Biometrics Privacy Impact Assessment Checklist for Public Educational Institutions in Alberta

Scott MacDormand

smacdorm@gmail.com

November 28, 2010

Submitted for partial completion of the requirement of the degree of

Master of Information System Security Management

Concordia University College of Alberta

Keywords: biometrics, privacy, FOIP, ISO/IEC, PIA

Abstract

This research stems from an assumption that the use of biometrics will eventually become commonplace in public educational institutions in Alberta. This paper proposes a Biometrics Privacy Impact Assessment Checklist (BPIAC) that can be used by public educational institutions in Alberta during the Privacy Impact Assessment processes. As the BPIAC is intended for public educational institutions in Alberta, it uses the Freedom of Information of Privacy Act as its legal reference, and two ISO/IEC standards to provide recommendations on how to meet any legal requirements under FOIP, as well as recommendations on how to meet other privacy concerns not necessarily covered under FOIP when it comes to the use of biometrics.

1 Introduction

1.1 The Freedom of Information and Protection of Privacy Act

The collection of unique and unchangeable information about individuals, its storage and its use have fuelled discussion about how Albertan (and ultimately Canadian) privacy laws should be applied to biometrics [6]. As biometric data is ultimately Personal Identifiable Information (PII), Alberta's privacy laws are equally applicable to biometric data as they are to any other types of personal information.

The Freedom of Information and Protection of Privacy (FOIP) Act [3] is Alberta's provincial public sector privacy statute, and therefore must be used by all public educational institutions in Alberta. As the BPIAC is intended for public educational institutions in Alberta, it will also use FOIP as its legal reference. The purposes of FOIP are:

a) *To allow any person a right of access to the records in the custody or under the control of a public body subject to limited and specific exceptions as set out in the Act.*
b) *To control the manner in which a public body may collect personal information from individuals, to control the use that a public body may make of that information and to control the disclosure by a public body of that information.*
c) *To allow individuals, subject to limited and specific exceptions as set out in the Act, a right of access to personal information about themselves that is held by a public body.*
d) *To allow individuals a right to request corrections to personal information about themselves that is held by a public body.*
e) *To provide for independent reviews of decisions made by public bodies under the Act and the resolution of complaints under the Act.*

These purposes constitute the general standards governing the collection, use and disclosure of personal information. Guidance surrounding specific compliance obligations is typically developed through the findings and rulings of the Information and Privacy Commissioner of Alberta.

The Privacy Commissioner of Alberta has investigated the application of Alberta's privacy laws to biometrics in the past. In two cases [4,5], the Privacy Commissioner examined the use of biometrics, which was used to clock employees in and out of work. The commissioner found that although the public institution's use of a biometrics was necessary as defined under Alberta's privacy laws, the need for these public institutions to provide a proper collection notice when implementing new information systems had not been met. These two cases indicate that the use of biometrics is not initially problematic with respect to Alberta privacy laws. If collected and protected correctly, using advanced and secure technologies, biometrics may be used by almost any institution – public or private. However, the findings of the two cases do not represent a "privacy carte blanche" for public educational institutions that may wish to implement biometrics.

Since the purpose of FOIP is fairly general, public educational institutions are left to apply FOIP to biometrics as best they can. In the face of new technologies, application of general principles by public educational institutions into unchartered territory could be challenging. This may mean that public educational institutions might be apprehensive to adopt or use biometrics for fear of violating privacy law. To find such guidance and/or recommendations, such institutions can turn to existing biometric standards to help ensure that they might be able to meet FOIP privacy requirements. In other words, adherence to a government created Act can be addressed in full or in part by referring to Standards which in turn can be applied through the use of developed Guidelines and/or Recommendations. The BPIAC was developed through this same general approach.

In the United States, this type of approach has been conducted with the Federal Information Security Management Act (FISMA) of 2002. FISMA was enacted to require federal agencies to provide information security for all information systems that support the operations and assets of said agencies. To meet the requirements, FISMA tasked the National Institute of Standards and Technology (NIST) with developing the standards (FIPS PUB 199 and 200) and producing the guidelines (NIST SP 800) that are used by the various federal agencies.

However, as Alberta has no existing standards or guidelines on the use biometrics, it makes sense that for our checklist, we choose a standard or set of standards that will most likely be universally accepted for use. In this case, the ISO/IEC standards related to privacy in biometrics were chosen.

1.2 ISO/IEC Biometric Standards

The BPIAC uses two ISO/IEC standards related to privacy:

- ISO/IEC TR 24714-1:2008 Biometrics – Jurisdictional and Societal Considerations for Commercial Applications – Part 1: General Guidance [2]
- ISO/IEC TR 24741:2007 – Information Technology – Biometrics Tutorial [1]

These standards are part of a larger set produced by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) Joint Technical Committee 1 (JTC 1) Subcommittee 37 (SC 37). The purpose of this larger set of standards is to support the standardization of biometric technologies pertaining to human beings and to support interoperability and data interchange among applications, systems, and jurisdictions [7]. This set of standards is probably the most comprehensive to date, with over 40 standards published and more being written. Canada is a contributor to ISO/IEC JTC 1 SC 37, and is currently contributing to standards that fall under the category of Harmonized Biometric Vocabulary and Definitions, of which ISO/IEC TR 24741:2007 is a part. It should also be noted that in the United States, the American National Standards Institute (ANSI) is also a contributor to the ISO/IEC JTC 1 SC 37 standards under the category of Biometric Testing and Reporting. NIST works closely with ANSI on the development of these biometric standards, providing needed technical expertise.

The ISO/IEC TR 24714-1:2008 Biometrics – Jurisdictional and Societal Considerations for Commercial Applications – Part 1: General Guidance standard addresses the impact of biometrics on privacy, health, safety, and other similar areas. The ISO/IEC TR 24741: 2007 – Information Technology – Biometrics Tutorial standard describes the main biometric technologies, along with some historical information. An annex describes the work of creating International Standards for biometrics and provides a layered model for the placement of the various International Standards being produced, with a short description of each. A second annex contains some of the terms and definitions currently used in these International Standards or the drafts of these International Standards.

2 The Biometrics Privacy Impact Assessment Checklist

See Appendix A for the complete BPIAC. See Appendix B for definitions used in the BPIAC.

The Biometrics Privacy Impact Assessment Checklist (BPIAC) was compiled through a literature review of FOIP, the PIA developed for FOIP, and the ISO/IEC standards described previously.

The BPIAC is designed to offer assistance to planners, implementers, and system operators of biometrics in Albertan public educational institutions. In particular, the BPIAC focuses on providing public educational institutions with a checklist that will provide a set of recommendations to help mitigate privacy risks of using biometrics with regards to topics shown in the following table.

Recommendation Type:	**Related BPIAC Section(s):**
FOIP compliance of biometrics.	A.1, A.3, A.8
Legal and societal constraints on the use of biometric data.	A.2, A.3, A.5, A.6, A.7
Accessibility for the widest population	A.3, A.4, A.5
Health and safety, addressing the concerns of users regarding direct potential hazards	A.3, A.4, A.5

In developing those checklist items regarding the FOIP compliance of biometrics, we first identified statutes in FOIP that had a corresponding recommendation in the ISO/IEC standards. From there, we selected only those statutes where ISO/IEC provides unique recommendations when it came to the use of biometrics. For example, both FOIP and ISO/IEC state that "users of the system should be given reasonable access to verify the correctness of the biometric data and to have incorrect data amended [2]." However, ISO/IEC fails to provide unique examples when applying this to biometrics, so this recommendation did not make it into the final checklist. On the other hand, both FOIP and ISO/IEC identify that "biometric information should be accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used [2]." In this case, ISO/IEC states that since biometric characteristics change frequently over a person's lifetime, biometric data will need to be more regularly updated than say, a person's name or address.

In developing the remaining checklist items regarding legal and societal constraints, accessibility, and health and safety, we identified recommendations in the ISO/IEC standards that may have to be considered by public educational institutions in Alberta when implementing biometrics. While these items are not required to meet privacy compliance requirements, they are deemed by ISO/IEC to be good practice for the use of biometrics. Again, we tried to identify those recommendations that are unique to biometrics, and not those that are generic and could be applied to any system where privacy might be an issue.

Finally, after the checklist items were identified, we went through FOIP's Privacy Impact Assessment and identified which question(s) from the PIA that our checklist pertains to, thereby completing the BPIAC. The completed BPIAC is intended to be a supplement to a Privacy Impact Assessment (PIA) [11,12,14] that a public educational institution in Alberta may wish to conduct.

A PIA is "not mandatory under the FOIP Act, but is recommended for major projects that involve the use or disclosure of personal information [15]." A major project would include an institution's decision to use biometrics. PIAs may also be made mandatory in the future under FOIP, as they are under Alberta's Health Information Act (HIA), so conducting one is in the best interest of the institution.

A PIA is a process that can assist an institution in reviewing the impact that a new program, administrative process or practice, or information system may have on individual privacy. In the case of the BPIAC, we focused on biometric systems. The PIA process is designed in such a way so that an institution can evaluate the proposed system for technical compliance with the FOIP Act, as well as assess any privacy implications for potential users of the system. In other words it is both a risk management tool and a diligence exercise. While only real breaches of privacy contravene the provisions of the FOIP Act, the perceptions of users of a proposed system can mean either success or failure of the system.

The PIA is an exercise in which the institution identifies and addresses privacy risks that may arise in the course of its operations. While PIAs are focused on specific systems, the process includes an examination of institution-wide practices that could have an impact on privacy. The PIA process requires an analysis of the potential impact of the system on privacy, as well as consideration of measures to mitigate or eliminate negative impacts to privacy.

Ultimately, a PIA provides documentation for the Information and Privacy Commissioner of Alberta and to potential users of the system that privacy issues related to the system have been appropriately identified and addressed. Acceptance of a PIA means that the Office of the Information and Privacy Commissioner is satisfied that the institution has addressed relevant considerations and is committed to the necessary level of privacy protection.

3 Conclusions

We have investigated creating a Biometrics Privacy Impact Assessment Checklist (BPIAC) that can be used by public educational institutions in Alberta during the Privacy Impact Assessment processes. As the BPIAC is intended for public educational institutions in Alberta, it uses the Freedom of Information of Privacy Act as its legal reference, and two ISO/IEC standards to provide recommendations on how to meet any legal requirements under FOIP, as well as recommendations on how to meet other privacy concerns not necessarily covered under FOIP when it comes to the use of biometrics.

What we found was that although our checklist addressed some of the general technical issues associated with the use of biometrics, and how to mitigate such issues, it did not address issues relating to accountability, policies, or procedures. This is because the two ISO/IEC standards chosen did not provide much in the way of specific guidance related to accountability, policies, or procedures. As an example, although the chosen standards state that the "biometric system should be designed to permit a secure audit of the use of biometric data including its deletion or removal from the biometric system [2]", it doesn't state or elaborate on how this might be unique to biometrics. It simply refers us to the ISO/IEC 27002:2005 standard, which is a code of practice for information security management.

There are of course improvements that can be made to the BTPIAC. For starters, we may not have identified all of the FOIP statutes where ISO/IEC has made specific recommendations as to the use of biometrics. The recommendations under ISO/IEC can be open to different interpretations by different individuals. This is why checklists and recommendations on how to meet privacy requirements are usually developed by a committee with many different backgrounds and levels of expertise. The checklist could be improved in such a manner.

Secondly, as stated earlier, the two biometric standards chosen are a small subset of a larger group of standards chosen to support the standardization of biometric technologies pertaining to human beings and to support interoperability and data interchange among applications, systems, and jurisdictions. It could be that one of the other ISO/IEC standards on biometrics provides recommendations related to accountability, policies, or procedures. It could also be that ISO/IEC produces more standards related to privacy as ISO/IEC 24714-1:2008 is currently the only one.

In a final statement, the author would like to acknowledge the help of his supervisor Dr. Pavol Zavarsky who provided much needed insight and guidance into the writing of this paper.

4 References

[1] *Information Technology – Biometrics Tutorial*. ISO/IEC TR 24741:2007.

[2] *Information Technology – Biometrics – Jurisdictional and Societal Considerations for Commercial Applications – Part 1: General Guidance*. ISO/IEC TR 24714-1:2008.

[3] Province of Alberta. (2009, October 30). *Freedom of Information and Protection of Privacy Act*. [Online]. Available: http://foip.alberta.ca

[4] Alberta Office of the Information and Privacy Commissioner. (2008, August 27*). Investigation Report P2008-IR-005*. [Online]. Available: http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2275

[5] Information and Privacy Commissioner of Alberta. (2008, August 7). *Investigation Report P2008-IR-001*. [Online]. Available: http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2217

[6] P. Backman & C. Kennedy. *Biometric Identification and Privacy Concerns: A Canadian Perspective*. [Online]. Available: http://www.airdberlis.com/Templates/Articles/articleFiles/584/Biometric%20Identification%20and%20Privacy%20Concerns.pdf

[7] Biometrics Institute. (2010, January 24). *International Standards*. [Online]. Available: http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=40

[8] Government of Alberta. (2009, November 26). *School Act and Regulations*. [Online]. Available: http://education.alberta.ca/department/policy/legislation/regulations.aspx

[9] identiMetrics. (2009, June). *Biometric Student Identification: Practical Solutions for Accountability & Security in Schools.* [Online]. Available: http://www.identimetrics.net/articles/Practical_Stu_ID_for_schools.pdf

[10] Frazier, E. (2004, April 26). *Implementing Biometric Technologies into Distance Learning.* [Online]. Available: http://www.bsu.edu/web/elfrazier/TechnologyAssessment.htm

[11] Treasury Board of Canada Secretariat. (2002, August 31). *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*. [Online]. Available: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2-eng.asp

[12] U.S. Department of Homeland Security. (2010, May 11). *Privacy Impact Assessment (PIA).* [Online]. Available: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_template.pdf

[13] Common Criteria Biometric Evaluation Methodology Working Group. (2003, August). *Biometric Evaluation Methodology Supplement*. [Online]. Available: http://www.cesg.gov.uk/policy_technologies/biometrics/media/bem_10.pdf

[14] Office of the Information and Privacy Commissioner of Alberta. (2001, January). *Privacy Impact Assessment: Instructions and Annotated Questionnaire*. [Online]. Available: http://www.oipc.ab.ca/ims/client/upload/pia-instructions-1.1.pdf

[15] Service Alberta. (2009). *FOIP Guidelines and Practices: Chapter 9: Privacy Compliance*. [Online]. Available: http://www.servicealberta.ca/foip/documents/chapter9.pdf

Appendix A Biometrics Privacy Impact Assessment Checklist

Each item of the checklist contains the following:

- Title: states the general privacy practice.
- FOIP Act: states the referenced statute in FOIP (including section number).
- ISO/IEC Standard: states the general guideline(s) given by ISO/IEC for the given FOIP statute. In some cases no FOIP statue exists, but the guideline is still valid and should be considered.
- PIA Question(s): states the related PIA question(s) from FOIP's PIA (including question number).
- Adopted?: checkmark if the privacy practice been adopted or considered.
- Recommendations: states the recommendations given by the selected ISO/IEC standards, with considerations and/or modifications taken from other documents such as the Alberta School Act [8].

A.1 Purpose of Collection of Data

FOIP Act:	ISO/IEC Standard:	PIA Question(s):	Adopted?
No biometric data may be collected by or for an institution unless: • it directly relates to and is necessary for an operating program or activity (section 33(c))	For (civilian) institutions the use of biometrics usually falls under the category of access control. Access control ensures that only individuals that are authorized can gain access to: a) a particular area within the institution (physical access) b) a particular resource (logical access) The use of biometrics for access control is primarily to increase overall security within an educational institution, and to reduce fraud.	Are organizational policies or procedures in place to ensure that there is a business purpose for all personal information collected? (question A6) Have the purposes for which the personal information is collected been documented? (question B8)	

Recommendations:

A few examples of the use of biometrics for access control that could be considered necessary might include:

1. Computer systems access: biometrics is used to authenticate (log on) individuals and give them access to the computer resources that have been granted to them as part of the computer system.
2. Identity cards: a biometric template (reference) of the individual (employee or student) is stored on a card which is used as an identity document.
3. Physical access control: biometrics is used to control the movement of individuals within the confines of a building or facility, such as a school. [9]
4. Time, attendance, and monitoring applications: biometrics is used to monitor 'clocking-in' or attendance of employees or students. [10]
5. Civil background checks: biometrics is used to check an individual for a criminal background, and thereby provide appropriate security clearances, or allow or deny employment, such as the case in educational institutions where the individual is dealing with children.

<table>
<tr><td colspan="4"><b>A.2 Limitation of Collection:</b></td></tr>
<tr><td><b>FOIP Act:</b>
N/A</td><td><b>ISO/IEC Standard:</b>
The biometric data collected should be limited to the minimum required for the functionality of the biometric system.</td><td><b>PIA Question(s):</b>
Has a listing of all personal information or data elements to be collected, used or disclosed in the project been prepared? (question B2)</td><td><b>Adopted?</b></td></tr>
<tr><td colspan="4"><b>Recommendations:</b>
The number of biometric templates that are created for an individual will likely depend on the type of authentication the institution is using. If the institution is using traditional two factor authentication, the creation of a single biometric template will usually be sufficient for the purpose of the system. Along with another factor such as a PIN or a password, the user will submit their biometric characteristic for authentication. However in some cases, the institution may wish to use two biometric characteristics for authentication. In this case, two biometric templates will need to be created from an individual. The inherent difficulty with creating and using two templates is, of course, acceptance. Individuals are much less likely to accept the use of two biometric characteristics than one.
Note: Biometrics have a unique characteristic in that they can be used in a type of one factor authentication. As biometric characteristics are inherently unique to every individual, they are sometimes suitable for replacement of two factor systems. In other words, and individual may only have to provide a fingerprint to be authenticated. This does carry some level of risk as every biometric system still has the chance for false acceptance. In this case, the system should be evaluated as to whether or not this type of risk is going to be assumed. For example, in a student lunch program that uses biometrics for authentication, a few false acceptances means that some students that are not entitled do in fact get “a free lunch” – which is perhaps acceptable.</td></tr>
</table>

<table>
<tr><th colspan="4">A.3 Use of Personal Data (Preference for Opt-Out)</th></tr>
<tr><th>FOIP Act:</th><th>ISO/IEC Standard:</th><th>PIA Question(s):</th><th>Adopted?</th></tr>
<tr><td>An institution may use biometric data only
• if the individual the data is about has consented to the use (and collection) of that data
• to the extent necessary to carry out its purpose in a reasonable manner
(section 39(1)(a,b))</td><td>If practical and feasible, preference for individuals to opt-in and opt-out of using the biometric system should be made available. In general, opt-out is the preferred option.</td><td>Does individual consent provide the primary basis for the collection, use and disclosure of personal information for this project? (question B6)
If potential risks related to privacy have been identified, have means to avert or mitigate those risks been incorporated into the project design? (question B13)</td><td></td></tr>
<tr><td colspan="4"><b>Recommendations:</b>
Every effort should be made by designers of the biometric system to cater to the maximum number of potential users, using creative and innovative designs. The biometric system should be designed to be as inclusive and non-discriminatory as possible to individuals unwilling or unable to participate. This becomes increasingly important as we consider that public educational institutions in Alberta also follow the Alberta School Act [8]. As part of the School Act, students in a special education program are entitled to an education, regardless of any physical, behavioral, or mental disability that they may have. Acceptance testing should be performed on the system before it is put into full operation. (see section A.5)
An alternative identification procedure should be made available for those individuals who want to opt-out because they are unable to use the biometric system. In some cases, users of the biometric system may have physical, behavioral, or mental disabilities that absolutely prevent them from using the biometric system – regardless of any compulsory requirement for using the system. For example, some individuals may have missing fingers, an inability to speak, uncontrolled body movements, a scar or deformity over the characteristic being captured, or simply lack the intelligence to use and understand the biometric system unassisted. In other instances, an individual may also have a medical condition that makes them sensitive to the light used in the biometric sensor, or they may have a compromised immune system and may be susceptible to pathogens found on the biometric sensor.
In other cases, an individual may want to opt-out for cultural, religious, or medical objections to the system. For example, in some cultures, covering the face or not taking photos of the face is the norm, so facial recognition biometrics would be viewed as intrusive. In some Christian denominations, hand biometrics is viewed as “the sign of the beast”. Other individuals may have strong objections because they view the use of certain biometrics as being unsanitary – even if disinfecting hand sanitizers are made available afterwards. Yet others may object because they believe that it will reveal an existing medical condition that they may want to keep private. Capecitabine, a caner fighting drug, can temporarily erase a person’s fingerprints, thereby indicating that the person if being treated for cancer.
Sometimes a workers or teachers council or union may be involved when employees refuse to use the biometric system. Many employees strongly object to employers having too much personal information about them, and view it as a strong invasion of their personal privacy.</td></tr>
</table>

A.4 Context of Use

FOIP Act:	**ISO/IEC Standard:**	**PIA Question(s):**	**Adopted?**
N/A	Biometric sensors are highly dependent on the physical environment in which they operate. Thus, as a technology, they may unknowingly add privacy risks to the biometric system to which they are attached. Thorough testing of the operation and placement of the biometric sensor should be conducted.	If potential risks related to privacy have been identified, have means to avert or mitigate those risks been incorporated into the project design? (question B13)	

Recommendations:

Biometric sensors are highly susceptible to:

- Climate: biometric sensors are sensitive to changes in temperature, humidity, and light. These climate changes may affect the ability of individuals to provide an adequate biometric sample.
- Contamination: biometric sensors may be placed in environments where they are exposed to chemicals, toxins, or dust that may affect their ability to take an adequate biometric sample. Biological contaminations of the sensor from repeated use may also affect the ability of sensors to take accurate readings.
- Location: biometric sensors placed outside may be subjected to higher levels of vandalism if they are left unattended or unmonitored. Biometric sensors placed in public places are more susceptible to interference from other individuals. For example, a noisy environment with many people may preclude the use of a biometric sensor that captures a person's voice.
- Position: biometric sensors should be placed so that they cater to the widest population possible. For example, the height of a biometric sensor should be useable by both the average population, as well as those individuals with physical disabilities, such as being in a wheelchair. As another example, individuals that are blind may need guidance – physical or verbal – to locate a biometric sensor.
- Support: if the biometric sensor is not working to one of the reasons listed above, assistance should be provided so that the user can progress. This goes back to providing an alternative means of identification as stated in section A.2.

A.5 Acceptance Testing

FOIP Act:	**ISO/IEC Standard:**	**PIA Question(s):**	**Adopted?**
N/A	Whenever possible, plans for acceptance testing of the biometric system should be made to help reduce privacy concerns.	Have key stakeholders been provided with an opportunity to comment on the privacy protection implications of the proposed project? (question B14)	

Recommendations:

One of the key factors in the successfulness of any biometric system is that it have a high level of user acceptance. Acceptance is a rather complicated issue, and depends on such diverse factors as privacy and data protection, ease-of-use, convenience, invasiveness, and health and hygiene. In particular, may users view the use of a biometric characteristic as being personal and intimate, whereas the use of a PIN or password is not.

Transparency of the overall biometric system is probably the single key factor in the successful use of the system. The more that potential users of the biometric system know about the details of the system, including any risks or advantages associated with the system, the more trust can be built in the use of the system.

As a suggestion, the following minimum steps should be taken towards increasing the acceptance of the biometric system:

1. Piloting of the biometric system should be undertaken and the acceptance factors determined for all individuals which will be potential users of the biometric system.
2. Survey the users of the biometric system in order to address any concrete concerns that they may have.
3. Although biometric systems may be designed initially for early adopters and/or specific target groups, subsequent extension to other groups of individuals may require additional testing and redesign.
4. Specific aspects related to biometrics include the need for re-enrolment as people age.
5. One way to improve user acceptance would be to adjust the threshold in a biometric system in order to reduce the rate of false rejections. However, this carries a corresponding penalty of a reduction in security. The relation between false acceptance and false rejections should be explained to the subjects.
6. Provide information and usage guidelines understandable for non-technical persons and, dependent on the user population, in different languages. Parents of students may not have English as their first language.
7. If acceptance testing is undertaken, the users of the biometric system should be allowed to familiarize themselves with the system in the context of the application.
8. Both education and marketing of the intended use of the biometric is crucial to address both the logically sound concerns and subjective cultural uncertainties.

A.6 Links to Other Data / Anonymity of Data

FOIP Act:	ISO/IEC Standard:	PIA Question(s):	Adopted?
N/A	If the biometric data is linked in the system to other personal information, care must be taken so that the system does not release that personal information to unauthorized individuals.	Are personal identifiers used to link or cross-reference multiple databases? (question B16)	

Recommendations:

One way to additionally anonymize biometric data – in particular the stored biometric templates - is to convert it into a “hash” value. The “hash” value can still be used for matching purposes within the system; however, it cannot be converted into its original raw form. In other words, the raw biometric characteristic captured by the biometric sensor cannot be reconstructed or regenerated [13].

A.7 Accuracy and Retention

FOIP Act:	ISO/IEC Standard:	PIA Question(s):	Adopted?
If the institution is going to use biometric or personal data to make decisions, it needs to ensure that • the data collected is accurate and complete (section 35(a))	Biometric data should be accurate, complete, and up-to-date for the purposes for which it is to be used.	Are organizational procedures in place to ensure that personal information correction and annotation are available when required? (question A6)	

Recommendations:

Biometric characteristics can change drastically over the course of an individual’s lifetime. This is especially true with young children who are constantly growing. As a result, the number of false rejections for an individual may increase over time. Therefore, it may be necessary to recollect biometric data for template creation at semi-regular intervals. Once a year may be enough for some individuals, while every six months may be needed for others.

In some rare cases, an individual may have a medical condition that causes them to prematurely age. In this circumstance, biometric template creation may have to be performed on a fairly regular basis.

A.8 Protection of the Data

FOIP Act:	ISO/IEC Standard:	PIA Question(s):	Adopted?
N/A	Biometric data should be protected against unauthorized use, access or processing. Backup and archived biometric data should have the same level of protection as biometric data in use by the system.	Have security procedures for the collection, transmission, storage, and disposal of personal information, and access to it, been documented? (question B17) If personal information will be used in the electronic delivery or services, have technological tools and system design techniques been considered which may enhance both privacy and security? (question B19)	

Recommendations:

Processing in a biometric system involves any operation or set of operations which might be performed on biometric data, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Opportunities for such misuse should be minimized during the design phase of the system, and should be built into the major subsystems of the biometric system. ISO/IEC provides standards that address these various subsystems. The major identified subsystems are:

- Data Capture
- Signal Processing
- Data Storage
- Matching
- Decision
- Transmission
- Administration

Note: It is well known problem that biometric sensors can be fooled by forgeries. In this context, “spoofing” is the use of a forgery of another person’s biometric characteristics in order to be recognized as that person. While forgery can result in a loss of privacy, it is an inherent problem that is not specific to only biometric systems. Improvements in technology will hopefully address the problem of “spoofing”, but for now, the choice of biometric characteristic that will be used in the system will result in specific risks that may need to be assumed. For more information, refer to the specific ISO/IEC standard for the type of biometric characteristic chosen.

Appendix B Definitions

The following definitions taken in full or in part from [1,2] are used in the BPIAC:

- Biometrics: automated recognition of individuals based on their behavioral and biological characteristics.
- Biometric characteristic: biological and behavioral characteristic of an individual that can be detected and from which distinguishing, repeatable features can be extracted for the purpose of automated recognition of individuals.
- Biometric system: a system used for the purpose of the automated recognition of individuals based on the behavioral and biological characteristics.
- Biometric sensor: a device that captures a signal from a biometric characteristic and converts it into biometric data.
- Biometric data: data captured from a biometric sensor that can be recorded as a biometric template for an individual or used for comparison with previously recorded biometric template to verify of identify a subject - at any stage of processing.
- Biometric template: biometric data stored about and individual that is used for recognition by comparison with other biometric data.
- Individual: of or for a particular person; single human being or item as distinct from a group.
- User: any person interfacing in any way with a biometric system.
- Processing: refers to any operation or set of operations which is performed upon personal data, such as collecting, recording, organizing, altering or adapting, retrieving, consulting, using, disclosing, aligning or combining, blocking, erasing or destroying.
- False acceptance: transactions in a biometric system that are incorrectly confirmed.
- False rejections: transactions in a biometric system that are incorrectly denied.
- Re-enrolment: process of establishing a new biometric template for an individual already enrolled in the database.