Office of the Information and Privacy Commissioner for Nova Scotia

Guidance for the Use of Criminal Record Checks By Health Profession Regulating Bodies

This guidance document was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia, at the request of the Nova Scotia Regulated Health Professionals Network. It is intended to assist Nova Scotia's health professional regulators in deciding whether or not their organizations have the authority under Nova Scotia's privacy legislation to collect, use, and disclose criminal record checks from members. It also makes 15 best practice recommendations for how to implement a criminal record check program.

Notice to Users

This document is intended to provide general information only. It is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with the *Freedom of Information and Protection of Privacy Act*, the Office of the Information and Privacy Commissioner (OIPC) cannot approve in advance any proposal from a public body. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Commissioner will keep an open mind. It remains the responsibility of each public body to ensure that it complies with its responsibilities under the legislation. Visit us at: www.foipop.ns.ca

BACKGROUND

Some, if not all, health profession regulators (regulators) in Nova Scotia have made it a practice to collect criminal record checks from members and potential members. This information is then used by the regulator to make decisions about licensing and renewals of licenses, for applicants and existing members (members). The regulators asked for some guidance from the Information and Privacy Commissioner[1] on this practice.

One of the purposes of the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*) is to ensure that public bodies are fully accountable to the public by preventing the unauthorized collection, use or disclosure of personal information. While only two regulators are listed in the Schedule of *FOIPOP*, it is likely that all regulators are subject to *FOIPOP* and the rules it sets out regarding the handling of personal information by virtue of the definition of "public body" set out in s. 3(1)(j) of *FOIPOP*.

Criminal record checks, by their nature, contain very sensitive personal information. Therefore, in order to conduct criminal record checks, regulators must satisfy the privacy rules in *FOIPOP*.

The following provides the rules and 15 best practice suggestions that regulators should consider when deciding whether to collect, use or disclose criminal record checks as part of the application and renewing processes.

COLLECTION

Collection Rules

There are three reasons (authorities) set out in *FOIPOP* which could allow regulators to collect personal information:

1. Collection is expressly authorized by another statute,
2. The collection is directly related to and necessary for an operating program or activity, or
3. The collection is for a law enforcement purpose. [2]

Collection occurs when a regulator gathers, acquires, receives or obtains personal information. There is no restriction on how the information is collected, which can mean obtaining a physical copy or simply viewing it. Note that the law does not permit a regulator to collect personal information based on the consent of the individual. Regulators must be authorized to collect personal information under one of the three reasons listed above.

Under *FOIPOP*, collection of personal information is prohibited unless *FOIPOP* authorizes the collection. Therefore, regulators must establish whether or not they have the authority under *FOIPOP* to collect personal information prior to collecting the criminal history of individuals. The

[1] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the independent oversight authority under the *Freedom of Information and Protection of Privacy Act*, the *Municipal Government Act*, the *Personal Health Information Act*, and the *Privacy Review Officer Act*. It is the role of the Commissioner to monitor how the privacy provisions are administered by conducting investigations into compliance, undertaking research, and informing the public about access and privacy matters.

[2] See s. 24(1) of *FOIPOP*. Note that "law enforcement" is defined in s. 3(1)(e) of *FOIPOP* and means policing, including criminal-intelligence operations, investigations that lead or could lead to a penalty or sanction being imposed, and proceedings that lead or could lead to a penalty or sanction being imposed.

regulators have identified that the authority they likely rely on for the collection of personal information through criminal record checks is that the information relates directly to and is necessary for an operating program or activity of the regulator.

FOIPOP states that personal information may be collected if it "relates directly to and is necessary for an operating program or activity." Therefore, to have authority to collect the personal information, the regulator must establish three things:

1. To "relate directly to", the information must have a direct bearing on the operating program or activity of the regulator.

2. To be "necessary for", it is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future. Nor is it enough that it would be merely convenient to have the information. The information need not be indispensable. In assessing whether personal information is necessary, one considers the sensitivity of the information, the particular purpose for the use, and the amount of personal information used in light of the purpose for use.

3. The collection must relate to an operating program or activity of the regulator, not to another organization (i.e. an employer where the member works).

Another potential authority for conducting criminal record checks is that a statutory provision exists that expressly authorizes the collection. Only one regulation in Nova Scotia specifically requires criminal record checks be provided to a regulator as part of an application/licensing process.[3]

Before collecting or continuing to collect criminal record check information, review your program and evaluate whether or not it is authorized under *FOIPOP*.

A regulator that determines it does not have authority to collect must stop collecting the information. All criminal record checks that were collected previously should be destroyed in accordance with the regulator's records retention schedule and in accordance with *FOIPOP.*[4]

If a regulator establishes that it does have authority under *FOIPOP* to collect personal information through criminal record checks, best practice is to then consider if it should proceed with collection and if so, to what extent. The following 15 best practices will help to guide regulators in establishing a *FOIPOP* compliant program.

[3] Driver Training Schools Regulations, see ss. 2, 3, 6, 15, 17: http://www.novascotia.ca/just/regulations/regs/mvdtschl.htm.

[4] Section 24(4) of *FOIPOP* states that when a public body uses personal information to make a decision that directly affects the individual, the public body must retain the information for at least one year.

Collection Best Practices

Minimize. Regulators should be careful to only collect the minimum amount of personal information that is necessary for the intended program or activity. This can be accomplished in two ways:

1. Conduct the least invasive form of check required: If only a criminal record check is required, ensure other forms of checks are not also conducted – such as a vulnerable sector check or a child abuse registry check.

2. Don't make copies: Regulators may only need to check if the criminal record check is "clean" or not. If the criminal record check is clean, it does not need to be kept at all. Regulators should have a way to note in the member file that the criminal record check was viewed and was clean - a copy should not be retained.

   In cases where the record is not clean, an appointment should be set up with the person responsible for discussing the member's options (see more below in "Use Best Practices").

Formalize. It is important to document the reasons for the collection of personal information. Best practices include:

3. Develop employee guidance: Regulators should develop appropriate written policies and procedures to guide their employees who are responsible for collecting and assessing the relevance of criminal record checks, and to ensure compliance with the privacy provisions (rules) of *FOIPOP*.[5]

Notify. Whether or not a copy of the criminal record check is retained, a collection is occurring. Regulators should have a notice of purpose available to members.

4. Notify and obtain consent from members: Provide a clear notification to members and applicants of the reason for the collection of criminal record check information. The notice should explain the purpose, nature and extent of collection of their personal information and should seek consent for any intended uses or disclosures of the information.

USE

Use Rules

Regulators have identified that the authority they rely on for using criminal record checks is that it is for the same purpose it was collected for – to assess the member's ability to be licensed.[6] However, as noted above, best practice is to obtain consent from members for the use of their personal information.

Accessing (looking at) personal information is a use. Regulators should be careful to only use personal information for authorized purposes and should limit access to only those employees that require the information to do their jobs.

[5] Found in ss. 24 to 30 of *FOIPOP*.

[6] This is a purpose authorized by s. 26(a) of *FOIPOP*. *FOIPOP* authorizes two other purposes – with consent (s. 26(b)) or if *FOIPOP* authorized another public body to disclose the information to the regulator (s. 26(c)).

Use Best Practices

Formalize. It is important to document the reasons for the use of personal information. Best practice includes:

5. Develop tools: Create a conviction relevance matrix. Identify which convictions would and would not be acceptable for licensing purposes. This tool can be amended over time as decisions are made about what is acceptable and what is not.

Centralize. Centralize the decision making about a member's ability to obtain a license. This practice will achieve the following privacy supportive practices:

6. Develop expertise: Centralizing decision making will allow the person making decisions to develop expertise (including the development of a conviction relevance matrix).

7. Limit access: Only those who are making the decisions will have access to the sensitive information.

DISCLOSURE

Disclosure Rules

FOIPOP provides for the disclosure of personal information with consent of the affected individual or in limited circumstances without consent. Disclosure includes the sharing of personal information with an employer.

Disclosure Best Practices

Don't disclose. Disclosure, even if authorized, is discretionary. Regulators should consider the following when deciding if disclosure is appropriate:

8. Passage of time: Given licensing happens prior to employment, a criminal record check that was provided to the regulator may be out of date by the time the member obtains employment (normally criminal record checks are valid for six months). A lot can happen in a person's life during that time, so the criminal record check may no longer be accurate and therefore would not serve the purpose it is intended for.

9. Shift responsibility: The employer could make its own request to the member directly, identifying its own authority for collection.

Get consent. If disclosing the actual criminal record check to the employer, ensure that consent is received from the member at the time of the disclosure. Keep in mind:

10. Informed consent: Having a member sign a blanket consent form as part of the application process will not generally be adequate. The consent to disclosure should be signed at or near the time of disclosure and should identify both the information to be disclosed and the organization to which the regulator is authorized to disclose the information.

Minimize. Regulators should be careful to only disclose the minimum amount of personal information that is necessary for the intended purpose. Best practice is that the regulators:

11. Don't provide copies: Regulators can simply confirm that the record is clean.

SECURITY

Security Rules

FOIPOP requires[7] regulators to have adequate security arrangements (administrative, physical, technical and personnel) in place to protect privacy.

Security Best Practices

Mitigate risk. Regulators should understand what the privacy implications are when collecting, using, disclosing, storing and disposing of personal information. This can be achieved by developing a privacy management framework[8] that includes the following best practices:

12. Conduct an assessment: Prepare a privacy impact assessment (PIA) to assess and mitigate privacy implications before beginning to collect, use or disclose criminal record check information.[9]

13. Limit access: Criminal record checks should be placed in locked cabinets, accessible to only people who are required to use the criminal record check as a function of their jobs. Electronic copies of criminal record check related information should be in secure drives with access limited to authorized personnel.

14. Develop policy: Without written policies and procedures in place, regulators have not taken responsible steps to safeguard personal information in their custody and control. Written policies and procedures will guide employees who are responsible for licensing to ensure compliance with the privacy provisions under *FOIPOP.*[10]

15. Records Management: Do not keep criminal record checks longer than necessary. Regulators should develop a retention schedule and ensure it is followed. Keeping records longer than needed increases the risks associated with storing personal information (such as breaches).

---

[7] S. 24(3) of *FOIPOP*. See the OIPC website for the Security Checklist which provides some preliminary guidance on what practices meet the minimum security requirements under *FOIPOP*: https://foipop.ns.ca/sites/default/files/publications/Reasonable%20Security%20Checklist%20for%20Personal%20Information%20%2822%20Sept%2015%29.pdf.

[8] For more details on how to implement a complete privacy management framework see the OIPC website for Privacy Management Program at a Glance and Privacy Management Program: Getting Started, both available at: http://foipop.ns.ca/publicbodytools.

[9] See the OIPC website for a PIA template for public bodies at: https://foipop.ns.ca/sites/default/files/publications/FOIPOP%20Tools/FINAL%20-%20FOIPOP%20PIA%20OIPC%202015%2009%2021.pdf.

[10] Essential *FOIPOP* policies include a privacy policy (describing collection, use & disclosure practices), breach management policy, records management policy and security policy. For more details on essential privacy policies review the privacy management program materials on the OIPC website www.foipop.ns.ca.