HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

GUIDE FOR A PRIVACY OFFICER AND SECURITY LEAD

Summary

This Guide assists clinics in documenting basic responsibilities of a Privacy Officer and Security Lead. Both roles play a vital role in:

- protecting patient information
- creating a culture of security
- establishing required measures to mitigate risk (safeguards)

Appointing the Privacy Officer and Security Lead and documenting their responsibilities is the first step in creating a culture of security at the clinic. Recognizing the process is complex, the Doctors Technology Office (DTO) created tools and resources. This Guide and the attached checklists can be adopted by clinics as guidance in creating their own framework, documentation, and training.

Why do Clinics Need a Privacy Officer?

Clinics and physician offices are subject to provincial private sector privacy law: the Personal Information Protection Act (PIPA). See the *Security Obligations Under PIPA* (pg 4) in the Physician Office IT Security Guide for more information about applicable regulations. The Privacy Officer is answerable to the College of Physicians and Surgeons and the Office of the Information and Privacy Commissioner.

As the Privacy Officer makes **all decisions** regarding the protection of patient sensitive information, it is recommended that the physician acts as Privacy Officer and in a solo practice, the physician is by default designated as the Privacy Officer.

> ***Note:***
>
> PIPA applies to organizations, not to individuals. There is no liability for a privacy officer if an organization fails to comply with PIPA.

The Privacy Officer takes leadership in creating a culture of security at the clinic. These tasks and responsibilities can be transferred to other care team members or to contracted professionals but the Privacy Officer retains the overall accountability for privacy and security of personal information.

The Privacy Officer ensures there is an ongoing monitoring of the clinic's practices and safeguards and can adopt the *Clinic Self-Assessment Checklist* for the process. With Security Lead help, the Privacy Officer reviews safeguards that are already in place and makes notes where the gaps are. They evaluate what safeguards clinic needs first and gradually address them.

Basic responsibilities are described in the *Checklist for Responsibilities of a Privacy Officer* attached to the bottom of this Guide.

Why do Clinics Need a Security Lead?

The Security Lead supports the Privacy Officer and is responsible for implementing safeguards protecting private information. This role requires professional experience in Information Technology and knowledge of industry standards for hardware and software in clinical setting. Technology expertise is necessary for the acquisition and installation of hardware and software, ongoing maintenance, and troubleshooting.

Clinics may choose different support models depending on their size or needs. It is highly recommended to contract a professional IT support and clinics can choose various levels of service. Refer to the IT Support Selection Checklist for Clinics for more guidance on the process.

Basic responsibilities are described in the *Checklist for Responsibilities of a Security Lead* attached to the bottom this Guide.

Tools and Resources

Both, the Privacy Officer and Security Lead, collaborate closely toward the same goal. Depending on specific situation at the clinic, responsibilities and tasks might be differently distributed and even contracted out.

Here is a list of resources created by the Doctors Technology Office to assist the Privacy Officers and Security Leads in their roles:

Physician Office IT Security Guide	User-friendly guide focusing on key safeguards for private practices to ensure their compliance with regulatory requirements. Concise (35 pages) reference for technical terminology and concepts.
Security Education	Information about current privacy and security learning opportunities offered by the DTO to physicians as well as office and clinic support staff.
Physician IT Security Resources	Guides, templates, and samples helping clinics with first steps in building a culture of security and implementing a framework for their privacy and security program.

Related Materials

Links below provide Privacy Officers with useful information and tools regarding information privacy:

BC Physician Privacy Toolkit	Based on "10 Fair Information Principles" this guide is created by Doctors of BC for private practice physicians. Contains applicable privacy resources and guidelines along with links to useful samples: Confidentiality Agreement for

	Employees, information sharing agreement, Patient Handout – Privacy of Your Personal Health Information
A Guide to B.C.'s Personal Information Protection Act - OIPC BC	The Office of the Information and Privacy Commissioner for British Columbia ("OIPC") developed this guide for businesses and other organizations to help with understanding the Personal information Protection Act ("PIPA"),
OIPC PrivacyRight	Developed by the Office of the Information and Privacy Commissioner (OIPC) this web-based education helps small businesses and organizations in BC understand their obligations under the Personal Information Protection Act (PIPA). Webinars, videos, and podcasts provide educational content in fun and easy to understand formats.
Privacy Breaches: Tools and Resources	OIPC document providing general information and describing key steps and actions to take when a privacy breach occurs. It applies to both public bodies and private organizations.
Privacy Breach Checklist	A form to be used by public and private organizations to respond to a privacy breach, and to decide whether to report the breach to the Office of the Information Privacy Commissioner.

For more information, guidance, or support contact:

Doctors Technology Office
604 638-5841
DTOinfo@doctorsofbc.ca
www.doctorsofbc.ca/doctors-technology-office

Checklist – Responsibilities of the Privacy Officer

COMPLIANCE

- ☐ Monitor privacy legislation, industry standards, and professional guidelines. Provide updates to clinic management and staff when significant changes occur.
- ☐ Collaborate with legal counsel to ensure terms and conditions meet privacy requirements.
- ☐ Evaluate staff compliance.

PRIVACY AND SECURITY PROGRAM FOUNDATION

- ☐ Oversee the development of privacy and security policies and procedures. Ensure staff can easily access both digital and printed documents.
- ☐ Review clinic procedures regularly and ensure staff is informed about any changes.
- ☐ Ensure that list of resources and emergency contacts are available to all staff in print and electronic formats.
- ☐ Ensure proper level of documentation supporting clinic in privacy and security protection. See the Recommended Documentation for Clinic Privacy & Security for more details.
- ☐ Ensure regular evaluations of the clinic safeguards. Utilize Clinic Self-Assessment Checklist.
- ☐ Be the first point of contact for external and internal privacy related questions, inquiries, or complaints.

STAFF TRAINING

- ☐ Ensure privacy and security training is included in the new staff orientation.
- ☐ Ensure regular refreshers are scheduled.
- ☐ Discuss incidents, threats, and problems with all staff to ensure full transparency and continuous improvement.

INCIDENT AND BREACH RESPONSE

- ☐ Oversee the investigation, documentation, and resolution of privacy and security breaches and incidents. Ensure the Privacy Breach Checklist published by OIPC is available in both digital and print format.
- ☐ Cooperate with the Office of the Information and Privacy Commissioner on investigations, complaints, or formal inquiries.

Responsibilities of the Security Lead

HARDWARE/SOFTWARE MAINTENANCE

- ☐ Develop, document, and maintain hardware and software standards and procedures accordingly to the industry best practices.
- ☐ Ensure clinic computer and information systems important for private information are up to date and monitored. Refer to the Guide for Asset Management for directions and tools.
- ☐ Ensure that technology acquired or developed meets the clinic security requirements.

INFORMATION ACCESS AND ACCOUNT MAINTENANCE

- ☐ Ensure appropriate security requirements for user access to clinic computer and information systems are defined. Refer to the Guide for Role-Based Access for directions and tools.
- ☐ Ensure individual access to clinic computer and information systems is properly monitored. Review the Guide for Role-Based Access and Guide for Password Management.
- ☐ Provide frequent updates to staff about the implemented safeguards.

INCIDENT AND BREACH MANAGEMENT

- ☐ Maintain necessary documentation to support problem resolution and incident investigation.
- ☐ Review and monitor information security incidents and ensure corrective actions and additional safeguards are implemented to mitigate risk.
- ☐ Act as a lead for investigation into security incidents and breaches and collaborate with Privacy Officer.

BUSINESS CONTINUITY AND DISASTER RECOVERY

- ☐ Document Business Continuity and Disaster Recover Plans to minimize impact on the clinic and patient care.
- ☐ Ensure that proper backup procedures are maintained, tested, and stored off-site if applicable.