AIMS Administrative Information Management System

AIMS INFORMATION CLASSIFICATION POLICY

1	Policy
	Appropriate levels of security measures must be applied to all information assets after determining the criticality and sensitivity requirements of the information through the use of risk assessment and classification. As part of the overall control environment for the protection of AIMS information/data, the classifications outlined in this Policy will guide the development of privacy and security requirements, policies, and controls.

2	Service Recipients
	AIMS will support the administrative functions of 3sHealth, Saskatchewan Health Authority (SHA), Saskatchewan Cancer Agency (SCA), and other service recipients of 3sHealth as defined from time to time (Service Recipients). It is important to note that 3sHealth is both the information management service provider (IMSP) for the Project and is also the trustee/custodian of its own information within AIMS.

3	Information Governance
	AIMS is a provincial system with 3sHealth and Other Service Providers providing information technology and management services and supporting business services to the Service Recipients. It is important to note that 3sHealth is using AIMS to manage its own business affairs and will be the custodian of the Personal Information (PI), Sensitive PI/Personal Health Information, and Sensitive PI/PHI (Organization Specific) entered on behalf of its employees. As it relates to PI, Sensitive PI/PHI and Sensitive PI/PHI (Organization Specific) (as defined in this Policy), the application and data architecture for AIMS creates situations where a Service Recipient that enters the information in AIMS will be the sole trustee/custodian of the information, but also where multiple Service Recipients access and enter information on the same record and will be co-trustees/custodians of the information. For more information, refer to the Information Governance Model as described in the AIMS Services/Access Policy.

4	AIMS Privacy Committee
	There is a supporting committee structure to support the information governance model discussed above.

5	Applicable Legislation
	The SHA and SCA are subject to the provisions of The Local Authority Freedom of Information Act (Sask) (LAFOIP) and The Health Information Protection Act (Sask) (HIPA). All of the other Service Recipients are also subject to LAFOIP, HIPA, or other similar privacy

	legislative or common law standards. It is important to note that this Policy and the controls included are subject to all Applicable Legislation.

6	Application
	This Policy covers all information owned, processed, and/or managed by AIMS and covers all users of the system (Users) whether employed by the Service Recipients, 3sHealth, or Other Service Providers

7	Ownership
	As per the information governance model discussed above, depending on the information in question, the ownership of the information within AIMS may be determined according to a single trustee/custodian model or co-trustees/custodians model. For more information, refer to the Information Governance Model.

8	AIMS Policies
	There will be other privacy and security requirements, policies, and controls put in place and approved in accordance with the proposed Information Governance Model to support AIMS. 3sHealth, in its role as information management service provider (IMSP), will only use and disclose information (other than Public Information) to provide the services. If information is to be used or disclosed outside of the services, the matter will be referred to the source Service Recipient(s). Public Information can be used and disclosed by 3sHealth as it sees fit.

9	Authority
	3sHealth is continued as a corporation under *The Health Shared Services Saskatchewan (3sHealth) Act* (3sHealth Act). 3sHealth receives its authority from and is governed by the 3sHealth Act. The 3sHealth Act empowers 3sHealth to provide services and participate in activities that will contribute to the health-care system in Saskatchewan. Specifically, when it comes to AIMS, Section 2-4(2)(a)(iii) of the 3sHealth Act empowers 3sHealth to establish, operate, administer, support, or manage financial, human resource, supply chain, and workforce management systems and programs.

4	Process
	Responsibilities 3sHealth must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information. Unique circumstances will be referred to the custodian/trustee Service Recipient(s). **Information Classification Categories** AIMS uses seven classification levels for categorizing information. The lowest level reflects

the least sensitive and the higher levels reflect the most sensitive information.

Once data on a system module has been classified into one of the seven levels, then that module should be installed and configured to conform to all directives for that classification and the ones below it. Each of the levels is a superset of the previous level.

1. Public Information

This classification applies to information that is public in nature and not subject to any confidentiality restrictions.

Some examples of information that fall under this category are as follows:

- Marketing material (fact sheets, brochures, etc.);
- Published research material;
- Job opening announcements;
- Press releases; and
- Material on the AIMS website.

2. Work Information

This classification applies to information that relates to the work to be completed by an employee or contractor or their job description.

Information falling in this category can be shared by organizations for the purposes of facilitating and managing the employment relationship.

The information will generally be used for internal use of the organizations and is not included in the definition of personal information under LAFOIP.

Some examples of information that fall under this category are as follows:

- Job description;
- Hours of work and location;
- Scheduling;
- Leave requests;
- Reports including employee name, number, and schedule; and
- Work product.

3. Internal Information (not including Confidential Information)

This classification applies to information that generally relates to communications between

employees that are not approved for general circulation outside AIMS. Its unauthorized disclosure would inconvenience AIMS but would not likely result in financial loss or reputational damage.

The information will generally be used for internal use of the organizations and is not included in the definition of personal information under LAFOIP.

Some examples of information that fall under this category are as follows:

- Internal announcements; and
- Internal e-mails and chats.

4. Confidential Information (not including Personal Information [PI])

This classification applies to sensitive organizational information which is intended strictly for use within AIMS. Its unauthorized disclosure could adversely impact an organization's employees, its service providers, its business partners, and/or its patients.

Information falling into this category must be controlled from creation to destruction. Such information must be made available only to the specific individuals who have the need and the right to know.

Some examples of information that fall in this category are as follows:

- Financial information (e.g., departmental budgets, payroll, general ledger balance, etc.);
- Technical information (e.g., encryption keys, IP addresses, passwords, etc.);
- Event reports (e.g., security event reports, issue event reports, etc.);
- Vendor confidential information (e.g., vendor information in contract bids, information in service contracts including fee per hour, etc.); and
- Vendor/supplier financial information.

5. Personal Information (PI)

This classification applies to information which is personal to a specific individual. Its unauthorized disclosure is prohibited by Applicable Legislation, and could adversely impact an organization, its employees, and/or its patients.

Personal Information (PI) must be controlled from creation to destruction. Such information should only be accessed by the specific individuals who have a need to know.

Some examples of information that fall in this category are as follows:

- A person's name and addresses;
- Telephone number; and
- Personal email address.

6. Sensitive PI/Personal Health Information (PHI)

This classification applies to information which is personal to a specific individual and of a particular sensitive nature, including personal health information. Its unauthorized disclosure is prohibited by Applicable Legislation and could adversely impact an organization, its employees, and/or its patients.

Sensitive PI/PHI must be tightly controlled from creation to destruction. Such information should only be accessed by the specific individuals who have a need to know.

Some examples of information that fall in this category are as follows:

- Personal health information;
- Personal financial information (e.g., bank account information or bank account numbers);
- A person's name in combination with any of the information listed here;
- Date of birth;
- Date of death;
- Country/Town/Region of birth;
- Credit card number;
- Passport number;
- Visa number or work permit;
- Tax registration number or national taxpayer identifier (e.g., SIN);
- Disabilities; and
- Driver's licences.

7. Sensitive PI/PHI (Organization Specific)

This classification applies to information which is personal to a specific individual, of a particularly sensitive nature. It may apply where information is unique to an employee's employment relationship with a single, specific employer, or where information is unique to a single Service Recipient providing a health service to a unique client/patient.

Sensitive PI/PHI (Organization Specific) must be tightly controlled from creation to destruction. Such information is not required to be shared and must only be accessed on a need-to-know basis by representatives of the specific Service Recipient that enters the information in the system.

AIMS INFORMATION CLASSIFICATION POLICY

	Sensitive PI/PHI (Organization Specific) should only be accessed by the Service Recipient that entered the information, unless: • **There is other legal authorization (e.g., authority under a common collective bargaining agreement);** • **Other authority under applicable legislation; or** • **The express consent of the individual has been obtained.** Sensitive PI/PHI (Organization Specific) should not be included in AIMS where it can be accessed by multiple organizations. Sensitive PI/PHI (Organization Specific) can be included in AIMS where its access is limited to the appropriate organization or Service Recipient and appropriate safeguards are in place. Each Service Recipient is responsible for determining whether it will include Sensitive PI/PHI (Organization Specific) in AIMS. Where a Service Recipient decides to include Sensitive PI/PHI (Organization Specific) in AIMS, it is responsible for ensuring appropriate policies and safeguards are in place to ensure that such information can only be accessed by the appropriate organization or Service Recipient. This issue will require ongoing management and communication with the Service Recipients.

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