 below for details.

4.7 Safeguards

PHI shall be protected by security safeguards that are appropriate to the sensitivity of the information.

4.7.1 Security Safeguards Implemented at eQOL

eQOL is committed to the highest standard of privacy protection and involves all levels of management in their privacy policy. eQOL has implemented administrative, technical and physical safeguards to maintain the privacy and security of PHI that is collected, used, or disclosed. These safeguards are in place to protect all forms of PHI, including electronic, written and verbal data. To protect our electronic PHI, both at rest and in transit, eQOL employs:

- Encryption of PHI on the patient facing component of our health management solutions;
- Encryption of PHI on the healthcare provider facing component of our health management solutions;
- Encryption of PHI stored on eQOL's backend database and data in transit between the patient and healthcare provider facing components and the database;
- Access tracking and audit logging capabilities for healthcare provider components and internal eQOL interfaces;
- Data stored on removable storage media and on laptops/computers are protected with strong passwords and stored with appropriate physical safeguards;
- Unique username and strong password login required for access to PHI;
- Session-timeout and logout after periods of inactivity.

Physical and administrative safeguards protect written, verbal and other forms of PHI. All paper documents and physical stores of PHI are kept locked in secure filing cabinets within the locking eQOL offices when they are not in use, and access to these secure areas is granted only to employees that require access to PHI to carry out their duties. All employees that handle PHI receive security and privacy awareness training prior to starting their duties and are encouraged to practice safe PHI handling practices on a day-to-day basis. Such practices include logging out of the system after use, locking computer screens and locking office doors when computer terminals are to be left unattended. Employees are also instructed to carefully conduct telephone calls to ensure that verbal PHI is not overheard and to be prudent when leaving voice messages.

eQOL has designated the PDM to oversee eQOL's compliance with our Privacy Policy and to address any privacy concerns should they arise. See section 4.1.1 for additional information about the role and responsibilities of the PDM.

4.8 Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1 Accountability and Transparency

eQOL's Privacy Policy is readily available electronically for HICs, and a physical copy can be made available to individuals that place a request. Prior to any agreement with HICs and patients, eQOL will make clear to all parties the PHI that will be collected and the purposes for that collection and use. Additionally, individuals may contact eQOL's PDM for further information about our privacy and security practices and to request additional information about PHI records that we maintain.

4.9 Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her PHI and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

4.9.1 eQOL's Individual Access Policy

Individuals have access to their recent PHI through the use of our health management solutions. Patients may also place requests for additional information regarding their PHI by contacting eQOL or their health care provider. If an individual feels that their PHI is inaccurate or incomplete, they may request a correction by contacting eQOL's support line or PDM at (647) 479-4615.

4.10 Challenging Compliance

An individual shall be able to challenge the organization concerning compliance with the 10 principles to the designated individual accountable.

4.10.1 eQOL's Compliance Policies and Measures

To maintain the privacy of the PHI under our care, eQOL will monitor the compliance of our internal personnel to the security procedures outlined in this Policy. eQOL will also strive to ensure that authorized HICs with whom agreements are made abide by the obligations established in the agreements they share with eQOL. eQOL may assist these HICs by providing reports on their behaviour from audit logs and usage tracking. These measures are established in an effort to prevent a security concern. However, should a privacy issue arise, eQOL has established a system for reporting issues and maintaining a record of the reported issue in compliance with PHIPA.

eQOL maintains records of reported problems relating to performance characteristics or safety, including consumer complaints that are received after selling a device or service package. A record of all actions that are taken in response to the reported issues will also be maintained.

In addition, eQOL has an established procedure to carry out an effective and timely investigation into any reported problem. Individuals may contact eQOL by phone or email. A technical support representative will manage those concerns and a record will be maintained in eQOL's complaint submission record, an online database that can be updated by any eQOL employee that contributes to the complaint submission handling process. Solutions and outcomes are also documented to facilitate the resolution of future problems that may arise.

In the event that an individual feels that their PHI has been compromised, eQOL has remote locking capabilities to ensure that the user's PHI is protected. Furthermore, if any security issues are identified in the software code, a secure update can be pushed remotely to the end users when a solution has been developed.

The PDM will further regulate eQOL compliance to these standards and will promote an environment of privacy and security awareness. This will be accomplished by ensuring that eQOL personnel are informed and aware of all services and activities related to PHI, as well as the appropriate measures that are to be taken to maintain the integrity of the PHI under eQOL's care. The PDM will be available to answer any questions or concerns from individuals and can clarify eQOL's Privacy Policy should there be any confusion.

5 Privacy Contact Person

For questions or concerns regarding eQOL's Privacy Policy, please contact eQOL's Product Development Manager, who administers the organization's privacy and security responsibilities.

Telephone	647-479-4615
Email	support@eqol.ca
Mail	eQOL Inc. 2487 Bloor Street West, Suite 1 Toronto, ON, Canada

	M6S 1R5

5.1 Complaint Submission

Complaints regarding eQOL's Privacy Policy may be submitted to the office of the Information and Privacy Commissioner of Ontario. The Commissioner may be contacted by:

Telephone	1-416-326-3333 1-800-387-0073
Fax	1-416-325-9195
Website	www.ipc.on.ca
Mail	Information and Privacy Commissioner of Ontario 2 Bloor Street East, Suite 1400 Toronto, ON M5G 2C8

6 References

The following documents and webpages were referenced during the creation or modification of this Policy:

Guide to Information Security for the Health Care Sector – Information and Resources for Complex Organizations. eHealth Ontario, 2010. http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_Complex.pdf

ISO/IEC 27002:2005(E) Information technology – Security techniques – Code of practice for information security management. http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf

PIPEDA Fair Information Principles. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/leg_c/p_principle_e.asp