COLLEGE OF PHYSICIANS
& SURGEONS OF ALBERTA

Privacy Directive
Protecting confidential information

1. PURPOSE

This Privacy Directive outlines the requirements and expectations of CPSA team members when managing confidential information, whether working at the office or through remote access. It details the administrative, physical and technical safeguards necessary to protect all confidential information.

2. DEFINITIONS

Definitions of terms used in this directive are in section 2 of the *Privacy and Confidential Information Policy*.

3. ADMINISTRATIVE SAFEGUARDS

a. CPSA has developed information privacy and security policies and procedures and will update them as necessary, at least every three years.

b. CPSA provides you (and vendors) with these policies and affirms that you have read, understood and will abide by them.

c. Collect, use and disclose the least amount of information necessary for the intended purpose and based on a valid need-to-know.

d. Where possible, ensure you make information anonymous before using or disclosing it.

e. CPSA restricts access to confidential information. You will only have access to the information if it's necessary to perform your job duties.

f. CPSA addresses confidentiality and security of information as part of the conditions of contracts.

g. CPSA provides all new team members with privacy and policy orientation on CPSA policies such as the *Privacy and Confidential Information Policy,* this directive, and other obligations.

h. CPSA trains all team members on their obligations when accessing and/or handling confidential information at the time of their policy orientation and then at least once every year.

i. You (and third-party vendors) must sign a Confidentiality Agreement identifying information protection standards and the requirement for policy compliance, as well as preventing the disclosure of confidential information during and after your employment.

j. You (and vendors) must handle the least amount of information necessary to accomplish assigned tasks. Take great care to prevent those without authorization from accessing information, even accidentally (e.g., position screens to prevent others from viewing, lock your devices when unattended, ensure printed material is properly stored and protected).

k. Leadership Team members are responsible for monitoring staff for compliance with the CPSA's policies and procedures.

l. IM and Corporate Services team members are responsible for identifying and maintaining an inventory of all CPSA assets.

m. You must not transmit confidential information verbally if a third party can overhear or intercept that conversation.

n. Ensure you (or another team member) accompanies any visitor to the appropriate meeting room or office.

o. A CPSA team member must monitor (i.e., security camera, visitor management system) or be present in the reception area during business hours when CPSA office is open to the public. No one is permitted behind the reception desk without permission.

p. Where practical, use pre-programmed numbers to send fax transmissions. Use addresses saved to an electronic address book or from a verified source to send emails.

q. Review pre-programmed numbers and saved email addresses every six months to ensure they are still accurate.

r. Send all fax transmissions with a cover sheet that indicates the information being sent is confidential.

s. Ensure all emails you send from a CPSA account include the following standard disclaimer:

> *This email may contain confidential and/or private information. Any unauthorized disclosure, copying or acting on the contents is strictly prohibited. If you received this email in error, please notify the sender and delete it.*

t. Take reasonable steps to confirm you send confidential information via fax and/or email to the intended recipient. Also confirm that the intended recipient received the information.

u. Document all privacy compliance issues, security breaches and/or loss of information/equipment assets (including access control items such as keys or fobs) in an incident report. Report these to CPSA's IM Team.

v. Retain confidential information in accordance with section 13 of the *Privacy and Confidential Information Policy* and in accordance with established Records Management standards.

w. Prior to disposal, CPSA documents confidential information by listing the records/files to be disposed of, the identity of the subject individual, the nature of the information and recording the date. A team member signs off that disposal has occurred.

x. CPSA enforces privacy obligations via contracts or other agreements with vendors and/or any recipients outside Alberta.

y. Leadership Team uses an arrival/departure/change process to manage and document access to information and/or information systems when team members are hired, their role changes and/or upon termination.

4. PHYSICAL SAFEGUARDS

a. Hold and store all confidential information in an organized, safe and secure manner.

b. When not in use, lock the cabinets used to store confidential information.

c. CPSA ensures our records storage areas are equipped with smoke detectors and fire extinguishers.

d. CPSA strictly controls the distribution of access control items. Upon employment termination, team members must return access cards.

e. Do not leave confidential information unattended in publicly accessed areas.

f. Position computer monitors so passers-by cannot view on-screen information.

g. CPSA ensures all network servers and critical electronic infrastructures are in locked cabinets in a secured area, and that the room is locked when not in use.

h. Where necessary, use privacy screens to prevent others from viewing confidential information unless looking directly at the screen.

i. Mail/courier personal, health and/or confidential information to another location by placing it in a sealed envelope, marked as confidential with 'attention to' the authorized recipient and transport/store it in a locked case or secured location.

j. Verify the identity and credentials of courier services used for the transportation of personal, health and/or confidential information.

k. Ensure fax machines are in a secure area.

l. Dispose of personal, health and/or confidential information in paper format in CPSA's secured shredding bins.

m. Clear all information on electronic data storage devices (e.g., surplus computers, internal and external hard drives, diskettes, tapes, CD-ROMS, etc.) prior to disposal or destruction.

5. TECHNICAL SAFEGUARDS

a. CPSA assigns you with a unique identifier (User ID) that restricts your access to confidential information and systems. You only have access to information required to perform your job duties.

b. Protect access to electronic information systems with passwords. Your passwords must be unique, self-selected and meet minimum complexity requirements.

c. Always keep passwords confidential. Don't write them down, post them publicly or share them with others.

d. Change passwords for electronic information systems every three months.

e. Set up your computer so it locks with a screen saver to protect against unauthorized access if you leave your computer unattended.

f. Encrypt documents with a password to protect confidential information sent by email.

g. CPSA audits information systems to detect unauthorized access and to prevent modification or misuse of information.

h. CPSA reviews audit trails every month and on an incident basis.

i. CPSA protects confidential information from unauthorized external access by a firewall.

j. CPSA has client-side protection software to protect information from unauthorized modification, loss, access or disclosure.

k. CPSA backs up all information systems nightly.

l. CPSA stores back-up information in a secure, locked environment. Responsible IM team members review information intended for long-term storage on electronic media on an annual basis to ensure the data is retrievable and to migrate the data to another storage medium if necessary.

6. COMPLIANCE

Team member (except for council/committee members) or vendor failure to comply with this policy is cause for disciplinary action up to and including termination of employment or business relationship and, where applicable, legal or other action. Council/Committee members' failure to comply with this policy is addressed by the council president.

If you have any questions or concerns about CPSA's handling of confidential information, please contact CPSA's Privacy Team.

7. REFERENCES

This directive falls under the *Privacy and Confidential Information Policy*.

Related Policies

- *Artificial Intelligence*
- *File Retention*
- *Internet Access & Use*
- *Prevention and Detection of Theft and Fraud*
- *Records and Information Management*
- *Software Standards*
- *Team Member Code of Ethics*

Privacy Directives

- *Acceptable Uses of Networks and Electronic Devices*
- *Access to Personal Information*
- *Privacy and Information Management Training*
- *Protecting Information when Contracting for Services*
- *Team Member Arrival/Departure*

Privacy How-to Sheets

- *Auto-Complete Settings in Outlook*
- *Locking & Securing Computers*
- *Privacy Breach Response*
- *Recording Audio or Videoconferences*
- *Redacting Information from Documents*
- *Secure Printing*
- *Sharing Confidential Information Electronically*

IT How-to sheets

- *Set-up Remote Access*

Corporate Services How-to sheets

- *Processes for Contract Management*