	DOCTORS NOVA SCOTIA
Section:	BOARD POLICY
Subject:	**Privacy Policy – Collection, use and disclosure of personal information**
Approved by Board:	May 2026

1.0 PURPOSE

1.1 Doctors Nova Scotia (DNS) is committed to protecting the privacy of personal information entrusted to the organization.

1.2 The purpose of this policy is to:

1.2.1 Outline how DNS collects, uses, discloses, retains, and safeguards personal information.

1.2.2 Ensure transparency and accountability in DNS privacy practices.

1.2.3 Ensure compliance with applicable privacy legislation.

1.2.4 Inform individuals about their rights regarding their personal information.

2.0 POLICY STATEMENT

2.1 DNS collects, uses, retains, and discloses personal information only for purposes that are reasonable and necessary to fulfill the organization's mandate and provide services to its members and clients.

2.2 DNS is committed to:

2.2.1 Collecting only the personal information necessary for identified purposes.

2.2.2 Obtaining consent where required.

2.2.3 Protecting personal information through appropriate safeguards.

2.2.4 Limiting access to personal information to authorized individuals.

2.2.5 Ensuring individuals can access and request correction of their personal information.

2.2.6 Maintaining transparent privacy practices.

2.3 DNS does not sell personal information.

3.0 SCOPE

3.1 This policy applies to:

3.1.1 All personal information collected, used, retained, or disclosed by DNS.

3.1.2 DNS staff and contractors.

3.1.3 Board and committee members

3.1.4 Third-party service providers acting on behalf of DNS where personal information may be accessed.

3.2 This policy applies to personal information relating to:

3.2.1 DNS members.

3.2.2 Individuals purchasing DNS products or services.

3.2.3 Individuals attending DNS events or programs.

3.2.4 Individuals participating in surveys or consultations.

3.2.5 Family members where information is required for benefits or insurance programs.

3.3 This policy does not apply to:

3.3.1 DNS employee records governed by internal HR policies.

3.3.2 Information that is publicly available as defined under applicable legislation.

4.0 DEFINITIONS

4.1 **Personal Information:** Information about an identifiable individual, such as name, home address, telephone number, email address, date of birth, and gender identity. Personal information does not include publicly available business contact information or personal health information governed by applicable health information legislation.

4.2 **Consent:** Voluntary agreement to the collection, use, or disclosure of personal information for identified purposes.

4.3 **Third-Party Service Provider:** An external organization contracted by DNS to perform services that may require access to personal information.

4.4 **Chief Privacy Officer:** The individual designated by DNS to oversee privacy compliance and respond to privacy inquiries or concerns.

5.0 GUIDING PRINCIPLES

DNS manages personal information according to the following principles:

5.1 **Accountability:** DNS is responsible for personal information under its control and has designated a Chief Privacy Officer responsible for compliance.

5.2 **Transparency**: DNS maintains clear and accessible policies regarding its privacy practices.

5.3 **Identifying Purposes**: The purposes for collecting personal information are identified before or at the time of collection.

5.4 **Consent**: DNS obtains consent for the collection, use, or disclosure of personal information where required.

5.5 **Limiting Collection**: Only the personal information necessary for identified purposes is collected.

5.6 **Limiting Use, Disclosure and Retention**: Personal information is used or disclosed only for the purposes for which it was collected unless otherwise permitted by law.

5.7 **Accuracy**: DNS makes reasonable efforts to ensure personal information is accurate and up to date.

5.8 **Safeguards**: Appropriate physical, organizational, and technological safeguards protect personal information.

5.9 **Individual Access**: Individuals have the right to request access to their personal information and request corrections where appropriate.

6.0 STANDARDS OF CONDUCT

Individuals who have access to personal information through DNS must:

6.1 Respect the confidentiality of personal information.

6.2 Access personal information only when necessary to perform their duties.

6.3 Protect personal information from unauthorized access, use, or disclosure.

6.4 Follow DNS policies and procedures relating to privacy and information security.

7.0 PROCEDURES

7.1 **Collection of Personal Information:**

7.1.1 DNS may collect personal information through membership applications, event registrations, surveys, and participation in DNS programs.

7.1.2 DNS may also receive relevant information from organizations involved in physician services or programs where appropriate and permitted by law.

7.2 **Use of Personal Information**

DNS uses personal information to:

7.2.1 Determine eligibility for membership and services.

7.2.2 Administer member programs and benefits.

7.2.3 Communicate information about services and opportunities.

7.2.4 Support advocacy, negotiations, and representation on behalf of physicians.

7.2.5 Conduct surveys and research for statistical and planning purposes.

7.2.6 Maintain accurate membership records.

7.3 **Disclosure of Personal Information**

7.3.1 DNS may disclose personal information to partner organizations or third-party service providers, including insurance providers, where disclosure is necessary to administer programs or deliver services.

7.3.2 In these circumstances, DNS will require formal data sharing agreements and will use secure portals or other approved secure methods to transfer personal information.

7.3.3 DNS will limit disclosure to the minimum amount of personal information that is strictly necessary for the identified purpose and requires recipient organizations to safeguard the information and use it solely for the purposes for which it was disclosed.

7.4 **Safeguards**

7.4.1 Breach Notification

DNS will respond to and report any privacy breaches in accordance with applicable privacy legislation. This includes notifying affected individuals and the Privacy Commissioner of Canada where there is a real risk of significant harm. Breaches will be investigated promptly, and corrective actions will be taken to prevent recurrence.

7.4.2 DNS protects personal information using appropriate physical, organizational, and technological safeguards. Access to sensitive information is limited to authorized personnel.

7.5 **Retention and Destruction**

Personal information is retained only as long as necessary to fulfill the purposes for which it was collected and to meet legal or regulatory requirements. Information is securely destroyed according to DNS's Records Retention Schedule when it is no longer required.

7.6 **Access and Correction**

Individuals may request access to their personal information held by DNS and request corrections where information is inaccurate or incomplete.

7.7 **Withdrawal of Consent**

Individuals may withdraw consent for the collection, use, or disclosure of personal information, subject to legal or contractual limitations. Contractual limitations may apply where personal information is necessary to administer ongoing programs, services, benefits, or third-party agreements, and where withdrawal of consent would prevent DNS from fulfilling its contractual obligations.

7.8 **Privacy Questions or Concerns**

Questions or concerns regarding privacy practices may be directed to the DNS Chief Privacy Officer.

8.0 RELATED DOCUMENTS

Related DNS policies may include:

- Information Systems and Data Security Policy
- Records Management Policy
- Code of Conduct
- Cybersecurity Incident Response Plan

9.0 ACCOUNTABILITY

9.1 The DNS Chief Privacy Officer is responsible for:

9.1.1 Overseeing compliance with this policy.

9.1.2 Responding to privacy inquiries and concerns.

9.1.3 Monitoring privacy practices.

9.1.4 Recommending policy updates.

9.2 The DNS Board of Directors is responsible for approval of this policy.

10.0 REVIEW CYCLE

This policy will be reviewed every three years or sooner if required due to legislative, operational, or governance changes.

Appendix A

Privacy Policy - Frequently Asked Questions for Members

1. What is personal information?

Personal information is information about an identifiable individual, such as your name, contact details, date of birth, and gender identity. It does **not** include publicly available business contact information or personal health information governed by health-specific legislation.

2. Why does Doctors Nova Scotia collect my personal information?

DNS collects personal information to:

- Determine eligibility for membership and services
- Deliver programs, benefits, and insurance offerings
- Communicate with you about services, events, and opportunities
- Support advocacy, negotiations, and physician representation
- Maintain accurate member records
- Conduct surveys

DNS collects only the information needed for these purposes.

3. How does DNS collect personal information?

Personal information may be collected through:

- Membership applications or renewals
- Event and program registrations
- Surveys
- Participation in DNS programs

4. Does DNS sell my personal information?

No. Doctors Nova Scotia does not sell personal information.

5. Who has access to my personal information?

Access to personal information is limited to:

- Authorized DNS staff or contractors who need it to perform their duties
- Trusted third-party service providers where necessary to deliver programs or services

All individuals with access are required to protect confidentiality.

6. Does DNS share my information with third parties?

In some cases, yes, but only when necessary. DNS may share limited personal information with partner organizations or service providers (such as insurance providers) to administer benefits or programs.

When this happens:

- Information sharing agreements are required.
- Secure systems and approved transfer methods are used.
- Only the minimum necessary information is shared.
- Recipients must safeguard the information and use it only for the agreed-upon purpose.

7. How does DNS protect my personal information?

DNS uses a combination of:

- Physical safeguards (e.g., controlled access to offices).
- Organizational safeguards (e.g., policies, training, role-based access).
- Technological safeguards (e.g., secure systems and portals).

8. What happens if there is a privacy breach?

If a privacy breach occurs:

- DNS will investigate it promptly.
- Affected individuals will be notified when required by law.
- The Privacy Commissioner of Canada will be notified if there is a real risk of significant harm.
- Corrective actions will be taken to prevent recurrence.

9. How long does DNS keep my personal information?

Personal information is kept only as long as necessary to:

- Fulfill the purposes for which it was collected, and
- Meet legal or regulatory requirements, such as for financial records or audits.

When no longer required, information is securely destroyed according to DNS's Records Retention Schedule.

10. Can I access my personal information?

Yes. You have the right to request access to the personal information DNS holds about you.

11. Can I request corrections to my information?

Yes. If your personal information is inaccurate or incomplete, you should request that it be corrected.

12. Can I withdraw my consent?

In most cases, yes. You may withdraw consent for the collection, use, or disclosure of your personal information.

However, withdrawal may be limited by:

- Legal requirements (such as for financial records, audits, complaint handling, or legal matters), or
- Contractual obligations where your information is necessary to administer ongoing services, programs, benefits, or third-party agreements.

DNS will explain any implications of withdrawing consent.

13. Does this policy apply to DNS employees?

No. Employee personal information is governed by internal human resources policies and not this Privacy Policy.

14. Who oversees privacy at Doctors Nova Scotia?

DNS has designated a **Chief Privacy Officer** responsible for:

- Privacy compliance.
- Responding to privacy questions or concerns.
- Monitoring privacy practices.
- Recommending policy updates.

15. How can I contact DNS about privacy concerns?

If you have questions or concerns about how your personal information is handled, you can contact the **DNS Chief Privacy Officer**.