COLLEGE OF PHYSICIANS
& SURGEONS OF ALBERTA

Privacy Directive
Protecting information when contracting for services

1. PURPOSE

CPSA may contract third party vendors whom may access or otherwise handle confidential information or information-related assets. This Privacy Directive outlines mechanisms to ensure we share and pass along our responsibilities and obligations with respect to protecting confidential information to those third party vendors as necessary.

2. DEFINITIONS

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

3. AGREEMENTS AND CONTRACTS

a. CPSA and all vendors who require access to confidential information, information systems, and/or CPSA assets **must** sign an agreement. This agreement clearly outlines information security provisions and/or binds the vendor to CPSA policies and procedures. This agreement survives employment and vendor termination.

   i. CPSA's Privacy Team will maintain template agreements. Leadership Team members will use this template when contracting for services as described in 3a. With input from the Privacy Team, Leadership Team members may customize the template to fit the situation as long as the intent of the agreement is not altered.

   ii. In addition to a confidentiality agreement between a vendor and CPSA, all individuals (employees, sub-contractors of the vendor) who may access, receive, or be exposed to the confidential information or information systems must also sign a confidentiality agreement. Individuals must sign this agreement before the contracted work commences. It remains in effect after termination/work is completed.

b. Following the implementation of this directive, all contracts are to include clauses addressing privacy and the protection of confidential information.

c. Where the contract with the vendor includes clauses addressing privacy and the protection of confidential information, a subsequent confidentiality agreement may not be required.

   - If confidential information or critical information systems are not accessed or otherwise handled by the vendor, a more detailed confidentiality agreement, described here, is likely unnecessary.

- CPSA's Privacy Team will work with the contracting Leadership Team member to determine the necessity to complete such an agreement.

d. Should a contract pre-dating the implementation of this directive not include sufficient reference to the vendor's responsibility to safeguard confidential information, a confidentiality agreement, described above, is required to bridge the gap until the contract is renegotiated.

e. A confidentiality agreement may also be required when the terms of the contract are preset by the vendor.

f. Agreements and/or contracts will include provisions for the return or destruction of information assets (including hardware, system documentation, and data) upon termination of the agreement, and in accordance with contract provisions reflecting records retention and data management policy.

4. CONTRACT CLAUSES

The following generic clause serves as an example that you may customize to fit the contract situation as long as the intent of the clause is not altered. For assistance with customization, consult CPSA's Privacy Team.

> *The College of Physicians & Surgeons of Alberta (CPSA) confirms that it will only disclose confidential information when lawfully authorized or required to do so, or when the disclosure falls within approved policy guidelines and only for approved purposes that have the express written consent of the individual.*
>
> *{Vendor} agrees to keep confidential information secure and confidential at all times, use it only for the task(s) stated in this contract and will not disclose, share, or sell this information to any other individual, organization, or business without the express written consent of the CPSA.*
>
> *{Vendor} further agrees upon completion of this contract, to not retain in any form, any confidential information disclosed by the CPSA, and agrees to permanently and conscientiously destroy or return the information to the CPSA.*

5. POLICIES

a. CPSA will provide vendors with a copy of all relevant CPSA policies and procedures and will ensure vendors sign to acknowledge receipt and declare their compliance.

b. CPSA's Privacy Team should receive all relevant third party information security and privacy policies before the contract work commences, and receive any revisions occurring after execution of the contract.

6. COMPLIANCE

Team member, with the exception of 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 a questions or concerns about the CPSA's handling of confidential information, please contact the CPSA's Privacy Team.

7. REFERENCES

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

Related Policies

- *Internet Access & Use*
- *Software Standards*
- *Records and Information Management*
- *File Retention*

Privacy Directives

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

Privacy How-to Sheets

- *Locking & Securing Computers*
- *Printing Private & Confidential Documents*
- *Privacy Breach Response*
- *Recording Audio or Videoconferences*
- *Redacting Information from Documents*
- *Responding to Access Requests-HPA*
- *Responding to Access Requests-PIPA*
- *Sharing Confidential Information Electronically*

Operations How-to sheet

- *Processes for Contract Management*