

# Core Competency Standards

Information Access and Protection of Privacy Professionals

knowledge access to information consentement policy  
personal information skill PIPA accès à l'information AIPRP  
certification training gouvernance experience principles  
protection PHIA sécurité PHIPA transparence vie privée  
accréditation renseignements personnels ATIP health  
records data impact assessment dataflow géolocalisation  
MFIPPA **Connecting People** professional  
due diligence **With Possibilities** awareness  
éthique expertise safeguards openness accountability  
santé standards risk législation biométrie FOIPOP  
framework CONSENT protection consultation HIA privacy  
integrity investigation breaches liberté technologie  
électroniques disclosure confidentiality LRPDE  
procedures documents éducation compliance droit à  
l'information PIPEDA



Canadian Association of Professional  
Access and Privacy Administrators



## About CAPAPA

The Canadian Association of Professional Access and Privacy Administrators (CAPAPA) is a non-profit association dedicated to the on-going professional development, education and expanded expertise of individuals who work in the access to information and protection of privacy field.

CAPAPA was incorporated under the Alberta Societies Act in June 2002 as a national association dedicated to Access and Privacy Professionals. CAPAPA was created in response to the growing demand for access to information and protection of privacy professionals in the private and public sectors. CAPAPA was also created to respond to the desire of access and privacy practitioners for meaningful professional certification. It is also a goal to respond to the need for professional standards and training for practitioners in terms that are consistent across the country.

CAPAPA's founders and volunteers have been working to create the structure and processes to distinguish those who perform access and privacy tasks as part of a profession, one that involves complex, outcome-based tasks that underpin democratic processes and commercial activities, tasks that should only be performed by trained, competent individuals possessing the necessary skills and experience.

CAPAPA's certification process and credentials provide recognition of these specialized skills and experience for the benefit of access and privacy professionals. CAPAPA has set high standards. Its credentials should serve as a signal to employers and the public that CAPAPA certified professionals have the ability to competently perform a variety of access and privacy tasks that organizations are legally obligated to provide.

CAPAPA has members from all levels of government, private sector organizations, academia, hospitals, school boards, law enforcement agencies, and many other sectors. Membership is open to those who are engaged or interested in the field of information access and protection of privacy.

CAPAPA's mandate is:

To advocate the ongoing professional development, education, and expertise of persons engaged or interested in the field of information access and privacy protection in Canada.

## CAPAPA Objectives

- To support the development of standards and best practices to establish benchmarks of excellence in the field of information access and protection of privacy.
- To communicate educational material and awareness initiatives to assist individuals improve their knowledge of the field of information access and protection of privacy.
- To provide a forum for discussion and debate of past and cutting-edge issues in the field of information access and protection of privacy.
- To offer members the opportunity to enhance career opportunities by networking with other colleagues and professionals in the field.

Copyright © 2009-2011. The Canadian Association of Professional Access and Privacy Administrators.

This copyrighted document may be copied and distributed for non-profit educational purposes only. The text of this document may not be altered without express authorization of the Canadian Association of Professional Access and Privacy Administrators — CAPAPA. This publication should be used as information only and not relied upon or construed as legal advice.



## About this Publication

CAPAPA has developed, on its own or jointly with other individuals and organizations, various publications for its certification program:

- Discussion Paper on Professional Certification, CAPAPA (June 2004) <http://www.capapa.org/certification.html>

The following papers were prepared by the Professional Standards and Certification Working Group, sponsored jointly by CAPAPA and the Canadian Access and Privacy Association (CAPA) and underwritten by a grant from the Privacy Commissioner of Canada.

- Professional Standards/Competencies (Phase 1 – March 27, 2007), <http://www.capapa.org/certification.html>
- Principles of Certification and Governance (Phase 1 – unpublished)
- Categories of Certificants (Phase 2 – unpublished)
- Continuing Competency Program (Phase 2 – unpublished)
- Complaints, ACR, Investigation and Discipline (Phase 2 – unpublished)
- Grandparenting (Phase 2 – unpublished)
- Registration and Entry to Practice Standards (Phase 2 – unpublished)
- Value Proposition (Phase 2 – unpublished)
- Phase 2 Certification Final Document (Phase 2 – December 10, 2007 – unpublished)
- Proposed Scope for Phase 3 Governance Final Document (Phase 3 – December 10, 2007 – unpublished)

## Acknowledgements

CAPAPA wishes to acknowledge the members of the CAPA-CAPAPA Professional Standards and Certification Working Group who generously contributed their time and effort from 2006 to 2007 to further the development of professional standards and certification:

Frank Work, Alberta Information and Privacy Commissioner (Working Group Chairman), Linda Girard, Association sur l'accès et la protection de l'information (AAPI), Alan Leadbeater, (formerly) Deputy Information Commissioner for Canada, Raymond D'Aoust, Assistant Privacy Commissioner for Canada, Stephen Johnston, Office of the Privacy Commissioner of Canada, Dr. Douglas Knight, University of Alberta, Pierre Beaudry, l'École Nationale d'Administration publique (ENAP)-University of Quebec, Drew McArthur, (formerly) TELUS Communications, Wayne MacDonald, University of Alberta, Larry Kearley, Canadian Access and Privacy Association (CAPA), and Carla Heggie (formerly CAPAPA).

The CAPA-CAPAPA Professional Standards and Certification Project was supported by the Office of the Privacy Commissioner of Canada, through a grant under the OPC Contributions Program and contribution of staff time; and the Offices of the Information Commissioner of Canada and the Alberta Information and Privacy Commissioner also made important contributions of in-kind resources.

I would like to acknowledge the CAPAPA directors and members in their commitment to building the association and increasing professional standards by supporting the development of professional certification processes.

Eric Lawton  
Director of Professional Certification  
April 22, 2009

These Core Competency Standards are based on the work noted above, and serve as the foundation for the following publications:

### **CAPAPA Professional Standards and Certification Project – Phase 2**

- CAPAPA Accreditation (April 2009)
- Certification – Frequently Asked Questions (April 2009)
- CAPAPA Common Body of Knowledge (CBK) (June 2009)
- CAPAPA Certification Handbook – Associate Access and Privacy Professional (AAPP) (June 2009)
- CAPAPA Certification Handbook – Certified Information Access and Privacy Professional (CIAPP) (August 2009)
- CAPAPA Training and Continuing Education (September 2009)
- CAPAPA Certification Governing Body (December 2009)
- CAPAPA National Certification Examination Process (2012)

### **CAPAPA Professional Standards and Certification Project – Phase 3**

- CAPAPA Certification Handbook – Chartered Access and Privacy Professional (CAPP) (2011)
- CAPAPA Certification Handbook – Master Access and Privacy Professional (MAPP) (2012)



## Table of Contents

1.	About CAPAPA Credentials.....	1
2.	CAPAPA Family of Credentials.....	2
	CAPAPA Qualification Levels .....	2
	Associate Access and Privacy Professional (AAPP) .....	3
	Certified Information Access and Privacy Professional (CIAPP).....	4
	Chartered Access and Privacy Professional (CAPP).....	6
	Master Access and Privacy Professional (MAPP).....	9
3.	Development of the Core Competencies.....	11
	How to Use Core Competency Standards .....	12
4.	Core Competencies.....	13
5.	Domains of Competency.....	14
	Access to Information.....	14
	Privacy .....	17
	Access and Privacy Management.....	19
	Access and Privacy Law — Future Domain .....	21
6.	Mapping Core Competencies to Professional Credentials.....	22



## 1. About CAPAPA Credentials

The Canadian Association of Professional Access and Privacy Administrators (CAPAPA) is a non-profit association dedicated to the ongoing professional development, education and expanded expertise of individuals who work in the access to information and protection of privacy field. CAPAPA's meaningful certification process and credentials recognize the specialized skills, knowledge, education and experience of access and privacy professionals across Canada.

CAPAPA has set high standards so that its credentials can serve as a signal to employers and the public that CAPAPA certified professionals have the ability to competently perform a variety of access and privacy tasks that organizations (in both the public and private sector) are legally obligated to provide.

In March 2009, the CAPAPA Executive Board of Directors approved plans to issue the first two CAPAPA credentials starting in 2009. They are:

Associate Access and Privacy Professional (AAPP) ©  
Certified Information Access and Privacy Professional (CIAPP) ©

The CAPAPA Board of Directors also approved plans to issue two higher-level designations in subsequent years:

Chartered Access and Privacy Professional (CAPP) ©  
Master Access and Privacy Professional (MAPP) ©

**Note about terminology:** CAPAPA's use of the term "access and privacy" should be broadly interpreted to include "Freedom of Information and Privacy" (FOIP), "Freedom of Information and Protection of Privacy (FOIPOP), "Access to Information and Privacy" (ATIP), "Information Access and Protection of Privacy" (IAPP), "Release of Information", "Data Protection", "Privacy Compliance" and all other terms for those who practice "access to information" or "privacy" tasks in the public or private sectors across Canada. Job titles are not reliable indicators of whether or not a position is an access or privacy position.



## 2. CAPAPA Family of Credentials

The following descriptions of the CAPAPA credentials are provided as background to enable the reader to understand how the credentials map to different job levels in the access and privacy field in the public and private sectors. Sample job descriptions are provided to illustrate how the CAPAPA designations are targeted to individuals at a certain level in the access and privacy field in terms of their experience, knowledge and skills.

### CAPAPA Qualification Levels

Experience Level	Academic Qualifications	Occupational Qualifications	CAPAPA Professional Designation	Educational* Level*
<b>Level 1</b> (Foundation)	Credits for 30 Education Points	1+ Years work experience	<b>AAPP•</b> (Associate)	Certificate or Diploma
<b>Level 2</b>	Credits for 100 Education Points	2-3 Years work experience	<b>CIAPP•</b> (Certified)	Under Graduate
<b>Level 3</b>	Credits for 150 Education Points	4-5 Years work experience	<b>CAPP•</b> (Chartered)	Post Graduate
<b>Level 4</b>	Credits for 150 Education Points	6+ Years work experience	<b>MAPP•</b> (Master)	Masters Doctorate



## Associate Access and Privacy Professional (AAPP)

The AAPP credential recognizes individuals with a demonstrated understanding of the fundamental knowledge of processes and terminology as defined in CAPAPA's Common Body of Knowledge (CBK). The AAPP credential designation is the foundation level for Access and Privacy Professionals. The AAPP credential is appropriate for Access and Privacy Professionals who provide support to a team and are capable of assuming full or partial responsibility for completing access and privacy tasks under the supervision of a more experienced Access and Privacy Professional. The AAPP credential recognizes an individual's competence in at least one (1) CAPAPA domain (access or privacy).

Eligibility requirement is no less than **1 year of directly-related experience in the last 3 years** and 30 points in

related access and privacy education and training. In the event that applicants do not entirely meet the education requirement, they may substitute up to 15 points (half) of the education requirement with evidence of substantial involvement in one of the access and privacy domains. Applicants must submit 2 references for individuals who have direct knowledge of the applicant's work in the access and privacy field in the 1 year of the applicant's recent experience and can attest to the applicant's competent performance of the tasks outlined in the CAPAPA Core Competencies. Candidates must also pass a multiple-choice exam or submit their application for the credential during the grandfathering period. Certification is valid for 3 years from the date the credential is awarded. Re-exam is required to renew the credential.

### Example #1 – Public Sector — Sample job description at AAPP level:

#### DUTIES

The Freedom of Information (FOI) Assistant coordinates Freedom of Information Act requests and provides guidance and advice to management, staff and the public regarding disclosure of agency records under FOIA. Duties include reviewing incoming information requests for clarity and reasonableness; researching problems and reviewing issues related to requests; providing guidance and technical assistance in light of current statutes and policies; assisting program offices in preparing appropriate and timely responses; ensuring proper tracking of requests and coordination among programs and with EPA Headquarters; and assisting in preparation of FOIA reports and other information materials.

#### QUALIFICATIONS

No education required. Minimum qualifying experience is one full-time year of experience performing administrative assistant assignments equivalent to the GS-09 level in the federal government. Such assignments must demonstrate responsibility for carrying out a variety of administrative support duties and assisting regional staff in responding to Freedom of Information Act requests. Applicant must demonstrate potential for learning and dealing with higher-level, more complex information requests and other aspects of the FOIA program.

The assessment questionnaire is designed to assess your ability to demonstrate the following knowledge, skills, abilities, and/or competencies:

Basic knowledge of FOIA policies and procedures

Ability to coordinate requests, maintain records, and provide guidance on the FOIA program

Skill in communication and customer service.

(U.S. Environmental Protection Agency – Freedom of Information Assistant; Office of Public Affairs, Environmental Information and Education Office, Competition #Reg 9-MP-2009-006; Dec. 12, 2008)



## Certified Information Access and Privacy Professional (CIAPP)

The Certified Information Access and Privacy Professional (CIAPP) designation is the second level in the CAPAPA certification model for Access and Privacy Professionals.

The CIAPP credential recognizes individuals with an intermediate level knowledge of privacy and access to information legislation and regulations; intermediate level knowledge of the jurisprudence, case law, precedents, and best practices relevant to access to information and privacy; knowledge of the principles, techniques and practices of compliance with access and privacy requirements in public or private sector organizations; knowledge of how to evaluate and analyze information, data, business and information technology systems; intermediate-level knowledge of archival, records management, risk management and information management principles and practices. The CIAPP credential also recognizes individuals' skills and experience in the application of that knowledge.

The CIAPP credential is appropriate for Access and Privacy Professionals who plan and carry out increasingly complex tasks to support an organization's compliance with access and/or privacy legislation, working under the direction of a more senior advisor or decision-maker. The Certified Information Access and Privacy Professional is capable of performing some or all of the following tasks:

- processing large, complex access to information requests,
- undertaking investigations into alleged privacy breaches,
- responding to privacy complaints,

- writing reports and recommendations for senior management,
- developing policies,
- conducting privacy impact assessments,
- handling complex access and privacy compliance issues.

The CIAPP credential recognizes an individual's competence, at an intermediate level, in the domains of access to information or privacy and access and privacy management.

To apply, candidates must have no less than **2 years directly-related work experience in the last 4 years** and 100 points of access and privacy-related education and training. In the event that applicants do not entirely meet the education requirement, they may substitute up to 50 points (half) of the education requirement with evidence of substantial involvement in one of the access and privacy domains. Applicants must submit 3 references for individuals who have direct experience of the applicant's work in the access and privacy field in the 2 years of the applicant's recent experience and can attest to the applicant's competent performance of the tasks outlined in the CAPAPA Core Competencies. Candidates must also pass a multiple-choice exam or apply during the grandfathering period. Experience can be in a relatively narrow area of specialization within one of the CAPAPA domains, however the CIAPP candidate must be knowledgeable in at least two (2) domains outlined in the Core Competencies. Certification is valid for 3 years from the date the credential is awarded. Re-exam is required to renew the credential.

### Example #3 – Public Sector — Sample job description at CIAPP level:

#### DUTIES

The Investigator conducts independent reviews and investigations of all complaints (related mostly to exemptions) made by the public against government institutions and agencies to ensure the government's compliance with the Access to Information Act and that the public's rights are upheld under the act; Provides advice to management of the Office of the Information Commissioner; Provides information/advice/education to federal officials, third parties, complainants and the general public on the application of the Access to Information Act; Mentors new investigators or employees.

#### QUALIFICATIONS

Education - University certificate in access to information and privacy.

Experience in providing advice to senior management regarding the resolution and disposition of complaints; Analyzing information and facts in preparing and presenting reports and evidence; Handling requests for records information and/or complaints; Writing letters and memos and responding to enquiries.

(Public Service Commission of Canada – Investigator; Offices of the Information and Privacy Commissioner Competition #IPC04778sFNF90; January 6, 2006)



**Example #2 – Public Sector — Sample job description at CIAPP level:**

**DUTIES**

The Case Review Analyst must be able to identify key issues and facts relevant to requests for review and have the discretion to maintain the confidentiality of documents provided to the Review Officer. The Case Review Analyst assists in the education of public body officials about the law and processes relating to access to information or protection of privacy through direct contact and delivery of portions of educational sessions. This key individual provides specialized research and support related to privacy and access to information; also analyses legislation and precedents to advise and assist members of the public seeking information about access to records and appeal processes under the Freedom of Information and Protection of Privacy Act as well as privacy issues.

**QUALIFICATIONS**

University degree and several years experience in a legal or research environment, or an acceptable equivalent.

Must possess a thorough knowledge of legislation and regulations (Federal, Provincial and Municipal) related to privacy and access and be able to use that knowledge to make competent decisions and plans.

The successful candidate will be an individual who is current on issues affecting public access and privacy protection with average communication skills, both verbal and written. A cover letter is required with your resume, outlining experience and related education and skills and indicating your knowledge of Freedom of Information and Protection of Privacy Matters. In this letter describe what you feel transparency means. Computer expertise at the working level is required.

(Nova Scotia Department of Justice – Case Review Analyst; FOIPOP Review Office Competition #004013; May 20, 2003)

**Example #4 – Private Sector — Sample job description at CIAPP level:**

The Privacy Officer (PO) will serve as the focal point for privacy compliance-related activities and responsibilities, as listed below. In general, the PO is charged with implementing company policies and procedures, conducting educational programs, and administering reviews relating to the company's privacy program.

The PO must demonstrate familiarity with the legal requirements relating to privacy and health care operations, as well as the ability to communicate effectively with and coordinate the efforts of technology and non-technology personnel.

**RESPONSIBILITIES**

(1) Provides leadership to the company's committees, work groups, and task forces charged with creating and implementing an enterprise-wide privacy program.

- Develops company privacy policies and procedures consistent with applicable laws, rules, and regulations.
- Ensures that processes are implemented to maintain compliance with federal and state laws related to privacy, security, confidentiality, and protection of information resources and health care information. This includes coordination with the Security Officer (SO) in evaluating and monitoring operations and systems development for security and privacy requirements.
- Develops, implements, and administers company-wide authorization procedures for access to, use, and disclosure of PHI.
- Develops, implements, and administers a company-wide procedure to allow individuals to exercise their rights to PHI under applicable state and federal laws.
- Develops and implements company-wide privacy training programs and, in conjunction with the SO, a security awareness and training program.
- Coordinates with the Corporate Compliance Officer (CCO) and HR to develop appropriate sanctions for employees or business partners that fail to comply with the company's privacy policies and procedures.
- Coordinates with the Quality Improvement Program to measure effectiveness, performance and quality of the company's privacy program.

(2) Coordinates with the CCO regarding corporate complaints and information relating to the company's privacy program and regarding investigation of all allegations of noncompliance with the company's privacy policies.

(3) Coordinates with the CCO, SO, and other applicable departments regarding the mitigation of the effects of any unauthorized or otherwise inappropriate release of health information.

(4) On a periodic basis, reports the status of the privacy program to the Executive Compliance Committee.

(5) Serves as a resource to the company's designated liaisons to regulatory and accrediting bodies for matters relating to privacy and security.

(Source: AIS's new HIPAA Security Compliance Guide on "The Interaction Between Privacy and Security," written by Kristy Kuhn and Nisha Shajahan of Strategic Management Systems, Inc.)



## Chartered Access and Privacy Professional (CAPP)

The CAPP is an advanced/senior level credential which will be available in 2010.

CAPP credential holders are capable of managing access and privacy staff, establishing a group or office, conducting training, or leading a project team.

The CAPP credential targets those who possess expert-level knowledge of access to information and privacy legislation and regulations, jurisprudence, case law and precedents, as well as expert knowledge of case management techniques and the principles and techniques of effective organization and time management.

CAPP credential holders interpret and apply, at the expert level, increasingly complex provisions of Access to Information and Privacy legislation, including exemptions and regulations, and plan and carry out increasingly complex investigations, including the most sensitive and complex cases.

CAPP credential holders may serve as the focal point for compliance-related activities and responsibilities. They can implement access and privacy policies and procedures, conduct educational programs, and administer reviews relating to the organizations privacy and access program.

The CAPP holder must demonstrate familiarity with the legal requirements relating to privacy and the business operations,

as well as the ability to communicate effectively with and coordinate the efforts of technology and non-technology personnel.

To apply for the CAPP designation, candidates must demonstrate no less than **4 years directly-related work experience in the last 6 years** and 150 points of access and privacy-related education and training. In the event that applicants do not entirely meet the education requirement, they may substitute up to 75 points (half) of the education requirement with evidence of substantial involvement in three of the access and privacy domains.

Applicants are required to demonstrate that they have attained broad and varied experience and mastery of substantive access and privacy principles and procedures. Applicants must submit 3 references for individuals who have direct experience of the applicant's work in the access and privacy field in the 4 years of the applicant's recent experience and can attest to the applicant's competent performance of the tasks outlined in the Core Competencies. Experience must cover three access and privacy domains.

Candidates must pass a multiple-choice exam or apply during the grandfathering period. Certification is valid for 3 years from the date the credential was awarded. Re-exam is required to renew the credential.



**Example #5 – Private Sector — Sample job description at CAPP level:**

POSITION TITLE: Privacy Manager

IMMEDIATE SUPERVISOR: Chief Privacy Officer

**DUTIES**

The Privacy Manager assists with activities related to the development, implementation, maintenance of and adherence to the corporation's privacy and access principles, policies and procedures in compliance with provincial and federal laws.

**Responsibilities:**

1. Assists with the identification, development, implementation, and maintenance of corporate information privacy and access policies and procedures in accordance with jurisdictional changes, legislated changes, and commissioner's recommendations; and in co-ordination with the corporation's management, the Privacy Working Committee, and CPO.
2. In the absence of, serves as Acting-CPO.
3. Assists the CPO with the project research, development and implementation of the corporation's Privacy Management Program; and policy, processes and education of the corporation's ethics and whistleblower program.
4. Hire, manage and lead department staff.
5. Establish and monitor department budget requirements.
6. Serves as privacy consultant to the corporation for all departments and provides interpretation and insight to business areas concerning corporate policy and procedures.
7. Assists CPO with ensuring compliance with privacy practices and consistent application of sanctions for failure to comply, for all individuals in the corporation's workforce, extended workforce, and all business associates; in collaboration with management, Human Resources, and legal counsel when necessary.
8. Works collaboratively with all corporate personnel involved with the release of personal information to ensure full coordination and cooperation under the organization's policies and procedures, and in compliance with applicable federal and provincial privacy and access laws.
9. Works collaboratively with applicable departments in overseeing stakeholders' rights to inspect, amend, and restrict access to personal information when appropriate.
10. Maintains and monitors a process for receiving, documenting, tracking, investigating, and taking action on complaints concerning the corporation's privacy and access policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
11. Cooperates with the Saskatchewan Information and Privacy Commissioner, Executive Government, other legal entities, and corporate officers in any compliance reviews or investigations.
12. Performs initial and periodic information privacy risk assessments and related ongoing compliance monitoring activities in co-ordination with the corporations' other compliance and operational assessment functions.
13. Initiates, facilitates and promotes activities to foster information privacy awareness within the corporation and related subsidiaries.
14. Consults, identifies, designs and ensures delivery of a corporate training strategy and privacy training to all employees, subsidiaries, contractors, business partners and other appropriate third parties.
15. Leads the SGI Privacy Working Committee.
16. Works with CPO and management, key departments, and committees to ensure the corporation has and maintains appropriate privacy and confidentiality consent forms, authorization forms, and information notices and materials reflecting current organizational practices and requirements.
17. Maintains current knowledge of applicable federal and provincial privacy laws and "best practices" to recommend corporate adaptation and compliance.
18. Serves as a committee member or liaison to, the Crown Privacy Committee.

**Education:**

- Certification as an IAPP (Information Access and Protection of Privacy) or evidence of continuing education toward certification.
- Degree in Administration or more than 10 years experience in a management capacity of the organization.



Knowledge/Skills/Ability:

- Comprehensive understanding of the organization's core business functions and customer needs and expectations.
- Knowledge and proficiency at interpreting information privacy laws, access, release of information, and related issues.
- Knowledge and understanding of investigative techniques.
- Demonstrated organization, facilitation, communication, and presentation skills.
- Knowledge in and the ability to apply the principles of project management and change management.
- Knowledge and understanding of privacy-enhancing and privacy-invasive technologies.
- Ability to collaborate with internal and external customers.
- A high level of integrity and trust.

(Source: SGI Privacy Manager Job Description)

**Example #6 – Public Sector — Sample job description at CAPP level:**

POSITION TITLE: Senior Coordinator

REPORTS TO: Senior Manager

DUTIES

Under the direction of the Director, Information and Privacy Office (IPO), the Senior Coordinator provides strategic expertise related to the delivery of services under the Freedom of Information and Protection of Privacy Act (FOIP) to public bodies under the Ministry of Children's Services. The Senior Coordinator is also responsible as the lead for the coordination and delivery of training and orientation to staff across all public bodies supported by the IPO. In addition, the Senior Coordinator would generally assume responsibility for covering off the Director in his absence.

The Senior Coordinator will be responsible for ensuring that the Children's Services Ministry receives the necessary strategic input from a privacy perspective into the development of policies and processes. Working on a consultative basis with middle-management levels within the various divisions and regions of that ministry, the incumbent will be responsible to provide appropriate and expert advice on the implications of privacy and access as initiatives and projects are developed and implemented.

QUALIFICATIONS

Requires an extensive knowledge of FOIP/privacy legislation, and the interplay between it and other legislation. The ability to review and interpret any piece of legislation that may relate to the management of personal information, and an understanding of how the legislation interrelates with the FOIP Act. This ability is critical in the provision of advice on how the various public bodies develop their policies and practices.

Knowledge of FOIP resources: Information and Privacy Commissioner Orders, Investigations and Practice Notes, legal opinions on FOIP issues, FOIP bulletins, annotated FOIP Act, Office procedures and the FOIP Guidelines and Practices.

Knowledge of government organization and operations, security processes and practices, records management requirements and procedures. Knowledge in the development and delivery of successful training programs. Skills required for the position include those that will focus on being able to transfer knowledge and understanding of complex legislation in a manner that ensures compliance with that legislation by all staff across a number of public bodies. This therefore entails not only the ability to develop and deliver effective education sessions, but also the ability to influence policy and practice without the advantage of positional authority.

Experience in the area of privacy legislation will be an extremely important asset, along with several years experience in the public sector and general administration; several years of direct program experience; experience related to program delivery, compliance determination and interpretation of Acts, Regulations and Policies and Procedures.

Leadership and business know-how: The incumbent is expected to be a self-starter in many respects. He/she will need to establish a presence and some recognition within the Ministry in order to ensure that there exists an awareness as to whom to turn to, and when to do so, for advice regarding privacy. At the same time, direction will come forward from the Director and at times from senior officials within the Ministry as various issues emerge.

(Alberta Ministry of Human Resources and Employment – Senior Coordinator, Corporate Services Division, Information and Privacy Office; Position Description, September 27, 2006)



## Master Access and Privacy Professional (MAPP)

The MAPP is a Masters/doctorate level credential recognizing the industry-leading knowledge and skills of individuals that may occupy senior management positions such as Director of an access and privacy office, Chief Privacy Officer, Commissioner or equivalent.

To apply, candidates for the MAPP will require **no less than 6 years directly-related work experience in the last 10 years**, submit recent position description/job responsibilities and have and 150 points of access and privacy-related education and training. In the event that applicants do not entirely meet the education requirement, they may substitute up to 75 points (half) of the education requirement with evidence of substantial involvement in three of the access and privacy domains. Applicants are required to demonstrate they have attained broad and varied experience and mastery of substantive access and privacy principles and procedures, and have lead innovative initiatives to create new standards, policies, procedures or technologies that support compliance with access and privacy principles.

Applicants must submit 3 references for individuals who have direct experience of the applicant's work in the access and privacy field in the 6 years of the applicant's recent experience and can attest to the applicant's competent performance of the tasks outlined in the CAPAPA Core Competencies. Candidates must pass an exam or apply during a grandfathering period.

Certification is valid for 5 years from the date the credential is awarded. Re-exam is not required to renew the credential; and the MAPP credential holder must provide details about his/her professional accomplishments in the past 5 years.

### Example #7 – Private Sector — Sample job description at MAPP level:

POSITION TITLE: Chief Privacy Officer (CPO)

IMMEDIATE SUPERVISOR: Chief Executive Officer, Chief Information Officer or Senior Executive.

#### SPECIFIC RESPONSIBILITIES

The CPO oversees all activities related to the development, implementation, maintenance of, and adherence to the Organization's policies and procedures covering the privacy, confidentiality and security of personal information. This includes access to personal information by clients and their designates, as well as amendments to personal information in compliance with current and upcoming federal and provincial laws and the Organization's information privacy practices.

Develops and implements a corporate Privacy Program that includes a statement of ethical principles and policies for the protection of personal information. Ethical principles will be based on the CSA Model Code for the Protection of Personal Information, a set of internationally accepted fair information principles.

Works with senior management and legal counsel to establish a corporate Privacy Committee responsible for privacy oversight activities.

Serves in a leadership and advisory role to the corporate Privacy Committee, senior management and other internal and external stakeholders.

Performs initial and periodic information privacy and security reviews, and conducts related ongoing compliance monitoring activities in coordination with the Organization's other compliance and operational assessment functions.

Works with senior management, legal counsel, key departments and committees to ensure the Organization has and maintains appropriate privacy, security and confidentiality measures and processes (e.g. consent forms, audit programs).

Oversees, directs, or delivers a corporate privacy and security educational training program for all employees and volunteers.

Participates in the development, implementation, and ongoing compliance monitoring of all business partner and associate agreements to ensure that privacy and security concerns, requirements and responsibilities are addressed.

Establishes with management and operations a mechanism to track client and staff access to personal information, within the purview of the Organization and as required by law to allow qualified individuals to review or receive a report on such activity.

Works cooperatively with the Director of Records and other stakeholder units in overseeing client rights to inspect, amend, and restrict access to personal information where appropriate.



Establishes and administers a process for receiving, documenting, tracking, investigating and taking effective action on all client and staff complaints concerning the Organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.

Initiates, facilitates and promotes activities to foster information privacy and security awareness within the Organization and its business partners.

Serves as a member of, or liaison to, the Organization's Research Ethics Review Board.

Serves as an information privacy liaison for system owners and users of the Organization's major information systems.

Works with all personnel involved with any aspect of the release of personal information to ensure full coordination and cooperation under the Organization's information privacy and security policies and legal requirements.

Maintains current knowledge of relevant international, federal and provincial privacy laws and standards and monitors advancements in privacy enhancing technologies.

Cooperates with the Office of the Information and Privacy Commissioner, other legal entities and organization officers in any compliance reviews or investigations.

Represents the Organization's information privacy and security interests with external parties (government bodies, other organizations and industry association) who undertake to adopt or amend privacy legislation, or who have questions about the Organization's information privacy and security practices.

#### QUALIFICATIONS

Experience in information privacy and security policy development, education, complaints investigation, information privacy and security technology assessment, and the use of privacy and security assessment tools such as privacy impact assessments, threat and risk assessments and corporate information security reviews. Experience should be relative to the size and scope of the Organization.

Knowledge and experience in relevant information privacy laws (e.g. The Personal Information Protection and Electronic Documents Act, Ontario Freedom of Information and Protection of Privacy Act), draft provincial privacy legislation (e.g. Draft Ontario Privacy of Personal Health Information Act), release of information and access laws.

Demonstrated skills in change management and project management.

Demonstrated organization, facilitation, communication and public presentation skills.

(Source: Ontario Sample Chief Privacy Officer Position Description, 2007)



### 3. Development of the Core Competencies

CAPAPA recognizes that most access and privacy professionals tend to spend most of their time performing predominantly access or privacy related tasks. In some cases, employers blend other corporate roles with access and privacy responsibilities, sometimes placing the access and privacy professional into dual reporting structures. CAPAPA also recognizes that, over the course of a career, however, most access and privacy professionals will develop a balanced understanding of the dual nature of the profession. This is reflected in the higher level CAPAPA credentials.

CAPAPA examined professional credentials of other associations and the details of their certification processes<sup>1</sup> and determined that a family of credentials would allow for career progression and recognition for increasing levels of experience similar to the Project Management Institute's credentials, which have been successful and are well-received by professionals and employers.<sup>2 3</sup>

With this goal in mind, CAPAPA set about to define the core competencies that employers and regulators should expect of a CAPAPA certified individual.

The access and privacy profession has existed in Canada for barely two decades. In the time since access to information and privacy legislation was introduced, only a handful of practitioners guidelines have been developed by large organizations for internal use. Consequently, few sources of information were available as guides for developing these core competencies.<sup>4</sup>

<sup>1</sup> In the CAPA-CAPAPA Professional Standards and Certification Project Phase 1 Report, Professional Standards/Competencies (March 27, 2007), Appendix B, "Environmental Scan - Approaches to Competencies and Standards" identifies thirteen representative Canadian organizations offering certified designations that were reviewed. The present analysis included these organizations as well as certification materials by the Alberta Arbitration & Mediation Society, ARMA International, Disaster Recovery Institute, Family Mediator <http://www.pmi.org/CareerDevelopment/Pages/PMICredentialOverview.aspx>

<sup>3</sup> Canadian Information Centre for International Credentials Guide to Terminology Usage in the Field of Credentials Recognition and Mobility in English in Canada <http://www.cicic.ca/en/Guide.aspx?sortcode=2.17.17>

<sup>4</sup> Sources include the Ontario Management Board Secretariat's Senior Management Group Core Competencies (2000), the Information Commissioner of Canada's "Career Progression Plan" (2008), the Human Resource Systems Group "Framework for Competency-based

In 2006, a CAPA-CAPAPA Professional Standards and Certification Working Group (PSWG) was established with a grant from the Privacy Commissioner of Canada. The PSWG created a list of core competencies that was published on March 27, 2007 in the Working Group's Phase 1 report.

The PSWG Phase 1 report contains extensive comments on how to interpret the list of competencies and their intended uses. A review of the Working Group's report was prepared as input to the current iteration of Core Competency Standards. That review is available upon request.

The Core Competency Standards are based on reflection and assessment of practices relative to the professional practice standards of other professions that are publicly available or that CAPAPA has received through direct contact; and from feedback about access and privacy practices from supervisors, peers, direct reports and others.

It is expected that feedback from members and other stakeholders on these core competencies will lead to refinements and possibly the addition of core competencies or more domains in future years. This would be a sign of healthy development in the access and privacy profession.

#### Exclusivity

The certification model introduced by CAPAPA is a "semi-protected" designation; it is not an "exclusive" designation that allows only a "registered" person to practice the profession. Accordingly, CAPAPA's credentials do **not** restrict who can perform access and privacy tasks, although employers may voluntarily adopt the requirement.

CAPAPA may in the future pursue a "protected" credential scheme in which a specific provincial statute or an Order-in-Council specifies a professional title and provides that a) only a person who is a full member of a particular professional organization may use that title, and b) that anyone who contravenes this requirement is guilty of an offence. CAPAPA has no plans to pursue an exclusive designation.<sup>5</sup>

Management" (2007), the Canadian General Standards Board "Competencies of the Federal Government Information Management Community" (2009), and the ISO/IEC International Standard 17024 "Conformity Assessment - General requirements for bodies operating certification of persons" (2003).

<sup>5</sup> See CAPAPA's Discussion Paper on Professional Certification (2004) for more details.



### Key Criteria

The key criteria used in identifying the required core competencies for access and privacy practitioners in Canada were that the competency must alone or together with other competencies:

- Define a set of skills and knowledge required to perform an access and privacy task in any organization in any jurisdiction
- Permit access and privacy knowledge and skill requirements to be defined for progressive CAPAPA professional designations, from entry level to Commissioner level
- Permit educational bodies to use the core competencies to design educational programs to train individuals to practice in the field of access and privacy

- Allow for specialization in a particular area of expertise within the profession
- Distinguish the access and privacy profession from other professions such as law, records and information management, information technology, information security, enterprise architecture
- Access and Privacy Professionals at every level must have the fundamental competencies, thereby ensuring a connectedness and a source of integration among all access and privacy professionals. In order to progress from one certification level to the next, each candidate will be required to demonstrate a mastery of the knowledge necessary to function at the next higher level for a particular competency; that they possess the skills and abilities necessary to perform the duties of the next higher level; and that they have successfully completed the activities required to function at the next higher level

### **How to Use Core Competency Standards**

Core Competency Standards will serve as attainment indicators for individuals in the following contexts:

**Education** - as Learning Outcomes for educational programs and training.

**Certification** - as concepts to be tested in certification examinations.<sup>6</sup>

**Employment** – as a starting point for position descriptions or job advertisements.

**Self-Assessment** – as an authoritative reference for self-assessment.

The AAPP credential recognizes an individual's competence in at least one (1) CAPAPA domain. If the individual is knowledgeable in more than one domain, that is a bonus.

The CIAPP credential recognizes that the individual is competent in at least two (2) domains. If the individual is knowledgeable in more than two domains, that is a bonus.

The CAPP credential recognizes that the individual is competent in at least three (3) domains.

The MAPP credential recognizes that the individual is highly knowledgeable and skilled in at least three (3) domains.

<sup>6</sup> See separate publications on certification requirements for each credential. Following a grandfathering period, certification requirements will include passing an examination. Examinations specific to each credential will cover situation- and fact-based scenarios that can be answered with the CAPAPA Core Body of Knowledge (CBK), the standard of access and privacy good practices, and other required reading material. Exams will be pass/fail based on achieving a minimum number of points.



## 4. Core Competencies

This section provides an overview of the core competencies that must be demonstrated by everyone who seeks to become a CAPAPA certified professional. The core competencies identify the base level of knowledge and skills that a person must reach or have before that person is deemed competent to carry out the practices of the access and privacy profession.

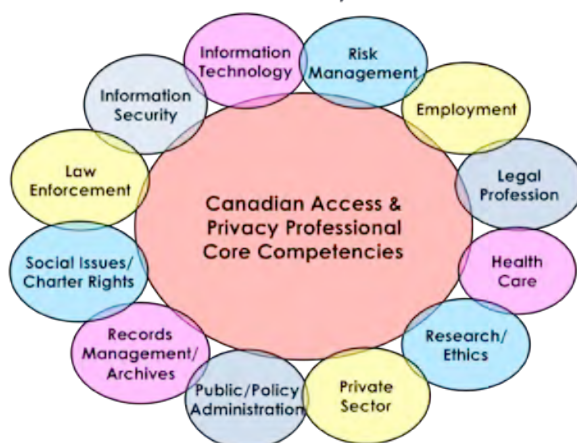
Access and Privacy Professionals possess unique knowledge and skills as outlined in Table 1 at the end of this section. However, the profession is multi-disciplinary in the sense that Access and Privacy Professionals require knowledge in the practices of related disciplines, such as Records Information Management, Information Security, Enterprise or Information Architecture, and Information Management. It is important to note the distinction CAPAPA makes between the Access and Privacy Profession and other disciplines.

For example, the **Records Information Management (RIM)** profession is considered to be separate from Access and Privacy, even though both deal with records. RIM is a discipline that develops policies and standards for the

institution in accordance with legislative requirements to make sure records can be found when needed for operational, legal or financial reasons. RIM professionals are knowledgeable about how to share information to minimize duplication of work, preserving documentation of decisions and actions, and assist business units with creating and maintaining records systems. RIM professionals manage the storage and use of records, and manage the process of archiving or destruction of records. As noted in the Core Competencies, CAPAPA is not targeting RIM professionals; however, similarities in the areas of practice necessitate a coordinated approach between RIM and Access and Privacy professionals.

Despite similarities between Access and Privacy, and Information Management (IM), important differences exist. IM specialists are knowledgeable about data standards, data and information analytics, and data quality issues. IM professionals are called upon to establish IM frameworks in organizations to ensure the organization maximizes the value of its information holdings because information should be treated as a critical asset like people, technology, buildings and vehicles.

### Multi-Disciplinary Access and Privacy Professionals





## **5. Domains of Competency**

### **Access to Information**

Generally speaking in Canada, every person has a right of access to a record, or part of a record in a public institution's custody or control. Documents held by private sector organizations are subject to similar access by individuals. In both cases, the right of access may be limited by mandatory or discretionary exemptions defined in the relevant privacy law or jurisdictional Freedom of Information statute. Exemptions include withholding personal information, and denying requests for access that are frivolous or vexatious.

Regulators and organizational leaders are generally in agreement that exemptions ought not to be claimed merely because they are technically available; rather, exemptions should only be claimed if they genuinely apply to the information at issue.

In both the private sector and the public sectors, the Access and Privacy Professional is responsible for ensuring that all statutory requirements under Freedom of Information/Access to Information/Privacy legislation for processing access requests are met. The obligations include corresponding with other personnel

and the requester, negotiating or mediating to narrow the scope of the request, locating records and identifying responsive records, and providing access to the records in compliance with the relevant legislation. The Access and Privacy Professional also typically supports the institution and trains staff to disclose information where no exemptions apply (proactive disclosure).

Access and Privacy Professionals in private sector organizations, even those whose title is "Privacy Officer", typically make decisions relating to all privacy and access issues. The role may have a dual reporting relationship to the Chief Executive Officer and/or corporate counsel.

Access to Information Professionals in public bodies usually makes decisions on non-contentious issues and routine requests if those duties have been formally delegated to the Access Professional. On contentious issues, the Access to Information Professional generally advises the head of the institution that holds accountability for making decisions.



	<i>COMPONENTS OF THE CORE COMPETENCY</i>	<i>MINIMUM REQUIREMENTS</i>
1. Understanding, Interpreting and Navigating the Legal Landscape	Understanding principles, rights, best practices and jurisdiction in providing access to information	<p>Knowledge of a jurisdiction's access to information legislation, regulations, principles, and the history of access and privacy legislation in Canada and internationally.</p> <p>Ability to find Commissioners orders or precedents or guidelines that are relevant to the processing of a particular access request to produce the best possible, acceptable outcomes given the particular factual, legal and rights-based context of a request, including privacy protection requirements.</p> <p>Ability to identify relevant corporate directives, policies, standards and best practices defining the process of administering Freedom of Information requests and protection of privacy.</p> <p>Ability to express general principles of access to information and privacy to non-experts.</p> <p>Collects and analyses information from a variety appropriate sources in order to understand issues.</p>
2. Managing Casework	Receiving and processing Access to Information Requests	<p>Knowledge of requirements and procedures for preparing responses and briefing materials to senior management and staff to respond to access requests</p> <p>Ability to collect information about the request from requesters and prepare documentation on the search for responsive records in compliance with legislative requirements.</p> <p>Develops clear goals, identifies priority activities and tasks, and adjust priorities as required.</p> <p>Customer-service orientation, providing service excellence to internal and external clients.</p> <p>Ability to use specialized computer applications without assistance.</p>
3. Managing Information and Records	Knowledge in the discipline of Records and Information Management	<p>Knowledge of archival, records and forms management processes, data security and information storage and retrieval systems.</p> <p>Tracks, evaluates and reports on progress towards strategic goals.</p> <p>Makes a continuous effort to improve response times and the process of searching for records.</p> <p>Ability to handle complex or highly contentious access requests.</p> <p>Ability to process a high volume (at least 50) Access to Information requests/Investigations/Complaints per year.</p>



	<i>COMPONENTS OF THE CORE COMPETENCY</i>	<i>MINIMUM REQUIREMENTS</i>
4.	Education and Raising Awareness about Access to Information	<p>Promoting Transparency and Confidentiality</p> <p>Advocates and follows best practices in applying exemptions and exclusions to prepare records for disclosure in compliance with legislation, including requests for personal information and personal health information.</p> <p>Acts ethically and fosters a work environment that reflects the content and the spirit of the CAPAPA Code of Professional Conduct and Ethics.</p> <p>Ability to participate in development and delivery of access to information training.</p> <p>Knowledge of the work environment (organizational awareness)</p> <p>Good communication and presentation skills (written and oral) to provide advice and guidance to management, clients and other stakeholders, including the ability to interact in a supportive manner with requesters and the officials within the institution who have custody of the information sought by the requester.</p>
5.	Mediation, Negotiation and Decision Making	<p>Building trust with requesters and regulators that legislative requirements are being followed.</p> <p>Knowledge of alternative dispute resolution techniques (theories, methods, techniques and practices).</p> <p>Knowledge of appeal and mediation processes and best practices for judicial reviews.</p> <p>Ability to inform the head of the institution or decision-maker who makes appropriate decisions about the access request and responding to the requester or Information Commissioner.</p> <p>Develops and implements strategies for investigations and resolution of complaints about access to information.</p> <p>Prepares decision letters and reports, both interim and final, with recommendations fully supported and analyzed.</p>



## Privacy

Privacy legislation, Fair Information Practices, industry best practices and Privacy Codes typically require that entities implement reasonable standards for protecting personal information in its possession. Individuals have an expectation that entities will use appropriate practices and procedures for collecting, storing, using, disclosing and disposing of personal information.

Breaches of privacy are hazardous to both individuals and organizations; therefore, most organizations adopt a risk-based approach to manage personal information.

It is the responsibility of the Privacy professional(s) to advise and support the organization in complying with privacy legislation and Fair Information Practices by conducting risk assessments, creating policies and

procedures for the protection of personally-identifiable information (PII) and other measures, training staff and minimizing the collection and retention of PII to what is strictly necessary to accomplish the business purpose and mission. The Privacy professional also develops and implements the incident response plan to handle breaches of PII.

CAPAPA considers the two domains of Access to Information and Privacy to be quite different from each other, and recognizes that Privacy Professionals in private sector organizations are typically responsible for both privacy and access functions, and Access to Information professionals in public bodies might be responsible for both privacy and access functions.

	<i>COMPONENTS OF THE CORE COMPETENCY</i>	<i>MINIMUM REQUIREMENTS</i>
6. Understanding, Interpreting and Navigating the Legal Landscape	Understanding principles, rights, best practices and jurisdiction in protecting privacy	Knowledge of a jurisdiction's privacy legislation, regulations, principles, and the history of access and privacy legislation in Canada and internationally. Knowledge of Commissioners orders, precedents and guidelines that are relevant to a particular privacy issue. Knowledge of relevant corporate directives, policies, standards and Fair Information Practices for privacy protection. Ability to analyze and make recommendations on appropriate policies, strategies and administrative steps to bring the business process or IT system into compliance. Ability to express general principles of privacy protection to non-experts.
7. Assessing and advising on risks	Knowledge of a range of analytical methods to assess privacy risks and skills in applying them	Knowledge of a range of privacy analysis methodologies such as Privacy Impact Assessments, privacy audits, and diagnostic tools. Knowledge of project management methodology, business and IT system development concepts, as well as conducting analyses, developing and implementing techniques and strategies. Specialized knowledge of information technology and advanced technology trends and concepts, security techniques, privacy enhancing technologies, organizational and technological directions and strategies. Strong strategic orientation skills to improve privacy compliance while achieving business goals. Anticipates areas where support or influence will be required and discusses situation/concerns with appropriate individuals.



	<i><b>COMPONENTS OF THE CORE COMPETENCY</b></i>	<i><b>MINIMUM REQUIREMENTS</b></i>
8. Investigating non-compliance	Responding to privacy breaches and complaints.	<p>Knowledge of investigative techniques such as interviewing, data and evidence collection, listening, cross-examination and research.</p> <p>Ability to develop effective relationships with senior management, colleagues, staff and stakeholders.</p> <p>Knowledge of organizational procedures to report privacy breaches to the Head of the institution and the Privacy Commissioner.</p> <p>Exercises judgment in knowing one's responsibilities within the organization and when to escalate an issue to a more senior person who exercises their judgment on the matter according to their level of responsibility.</p> <p>Champions access and privacy best practices to internal staff and acts as a role model for others.</p>
9. Education and Raising Awareness about Privacy	Promoting Transparency and Confidentiality	<p>Ability to participate in development and delivery of privacy training.</p> <p>Knows when to use formal or informal processes to respond to privacy issues.</p> <p>Ability to create policies, procedures, guidelines and other tools to improve institutional privacy compliance.</p> <p>Ability to visualize and describe enterprise-wide compliance and reputational risks and develop strategies to address them.</p> <p>Ability to handle complex privacy-related tasks with little supervision.</p>
10. Information Management	Knowledge of the principles, concepts and methods of Information Management, Information Security and Enterprise Architecture	<p>Knowledge of the discipline of Information Management, IM rules, tools and resources.</p> <p>Knowledge of techniques for analyzing and modeling business activities, workflows, organizational and other technical structures.</p> <p>Good understanding of related disciplines, such as Information Security, Enterprise Architecture (including privacy architecture), auditing, controllership and governance, risk management.</p> <p>Knowing when a business process or IT system and its components falls within corporate principles, policies, procedures and guidelines, laws, regulations, and where it does not.</p> <p>Prepare decision letters and reports, both interim and final, with recommendations fully supported and analysed.</p>



## Access and Privacy Management

This domain encompasses core competencies that an individual must have to lead an organizational unit that:

- manages Freedom of Information requests and privacy risk management activities
- handles inquiries on privacy and access to information issues
- delivers training on access and privacy
- helps or leads the development of policies related to the organization's responsibilities under privacy and FOI legislation and

- sets priorities for acquiring or building resources to respond to those activities.

This is not an exhaustive list. The Access and Privacy Management functions include providing expert advice in the event of a privacy or security breach where personal information has been disclosed without authorization.

	<i>Components of the Core Competency</i>	<i>Minimum Requirements</i>
11. Understanding, Interpreting and Navigating the Legal Landscape	Understanding principles, rights, best practices and jurisdiction in providing access to information and protecting privacy	Knowledge of the jurisprudence, case law and precedents relevant to access to information and privacy legislation and their regulations. Knowledge of how to evaluate and analyse information, data, evidence and findings of fact. Sophisticated ability to use a personal computer, conduct research on the internet and use a variety of software. Understands the impact of foreign legislation on the organization's ability to disclose or collect data in compliance with access and privacy legislation, policies and best practices, and develops appropriate risk countermeasures. Monitors a range of external information sources to identify new developments in access and privacy rules and issues and proactively adapts corporate directives, policies, standards and best practices as appropriate.
12. Management and leadership	Managing and leading staff	Knowledge of management principles and practices. Leads teams to achieve organizational goals; communicates and motivates a team to achieve results. Seeks common ground between multiple parties to achieve results and manages conflicts when consensus cannot be found. Analyzes and problem-solves in a creative and flexible way based on an understanding of issues, goals and cultures in own and other organizations. Gathers information from vendors/suppliers, reviews and analyzes contracts, agreements and memorandums of understanding to assess their impact and implications on data flows and their relevance to the organization's business needs, as well as risks and vulnerabilities.



	<b><i>Components of the Core Competency</i></b>	<b><i>Minimum Requirements</i></b>
13. Leading Change	Contribute to the development and delivery of training programs targeted to new and current employees and officials; promote transparency and confidentiality	Supports changing enterprise culture and methods of operating to improve compliance and quality of services, and to minimize risks. Influences policy processes and outcomes. Trains employees to act ethically in all dealings and answer questions or direct them to appropriate subject matter experts where they can find the information they need. Ability to develop work plans, set limits, prioritize activities, create performance indicators, organize people, and give appropriate directions to internal and external parties. Knowledge of how to develop and manage access and privacy projects, including writing business cases, identifying resources, defining timelines, formulating budgets, tracking resources and project-related expenditures.
14. Making decisions		Knowledge of the organization's policy development, decision-making and strategic planning processes, resource management policies and practices, and operational cycles. Integrates and provides support to privacy impact assessment requirements in enterprise project management and governance processes. Understands the political, social and economic and technological environments of the organization. Ability to negotiate rules and tools to manage information flows between the organization and partners/service providers, as well as define roles and responsibilities for the employees and sub-contractors of the partner/service provider. Knows when to consult or bring in a subject-matter expert, how to find the right expert, and to manage his or her input effectively.
15. Communicates effectively		Provides clear and constructive feedback in concrete terms for development purposes. Good communication and presentation skills (written and oral) to provide advice and guidance to management, clients and other stakeholders. Follows through on commitments to resolve customer issues and needs on a timely basis. Maintains clear communication with customers regarding their expectations and monitors customer satisfaction. Collects, analyzes and reports statistical data regarding enterprise access and privacy issues.



## Access and Privacy Law — Future Domain

“Access and Privacy Law” has not yet been recognized as a specialized area of practice by most Canadian law societies. Law faculties and continuing legal education opportunities offer only limited opportunities for practical training for the practice of advising clients on privacy and access laws.

Legal expertise is often needed in all kinds of Access and Privacy. The growing complexity of the legal framework for FOI and Privacy has reached the point where organizations need some form of assurance about the unique FOIP knowledge that a lawyer should have to provide good counsel to the organization.







Whether that assurance comes from CAPAPA or an existing lawyers’ society has not been resolved; nevertheless, there is merit in CAPAPA initiating the discussion on necessary legal knowledge and skills.

The goal is to know what minimum qualifications should be expected of a lawyer for an organization to have confidence in that individual’s advice in FOIP matters. Once the qualifications are available either from the CAPAPA Common Body of Knowledge or another source, acquiring the services of a FOIP lawyer could follow a process that is similar to the search for a qualified Privacy Officer or Access Coordinator.

	<i>COMPONENTS OF THE CORE COMPETENCY</i>	<i>MINIMUM REQUIREMENTS</i>
16. Understanding, Interpreting and Navigating the Legal Landscape of Access and Privacy	Understanding principles, rights, best practices and jurisdiction in providing access to information and protecting privacy	Training in: <ul style="list-style-type: none"><li>• Federal Access to Information and Privacy laws, PIPEDA</li><li>• Health sector legislation</li><li>• Employment law – access to employee records, employee privacy rights</li><li>• Internet law – collection, use and disclosure of personal information</li><li>• Provincial Access to Information and Privacy laws – exclusions, Commissioner’s rights and powers, appeals, judicial reviews, requester’s rights</li><li>• Consumer Protection issues</li><li>• Third party contract provisions</li><li>• Knowledge of the oversight and redress mechanisms for FOI and Privacy violations</li><li>• Charter of Human Rights and Freedoms</li><li>• European Union directives and Data Protection Acts</li><li>• US privacy framework</li></ul>
17. Representing/ Advising clients		Represent/Advise clients with respect to interpreting Access and Privacy Legislation Represent/Advise clients with respect to Commissioners decisions and Orders Representing clients in drafting and/or negotiating access and/or contractual privacy provisions
18. Legal training		Must be licensed to practice in the jurisdiction where the client is located
19. Preparing documents, negotiating with other parties		Preparing a client for mediation, arbitration, or judicial reviews Drafting/negotiating outsourcing agreements and contract provisions to protect personal information Preparing forms on delegation of authority under the Act.



## 6. Mapping Core Competencies to Professional Credentials

Competency Domains/Credential	AAPP	CIAPP	CAPP	MAPP
	Competency in 1 domain	Competency in 2 domains	Competency in 3 domains	Strong in 3 domains
Access to Information	Here or 	Here and 	Here and 	
Privacy	Here	Here	Here and 	
Access and Privacy Management			Here	

## **CAPAPA**

Suite 330, Unit 440  
10816 Macleod Trail SE  
Calgary, Alberta, Canada T2J 5N8

[www.capapa.org](http://www.capapa.org)

**Canada's Voice of Privacy and Access**  
**la porte parole canadienne pour l'accès et la vie privée**