Health Shared Services

Privacy Management Program

Revised: June 2026

Introduction

Alberta's Provincial Health Agencies (PHA) and Provincial Health Corporations (PHC) have Transitional Service Agreements with Health Shared Services' (HSS) to provide privacy services, including the Privacy Management Program (PMP).

This PMP applies to: Acute Care Alberta, Alberta Health Services, Alberta Precision Laboratories, ALTA Paramedic Health, Assisted Living Alberta, Cancer Care Alberta, Health Shared Services, Cancer Care Alberta, Primary Care Alberta and Recovery Alberta.

The PMP is reviewed regulatory according to organizational standards and processes.

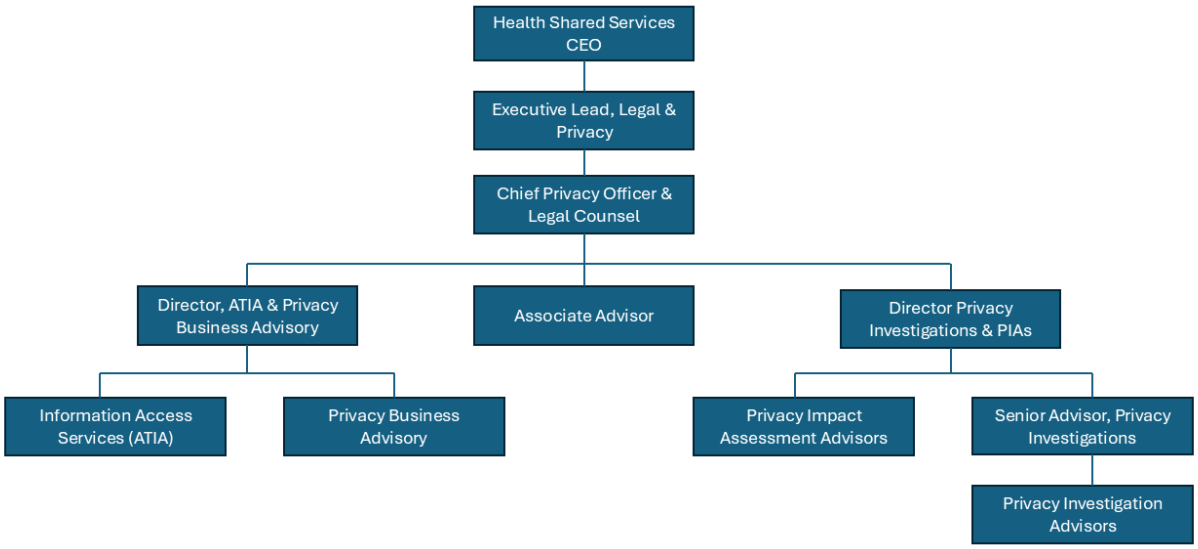
Delegation of Responsibilities

Health Shared Services' (HSS) Chief Executive Officer is the designated head of HSS for the purposes of the *Access to Information Act* (ATIA), *Protection of Privacy Act* (POPA) and the *Health Information Act* (HIA). The HSS CEO has delegated specific responsibilities under these Acts to the following leaders and their teams:

Chief Privacy Officer & Legal Counsel

- promote compliance with ATIA, POPA and HIA within daily healthcare system activities including in research activities by establishing policies and procedures,
- ensure ATIA, POPA and HIA education and training is available to all individuals with access to HSS-managed systems and information in the custody and control of HSS,
- ensure there is a process to address responding to information access requests and corrections in accordance with ATIA, POPA or HIA,
- support investigations into privacy-related incidents, including suspected violations of ATIA, POPA, or HIA,
- facilitate logging, monitoring and auditing of HSS-managed electronic information systems and PHA/PHC owned and/or operated facilities for compliance with ATIA, POPA, or HIA,
- ensure that HSS has appropriate guidance, controls, and escalation processes to manage audits and investigations to conduct any potential privacy breach investigations in a fair and reasonable manner,

- liaise with the Office of the Information and Privacy Commissioner (OIPC), including receiving and responding to queries and managing all aspects of PHA/PHC-related OIPC inquiries, reviews, and investigations including mandatory reporting obligations,
- facilitate Privacy Impact Assessments and submit them to the OIPC,
- oversee artificial intelligence and machine learning initiatives undertaken by the PHA/PHC, and
- Lead the Information and Privacy team tasked with completing the day-to-day implementation of the privacy program (see image).



Chief Information Security Officer

- promote compliance with ATIA, POPA and HIA within daily healthcare system activities including in research activities by establishing policies and procedures,
- develop and manage information risk management governance and the information risk management program,
- develop and manage the necessary specialist staff resources, processes, and technology,
- commission external audits and/or assessments of the information risk management program,
- oversee artificial intelligence and machine learning initiatives undertaken by the PHA/PHC, and
- manage adherence to international standards and frameworks.

Senior Provincial Director, Health Information Management (HIM)

- promote compliance with ATIA, POPA and HIA within daily healthcare system activities including in research activities by establishing policies and procedures,
- ensure access and disclosure education and training is available to all individuals with access to HSS-managed systems and information in the custody and control of HSS,
- respond to information access requests and requisite corrections in accordance with the HIA,
- facilitate audits of access and disclosure activities documented within HSS-managed electronic information systems and PHA/PHC owned and/or operated facilities for compliance with the HIA, and
- supporting the Chief Privacy Officer on HIM – Provincial Services, Access and Disclosure activities in relation to PHA/PHC-related OIPC inquiries, reviews, and investigations.

Capital Management

- responsible for the management, maintenance, and enforcement of physical access to provincial health system facilities.

All PHA & PHC employees, members of the medical and midwifery staffs, students, residents, volunteers, and other persons acting on behalf of a PHA and/or PHC are responsible to:

- demonstrate and hold each other accountable to demonstrate the behaviours outlined in the Privacy Protection and Information Access Policy,
- uphold the confidentiality, integrity, and availability of HSS-managed electronic information and technology-based systems, and
- fully cooperate with all activities undertaken to ensure compliance with ATIA, POPA including investigations relating to privacy, requests for access to information, and requests for correction.

Contracted Service Providers using, accessing or provisioning PHA and/or PHC information or HSS-managed IT resources are responsible to:

- demonstrate the behaviours outlines in the Privacy Protection and Information Access Policy,
- implement and maintain controls for the security of information and IT resources and comply with applicable HSS policies, procedures, and standards,

- submit their privacy programs for assessment prior to being granted privileges for access to PHA/PHC information or HSS-managed IT resources, and
- adhere to all contractual agreements relating to the access to and use of health, personal and business information including, but not limited to, reporting privacy breaches and maintaining confidentiality.

Supporting Documentation

- **Policies & Procedures**
  - Delegation of Authority and Responsibilities for Compliance with ATIA, POPA & the HIA Policy 1108
  - Privacy Protection and Information Access Policy 1177

Access to Information (Personal, Health & Business)

HSS is committed to meet its legal obligations under ATIA, POPA, and the HIA to provide timely access to information held in the custody and control of the provincial healthcare system, including responding to information requests within 30 business days. All employees who receive an information request are responsible to conduct a thorough search for responsive records and for providing the records in their original format to the Information Access Services Advisor or Access and Disclosure Advisor (as applicable) within the timeframe specified.

Informal Requests

Personal and business information may be requested through established informal sources and channels such as Community Engagement & Communications, Data Analytics, HealthLink, Environmental Public Health, or Human Resources. HSS recommends using these informal processes when possible.

Informal requests for health information may be made directly to an individual's healthcare provider at the time of their appointment. Providers may use Quick Release or Quick Disclosure functionality in Connect Care to respond to these requests. MyChart also provides patients and their proxies with direct access to their health information in Connect Care (the HSS-managed electronic medical record).

Formal Requests

Formal access to information requests for personal, business and health information are managed by HSS' Information & Privacy Team and the Health Information Management Department respectively. Requests for personal or health information require the explicit recorded consent of the individual who is the subject of the information, or the individual's authorized representative, unless disclosure without consent is authorized by law. A reasonable fee may be associated with making an information request as outlined by ATIA, POPA and the HIA.

Formal requests for health information made under the *Health Information Act* are processed by the Access & Disclosure team. Access requests may be made using the Request to Access Health Information form and submitted by email to disclosure@hssab.ca or by mail addressed to the attention of Disclosure Help Line, Room OE1.01, 8440-112 Street, Edmonton AB, T6G 2B7. Members of the public may learn more about requests to access health information at: Access & Disclosure | Alberta Health Services.

Formal requests for personal and business information made under the *Access to Information Act* are made via the Health Shared Services Public Access Portal, by email to privacy@hssab.ca, or by mail addressed to the attention of Information & Privacy, 5th Floor, North Tower, Seventh Street Plaza, 10030-107 Street, Edmonton AB, T5J 3E4. Members of the public may learn more about requests to access personal or business information at: Information Requests | Alberta Health Services

Proactive Information Disclosures

Some business information is proactively and routinely disclosed on organizational websites including but not limited to:

- Directory of Personal Information Banks (as required by POPA s. 57)
- A list of all manuals, handbooks and guidelines used by employees in decision-making processes that affect the public (as required by ATIA s. 91)
- Recent news, advisories and stories
- Provider contact information (Alberta Find a Provider)
- Bylaws and Corporate Policies
- Public Health Inspection Reports

Correction and/or Amendment Requests

Individuals may also request amendments or corrections to their own health or personal information. In the case of a requested amendment or correction, Health Shared Services

(HSS) makes reasonable efforts to confirm the accuracy of the public health system records while reserving the right to restrict or decline to make amendments to records. For example, professional opinions will not be corrected.

Requests for health information correction or amendment requests may be submitted by email to ChartCorrection@hssab.ca or by mail addressed to the attention of HIM – Chart Correction, Walter C. Mackenzie Health Services Centre, 0E1, 8440-112 Street NW, Edmonton AB, T6G 2B7.

Requests for personal information correction or amendment requests may be submitted by email to privacy@hssab.ca or by mail addressed to the attention of Information & Privacy, 5th Floor, North Tower, Seventh Street Plaza, 10030-107 Street, Edmonton AB, T5J 3E4.

Audit Log Requests

HSS permits individuals to request an audit log of all access to their health information. Requests for access to Netcare audit logs are made directly to Primary and Preventative Health Services via the Alberta Netcare website.

Audit log requests of HSS-managed systems may be submitted by email to privacy@hssab.ca or by mail addressed to the attention of Information & Privacy, 5th Floor, North Tower, Seventh Street Plaza, 10030-107 Street, Edmonton AB, T5J 3E4.

Complaints

HSS accepts complaints about the collection, use or disclosure of identifiable health or personal information via the publicly available Privacy Intake Line (privacy@hssab.ca) or by mail addressed to the attention of Information & Privacy, 5th Floor, North Tower, Seventh Street Plaza, 10030-107 Street, Edmonton AB, T5J 3E4.

When received, the complaint will be forwarded to the most appropriate team member to address (e.g., the Advisor who originally processed the request). All effort is made to resolve the concern before it is directed to the Office of the Information and Privacy Commissioner (OIPC). When a resolution to the complaint cannot be reached, HSS will collaborate fully with any relevant investigation opened by the OIPC. If a complaint moves to the court system, the HSS Information & Privacy team will be supported by the appropriate HSS legal team.

Supporting Documentation

- **Best Practices & Guidance**
  - InfoCare ATIA Call for Records FAQ
  - ATIA Call for Records Flowchart
  - Access to Information Act (ATIA) FAQ
  - ATIA – Making Resources Publicly Available – FAQ
  - Records Search Checklist
  - ATIA Requests 30-Day Timeline
  - ATIA – What Counts as a Record?
  - A Manager's Guide to Handling ATIA Requests for Emails
  - Assisting those who experience Domestic Violence – Clare's Law
  - HIA – Correction or Amendment Request
  - Disclosures to Law Enforcement
    - Contacting Family about Injuries, Illness or Death
    - Emergency Medical Services and Emergency Health Services Act
    - FAQs – Disclosures to Law Enforcement
    - Gunshot and Stab Wound Mandatory Disclosure Act
    - Missing Persons Act
    - Possible Commission of an Offence
    - Prevent Fraud or Limit Abuse of Health Services
    - Providing Witness Statements to Law Enforcement
    - Requests for Personal Information
    - Significant Risk of Harm
    - Subpoenas, Warrants and Orders
  - Guidelines fore the Disclosure of Health Information
  - Information Requests During Census and Elections
  - Data Disclosure Requirements: Health Information Disclosures to External Parties
  - Requests for Data from Outside AHS (Data Disclosures) Workflow
  - InfoCare: Sharing Health Care Provider Information with Patients
  - Connect Care Quick Release
  - Connect Care Quick Disclosure Tip Sheet
- **Forms**
  - Access Audit Log Request Health Information Act
  - Call for Records
  - Consent to Disclose Health Information
  - Consent to Disclose Personal Information
  - Health Information Access Request
  - MyChart Account Access Request (by parents, guardians or authorized representatives)
  - Research/Non-Research/Data Request

- **Forms (continued)**
  - Request for CPSM Records
  - Request to Access Information
  - Request to Correct or Amend Health Information (Health Information Act)
  - Request to Correct or Amend Personal Information Protection of Privacy Act (POPA)
  - Student Immunization Record Information Request
- **Policies & Procedures**
  - Collection, Access, Use, and Disclosure of Information Policy 1112
  - Legal Hold Procedure 1133-04
  - Research Information Management Policy 1146
  - Privacy Protection and Information Access Policy 1177

Breaches of Personal & Health Information (Privacy Incident Management)

A privacy breach involves any incident of, suspected or confirmed, unauthorized collection, use, access, disclosure or disposal of health or personal information. A privacy breach may be caused by human error (deliberate or unintentional) or technical error, resulting in failure to comply with established policies, procedures, or the *Access to Information Act* (ATIA), the *Protection of Privacy Act* (POPA) or the *Health Information Act* (HIA). Upon discovery of a breach, all employees of the provincial healthcare system must take immediate action to contain and recover any information involved within a breach. HSS conducts any potential privacy breach investigations in a fair and reasonable manner and in accordance with departmental protocols.

All employees are responsible to:

- immediately report the breach to the Information & Privacy Department, and
- cooperate with the assigned Investigation Advisor.

Managers are responsible to:

- notify affected individuals about the breach when instructed by the assigned investigator,
- ensure recommendations made by the investigator are implemented within their program area,
- document any outstanding privacy and information security risks, and
- ensure that appropriate safeguards are in place to prevent any future breaches.

The Information and Privacy Investigation Team is responsible to:

- review reported breaches in a timely manner and complete an assessment of harm,
    - if the legislative threshold of harm is met, the team will provide a letter to the responsible manager to provide to the affected individual(s) and will make all necessary notifications to the Information and Privacy Commissioner and the Minister
- engage with other program areas, including but not limited to, Human Resources, and Ethics & Compliance and Protective Services, as appropriate for the investigation
- oversee recommendations to correct the breach including but not limited to:
    - changes in policies, procedures, or practices;
    - education through in-service programs; and
    - disciplinary action up to and including dismissal

The Human Resources Team is responsible to:

- Lead the incident investigation,
- Conduct employee interviews as required to support the investigation, and
- Recommend disciplinary action up to and including dismissal, as required.

Supporting Documentation

- **Best Practices & Guidance**
  - Mandatory Breach Reporting
  - InfoCare: Preventing Common Privacy Breaches in Connect Care
  - InfoCare: Privacy Breach Response Quick Reference
  - Preventing Personal Information Privacy Breaches
- **Forms**
  - Report a Privacy Breach/Incident
- **Policies & Procedures**
  - Access to Information (Physical, Electronic, Remote) Policy 1105
  - Contractor Requirements for Security and Privacy of Information and Information Technology Resources Policy 1107
  - Delegation of Authority and Responsibilities for Compliance with ATIA, POPA & the HIA Policy 1108
  - Collection, Access, Use, and Disclosure of Information Policy 1112
  - Information Security and Privacy Safeguards Policy 1143
  - Monitoring and Auditing of Information Technology Resources Policy 1144
  - Privacy Protection and Information Access Policy 1177

Consent

HSS collects, uses and discloses identifiable health, personal and business information as authorized by the *Access to Information Act* (ATIA), *Protection of Privacy Act* (POPA) or the *Health Information Act* (HIA), as relevant. Consent is not required to collect or disclose non-personal or synthetic data.

Where no legislative authority exists for a specific collection, use or disclosure PHAs/PHCs will obtain consent for the collection, use or disclosure from the individual that the information is about.

PHAs/PHCs will not obtain consent on behalf of another custodian or another public body, and vice versa, unless doing so is part of a written service agreement.

Written or Electronic Consent

The preferred and recommended form of obtaining consent is written or electronic. HSS-approved consent forms should be the first choice for obtaining written consent.

When an email is accepted, rather than using the HSS form, the consent must meet the requirements set forth in the relevant legislation including, but not limited to:

- The name of the individual providing the consent,
- Identifying the specific information to which the consent applies,
- From whom information may be collected (e.g. employer reference) or to whom information may be disclosed (e.g. employer) and how it may be used, and
- The effective date of the consent and the date on which it expires.

Consent forms may be sent and received via letter mail, email or MyChart.

Oral Consent

Until such time as an oral consent policy has been approved, oral consent is only permitted to collect or disclose health or personal information when seeking written or electronic consent is unreasonable or may interfere with care. Examples of when oral consent may be appropriate include, but are not limited to:

- individual doesn't have access to reliable telecommunications equipment, or
- the collection or disclosure is made via telephone during a call in which the individual that the information is about is present to provide consent.

When oral consent is obtained, the minimal information that must be included is:

- The name of the individual providing the consent, and their authority to do so,
- The specific information to which the consent requires,
- From whom the information may be collected (e.g. employer reference) or to whom information may be disclosed (e.g. employer) and how it may be used.

Oral consent must be documented using a note outlining the above items made on the individual's record (e.g. health record, personnel record, etc.).

Oral consent may be accepted for short-term purposes only (e.g. for one counseling session but not for the individual's entire relationship with the individual collecting the consent) and written consent must be obtained as soon as is reasonably possible.

Supporting Documentation

- **Best Practices & Guidance**
  - Consent in Healthcare
  - Consent in Healthcare Decision Tree
  - HIA – Consent Requirements
- **Forms**
  - Consent to Collect, Use, and Disclose Stories, Photos and/or Video and Sound Recordings
  - Consent to Disclose and Transfer Health Information
  - Consent to Disclose Health Information
  - Consent to Disclose Personal Information
  - Reference Consent(s)
- **Policies & Procedures**
  - Collection, Access, Use, and Disclosure of Information Policy 1112
  - Privacy Protection and Information Access Policy 1177

Information Classification & Management

HSS collects, uses and discloses varying categories of information defined by the *Access to Information Act* (ATIA), the *Protection of Privacy Act* (POPA) and the *Health Information Act* (HIA). This includes:

- **Personal Information**
  - Personal information (as defined by ATIA & POPA) may include but is not limited to recruitment, employee benefit administration, payroll and compensation, pension, internal personnel management, monitoring system access, workplace health and safety programs, ability management programs, and clinical support programs.
  - Personal information is retained and destroyed per the Records Retention Schedule.

- **Health Information**
  - Health information (as defined by HIA) may include but is not limited to name, date of birth, provincial health care number, address, health history, and any other information needed to provide the required health services.
  - Health information is retained and destroyed per the Records Retention Schedule.

- **Data Derived from Personal Information**
    - Data derived from personal information (as defined by POPA) may include but is not limited to: data created as part of an approved data matching project.
    - Data derived from personal information is destroyed or anonymized (i.e. becomes non-personal data) once the purpose of the creation is complete.

- **Non-Personal Data**
    - Non-personal data (as defined by POPA) may include but is not limited to data sets curated by the Data and Analytics team upon request for planning and system management.
    - The elements that must be removed from a data set to be considered non-personal data are described in the Non-Identifying Health Information Standard IPO-2013-0004. Non-personal data must not include:
        - Names (including initials),
        - Geographic subdivisions smaller than a province including street address, city, county, precinct, postal codes except for the initial three digits of a postal code if, according to the currently publicly available data from the Census Bureau:
            - The geographic unit formed by combining all postal codes with the same three initial digits contains more than 20,000 people
            - The initial three digits of a postal code for all such geographic units containing 20,000 or fewer people are changed to 000,
        - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death,
        - All ages over 89 and elements of dates indicative of such age (such ages must be aggregated into a single category of 90 or older),
        - Telephone numbers,
        - Fax numbers,
        - Email addresses,
        - Social insurance number,
        - Medical record numbers,
        - Health plan beneficiary numbers (e.g., PIN, ULI),
        - Account numbers,
        - Certificate/license numbers,
        - Vehicle identifiers and serial numbers including license plate numbers,
        - Device identifiers and serial numbers,

        - Web universal resource locators (URLs),
        - Internet protocol (IP) addresses,
        - Biometric identifiers including fingerprints and voice prints, and
        - Full-face photographic images and any comparable images.

    - Each team that creates non-personal data in their process of doing business is responsible to maintain records which describe the:
        - personal information or data derived from personal information used to create the non-personal data,
        - purpose for creating the non-personal data,
        - method used for creating the non-personal data, and
        - assessment done to ensure that the identity of the individual who is the subject of the information cannot be identified or re-identified from the data.

    - Non-personal data will not be disclosed to other public bodies unless the disclosure is for
        - Research and analysis,
        - Planning administering, delivering, managing, monitoring or evaluating a program or service, or
        - One or more prescribed purposes.

    - Non-personal data will only be disclosed when an agreement is in place between HSS and the recipient stating that the recipient will
        - Ensure the security and confidentiality of the information,
        - Not re-identify or attempt to re-identify the non-personal data,
        - Not use the non-personal data for any reason other than the stated purpose without HSS' written permission, and
        - Destroy the non-personal data when the purpose for its use is complete unless HSS has provided written consent otherwise.

- Synthetic Data

    - Synthetic data (as defined by POPA) may include but is not limited to: 'Mock Data' created by the Data and Analytics team used for testing.

Decisions regarding the collection, use and disclosure of any of the above categories of information are made based on the information classification policy.

Information Classification

All information in the custody and control of the provincial healthcare system shall have an information classification level and corresponding labelling and handling controls applied to it. Information will be protected in accordance with the applied classification.

Classification levels help dictate security controls that are required to protect health information, personal information, and business information.

Designated classifications used by HSS are:

- *Restricted* - applied to information where unauthorized disclosure could cause serious risk or harm to any individual, the provincial healthcare system, third-party, or to the integrity, image, service delivery, or sustainability of the provincial healthcare system.

- *Confidential* – applied to information where unauthorized disclosure could cause moderate risk or harm to any individual, the provincial healthcare system, third-party, or to the privacy of individuals, compromise the organization's ability to respond to disaster, or threaten the secure containment of vital records. All personal and health information is automatically classified as confidential.

- *Protected* - applied to information where unauthorized disclosure could cause low risk or harm to any individual, the provincial healthcare system, or third party. Protected information is only available to people who are authorized to view protected information.

- *Public* - applied to information which can be distributed to any person inside or outside of the provincial healthcare system.

Collection Statements

Collection statements are available on documents collecting identifiable health or personal information which meet the requirements set out in privacy legislation.

Collection statement posters are available in all facilities which include:

- The legislative authority for the collection, use and disclosure of the identifiable health or personal information,
- What identifiable health or personal information is collected,
- How identifiable health or personal information is used,

- How identifiable health or personal information is protected,
- Who can use/disclose identifiable health or personal information,
- Individual rights regarding identifiable health or personal information, and
- Contact information for the Chief Privacy Officer.

Records Retention Schedule

All health, personal and business records are maintained for a minimum of one year unless they are classified as transitory according to HSS policy. A records retention schedule has been created for all non-transitory records in the custody and control of the provincial healthcare system. Records are securely destroyed at the end-of-life following approved processes.

Transitory Records do not have a defined retention period, however these records are not kept indefinitely or destroyed immediately. The business area is responsible for determining the value of these records and retaining them only as long as they actively provide value and meet business needs.

Supporting Documentation

- **Best Practices & Guidance**
  - ATIA – Transitory Records
  - Physical Storage of Records
- **Forms**
  - Records Destruction Authorization (Paper, Electronic or Hybrid)
  - Records Retention Schedule Change Request Form
- **Policies & Procedures**
  - Records Management Policy 1133
  - Records Retention Schedule 1133-01
  - Official Records Destruction Procedure 1133-02
  - Transitory Records Procedure 1133-03
  - Information Classification Policy 1142
  - Monitoring and Auditing of Information Technology Resources Policy 1144
  - Scanning and Digitization Policy 1191
  - Non-Identifying Health Information Standard IPO-2013-0004
  - Enterprise Risk Management Framework

Privacy Impact Assessments

HSS is committed to ensuring that new or changed practices and systems implemented within the organization are assessed for any potential impacts on individual privacy and for compliance with the *Access to Information Act* (ATIA), the *Protection of Privacy Act* (POPA) and the *Health Information Act* (HIA). The PIA process implemented by HSS provides documented assurance that privacy issues related to personal information and health information in the custody and control of HSS have been appropriately identified and addressed.

HSS conducts PIAs for initiatives involving individually identifying health information (as defined by the HIA) when:

- there is a collection, use, or disclosure of new health information that was not previously collected, used, or disclosed,
- new parties are granted access to health information,
- a new service delivery or management technology that stores, transmits, or retrieves health or personal information is implemented,
- a new or different Electronic Health Record (EHR) system is implemented or an existing EHR is being changed,
- entering into agreements with new business partners or vendors who will have access to health information in the custody or control of the provincial health system
- establishing new health care delivery models,
- establishing a new program or group that will collect, use or disclose health or personal information deemed to be of high sensitivity (note that for these purposes all health information is deemed to be highly sensitive),
- introducing new or revised administrative practices or information systems related to the collection, use or disclosure of health or personal information,
- implementing new health information repositories,
- data matching health information in the custody and control of HSS with data from another custodian or non-custodian,
- health information will be used to develop or be input into innovative technologies (such as AI), or
- the Commissioner explicitly requests the creation of a PIA.

HSS conducts PIAs for initiatives involving individually identifying personal information (as defined by ATIA/POPA) when:

- there is a collection, use, or disclosure of new personal information that was not previously collected, used, or disclosed,

- a new service delivery or management technology that stores, transmits, or retrieves personal information is implemented,
- entering into agreements with new business partners or vendors who will have access to personal information in the custody or control of the provincial health system,
- establishing a new program or group that will collect, use or disclose personal information deemed to be of high sensitivity (note that for these purposes all health information is deemed to be highly sensitive),
- introducing new or revised administrative practices or information systems related to the collection, use or disclosure of personal information,
- data matching personal information between two or more public bodies,
- establishing repositories that facilitate future research studies,
- the practice, program or service will involve the personal information of a significant percentage of Albertans,
- a common or integrated program or service is established,
- personal information will be used to develop or be input into innovative technologies (such as AI), or
- the Commissioner explicitly requests the creation of a PIA.

HSS submits all health information related PIAs to the OIPC for review. Personal information PIAs are submitted to the OIPC as prescribed by POPA.

While the Repository Owner is ultimately responsible for the completion of the Privacy Impact Assessment (PIA), the Information and Privacy Team will:

- determine whether a PIA is required,
- submit PIAs to the OIPC for review upon timely receipt of the PIAs from repository owners,
- retain, in accordance with the Records Retention Schedule, copies of PIA and documentation which address the OIPC's concerns,
- review and submit any amendments to PIAs to the OIPC, and
- support repository owners in meeting their responsibilities (including providing standards and educational materials).

Supporting Documentation

- **Best Practices & Guidance**
  - ATIA – Transitory Records
  - Physical Storage of Records
- **Forms**
  - Records Destruction Authorization (Paper, Electronic or Hybrid)
  - Records Retention Schedule Change Request Form
- **Policies & Procedures**
  - Records Retention Schedule 1133-01
  - Information Classification Policy 1142
  - Monitoring and Auditing of Information Technology Resources Policy 1144

Artificial Intelligence (AI)

Artificial Intelligence (AI) that has not been assessed for privacy and information security risks (i.e. Privacy Impact Assessment), by HSS is not approved for use. If an unapproved AI tool/service/feature is to be used, only information classified as public can be disclosed.

Individuals choosing to use AI remain fully accountable for decisions made based upon AI output and must:

- Verify the accuracy, completeness and relevance of results,
- Ensure that output content aligns with applicable legislation, standards and policies,
- Apply the correct level of clinical, operational or technical oversight, and
- Use critical thinking and professional/clinical judgement to assess wither the output is appropriate for the situation.

Microsoft CoPilot

Microsoft CoPilot has been assessed and accepted for use by HSS. When staff are logged into Microsoft CoPilot with the credentials provided by their employer, any classification of information may be used. Information input into the HSS instance of Microsoft CoPilot is not used to train AI systems and is retained for a limited time. Microsoft CoPilot cannot access HSS databases. The recommended use cases for Microsoft CoPilot include creating, editing or summarizing content and learning about a specific topic (e.g. find the latest research on…).

HSS Websites

HSS-managed websites use cookies to collect anonymous statistical information such as browser type, screen size, traffic patterns and pages visited. This information helps HSS provide site visitors with better service. HSS does not store personal information in cookies and site visitors may change the settings on their web browser to deny cookies if desired.

HSS-managed websites also use automated analysis and processing technology to provide personalized services such as chat. Any personal information collected and processed by these tools is never shared externally.

Supporting Documentation

- **Best Practices & Guidance**
  - Ethics and Governance of Artificial Intelligence for Health
  - How to recognize a deep fake
  - Misinformation / Disinformation Cheat Sheet
  - Recommendations for Responsible & Sustainable Implementation of Artificial Intelligence in AHS
  - Third-Party Artificial Intelligence (AI) Best Practices
- **Policies & Procedures**
  - Monitoring and Auditing of Information Technology Resources Policy 1144

Safeguarding & Securing Information

HSS has a duty to protect the security, privacy, and confidentiality of information in its custody and control. Information security and privacy safeguards implemented by HSS help to ensure the integrity and accuracy of the provincial healthcare system's information are maintained. These safeguards ensure HSS is able to assess and manage risks associated with the collection, use, and disclosure of information in its custody and control.

Physical, administrative, and technical access controls are in place at all provincial health system facilities containing information classified as restricted, confidential, or protected, information processing and storage, and IT resources. Access levels and privileges are restricted to the minimum required to fulfill an individual's roles and responsibilities within the provincial health system.

These controls may include, but are not limited to:

- *Administrative Safeguards*
    - Established policies, procedures, standards and best practices
    - Staff identification badges
    - Required Organizational Training and optional training modules
    - Criminal records check at hire
    - Contractor evaluation as part of the competitive bid process
    - Contractor agreements
- *Physical Safeguards*
    - Surveillance video & alarms
    - Staffed reception desks
    - Card and key controlled entry doors and access codes
    - Periodic physical security assessments of facilities and equipment
- *Technical Safeguards*
    - Unique user IDs and passwords
    - Logging of all user accesses and periodic review of the access
    - EMR Smart Audit tool which flags anomalies based on assigned roles
    - EMR Confidentiality features (e.g. Break-the-Glass, Private Encounter)
    - Encryption of mobile wireless devices, laptops, and mobile storage devices
    - Email encryption software

Smart Audit Tool (Logging & Monitoring)

HSS has a legislative duty to safeguard health information under its custody and control, including patient information housed in Connect Care. To help us meet this duty we use a Smart Audit Tool (SAT). The SAT runs in the background of Connect Care 24/7 and monitors and analyzes all accesses to Connect Care for unusual activity. All flagged accesses are reviewed manually to confirm the SAT findings. If the validation review verifies that the flagged access may be suspicious, the access will be investigated as a potential privacy breach.

Internal Audit

HSS' Information & Privacy team leverages the organization's Internal Audit program to regularly evaluate existing operations, controls, and governance processes. Internal Audit

reviews focus on identifying organizational risks and provide recommendations to strengthen our organizational program.

Supporting Documentation

- **Best Practices & Guidance**
  - Confidentiality Quick Reference
  - Connect Care Confidentiality Tip Sheet
  - Logging & Monitoring
- **Policies & Procedures**
  - Access to Information (Physical, Electronic, Remote) Policy 1105
  - Clinical Information System User Deactivation Procedures 1105-01
  - Remote Access Standard 1105-02
  - Multi-Factor Authentication Standard 1105-03
  - Contractor Requirements for Security and Privacy of Information and Information Technology Resources Policy 1107
  - Information Technology Acceptable Use Policy 1109
  - Transmission of Information by Facsimile or Electronic Mail Policy 1113
  - Emailing Personal Identifiable Health Information Procedures 1113-01
  - Business Continuity Planning for Information Technology Resources Policy 1140
  - Change Control for Information Technology Resources Policy 1141
  - Information Security and Privacy Safeguards 1143
  - Monitoring and Auditing of Information Technology Resources Policy 1144
  - Cloud Computing Security Standard 1197
  - Virus and Malicious Code Protection Standard ITSC-10-00410

Research & Data Matching

Research

HSS permits the use and disclosure of information for the purpose of research in accordance with the *Health Information Act* (HIA) and the *Protection of Privacy Act* (POPA); and any conditions set by HSS and/or for a Research Ethics Board (REB). A privacy assessment and/or Privacy Impact Assessment is required when a repository is created to facilitate research or quality improvement initiatives. Disclosure agreements are required, in accordance with the HIA and POPA, where information is disclosed by a PHA/PHC for research purposes.

Repository owners must ensure that researchers have signed appropriate disclosure agreements with HSS before disclosing information to researchers. Further, disclosure agreements are required when information is disclosed by HSS for research purposes. Disclosure agreements are not required for activities related to non-Research Ethics Board approved quality improvement, program evaluation or education of health services providers.

HSS does not permit researchers to directly approach patients to invite them to participate in research.

Data Matching

Data matching occurs when personal or health information is linked between two or more databases or electronic sources of information to create new data which identifies the individual, called data-derived from personal information (as per POPA). HSS permits data matching in accordance with the *Protection of Privacy Act* (POPA) and the *Health Information Act* (HIA).

Data matching must not create harm for the individuals that the information is about, and the result of the data matching project must be in the public interest. Prior to conducting data matching a PIA is required.

Personal information cannot be collected specifically for the purpose of data matching. Personal information for data matching must only be collected from another public body.

Data matching is only permitted for:

- Research and analysis,
- Planning, administering, delivering, managing, monitoring or evaluating a program or service, or
- One or more prescribed purposes.

Supporting Documentation

- **Best Practices & Guidance**
  - Data Disclosure Requirements: Health Information Disclosures to External Parties
  - Guidelines for the Disclosure of Health Information
  - Requests for data from Outside AHS (Data Disclosures) Workflow
- **Forms**
  - Research/Non-Research/Data Request Form
- **Policies & Procedures**
  - Research Information Management Policy 1146
  - Approaching Patients about Research and Clinical Trial in Alberta Health Services Settings Procedure 1146-01

Education & Training

Health Shared Services (HSS) provides robust learning support, including, but not limited to, new employee orientations, required organizational learning and leadership development. Education and training materials endorsed by the HSS Information & Privacy team are listed below.

Mandatory Training

- Required Organizational Learning (ROL) – InfoCare – On Our Best Behaviours is mandatory privacy and information security training for all affiliates and employees at hire.

  This course fulfills the Annual Continuing Education requirements for Privacy and Information Security. This course provides an introduction and overview of the InfoCare Behaviours and provides participants with the opportunity to explore how the Behaviours can be applied in their day-to-day tasks. Participants may choose either the clinical or non-clinical path for learning based on their role. Participants will: become familiar with and able to recognize the InfoCare Behaviours; understand how to apply the InfoCare Behaviours in their daily tasks to collect, use and share information appropriately; understand the impact of poor behaviours on patients, co-workers and the PHA/PHC; agree to the terms within the Confidentiality & User Agreement.

Recommended Training

- On-Demand e-Learning Modules

    - Privacy Breach Awareness
      This module provides instruction and tests participant's knowledge in respect to the appropriate collection, use, access and disclosure of health information and personal information; and the consequences that may apply when a privacy breach occurs. Participants will understand how to identify and report privacy breaches; how to identify practical ways to prevent privacy breaches; the consequences of privacy breaches.

    - HIA Awareness
      Overview of Alberta's Health Information Act (HIA), including individual's right of access, collection, use, disclosure, retention and disposal of health information. Users will understand the appropriate collection, use, disclosure and retention of health information under the HIA; the key terms with respect to the HIA including collection, use, disclosure, custodian, affiliate, PIA, research, 'need to know' and 'least information'; the rights and powers granted to an individual under the HIA. Participants will also learn how to appropriately collect and use health information and ensure all disclosures of health information are necessary and appropriate.

    - POPA Awareness
      Overview of Alberta's Protection of Privacy Act (POPA), including a public body's duties specific to the collection, use, disclosure and safeguarding of personal information. Participants will: understand the duties of a public body when collecting, using, disclosing and safeguarding personal information; define key terms with respect to POPA including 'data derived from personal information', 'non-personal data', and 'synthetic data'; be able to apply best practices for appropriately using personal information; understand a public body's responsibilities specific to Mandatory Breach Reporting.

    - ATIA Awareness
      Overview of Alberta's Access to Information Act (ATIA), including an individual's right of access and a public body's duties in responding to information access requests. Participants will understand: the rights and powers of an individual to make and access to information request; key terms with respect to ATIA including affiliate, personal information, business information, informal request and formal request; how to respond to a Call for Records request, including

conducting a thorough search; and how responsive records are processed once they are provided in response to a Call for Records request.

- EPIC – Connect Care Appropriate Access
  This course is designed to outline a user's responsibility when using Connect Care. The course will review appropriate system use, the importance of safeguarding patient information and consequences if a breach occurs in Connect Care. At the end of this course participants will be able to: define and describe appropriate use; safeguard information against unauthorized access, disclosures, or misuse; identify practical ways to prevent privacy breaches; know how to obtain personal health information properly.

- Records Management – Official and Transitory Records
  This course expands participant knowledge of official and transitory records, including: how the way they manage records can bring risk to the participant and the organization; the difference between Official and Transitory records, including examples of each; approved record storage locations based on if a record is official vs. transitory; retention and destruction requirements; common scenarios and use cases.

- Records Management – Records Retention Schedule
  This course will enhance participant knowledge of the AHS Records Retention Schedule. The Records Retention Schedule applies to any medium of record (paper, electronic, or hybrid) that must be retained for a specific period of time. It identifies how to classify records, how long to keep records, when the retention starts, and what to do with records that have met their retention. Participants will: gain an understanding of the Records Retention Schedule; learn how to maintain the Records Retention Schedule effectively; be able to use the interactive Records Retention Schedule to identify retention requirements for their records; be able to apply proper procedures for destroying records covered by the Records Retention Schedule.

- Instructor-Led Training

  - ATIA – Creating Records with ATIA in Mind
    This virtual course will provide tips and tricks on creating records with the Access to Information Act (ATIA) in mind. Employees should be able to provide advice to decisions makers to allow them to arrive a well-reasoned decisions without fear of being wrong or appearing foolish if these frank deliberations

were made public. Often it is how something is written that will determine whether or not advice can be withheld from disclosure. Participants will: understand the best language to use when providing advice in documents; understand how to structure documents so that advice can be easily identified and redacted; have a high-level understanding of the reasons why redactions can and cannot occur (e.g. business information, personal information, advice).

- ATIA – Call for Records
  This virtual course provides instruction on the legal responsibilities of employees and organizational processes with regard to the Access to Information Act (ATIA) access to information requests. It addresses the Call for Records process, when fee estimates occur, how timelines work and what happens prior to records being released. It will also have targeted information management tips and tricks to make the ATIA access request process smoother. Participants will understand: when a Call for Records is issued and how to respond if they receive one; when the fee estimate process should be initiated; legislated timelines for responding to ATIA access requests; how records are evaluated and redacted prior to being released; records management skills to assist them to respond to ATIA access requests.

- ATIA / POPA – Disclosing Employee Information
  This virtual course will provide guidance on appropriately responding to employee information requests from third parties. Topics covered include a review of applicable sections of the Access to Information Act (ATIA); requirements of third parties making a request; and examples of common requests including WCB, Service Canada, Canada Revenue Agency, Professional Regulatory Bodies, Law Enforcement, Lawyers and Insurance Companies. Participants will understand when disclosures of personal information are authorized by ATIA; the requirements of third parties making the request; and review examples of standard responses for the most common third-party employee information requests received by organizations supported by HSS Privacy.

- Targeted Training

  - New Manager Prep Program (NMPP)
    Virtual sessions provided for managers. The course focuses on the application of privacy legislation & InfoCare behaviours in practical situations.

- Human Resources Business Partnership (HRBP) Orientation
  Virtual sessions provided for all HRBP new hires across the province. Course focuses on ATIA/POPA including appropriate collection, use and disclosure, creating records with ATIA in mind, responding to information access requests, and disclosing employee information.

- Protective Services Orientation Program
  Virtual sessions provided for the Edmonton & Calgary new hire classes. Course covers privacy legislation, appropriate collection of information, disclosure with consent, and disclosure without consent as applied to Protective Services scenarios.

- Volunteer Privacy Orientation
  Video must be viewed by all volunteers who will not require access to HSS-managed systems.

- **Customized On-Demand Training**

  Our knowledgeable team of Privacy Business Advisors develops training specifically to meet the needs of teams supported by Health Shared Services (HSS). Presentations may be provided online or in person.

Privacy Literacy Resources

- **InfoCare**

  InfoCare is the central source for information on privacy and information security at HSS. The program promotes a culture of Information Access and Privacy based on the building blocks of the 10 InfoCare Behaviours found in Policy 1177.

  - InfoCare Moments
    Monthly InfoCare moments are available to all Custodians and Affiliates supported by the HSS Information & Privacy Team. These moments highlight timely privacy and information security guidance and are available on Provincial Health Agency (PHA) /Provincial Health Corporation (PHC) intranet sites.

  - InfoCare Resources
    Developed to help healthcare workers apply the InfoCare Behaviours/Privacy legislation in their daily tasks. Resources include posters, one pagers, FAQs, videos and more.

- InfoCare Coaches Network

  There are over 450 coaches across the provincial healthcare system representing all Provincial Health Agencies (PHA) and Provincial Health Corporations (PHC). This program creates a culture of shared responsibility and ownership for privacy & information security, empowers peer-to-peer support and encourages regular conversations about privacy & information security. All coaches receive an orientation, exclusive monthly materials to share with their teams, and quarterly coaches councils to expand their confidence with privacy and information security matters.

- **30 Second Pauses**

  30 Second Pauses highlight some recent examples of privacy breaches from real HSS-supported employees and how they could have been prevented. All names and identifying information have been removed to protect those affected.

- **Privacy Report Cards**

  Sent to members of the Provincial Health Corporation (PHC) and Provincial Health Agency (PHA) executive teams quarterly. Provides portfolio updates on key privacy indicators including training, breaches, access requests, privacy impact assessments and InfoCare coaches.

Supporting Documentation

- **Best Practices & Guidance**
  - InfoCare Insite page
  - Information & Privacy Insite page
- **Policies & Procedures**
  - Contractor Requirements for Security and Privacy of Information and Information Technology Resources Policy 1107
  - Information Security and Privacy Safeguards Policy 1143