

INFORMATION MANAGEMENT AGREEMENT

THIS AGREEMENT is made effective as of the __14th__ day of July, 2020.

BETWEEN:

THE GOVERNORS OF THE UNIVERSITY OF CALGARY
(referred to as "University")
- and -

ALBERTA HEALTH SERVICES
(referred to as "AHS")

WHEREAS:

- A. AHS' Analytics - Enterprise Data Warehouse Services team ("AHS Analytics") wishes to utilize a High Performance Computing (HPC) environment for various analytical workloads.
- B. The University can offer an HPC environment with CPU, GPU and high performance storage components, through the University's IT Department's Secure High Performance Computing Cluster (referred to as the "Cluster" in this Agreement).
- C. Section 66(2) of the *Health Information Act* mandates that AHS, as a Custodian, must enter into an agreement with an information manager for the provision of information management or information technology services relating to health information.
- D. The intent of this Agreement is to satisfy the requirements of the *Health Information Act* and to govern the management of AHS' Data by the University using the University's Cluster.

THEREFORE, THE PARTIES TO THIS AGREEMENT WITNESS that in consideration of the premises and of the mutual covenants and agreements herein contained and for other good and valuable consideration, the receipt and sufficiency of which is hereby irrevocably acknowledged, the Parties hereby covenant and agree as follows:

1.0 Definitions

1.1 In this Agreement:

- (a) "AHS Analytics" has the meaning set forth in the recitals to this Agreement.
- (b) "Authorized System Administrators" are technical administrators authorized by the University, with root privilege on the Cluster, as required for standard system maintenance tasks.
- (c) "Authorized User" is a user authorized by AHS and the University in accordance with section 17 to have access to the Data.
- (d) "Cluster" shall mean the MARC cluster, a secure, high performance computing environment and Secure Computing Data Storage (SCDS)

managed by the Information Technologies (IT) department at the University for the purpose of providing the Information Management Services.

- (e) “Custodian” has the meaning set forth in s. 1(1)(f) of the *Health Information Act* (Alberta).
- (f) “Data” shall mean any individual or aggregate source of healthcare and personal health information for which AHS is the Custodian and is provided to the University by AHS related to the Information Management Services provided by the University.
- (g) “FOIP” shall mean the *Freedom of Information and Protection of Privacy Act* (Alberta) and any regulations made thereunder, as may be amended from time to time.
- (h) “Health Information Act” or “HIA” shall mean the *Health Information Act*, R.S.A, 2000, H-5 and any regulations made thereunder, as may be amended from time to time.
- (i) “Information Management Services” means those information services provided by the University listed in Schedule A attached hereto and forming part of this Agreement.
- (j) “Information Product” or “Information Products” means any information output, including, but not limited to aggregated data, tables, figures, and graphics, produced by the efforts of AHS analysts using the Data on the Cluster.
- (k) “Party” or “Parties” shall mean the Parties to this Agreement, as the context requires.
- (l) “Policies” has the meaning set forth in section 4.1 of this Agreement.
- (m) “RCS” has the meaning set forth in section 4.1 of this Agreement.
- (n) “Representatives” means any directors, officers, employees, partners, agents, counsel, professional advisors or other authorized persons who have a need to access the Data for the purpose of providing the Information Management Services to AHS.

2.0 Appointment of Information Manager

- 2.1 AHS hereby appoints the University as an information manager for the purpose of providing AHS with Information Management Services.

3.0 Compliance with HIA and FOIP

- 3.1 The relationship of AHS to the University pursuant to the terms of this Agreement is solely that of Custodian to information manager.

3.2 The University agrees that it is aware of and will comply with the provisions of the *Health Information Act*, FOIP and any other applicable legislation and this obligation shall survive the termination of this Agreement for as long as the University holds or has access to Data.

4.0 Joint Obligations

4.1 Members from AHS Analytics and the University including the University's Research Computing Services group ("RCS"), will meet annually to conduct a review of the AHS Data stored on the Cluster to assess what actions, if any, are required to maintain compliance with the following AHS policies (the "Policies"):

- (a) AHS' Information Security And Privacy Safeguards Policy which is attached hereto as Schedule B and forms a part of this Agreement;
- (b)
- (c) The Server Logging & Auditing requirements set out in Schedule B; and
- (d) AHS' Records Management Policy and associated Data Retention Schedule which is attached hereto as Schedule C and forms a part of this Agreement.

4.2 It is agreed by the Parties that the Cluster and the Data residing on the Cluster shall not be used in the provision of patient care, including but not limited to clinical decision making.

5.0 University Obligations

5.1 In addition to its obligations in section 3.2 above, the University shall only collect and use the Data and Information Products for the purpose set forth in this Agreement and shall provide the Information Management Services in compliance with the provisions set forth below:

- (a) The University will provide AHS with a secure environment for the storing and processing of data. AHS users will be supported through existing University processes as per University regular Service Level Agreement.
- (b) HPC Service Support for the Cluster is provided by the University based on a best effort basis. Such support will be provided during business hours, within priority established by the RCS.
- (c) The University will provide AHS with Data storage for as long as specific projects remain active and shall otherwise comply with the Policies for removal of the Data from the Cluster and any additional directions which AHS may provide from time to time.
- (d) The University agrees that all Data on the Cluster is confidential and shall protect the Data and Information Products against such risks as unauthorized access, use, disclosure, destruction, or alteration by unauthorized users, and shall limit access to the Data to only the Authorized Users in accordance with section 16 of this Agreement.

- (e) Without limiting any other provision, the University shall comply with section 60 of the Health Information Act and section 8 of the Health Information Regulation made under the Health Information Act with respect to the security and protection of the Data. Specifically, the University agrees to implement and maintain reasonable safeguards to maintain the security, protection, availability and integrity of the Data as further described in Schedule A.
- (f) The University shall provide audit logs to designated AHS personnel, as required by the Server Logging Schedule and as otherwise required by AHS upon AHS' reasonable request.

5.2 The obligations of the University under this section 5 shall survive any termination of this Agreement or for as long as University holds or has access to Data.

6.0 AHS Obligations

6.1 In order to support adequate Data life cycle management and access provisioning activities by the University, AHS shall:

- (a) Provide the required Data to the staging area, along with appropriate technical metadata.
- (b) Remove Data from the Cluster and staging area (SCDS) upon completion of individual projects.
- (c) Provide the University with information about respective project team members fulfilling the roles of Information Trustees and Information Stewards (see University of Calgary Information Asset Management Policy) so that University can support access provisioning requests. See Schedule "D" for documentation.

7.0 Authorized Access

7.1 The Parties are authorized to provide access to the Data to those Authorized Users identified by each Party in such a manner as is specifically set forth in accordance with section 17. Each Party is responsible to notify the other Party, in accordance with section 17, of changes to the list of Authorized Users.

8.0 Ownership and Control of Information

8.1 The Parties acknowledge that for the purposes of the Health Information Act, the Data and Information Products remain under the custody and control of AHS.

8.2 If the University receives any request for the Data or Information Products, under the Health Information Act it shall as soon as practical refer such request to AHS.

8.3.1 AHS is under no obligation to provide the University with any Data, and has the right to cease providing Data to the University at any time for any reason.

9.0 Collection from other Custodians or Persons

9.1 The Parties agree and acknowledge that other custodians will be utilizing the Cluster for data storage and analysis, collecting health information that is not AHS' Data. Data will not be shared among information custodians unless authorized under a separate agreement.

10. Requests for Access, Correction, or Amendment of Information

10.1 The University will refer access requests under Part 2 or Part 5, Division 3 of the Health Information Act to AHS. Any request to amend or correct the Data or Information Products shall be referred to AHS. Such referrals shall be made as soon as reasonably practical bearing in mind the statutory time lines for reply inherent in both statutes.

11. Expressed Wish of Individual Relating to the Disclosure of Health Information

11.1 As the Data or Information Products are not collected by the University, any expressed wish of an individual relating to disclosure shall be addressed by AHS at the point of Data collection.

12.0 Breaches, Term and Termination

12.1 If the University becomes aware of a breach of any term or condition of this Agreement it shall immediately notify AHS and, if appropriate, take reasonable steps to remedy the breach.

12.2 The term of this Agreement shall commence on the date this Agreement is signed by both Parties and shall continue until the University no longer provides any Information Management Services, holds Data, or has access to Data, to a maximum of five-years.

12.3 AHS may immediately terminate this Agreement upon written notice to the University with or without cause.

12.4 The University shall discontinue provision of Information Management Services to AHS for the Data should this Agreement be terminated.

13.0 Notice

13.1 Every request, notice, delivery or written communication provided for or permitted by this Agreement shall be in writing and delivered to, or mailed, postage prepaid; email to the Party to whom it is intended as hereinafter set forth; namely

(a) If to the University:

Karen Jackson
General Counsel
University of Calgary
2500 University Dr NW, Calgary, AB T2N 1N4
Ph: (403) 220-4195

(b) If to AHS:

Alberta Health Services

Information and Privacy Office
10101 Southport Road S.W.
Calgary, AB
T2W 3N2
Ph: 403 943-0424

14.0 Amendments and Additions

This Agreement shall not be modified, amended, or in any way varied or changed, except by a duly written executed instrument by the Parties.

15.0 Choice of Law

The terms and conditions of the Agreement shall be subject to and construed pursuant to the laws in force in the Province of Alberta.

16.0 Severability

Each provision of this Agreement shall be severable from every other provision of this Agreement for the purpose of determining the legal enforceability of any specific provision unless to do so affects the entire intent and purpose of this Agreement.

17.0 Authorized Users

The University and AHS shall mutually agree on those Authorized Users with access to Data. A list of Authorized Users shall be maintained by the University and shall be made available to AHS upon request.

18.0 Conflict

This Agreement sets forth the complete understanding of the Parties with respect to this subject matter and supersedes all other prior and contemporaneous agreements, written or oral, between them concerning the subject matter. In the event of any conflict between the provisions of this Agreement and the provisions of any other agreement between the Parties, the provisions of this Agreement shall control.

19.0 Waiver


No consent or waiver, express or implied by any Party of any breach or default by the other Party in the performance of any obligations hereunder shall be deemed or construed to be a consent or waiver to any other breach or default in the performance by such other Party of the same or any other obligation of such Party hereunder. Failure on the part of any Party to complain of any act or failure to act of any other Party or to declare any Party to be in breach or default, irrespective of how long such failure continues, shall not constitute a waiver by such party of its rights hereunder. No failure or delay by a Party in exercising any of its rights or pursuing any remedies available to it hereunder or at law or in equity shall in any way constitute a waiver or prohibition of such rights and remedies in the event of a breach of this Agreement.

20.0 Execution and Delivery

This Agreement may be executed in any number of counterparts, each of which will be deemed to be an original, and all of which taken together will be deemed to constitute one and the same instrument. Delivery of an executed signature page to this Agreement by any Party by electronic transmission will be as effective as delivery of a manually executed copy thereof by such Party.

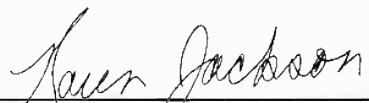
IN WITNESS WHEREOF, the Parties hereto have executed this Agreement as of the date first written above.

Alberta Health Services

Per:  2020-07-14
Jeffrey Bakal

Per:  2020-07-13
Stafford Dean

The Governors of the University of Calgary

Per: 
Karen Jackson, General Counsel

Schedule A

Information Management Services

Hardware Description

The secure Cluster consists of

1. A secure University network zone, not accessible from outside the University. Access to the secure network is either through a secure VPN (separate from the University's normal VPN) or through a Citrix connection, both of which use two factor authentication.
2. The login node is the single point of access for users. This is the only way for a regular user to access the Cluster, transfer data and run jobs. SCDS data transfers, through mounting the appropriate SCDS shares is the only allowable inbound protocol to move data. The login node connects to the secure network and the internal cluster network. Two factor authentication can be set up on the login node for external access if required.
3. The admin node is the point of access for system administrators. Regular users do not have access to the admin node. SSH is the only inbound protocol allowed on the admin node. The admin node connects to the secure network and the internal cluster network and is used for system maintenance tasks. Two-factor authentication can be set up on the admin node if required.
4. The internal cluster network which connects all the compute nodes, storage and login/admin nodes through a private, non-routable network that is not accessible outside the cluster. Currently, this is 10Gbs to all the compute nodes.
5. The compute nodes. These are servers that user's jobs run on. The compute nodes can see each other (for jobs that span nodes) and the storage system. The compute nodes are not accessible from outside the cluster. Access to the compute nodes is allowed from the login node by users only if they have a job running on the compute node. Due to the various services that run on the compute nodes (SLURM job schedule, monitoring daemons, etc.), inbound connections are allowed to the compute nodes only from the internal network. Compute nodes cannot NAT out.

The storage system. This is a NetApp FAS8200 NAS that sits on a separate storage network with a network router between the storage and the two clusters that the storage attaches to. From the network router, part of the file system gets VLANed to our ARC general purpose cluster and the other part of the file system gets VLANed to theCluster. The disks in the storage system never leave the data centre except for shredding by a properly licensed service provider. The two clusters have separate file systems (secure and non-secure file systems) that only get mounted on the appropriate cluster. Access to each file system is controlled by both a VLAN and export control in the NAS. The storage system is managed by the University IT's storage group.

Security Controls

1. User management: access the Cluster is based on user accounts utilizing University's Active Directory. Account requests and changes to account status will go through IT's Service Now ticketing service which will generate audit logs. System administrators from RCS will need to login to the admin node and possibly through the admin node to the login node for maintenance purposes. RCS analysts may also need to connect to the login node to help our users. The storage administrators from I.T.'s storage team will have access to the storage system for support and maintenance purposes. A list of all non-researcher users can be provided and those individuals can undergo specific training as required.
2. Permissions: Access to AHS data is managed through Linux file and directory permissions. AHS staff will belong to a Linux group whose members will have access to the directory which houses the data.
3. Change management: All customizations pertaining to the operating system and user account management (except the passwords, which are maintained in AD) will be managed by the Puppet configuration management system. All changes to Puppet are tracked through a revision control system. Any changes to the operating system not configured in Puppet, will revert to their puppet setting when the next Puppet run completes. All compute nodes and the login and admin nodes are managed through Puppet.
4. Iptables: All external facing nodes (login and admin) use Linux iptables to only allow ssh inbound. All other inbound ports are blocked off. Outbound connections are NOT allowed from any compute nodes or the login node.
5. OS patching: Standard patching of the Operating System is patched on a regular basis, usually twice a year. Security patches are applied shortly after the appropriate patch is available.

Data Movement

AHS Data to be processed on the Cluster will need to be staged. This will be accomplished by utilizing the University's SCDS storage system. SCDS is a secure storage system designed for storing Level 4 data and has appropriate logging and encryption controls enabled that meet AHS' requirements. SCDS maintains snapshots to guard against data loss and also maintains a second copy in a geographically separate data centre for disaster recovery.

A method will need to be built to allow AHS personnel to stage Data from AHS to SCDS with sufficient bandwidth so not to be restricted in the amount of data that can be moved in a reasonable amount of time.

SCDS will log all file creation, modification and deletes and which user mounted which network share. This will allow an audit trail to be built that records when Data gets staged to SCDS from AHS and by whom.

Once Data is moved to SCDS, the appropriate SCDS file share can be mounted on the Cluster login node and the data copied to the shared Cluster secure file system. From then on, all processing will be done on the Cluster file system and any derived data can be copied back to SCDS.

AHS Data Isolation

The data from AHS will be isolated from access by non-AHS users of the cluster through a separate directory structure and Linux user/group permissions as well as directory permissions. AHS authorized users shall belong to a group whose members access granting will be auditable for reporting purposes.

Computation

Once data is staged to the internal Cluster file system, processing of the data will be done using a batch system. Work flows will need to be encapsulated into a job script and submitted to the SLURM job schedule. The job scheduler will match the job's resource parameters to available computing infrastructure and start the job when resources become available.

Schedule B Information Security and Privacy Safeguards Policy

The AHS Information Security and Privacy Safeguards Policy is located at:

<https://extranet.ahsnet.ca/teams/policydocuments/1/clp-ahs-pol-information-security.pdf>

Logging and Auditing

AHS has a legal and ethical responsibility to protect, manage, and secure health and personal information within its custody or under its control to maintain the confidence of patients and stakeholders. Logging and auditing is a managerial activity performed to protect information assets in alignment with privacy and confidentiality regulations and business requirements. The goal of logging and auditing is to provide management with objective, unbiased assessments, and rational, practical recommendations through recurring control activities with responsibility to analyze, validate, counsel, and recommend policies, standards, and activities related to data privacy security management.

The following access elements will be captured, retained and destroyed according to the AHS Records Retention schedule (See Schedule C)

A log file containing

- User Id (UofC ID)
- Date/Time of Access
- Type of Action performed (Metadata Access)

To be retained and released when requested:

- Role of Person within University of Calgary
- Name of Organization (i.e. UofC / AHS)
- Name of the individual in respect of whom an access is performed

These criteria will be captured and retained for every access to the information.

Data movement

Logging for data movement is performed on SCDS which records time stamps and user ID for all create/read/write/delete/print operations. These logs will capture any data moving onto or off of the Cluster.

Connection Logs

Connection logs also exist on the login and admin nodes and the file system management portal. Time-stamped job logs detailing user IDs running jobs and the job parameters requested will also be kept and sent as part of the monthly update.

Schedule C
Records Management Policy and Data Retention Schedule

The AHS Records Management Policy is located at:

<https://extranet.ahsnet.ca/teams/policydocuments/1/clp-ahs-pol-records-management.pdf>

The AHS Records Retention Schedule is located at:

<https://www.albertahealthservices.ca/assets/info/hp/him/if-hp-him-records-retention-schedule.pdf>

Schedule D
University of Calgary Information Asset Management Policy

<https://www.ucalgary.ca/policies/files/policies/information-asset-management-policy.pdf>

