foip bulletin

Number 17 | Revised March 2009

Consent and Authentication

CONTENTS

INTRODUCTION

The *Freedom of Information and Protection of Privacy Act* (the FOIP Act) requires a public body to obtain consent "in the prescribed manner" for the use or disclosure of personal information under **Part 2** or for a request for access to third party personal information. The prescribed manner for giving consent is set out in **section 7** of the FOIP Regulation and has been limited to consent in writing. The FOIP Amendment Regulation 2006, which came into force on February 8, 2006, made significant changes to the way consent may be given.

The Select Special FOIP Act Review Committee recommended that the FOIP Regulation explicitly provide for electronic consent and allow for oral consent. The Committee wished to support the trend towards a multi-channel service delivery model and recognized that the writing requirement creates a barrier to providing consent in certain circumstances. At the same time, the Committee acknowledged that appropriate privacy protection for personal information must be in place.

The FOIP Amendment Regulation 2006 implements the recommendation of the Select Special FOIP Act Review Committee by amending **section 7** of the FOIP Regulation to provide for consent in writing, consent in electronic form and oral consent.

This Bulletin explains the new provisions for consent in **section 7** and provides guidance with respect to the policies or "rules" that public bodies must establish in order to accept consent electronically or orally.

KEY CONCEPTS

The amendments to **section 7** of the FOIP Regulation

- establish a regime where there are common standards for consent, whether the consent is given on paper, electronically or orally

- follow the principles of "functional equivalence" in the *Electronic Transactions Act* to establish medium-neutral rules for what constitutes reliable consent (a method of consent is "functionally equivalent" to another if it fulfils the same function, even if it is not in the same form)
- permit, but do not require, a public body to accept electronic or oral consent
- allow an individual to provide consent in writing even though the public body may accept electronic or oral consent for the purpose for which consent is being given

Section 7 continues to apply only to consent given for the use of personal information under **section 39(1)(b)**, the disclosure of personal information under **section 40(1)(d)** and access to third party personal information under **section 17(2)(a)** of the FOIP Act. It does not apply to consent for disclosure of business information under **section 16(3)(a)** of the Act.

There is also no change to the content of the consent required for purposes of **section 39(1)(b)** or **40(1)(d)** of the FOIP Act. The individual giving the consent must identify the personal information that is to be used or disclosed (**sections 39(1)(b)** and 4**0(1)(d)**) and must specify how the information may be used and to whom the information may be disclosed (**section 7(2)(b)** of the Regulation).

Common standards

Whether a consent is given in writing, in electronic form or orally, there are certain requirements that are common to all three forms of consent:

- there must be a record of the consent over which the public body has control
- the identity of the person giving consent must be authenticated
- there must be a reliable link between the person giving the consent and the consent itself

A familiar example is when an individual provides consent on a printed form. The signature on the form authenticates the identity of the person who is giving consent, the text and the signature appear together on the form and the public body retains the form in its files, so all three requirements are met.

The standards for electronic and oral consent are neither higher nor lower than those required for consent in writing. Electronic and oral consent do not have to be more reliable than their written equivalent. The public body need only be satisfied that the person giving the consent is who he or she purports to be. Naturally, if a public body is aware of suspicious circumstances, it would be a good practice to investigate the matter further, whether the consent is given in writing, electronically or orally.

Authentication of identity

Privacy protection requires verifying or "authenticating" the identity of the individual giving consent. When an individual visits a government office, there may be several different ways to ensure that the individual is who they say they are. However, when the contact is by telephone, as when an individual contacts a public body through a call centre, or over the Internet, the level of assurance that someone is who they say they are is lower. Assurance is increased if the office has processes in place to authenticate the individual's identity.

Authentication of identity is the process of proving or ensuring that someone is who he or she purports to be. It answers the question "Are you who you say you are?" This differs from "identification," which establishes who you are.

Authentication typically relies on one or more of the following:

- something you know (e.g. password, security question, PIN, mother's maiden name)
- something you have (e.g. smart card, key, hardware token)
- something you are (e.g. biometric data, such as fingerprints, iris scans, voice patterns)

A public body should keep the following points in mind when developing an authentication process.

- **The level of authentication should be appropriate to the nature of the use or disclosure and the sensitivity of the personal information involved**

The FOIP Act requires that a public body protect personal information against unauthorized use or disclosure. The degree of authentication must be appropriate to the nature of the use or disclosure and the sensitivity of the personal information involved. In circumstances requiring a higher level of authentication, a public body may wish to use multi-factor authentication, i.e. two or more forms of authentication to confirm identity.

- **Avoid the use of a common identifier**

A public body should avoid an authentication process involving the use of a common identifier by a number of different public bodies and programs. The use of a common identifier increases the risk of data matching and improper linking of personal information. For example, a call centre providing services to a number of public bodies should not use a single identifier (e.g. operator's licence number) as the authentication process for all its public body clients.

- **Notice under section 34(2) for the collection of new personal information for authentication purposes**

Authentication processes that rely on an individual confirming personal information already in the public body's custody or control will not require notice under **section 34(2)** of the FOIP Act. For example, notification is not required where the authentication process involves an individual stating something known by the public body, such as the last program the individual participated in with the public body, or the amount of funds received under a benefits program. The public body is not collecting new information but is using the information given by the individual to verify previous transactions. This would be considered a consistent use.

Any new collection of personal information would require notification of the authority for the collection, the purpose of the collection, and contact information of an individual within the public body who can answer questions about the collection.

- **Authentication and the exercise of the right of consent by other persons**

When a public body receives a consent from a person exercising the right of consent of another person under **section 84** of the FOIP Act, the public body must authenticate the identity of the person exercising the right.

CONSENT IN WRITING

For the purposes of **section 7** of the Regulation, consent in writing means consent given on paper.

Prior to the amendments, consent in writing did not require a signature. For example, a written consent would have been valid if it contained a typed name rather than a signature. In keeping with the concept that there should common standards for oral, electronic and written consent, a signature requirement has been added for consent in writing (**section 7(4)**).

A signature on a document is a form of authentication that lets a public body identify the person who is purporting to sign the document, shows the signatory's intent to be bound by the document and, perhaps most importantly, links the signatory with the text of the document.

A signature requirement for written consent is a reasonable expectation of individuals. It is likely that individuals already sign the document that contains their consent.

Written consent given before the coming into force of the amendments

The new provisions are prospective in effect. A written consent given prior to the coming into force date of the amendments and that did not expire before that date will continue to be valid after that date, even if it does not include a signature.

Example: An individual may have given a public body a continuing consent under **section 17(2)(a)** of the Act for the disclosure of certain personal information whenever an access request is made for that information. The consent continues to have effect after the coming into force date of the amendments until such time as the individual withdraws the consent or sets an expiry date.

CONSENT IN ELECTRONIC FORM

Section 7(5) of the Regulation permits, but does not require, a public body to accept consent in electronic form. It does so by establishing the electronic "functional equivalent" to consent given in writing on paper.

Section 7(5) incorporates the functional equivalency rules set out in the *Electronic Transactions Act* for a record requiring a signature that is to be provided to a public body. The requirements of **section 7(5)** support the policy purposes behind the original requirement that consent be in writing. When satisfied, the requirements allow consent in electronic form to have the same legal effect under the FOIP Act as paper-based consent.

"Electronic" is defined in **section 7(1)(a)**. The definition is sufficiently broad to address the increasingly grey area between voice and electronic communications. The only requirement is that the format be digital or some other intangible form. This ensures that the definition does not extend to paper documents, which have similar capabilities to electronic media.

Electronic consent can take many forms, such as sending an e-mail, clicking on an icon or button on a website, or submitting a file on a computer disk. Whatever the format, the consent will be valid only if it meets *all* of the following requirements.

- **The head of the public body has established rules respecting the purposes for which consent in electronic form is acceptable**

Section 7(5)(a) recognizes that the public body is in the best position to determine the purposes, if any, for which it is appropriate to accept electronic consent.

The determination is not to be made on a case-by-case basis. Rather, **section 7(5)(a)** requires the public body to establish a policy or "rules" that set out the purposes for which it will accept electronic consent. This will require public bodies to examine their programs and services and determine how they use or disclose information, the sensitivity of the personal information involved, the parties to whom the information will be disclosed (e.g. another public body, a private sector organization or another individual), and the associated risks for accepting electronic consent in those circumstances.

Example: A public body may have a rule that it will accept consent in electronic form for use of personal information to make a change of address, but not for disclosure to a third party of personal information about participation in a program.

The head of the public body must approve the rules that establish the purposes for which electronic consent will be accepted by the public body.

- **The consent is being given for one or more of the established purposes**

Section 7(5)(b) reinforces the principle that a public body cannot accept consent in electronic form for a purpose that is not permitted under the rules. Electronic consent will only be valid if it is given for one or more of the purposes the public body has set out in its rules. For example, if the head of the public body has not approved consent in electronic form for a particular purpose, a front-line employee cannot take the initiative to accept electronic consent for that purpose. Public bodies will need to ensure their affected staff know the "rules."

- **The public body has explicitly communicated that it will accept consent for those purposes**

Section 7(5)(c) requires the public body to expressly communicate to the public the purposes for which it will accept electronic consent. Acceptance cannot be inferred from the public body's conduct. For example, the fact that a public body has an e-mail address does not mean that the public body is accepting consent in electronic form. **Section 7(5)(c)** underscores the principle that a public body cannot be compelled to accept electronic consent for purposes other than those established in the rules.

Express communication could include posting a notice on a website or publishing a statement in a program guide, brochure or newsletter.

- **The consent must be accessible and capable of being retained by the public body so as to be usable for subsequent reference**

Sections 7(5)(d)(i) and **(ii)** recognize that the main functional purpose of a written document is to establish memory; that is, to create a reliable, durable record of the transaction for future reference.

Consent is "accessible" if it is understandable and available. Consent is "capable of being retained" if the public body has control over the consent for future reference. For example, the requirements will not be met if the electronic file containing the consent can only be opened once, has a built-in mechanism that will erase it at a fixed point in time, or cannot be stored in some manner. Being able to retain the consent preserves the integrity of the consent and creates a record of the consent for the public body.

The means of retention are not specified as they will differ for the different electronic formats used for giving consent. The length of time for which the consent must be usable for subsequent reference is also not specified, but the requirement for durability should not be greater than that for paper. The public body's retention policies that apply to a record containing a written consent should apply to a consent in electronic form, where possible.

- **The consent must meet any information technology standards established by the public body**

General permission to submit consent in electronic form may expose public bodies to a variety of formats and media that they may not have the capacity to handle or that may not be appropriate for the purpose in question. **Section 7(5)(d)(iii)** allows a public body to set its own standards for incoming electronic consents. These may be nothing more than specifications for hardware and software and rules on the medium of the communication (e.g. use of e-mail, computer disks).

When establishing information technology standards, public bodies should consider putting in place methods for preventing or correcting errors, particularly with the use of computers. For example, it is easy to hit the wrong key or click the mouse on the wrong spot on a screen and send a message that was not intended. One way to address this would be for a message to come on the computer screen stating what the person has consented to and asking the individual to confirm.

Although a public body is not required to acknowledge receipt of the consent, the public body may choose to also establish rules for acknowledgement.

The use of new information technologies for managing personal information may require a privacy impact assessment (PIA).

- **The consent must include an electronic signature of the person giving the consent**

An electronic signature is a paperless way to sign a document using an electronic symbol or process attached to or associated with the document.

"Electronic signature" is defined in **section 7(1)** as "electronic information that a person creates or adopts in order to sign a record and that is in, attached to or associated with the record." **Sections 7(5)(f)** and **(g)** set out additional requirements:

- the electronic signature must be reliable for the purpose of identifying the person giving consent,
- the electronic signature must meet any information technology standards or requirements established by the public body as to the method of making the signature and its reliability, and
- the association of the electronic signature with the consent must be reliable for the purpose for which the consent is given.

These provisions establish that the purpose of an electronic signature is the same as a handwritten signature on paper. It is a method of authenticating the identity of the person providing the consent, it shows the signatory's intention to sign, and links the person giving the consent with the consent itself.

The definition makes it clear that the electronic signature does not have to resemble a handwritten signature (although it is possible to create a digital picture of a handwritten signature). The electronic signature is simply required to be electronic information created or adopted by the signatory as his signature. However, it must also be reliable for verifying the signatory is who he or she purports to be.

Where an individual's right to consent is being exercised under **section 84** of the Act by a person rather than an individual, such as an incorporated

solicitor or the Public Trustee, it is sufficient if the signature is the electronic signature of the office of that person.

The definition of electronic signature also recognizes that a core functional purpose of a signature is to link a person with a document. Although an electronic signature will not necessarily be incorporated into the electronic consent in the way that an ink signature is to paper, it must be attached to or associated with the consent in some way. The association of the electronic signature with the consent must also be reliable for the purpose for which the consent is being given.

For example, a public body may decide an electronic signature that appears on an e-mail from an employee that has been sent within a secure network is reliable for most purposes. In other situations, public bodies may decide there is a need for a more sophisticated form of electronic signature (e.g. as in a public key infrastructure system).

An electronic signature submitted to a public body must meet any information technology standards and requirements established by the public body about the method of making an electronic signature or its reliability.

CONSENT THAT IS GIVEN ORALLY

Section 7(6) of the Regulation sets out the requirements for oral consent. They are adapted from the principles that apply to consent in electronic form and are set out within the Regulation in a format that parallels the provisions of **section 7(5)**.

Black's Law Dictionary (7th ed.) defines "oral" as "spoken or uttered; not expressed in writing." While there may be some discussion as to whether certain communications are oral or electronic in nature, the oral consent provisions in **section 7(6)** can be considered as encompassing consent given in speech, whether in person, by telephone or some other means of spoken communication.

Hearing or speech-disabled individuals may use a teletypewriter (TTY) to communicate by telephone with a public body. Specially trained operators of the individual's telephone service provider relay the telephone conversation between the individual and the public body. It would be reasonable to consider the use of TTY as a form of spoken communication for purposes of oral consent under **section 7(6)**.

A public body is permitted, but not required, to accept oral consent. For the consent to be valid, *all* of the following requirements must be met.

- **The head of the public body has established rules respecting the purposes for which consent given orally is acceptable**

Section 7(6)(a) requires a public body to establish "rules" that define the purposes for which it will accept consent given orally. Oral consent must be appropriate for the purpose for which the public body is using or disclosing the personal information under **Part 2** of the Act. Factors to be considered include the circumstances under which the information is to be used or disclosed, the nature of the personal information involved, the party to whom the information will be disclosed and the risks associated with permitting oral consent.

Example: An individual has applied for a certain program of the public body. The individual is not eligible for that program but may be eligible for a program operated by another branch within the public body. The public body may have a rule allowing oral consent to be accepted from the individual for the purpose of passing on the individual's personal information to the other program area.

Example: A student is eligible for a certain scholarship offered by an organization outside the school. The school may have a rule that it will accept the student's oral consent to disclose the student's grades to the scholarship organization.

The head of the public body must approve the rules that establish the purposes for which oral consent will be accepted by the public body.

- **The consent is being given for one or more of the established purposes**

As exists with electronic consent, **section 7(6)(b)** states that a public body cannot accept oral consent for a purpose that is not permitted under the rules.

- **The public body has explicitly communicated that it will accept consent that is given orally**

Section 7(6)(c) requires the public body to expressly communicate to the public the purposes for which it will accept oral consent. For example, a public body could post a notice on a website or at its front counter, include a statement in a newsletter to its clients, or have the service representative at the call centre confirm that oral consent is acceptable for the caller's purpose.

- **There is a record of the consent which is accessible and capable of being retained by the public body so as to be usable for subsequent reference**

Sections 7(6)(d)(i) and **(ii)** provide that oral consent will be valid only if a record can be made of the consent and the public body has access to and control over the record for future reference.

Section 7(7) specifies the acceptable methods for recording oral consent. The public body must choose the method of recording that is appropriate for the purpose for which the consent is being given and the nature of the information involved.

(a) An audio recording of the consent created by or on behalf of the public body

An audio recording is an objective record of the consent given orally. A public body may create its own audio recording or it may hire another body to make an audio recording for it. Where a contractor is hired to make the recording, the public body will need to establish that the record is under the control, if not in the custody, of the public body and how the public body will access the record.

This provision refers only to recording the consent portion of the conversation, not the entire conversation.

Example: An individual is giving oral consent over the telephone for a particular purpose. The public body activates its recording mechanism so as to capture only that part of the conversation where the individual verifies his or her identity and states what he or she is consenting to.

(b) The consent is documented by an independent third party

It may be appropriate for the record of oral consent to be created by an independent third party, such as a non-profit organization trusted by the public body and client group or an organization qualified to audit this kind of activity. One method of doing so would have an individual's telephone call to the public body momentarily transferred to a third party who confirms the details of the consent and documents the consent.

The public body may permit the third party to determine the manner of documentation or may set certain criteria. The public body must have access to and control of the record. The public body should also establish that personal information collected by the third party can be used only for the purpose of recording the consent.

(c) The consent is documented by the public body in accordance with rules established by the head of the public body

This option is available only for narrowly defined purposes and specific circumstances where it would be appropriate for the public body to document the consent (e.g. to disclose a change of address to another public body). It is not intended that a public body create a blanket policy to accept oral consent for all purposes or on a case-by-case basis at the discretion of an employee.

The head of a public body must establish in rules the purposes and circumstances in which the public body may document consent given orally. The head may also wish to establish rules regarding the method by which the documentation is to be made. For example, the public body may require employees receiving the consent to makes a contemporaneous written and signed entry in a log detailing the text of the consent, who gave the consent, how identity was verified and the date and time the consent was given.

If public body decides to use this option for recording oral consent, the public body should also put in place a process to ensure that the documentation is being done in compliance with the established rules.

- **The public body must have authenticated the identity of the individual giving consent**

For oral consent to be valid, the public body must verify that the individual giving the consent is who they say they are (**section 7(6)(e)**). Various methods may be used; for example, a "shared secret" where the individual provides some information known only to him or her and the public body, such as information about a previous transaction, a case number or a password created for the purpose of authentication.

- **The method of authentication must be reliable for verifying the identity of the individual and for associating the consent with the individual**

The reliability of the method of authentication for verifying the identity of the individual giving oral consent and for associating or linking the individual with the consent will depend on the purpose for which the consent is being given. A higher degree of reliability would be required for consent to the use or disclosure of very sensitive personal information.

It is not sufficient to authenticate identity but have no way to link the individual with the information of what they consented to.

Example: An audio recording could include the public body's employee asking for the individual's consent to a particular use or disclosure, and asking the individual to answer a question to which only that individual would know the answer in order to authenticate the individual's identity.

REVIEW BY THE COMMISSIONER

In the event of a review or a complaint where an individual argues that consent was not given, the public body is likely to bear the burden of proving consent was given. The public body, as the keeper of the record, is in the best position to establish that the consent met the requirements of the Act and the Regulation.

TIPS FOR IMPLEMENTATION

A public body deciding to exercise the option of accepting electronic or oral consent may wish to start with a low-risk transaction that has the following characteristics:

- the transaction is routine and low in volume
- only a small number of clients are affected
- only a small number of staff are involved
- the personal information is of a non-sensitive nature
- the consent is for the use of the personal information within the public body
- the use is beneficial to the individual
- staff are aware of the form in which consent can be accepted, the method for authenticating the individual's identity, and the manner in which the consent is to be recorded

The head of a public body must approve the rules that set out the purposes for which electronic or oral consent may be accepted. The head must also set out in rules when it would be appropriate for the public body to document a consent that is given orally. It may be necessary for a public body to amend an existing delegation instrument (that delegates the functions of the head of the public body to another person) to allow the delegate to approve the rules.

A public body may wish to consider including in the record of any consent given the date and, if necessary, the time of when the consent was given.

It may be advisable for a public body to consult with its corporate information officer when the public body is establishing information technology standards for electronic consent.

Currency

This Bulletin takes into consideration decisions issued by the Office of the Information and Privacy Commissioner of Alberta up to December 31, 2008.

Purpose

FOIP Bulletins are intended to provide FOIP Coordinators with more detailed information for interpreting the *Freedom of Information and Protection of Privacy Act*. They supply information concerning procedures and practices to assist in the effective and consistent implementation of the FOIP Act across public bodies. FOIP Bulletins are not a substitute for legal advice.

Further Information

Access and Privacy
Service Alberta
3rd Fl., 10155 – 102 Street
Edmonton, Alberta T5J 4L4
Phone: 780-427-5848
Website: foip.alberta.ca