AIMS Administrative Information Management System

AIMS SERVICE AND ACCESS POLICY

1 Note

1. YOUR ACCESS TO AIMS IS CONDITIONAL ON YOU AND THE ORGANIZATION YOU ARE ASSOCIATED WITH AGREEING TO COMPLY WITH AND BE LEGALLY BOUND BY THIS SERVICES/ACCESS POLICY.

2. PLEASE REVIEW IT CAREFULLY.

3. IF YOU ARE EMPLOYED BY OR ASSOCIATED WITH THE SASKATCHEWAN HEALTH AUTHORITY OR THE SASKATCHEWAN CANCER AGENCY: BY ACCESSING AIMS, YOU ARE CONFIRMING THAT YOU ARE AWARE OF YOUR ORGANIZATION'S POLICIES, PROCEDURES, AND WORK STANDARDS, AND THAT (TO THE EXTENT APPLICABLE) YOU AGREE TO ACT IN COMPLIANCE WITH THEM WHILE USING AIMS.

4. IF YOU ARE EMPLOYED BY OR ASSOCIATED WITH ANY OTHER AUTHORIZED PROVIDER ORGANIZATION (SERVICE RECIPIENT), PLEASE READ THIS POLICY CAREFULLY. BY ACCESSING AIMS: (I) YOU CONFIRM YOU ARE AUTHORIZED BY YOUR ORGANIZATION TO ACCESS AIMS; (II) YOU AGREE TO COMPLY WITH AND BE LEGALLY BOUND BY THE PROVISIONS OF THIS SERVICES/ACCESS POLICY; AND (III) YOU ARE CONFIRMING THAT YOU ARE AWARE OF YOUR ORGANIZATION'S POLICIES, PROCEDURES, AND WORK STANDARDS AND THAT (TO THE EXTENT APPLICABLE AND NOT INCONSISTENT WITH THIS POLICY) YOU AGREE TO ACT IN COMPLIANCE WITH THEM WHILE USING AIMS.

5. NOTHING IN THIS POLICY SHALL ALTER THE LEGAL RIGHTS OR OBLIGATIONS OF SERVICE RECIPIENTS UNDER APPLICABLE PRIVACY OR OTHER LAWS.

6. THIS SERVICE/ACCESS POLICY IS INCORPORATED INTO THE 3SHEALTH AMS AND AIMS CUSTOMER FEE AGREEMENT.

2 High Level Policy

This Policy applies to the Administration Information Management System implemented by 3sHealth on behalf of the Saskatchewan health system in Saskatchewan (**AIMS**).

The data included in AIMS includes personal information (PI) and personal health information (PHI), as well as other confidential and sensitive information (collectively the **AIMS Data**). The AIMS Data must be maintained in confidence and treated as confidential. In addition, as discussed below, the Service Recipients who store and process the PI and PHI of their employees and patients/customers within AIMS are subject to specific privacy laws.

Access and use of the AIMS Data is restricted to authorized purposes only as described in this Policy. Access or use (including viewing and secondary use) or disclosure for any other purpose is strictly prohibited.

3 Background

Health Shared Services Saskatchewan (**3sHealth**), on behalf of the Saskatchewan Health Authority (**SHA**), Saskatchewan Cancer Agency (**SCA**), and their affiliate organizations, and other health-care organizations (collectively, the **Service Recipients**), and with the approval of the Government of Saskatchewan, launched a provincial initiative to transform and consolidate the manner in which administrative information services are delivered in the Province of Saskatchewan by procuring AIMS.

AIMS is intended to operate as a province-wide administrative information management system solution to provide enterprise resource planning functionality including human capital management, finance, supply chain, and business intelligence to the Service Recipients (the **AIMS Services**). The specific AIMS Services to be provided to a specific Service Recipient will be documented in the AMS and AIMS Customer Fee Agreement signed by the Service Recipient.

4 Information Classification

The AIMS Information Classification Policy provides a description of the various applications making up AIMS and the associated data elements, including the identification of Personal Information (PI) and Personal Health Information (PHI) included in AIMS.

The AIMS Information Classification Policy includes the following seven classification levels for classifying information:

1. Public Information;
2. Employment Information;
3. Internal Information;
4. Confidential Information;
5. Personal Information (PI) – This category includes basic personal information such as name, address, and telephone number;
6. Sensitive PI/PHI – This category includes more sensitive PI, such as SIN and bank account information. This category also includes all PHI. This is essentially the core employment information needed to manage and administer the employment relationship (e.g., Payroll information);
7. Sensitive PI/PHI (Organization Specific) – This is Sensitive PI/PHI that relates to a specific employee and a specific organization. This is most important for Co-Employed Employees where one Service Recipient has entered information into AIMS that cannot be shared with the other employers. A key mitigation step within AIMS is the non-inclusion of Organization Specific information within the core employment record due to legislative and privacy concerns.

5 Information Governance

For information governance purposes, the PI/PHI included in AIMS can be further broken down into the following two categories:

(a) Employment Information (PI/PHI) – The HCM and other applications will include PI and PHI for employees relating to the management and administration of their employment relationship with 3sHealth and the Service Recipients. The PI and PHI will be stored using a single data set for each employee (i.e., there won't be multiple employee records for each organization that employs the individual).

(b) Health Information (PI/PHI) – The Finance application will include limited PHI for patients/customers based on billing for uninsured health services. The PHI will include patient/customer registration information, details on the health service required, and related charges. The patient/customer's registration information will be stored once for each patient in the "customer registry" in the Finance application.

The below chart addresses the different governance situations with respect to Employment Information (PI/PHI) and Health Information (PI/PHI) using the classifications for PI and PHI outlined in the Information Classification Policy.

Health Information (PI/PHI) – Uninsured Services for patient/client – Financial Systems

Type of Information	**Classification**	**Trusteeship/custodianship**	**Authorized Use to support need to know**
Patient/Client Registration Information (Finance Application) Uninsured Services Registration Information	Sensitive PI/PHI (6)	Single trustee/custodian The last Service Recipients who have provided uninsured health services to the individual patient/client and recorded the transaction in AIMS will be the trustee/custodian for that patients/client's registration information. All Service Recipients who provided uninsured services in the past would	Provision of Current Services Facilitate payment for services Manage historical record for past services To confirm accuracy, Service Recipients should confirm all Registration Information with

		have the right to access this information for previous services provided.	the patient/client and confirm accuracy in AIMS
Specific Information for a specific uninsured health service (Finance Application) Uninsured Services Specific Service and Cost	Sensitive PI/PHI (Organization Specific) (7)	Single trustee/custodian The Service Recipient who provided the health service is the sole trustee/custodian	Access restricted in AIMS should be to the Service Provider who provided the Service.

Employment Information (PI/PHI) – Single Employer – HCM

Type of Information	Classification	Trusteeship/custodianship	Authorized Use to support need to know
Employment Information (HCM - Core HR and MyConnection) (Single Employer)	Personal Information (5) & Sensitive PI/PHI (6)	Single trustee/custodian The single employer will be the sole trustee/custodian	Manage and administer the employment relationship
Employment Information Organization Specific (HCM - Core HR and MyConnection) (Single Employer)	Sensitive PI/PHI (Organization Specific) (7)	Single trustee/custodian The single employer will be the sole trustee/custodian	Manage and administer the employment relationship Note: Key mitigation within AIMS is the non-inclusion of Organization Specific information due to legislative and privacy concerns.

Employment Information (PI/PHI) – Co-Employed – HCM

Type of Information	Classification	Trusteeship/custodianship	Authorized Use to support need to know
Employment Information (HCM - Core HR and MyConnection) (Co-Employed)	Personal Information (5) & Sensitive PI/PHI (6)	Co-trustees/custodians All Employers for the co-employed individual are co-trustees/custodians for the co-employed employee's information	Manage and administer the employment relationship To confirm accuracy, Service Recipients should confirm all Employment Information and confirm accuracy in AIMS
Employment Information Organization specific (HCM - Core HR and MyConnection) (Co-Employed)	Sensitive PI/PHI (Organization Specific) (7)	Single trustee/custodian The Service Recipient who entered the information is the sole trustee/custodian for the information entered by them	Manage and administer the employment relationship Access in AIMS should be restricted to the Employer who entered the information Note: Key mitigation within AIMS is the non-inclusion of Organization Specific information due to legislative and privacy concerns.

Employment Information (PI/PHI) – Successor Employers – HCM

Type of Information	Classification	Trusteeship/custodianship	Authorized Use to support need to know
Employment Information (HCM - Core HR and MyConnection) (Successor Employers)	Personal Information (5) & Sensitive PI/PHI (6)	Single trustee/custodian The Current Employer will be the sole trustee/custodian of the employed individual's record. All Previous Employers of the employed individual will have a right of access to the historic portion of the employed individual's record as it relates to the time the Employee was engaged by the specific Previous Employer.	Current Employer: Manage and administer the current employment relationship Previous Employer: Manage the historical record – past relationship. After trustee/custodianship transfers, the previous employer will have the right to request a copy of the historical employment record To confirm accuracy when hiring the employee, Service Recipients should confirm all Employment Information and confirm accuracy in AIMS
Employment Information (Organization specific) (HCM - Core HR and MyConnection) (Successor Employers)	Sensitive PI/PHI (Organization Specific) (7)	Single trustee/custodian The Service Recipient who entered the information is the sole trustee/custodian for the information entered by them	Manage and administer the employment relationship Access in AIMS should be restricted to the Employer who

			entered the information Note: Key mitigation within AIMS is the non-inclusion of Organization Specific information due to legislative and privacy concerns.

The chart above includes the concept of co-trustees/custodians. For example, this is the case for co-employed employees.

The concept of co-trustee/custodians arises where two organizations have control over PI or PHI. Each of the co-trustees/custodians will retain all their rights and obligations under applicable legislation. In a co-employment situation, the employers will need to work together to address any accuracy or privacy concerns raised by the co-employed employee.

For more information, please refer to the AIMS Information Governance Model.

For the purposes of this Policy, a Service Recipient will be referred to as the "Associated Service Recipient" where it is the trustee/custodian or co-trustee/custodian for PI and PHI as determined using the chart above.

6 Scope and Purpose

This Policy applies to:

a) all Service Recipients who create, store, and access AIMS Data within AIMS;
b) all employees or contractors employed or engaged by the Service Recipients, who access the AIMS Data within AIMS (the "**Users**").

The purpose of this Policy is to:

a) act as a data access/sharing agreement setting out responsibilities and rules of access for the Service Recipients and their Users to the AIMS Data; and
b) act as an information management services agreement between each Service Recipient and 3sHealth, SHA, and the other Service Providers.

7 Legislative Authority – Varies based on the Service Recipient

The Freedom of Information and Protection of Privacy Act (**FOIP**).

The Local Authority Freedom of Information and Protection of Privacy (**LAFOIP**).

The Health Information Protection Act (**HIPA**).

The Health Shared Services Saskatchewan (3sHealth) Act (the **3sHealth Act**).

8 Supporting Documents

Your Organization’s Privacy and Security Policies.

9 MyConnection

A copy of this policy and the related documents will be maintained under the Privacy Tab on MyConnection.

10 Detailed Privacy Policy

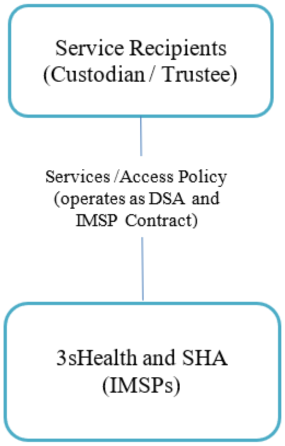
10.1 Accountability

Please see the chart above regarding accountability and trusteeship/custodianship for the Personal Information (PI) and Personal Health Information (PHI) in the AIMS Data.

Each Service Recipient shall:

(a) appoint an individual who will be responsible for privacy for AIMS;
(b) with respect to AIMS Data within their trustee/custodianship or control or systems within their trustee/custodianship or control, establish policies and procedures to maintain administrative, technical, and physical safeguards that will:
  (i) protect the integrity, accuracy, and confidentiality of AIMS Data;
  (ii) prevent the loss of AIMS Data; and
  (iii) prevent the unauthorized access to or use, disclosure, or modification of AIMS Data;
(c) ensure they have appropriate safeguards in place and are otherwise in compliance with HIPA, FOIP, LAFOIP, or other applicable privacy or other laws; and
(d) ensure all staff and personnel accessing AIMS have completed appropriate privacy and security training. Supplemental privacy training resources are available on the MyConnection Privacy Tab.

3sHealth and SHA will be acting as information management service provider for AIMS for the Service Recipients.



3sHealth will coordinate services from the Other Service Providers. It is important to note that 3sHealth has PI and PHI within AIMS for its own employees and will be responsible and accountable as the custodian/trustee for the PI and PHI for its employees.

Each Service Recipient will be asked to sign a 3sHealth AMS and AIMS Customer Fee Agreement that will document the particular services and fees specific to the Services Recipient.

Please see Schedule A for additional legal terms that apply to the Services being provided by 3sHealth and SHA and the other Service Providers.

Each Service Recipient hereby authorizes the sharing of AIMS Data by 3sHealth and its authorized representatives as follows:

- with the other Service Recipients as specifically authorized in this Policy;
- to SAHO Inc. and the Ministry of Health as authorized by law or the applicable collective bargaining agreement. For example, aggregate employment information is provided to SAHO Inc. for the purposes of facilitating and supporting the collective bargaining process;
- other third parties as authorized under the applicable collective bargaining agreement; or
- as otherwise authorized by the applicable Service Recipient.

10.2 Additional Policies/Procedures

The Service Recipients and their Users accessing AIMS agree:

(a) to follow the policies and procedures provided by 3sHealth from time to time.

3sHealth will make sure all Service Recipients are made aware of any new policies or procedures;

(b) to comply with any reasonable AIMS communications, guidelines, or protocols provided by 3sHealth to the Service Recipients from time to time;

(c) to respect all User and access restrictions within AIMS; and

(d) to ensure they have confirmed they have obtained the appropriate level of consent (express, implied, or no consent) for any particular collection, use, and/or disclosure of the AIMS Data. The Service Recipient remains responsible to management consent with their employees and patients.

10.3 Limiting Collection, Use, and Disclosure

Each Service Recipient and its Users may only access (use) AIMS Data for which it is the Associated Service Recipient as determined in accordance with the above chart (for example, the Employee Data should only be accessed to manage and administer the employment relationship). Further, each Service Recipient and its Users should only access and use the AIMS Data on a need-to-know basis in accordance with the above chart.

10.4 Accuracy

All Service Recipients and their authorized Users will take reasonable steps to ensure the accuracy and currency of any information entered into or updated by them within AIMS.

Where required, the Service Recipients will confirm information within AIMS is accurate directly with the individual patient/client or individual employee.

10.5 Safeguards

Each Service Recipient agrees that appropriate physical, organizational, and technological measures will be put in place within their organization to protect the security and confidentiality of the AIMS Data and to ensure that this data is only used on a need-to-know basis for the purpose set out in the above chart.

Each Service Recipient agrees to follow any reasonable security procedures delivered by 3sHealth to the Service Recipients.

Each Service Recipient will be responsible to ensure it has a reasonable cybersecurity program in effect to prevent cybersecurity breaches and ransomware attacks and has a reasonable incident response plan in place to effectively deal with cybersecurity breaches and ransomware attacks should they occur.

10.6 Openness

Each Service Recipient will ensure that employees and patients/clients have reasonable access to the organization’s privacy and security policies and procedures.

10.7 Individual Access/Amendment

All requests by employees or patients/clients to access or amend their AIMS Data within AIMS will be referred to the accountable Service Recipient(s) as per the chart above in Section 4 of this Policy.

3sHealth will provide reasonable assistance under the direction of the accountable Service Recipient.

10.8 Complaints

All complaints relating to AIMS will be referred to the Associated Service Recipient(s).

All Service Recipients agree to have appropriate and reasonable policies, procedures, and forms to address privacy concerns or complaints raised by employees or patients/clients.

Any unresolved complaints may be forwarded by the complainant to the Office of the Information and Privacy Commissioner (Saskatchewan).

10.9 Limits on Authority

For greater certainty and notwithstanding anything in this Policy, except for PI/PHI for employees of 3sHealth, 3sHealth has no ownership or control over the PI/PHI stored or processed in AIMS. The Service Recipients retain all ownership and control over the PI/PHI for employees and patients/clients as described in the chart above.

10.10 Amendment

This Policy may be amended from time to time by 3sHealth and all amendments will only be effective when delivered to the Service Recipients.

10.11 Service Recipients’ Authority

This Policy is not intended to be a delegation of any authority or discretion of a Service Recipient under HIPA, FOIP, LAFOIP, or any other applicable laws. At all times, each Service Recipient maintains control of the AIMS Data for which it is the Associated Service Recipient as determined in accordance with the chart listed above.

10.12 Breach Reporting Obligations

All Service Recipients will report security or privacy incidents involving the AIMS Data to the 3sHealth Privacy Officer, who will then refer privacy complaints and concerns to the applicable organization's privacy officer(s). As much information as can be provided must be provided to the 3sHealth Privacy Officer.

3sHealth will advise the Associated Service Recipient of any security or privacy incidents involving the AIMS Data.

5 Schedule "A"

3SHEALTH SERVICE TERMS AND CONDITIONS

1. Restrictions on Use and Disclosure of AIMS

Each Service Recipient agrees:

(a) to take all reasonable steps to protect and maintain the confidentiality of the software and systems associated with AIMS, at all times using the same care and discretion to avoid disclosure or dissemination of the AIMS Data as the Service Recipient uses with its own confidential information;

(b) to take all reasonable steps to prohibit, and to cooperate with 3sHealth in the prohibition of, the reverse engineering, decompilation, or disassembly of AIMS, or the making of derivative works of AIMS; and

(c) to limit access to AIMS to those Users who have a need to know, and Users agree to only access AIMS for that purpose.

2. Service Recipient Responsibilities

Each Service Recipient will be responsible for the following:

(a) Managing and being responsible for all Users and user IDs authorized by them. This will include:

(i) determining who is to access the AIMS Data and the appropriate level of access for each User and User Role; and

(ii) advising 3sHealth as soon as possible of any User who has been terminated or who may pose a security risk. It is important that 3sHealth is advised as soon as possible so that appropriate steps may be taken to disable the User's user ID;

(b) ensuring all staff attend training sessions recommended by 3sHealth;

(c) granting representatives of 3sHealth reasonable access to any end-user system, which access includes without limitation both physical access and electronic access via telecommunications or other network connections, for the purpose of managing the application and monitoring/auditing access and use. This access will (except in emergency circumstances) be subject to reasonable notice and consultation with the Service Recipient; and

(d) Each Service Recipient will be responsible to ensure it has a reasonable cybersecurity program in effect to prevent cybersecurity breaches and ransomware attacks and has a reasonable incident response plan in place to effectively deal with cybersecurity breaches and ransomware attacks should they occur.

3. **<u>3sHealth Responsibilities</u>**

3sHealth agrees to be responsible for the following:

(a) providing the 3sHealth Services to the Service Recipient;

(b) maintaining all AIMS Data in strict confidence;

(c) accessing and using the AIMS Data only for the following purposes:

(i) use or disclosure of the AIMS Data to the extent necessary to provide the 3sHealth Services; and

(ii) any other purpose authorized in writing by the applicable Service Recipient; and

(d) to ensure appropriate and reasonable safeguards are in place to protect the AIMS Data and to ensure the accuracy and integrity of the AIMS Data when it is within systems or networks within 3sHealth's control.

4. **<u>Disclaimer and Limitation of Liability</u>**

(a) 3sHealth will take reasonable steps to maintain the availability of AIMS and 3sHealth Services, and will ensure AIMS contains reasonable safeguards to protect the accuracy and integrity of the AIMS Data.

(b) The 3sHealth Services, as well as AIMS and other 3sHealth-provided applications accessible by the Service Recipients, are provided on an "as is" and "as available" basis. There is no warranty or guarantee that the 3sHealth Services or AIMS will be available, or that the AIMS Data contained therein will be accurate or complete. It is expressly recognized that the AIMS Data may be incomplete and should be reviewed with subject employees/patients for completeness and accuracy by the Service Recipients and their authorized Users;

(c) Use of AIMS and the AIMS Data is at the Service Recipient's sole risk and is in no way intended to replace or be a substitute for professional judgment;

(d) In no event will 3sHealth, SHA, the Service Providers or their employees, contractors or agents be liable for any special indirect or consequential damages for any act or omission, regardless of whether the action for such damages is brought in tort, including without limitation negligence and contract including without limitation fundamental breach; and

(e) The total aggregate liability limit for 3sHealth, SHA, or any of the other Service Providers to each Service Recipient will be limited to actual direct damages not to exceed the fees paid by that specific Service Recipient for the Services for the past six months.

5. **<u>Security Notice</u>**

(a) 3sHealth and the Service Providers may monitor access to AIMS to protect the AIMS Data and security of AIMS. By accessing AIMS, the Service Recipients and their Users are expressly consenting to these monitoring activities.

6. **<u>Termination</u>**

(a) 3sHealth may terminate a Service Recipient's access to the 3sHealth Services immediately upon material breach of this Schedule or the Policy by the Service Recipient or its Users and failure to cure the breach within 10 days of written notice of the breach;

(b) The Service Recipients may terminate the 3sHealth Services:

(i) without cause as stated in the 3sHealth AMS and AIMS Customer Fee Agreement; or

(ii) immediately upon material breach of this Schedule or the Policy by 3sHealth and failure to cure the breach within 10 days of written notice of the breach;

(c) Upon termination of a Service Recipient's access to AIMS, the employee/patient data for that the Service Recipient will be transferred to the Service Recipient. The Service Recipient will be responsible for all reasonable costs associated with such transfer and termination (if the termination was on a without cause basis).

AIMS SERVICE AND ACCESS POLICY

10	**Approval Date**	*This policy was approved on*: **June 19, 2024**
11	**Review Date(s)**	*This policy needs to be revised on*: **June 19, 2025**
12	**Enquiries**	Any questions or clarification required should be referred to the 3sHealth Privacy Officer at InformationManagement@3sHealth.ca
13	**Policy Owner**	3sHealth Privacy Officer