Gaps Assessment Checklist

A. PRIVACY CHARTER

❑ 1. Scope – all people, all information, all places

Principles

❑ 2. protect confidential information from unauthorized use, disclosure, modification, or access to the information
❑ 3. right of access / correction
❑ 4. inform individuals of the legal authority and purpose of collection, and contact information if questions arise
❑ 5. general statement about use, disclosure, and consent for other uses, disclosures
❑ 6. minimum information, on a need to know basis
❑ 7. independent review of decisions
❑ 8. penalties / sanctions

B. ROLES AND RESPONSIBILITIES

❑ 1. functional overview:
- Business areas, funding

❑ 2. partnership/association agreements
❑ 3. designate a Privacy Officer(s)--responsibilities:
❑ 4. • identify compliance issues
❑ 5. • develop / maintain policies and procedures
❑ 6. • ensure staff aware of duties, roles, and responsibilities
❑ 7. • provide advice re.2 interpretation, release / non-release of information
❑ 8. • respond to requests for access / correction
❑ 9. • ensure security and protection
❑ 10. • liaise with the OIPC

C. RIGHT OF ACCESS

❑ 1. Ensure right of access / correction

Access procedures

❑ 2. routine requests
❑ 3. authorized representatives
❑ 4. who will receive requests?
❑ 5. who will review records for release? (must review all significant requests)
❑ 6. fees
❑ 7. fee estimates procedures

Must refuse disclosure:

❑ 8. third party information, unless provided by the applicant, or request is from authorized representative
❑ 9. results of an investigation
❑ 10. when prohibited by law

May refuse to disclose:

- ❑ 11. immediate and grave harm to health / safety
- ❑ 12. would identify a confidential source
- ❑ 13. advice and deliberations
- ❑ 14. prejudice the use or results of audits or assessments.

Correction Procedure

- ❑ 15. correction of basic information
- ❑ 16. see above re. timeline, fees, who receives / reviews
- ❑ 17. opinions
- ❑ 18. advise others that a correction / statement was made
- ❑ 19. statement of disagreement

Administration

- ❑ 20. time limits, fees
- ❑ 21. response to applicant
- ❑ 22. supervised review of records

D. INFORMATION HANDLING AND SECURITY

- ❑ 1. To protect confidential information and guard against unauthorized access, collection, use, disclosure or destruction.

Administrative Safeguards

Do you have/will you develop

- ❑ 2. policies and procedures
- ❑ 3. staff training, monitoring
- ❑ 4. confidentiality oath
- ❑ 5. accompany visitors to internal offices
- ❑ 6. least amount of information, need to know
- ❑ 7. verbal transmission
- ❑ 8. PIAs for new systems/access/security risks
- ❑ 9. security breaches and process
- ❑ 10. retention schedules
- ❑ 11. shredding of confidential information
- ❑ 12. destruction documented

Technical Safeguards

- ❑ 13. user IDs (role-based, case-based), don't share
- ❑ 14. passwords - change regularly, screen savers
- ❑ 15. encrypt personal information if sent via e-mail over public or external networks
- ❑ 16. audit trails – design, implement, review regularly
- ❑ 17. back-ups – off-site storage of tapes, review regularly, migrate as necessary
- ❑ 18. use of remote workstations – read-only? Passwords?
- ❑ 19. storage of information on remote workstations
- ❑ 20. laptop computers – storage when not in use, storage of info. on hard drive

Physical Safeguards ** See Walkthrough Checklist

E. COLLECTION, USE AND DISCLOSURE

Collection

- ❑ 1. Collect for an authorized use purposes only (see below)
- ❑ 2. Collect directly from the individual or his / her authorized representative, unless:
- ❑ 3. ▪ with consent
- ❑ 4. ▪ direct collection would compromise the interests, purpose, accuracy, safety
- ❑ 5. ▪ direct collection is not reasonably practicable
- ❑ 6. ▪ inform Public Trustee / Public Guardian
- ❑ 7. Must inform the individual of authority, purpose, contact – poster, brochure

Use

- ❑ 8. Use for authorized purposes only:
- ❑ 9. ▪ investigations, discipline proceedings, practice reviews or inspections
- ❑ 10. ▪ research
- ❑ 11. ▪ further education
- ❑ 12. ▪ comply with legislation
- ❑ 13. ▪ internal management e.g. policy development, QA
- ❑ 14. ▪ manage human resources
- ❑ 15. Use only to perform assigned duties

Disclosure

- ❑ 16. To the individual or authorized representative
- ❑ 17. To someone else, with consent e.g. lawyers
- ❑ 18. Consent requirements: authorization, purpose, recipient, acknowledgment, effective date, revocation
- ❑ 19. Without consent:
- ❑ 20. ▪ compelling circumstances affecting health and safety, with notice
- ❑ 21. ▪ to contact family members / friend if injured, ill or deceased
- ❑ 22. ▪ subpoena, warrant or court order
- ❑ 23. ▪ to obtain legal services
- ❑ 24. ▪ research or statistics; archival purposes
- ❑ 25. ▪ health and safety at issue
- ❑ 26. ▪ conducting legally authorized investigations or for debt or payment purposes
- ❑ 27. ▪ if authorized or required by legislation (e.g. WCB) or for audit purposes
- ❑ 28. Disclosure log: recipient, date and purpose, description
- ❑ 29. Consider wishes of the individual
- ❑ 30. Least amount of information at the highest level of anonymity

F. INFORMATION SECURITY IN CONTRACTING

- ❑ 1. To ensure appropriate information management and security practices by third parties contracted to provide services to, or on behalf of organization
- ❑ 2. Includes contractors, consultants, support service providers or business partners, even after termination
- ❑ 3. no access without signed agreement
- ❑ 4. contractors to meet or exceed organizational standards, provide their own standards
- ❑ 5. confidentiality (non-disclosure) agreement
- ❑ 6. report breaches of confidentiality and privacy
- ❑ 7. disaster recovery and system backup (e.g. contracts with information managers)

- ❑ 8. return hardware, information, system documentation
- ❑ 9. records retention
- ❑ 10. access to premises/systems for monitoring compliance

G. RESEARCH

- ❑ 1. To outline considerations and procedures for disclosure for research purposes
- ❑ 2. Requests to be written and accompanied by ethics approval (designated ethics committee)
- ❑ 3. Researcher must abide by conditions imposed by ethics committee or organization
- ❑ 4. Researcher must enter into agreement with organization to:
- ❑ 5. • comply with ATIPP
- ❑ 6. • comply with conditions re. use, protection, disclosure, return or disposal of the information
- ❑ 7. • comply with any requirements re. safeguards
- ❑ 8. • use only for research purposes
- ❑ 9. • individual names not published
- ❑ 10. • no further contact with individuals
- ❑ 11. • inspection of researcher premises
- ❑ 12. • pay fees, as required

H. TRANSITORY RECORDS

- ❑ 1. don't need to document
- ❑ 2. temporary information (message slips, invitations)
- ❑ 3. duplicates (e.g. documents scanned)
- ❑ 4. publications (articles, newspapers)
- ❑ 5. direct mail (advertisements, brochures, promotional materials)
- ❑ 6. blank forms, disks, videos, tapes
- ❑ 7. draft documents (draft reports, working notes)
- ❑ 8. destroy soon after use
- ❑ 9. retention of documents scanned

PYHSICAL WALKTHROUGH

- ❑ 1. notification posters / brochures
- ❑ 2. reception partitioning
- ❑ 3. video surveillance / cameras
- ❑ 4. on-site storage
- ❑ 5. off-site storage
- ❑ 6. staff nametags
- ❑ 7. fire extinguishers
- ❑ 8. smoke detectors
- ❑ 9. sprinklers
- ❑ 10. locked rooms
- ❑ 11. locked cabinets for
  - files
  - servers
  - computers
- ❑ 12. key distribution

- ❑ 13. building alarms / codes
- ❑ 14. positioning of computer monitors
- ❑ 15. privacy screens
- ❑ 16. physical transmission of confidential info. – envelope, car, courier
- ❑ 17. fax machines – location, speed dial, cover sheet, confirm receipt
- ❑ 18. disposal of electronic equipment / devices (computers, hard drives, diskettes, tapes, CD-ROMS, etc.)

ADDITIONAL NOTES: