INFORMATION SHARING AGREEMENT

IHA-ISA-HCP-202X-ISA#-MSP#

This Agreement is effective as of the day of 202X.

BETWEEN:

Interior Health Authority, a regional health board established under the *Health Authorities Act* (British Columbia) ("IHA")

AND:

(the "Physician/Provider")

(each a "Party," and collectively the "Parties")

WHEREAS:

A. IHA operates and maintains the IHA System;

B. IHA has control over and stewardship of the Personal Information contained within the IHA System;

C. IHA is responsible and accountable for provisioning and de-provisioning access to the eHealth Viewer System;

C. IHA wishes to provide access to the Systems and the Data therein to health care professionals, as defined in the Health Professions Act to enhance patient care by ensuring that health information about patients to whom such health care professionals are providing care is available to them on a timely basis;

D. IHA has designated the Provider as eligible to access the Systems and Data therein from the Physician/Provider's Office for the purposes of providing care to Patients and on the other terms and conditions of this Agreement; and

E. Each Party is either

i. a "public body" under FIPPA that delivers publicly-funded public health services in British Columbia; or

ii. a "private sector" health care Physician/Provider operating under PIPA that delivers health care services to individuals in British Columbia.

THEREFORE, in consideration of the mutual premises, covenants and agreements set out herein, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. INTERPRETATION

1.1 Definitions

In this Agreement the following terms will have the following respective meanings:

a. "**Agreement**" means this information sharing agreement (ISA) and includes the schedules thereto;

b. "**Acceptable Use Policy**" means the IHA policy *AR0100 - Acceptable Use of Information Systems* as amended or replaced from time to time;

c. "**Access**" means disclosure of Data by provision of the ability to view the Data in the Systems;

d. "**Access Management Portal"** (AMP) means the IHA provided application to request and remove user access to the Systems;

e. "**Collection**" means the copying of information into paper or electronic form;

f. "**Commissioner**" means the Commissioner appointed under FIPPA;

g. "**Conflicting Foreign Order**" means any order, subpoena, directive, ruling, judgement, injunction, award or decree, decision, request or other requirement issued from a foreign court, agency of a foreign state or other authority outside Canada, or any foreign legislation, compliance with which would likely render a Party or its employees in non-compliance with FIPPA or PIPA;

h. "**Contact Information**" means contact information as defined in FIPPA;

i. "**Control**", with respect to Data, means the power or authority and accountability to manage the Data throughout its life cycle, including restricting, regulating and administering its use or disclosure in accordance with applicable legislation;

j. "**Custody**", with respect to Data, means having physical or logical possession of the Data. Physical or logical possession may include responsibility for access, managing, maintaining, preserving, disposing, and providing security;

k. "**Data**" means Personal Information as defined in FIPPA;

l. "**Data Matching**" means a computerized or manual comparison of a database(s) or set(s) of records with another database(s) or set(s) of records where files are merged or "linked" on one or more specific data elements with the intent of generating a new body of Data;

m. "**eHealth Conformance Standards**" means the British Columbia Professional and Software Conformance Standards Electronic Health Information Exchange Volume 7 (Electronic Health Record Service Information Privacy) and Volume 8 (Information Security) as published by the British Columbia Ministry of Health and as amended from time to time;

n. **"eHealth Viewer System"** means the Provincial eHealth Viewer (aka *CareConnect*) system, which is accessible from the IHA clinical system (Meditech), and provides authorized caregivers secure view only access to a patient-centric, electronic health record (EHR) consisting of integrated clinical information provided by multiple contributors , the Control of the Data remains with each respective contributor of Data while Custody of the Data is maintained by the Ministry of Health.

o. "**FIPPA**" means the *Freedom of Information and Protection of Privacy Act* [RSBC 1996] Ch. 165 as amended or replaced from time to time;

p. "**Foreign Demand for Disclosure**" means a foreign demand for disclosure as defined in FIPPA;

q. "**HPA**" means the *Health Professions Act*, [RSBC 1996] Ch. 183 as amended or replaced from time to time;

r. "**IHA System**" means any IHA operated information system consisting of Data in IHA's Custody and under its Control;

s. "**Loss**" means cost, losses, damages, liabilities and expenses (including all reasonable legal costs, fees and expenses);

t. "**Office**" means those places of normal business practice of a Physician/Provider, including an office in the Physician/Provider's home, all to be in the Province of British Columbia only;

u. "**Parties**" means the signatories to this Agreement;

v. "**Patient**" means an individual with whom the Physician/Provider has a clinical relationship and who receives health care services from the Physician/Provider;

w. "**Person**" means any natural person, sole proprietorship, partnership, corporation, trust, joint venture, governmental authority or any incorporated or unincorporated entity or association of any nature;

x. "**PIPA**" means the *Personal Information Protection Act*, [SBC 2003] Ch. 63 as amended or replaced from time to time;

y. "**Signatory**" means a Supervised Person who may act for the Physician/Provider to request and revoke access for other Supervised Person(s) via the IHA AMP

z. **"Stewardship**" means having legal and ethical accountability for the collection, use, disclosure, management and overall protection of data;

aa. "**Supervised Person(s)**" means the employees, agents, representatives or associates in the Physician/Provider's Office who have been designated by a Physician/Provider to access the Systems and the Data therein from the Physician/Provider's Office for the purposes of supporting the provision of care to Patients by the named Physician/Provider; and

bb. "**Systems**" means collectively IHA System and the eHealth Viewer system.

2. IHA AUTHORIZATION

Subject to the terms and conditions hereof, IHA hereby authorizes the Physician/Provider to access the Systems and the Data therein on the terms and conditions set out herein.

3. PROFESSIONAL STATUS

3.1 Health Care Professional in Good Standing

The Physician/Provider represents and warrants that the Physician/Provider is and will at all times throughout the duration of this Agreement be a health care professional as defined by the HPA and is and will at all times be in good standing with the applicable professional college for the Physician/Provider's profession.

3.2 Obligation to Notify

In the event that the Physician/Provider is no longer a health care professional as defined by the HPA or is not in good standing with the applicable professional college for the Physician/Provider's profession, the Physician/Provider will immediately notify the IHA Information Privacy & Security Office of this fact in writing.

4. COMPLIANCE WITH APPLICABLE LAWS

The Parties will comply with FIPPA and PIPA to the extent that such legislation applies to the Parties while performing their obligations and exercising their rights under this Agreement.

The Parties acknowledge that they are familiar with the sections of FIPPA and PIPA that govern the use of Data in their respective environments.

5. CUSTODY AND CONTROL, ACCESS, COLLECTION, USE AND DISCLOSURE

5.1 Custody and Control of Data

(a) Where Access to IHA System is made available to the Physician/Provider , all such Data will be disclosed to the Physician/Provider by IHA pursuant to IHA's authority to do so under FIPPA and other applicable legislation and where Access to the eHealth Viewer System is made available to the Physician/Provider, all such Data will be disclosed to the Physician/Provider by the respective Data contributor for the eHealth Viewer System with authority to do so under FIPPA, PIPA and other applicable legislation .

(b) Data disclosed to the Physician/Provider from an IHA System remains in the Custody and under the Control of IHA and Data disclosed to the Physician/Provider from the eHealth Viewer System remains under the control of the respective contributor of the Data while Custody of the Data is maintained by the Ministry of Health. Data accessed and subsequently collected by the Physician/Provider into any paper or electronic form, will be collected by the Physician/Provider pursuant to the Physician/Provider's legal authority to collect the Data under PIPA or other applicable legislation, and is deemed thereafter to be in the Custody and Control of the Physician/Provider. The Physician/Provider is then solely and wholly responsible for the privacy and the administrative, technical and physical security of the Data pursuant to, and consistent with, its obligations under PIPA.

(c) Where the Physician/Provider discloses Data into an IHA System, all such information will be disclosed to IHA by the Physician/Provider pursuant to the terms and conditions of PIPA or other applicable legislation. Data disclosed into an IHA System in this manner is collected by IHA pursuant to IHA's legal authority to collect it under the *Hospital Act*, the *Health Authorities Act*, FIPPA and other applicable legislation (as amended or replaced from time to time) and is deemed thereafter to be in the Custody and Control of IHA.

5.2 Access to Data

Data may be accessed by the Physician/Provider for the purpose of providing care to patients and pursuant to and consistent with PIPA and FIPPA.

5.3 Collection, Use and Disclosure of Data

With respect to the collection, use and disclosure of Data:

(a) the Physician/Provider represents and warrants that it has, and will at all times have, the authority to collect such Data under PIPA;

(b) the Physician/Provider will ensure it has the requisite consent of each Patient, or the Patient's legal representative, to collect and use the Data pertaining to that Patient in the Systems; and

(c) the Physician/Provider will use and disclose any Data collected from the Systems in a confidential manner and subject to the provisions of PIPA.

5.4 Notification to the Public

If the Physician/Provider discloses Data into an IHA System, the Physician/Provider warrants and will ensure that it has effectively notified the individual the Data is about as required by PIPA.

5.5 Data Matching

The Physician/Provider will not perform any Data Matching of the Data in the Systems without the prior written consent of IHA, unless required or permitted under applicable law.

5.6 Storage of Data

Notwithstanding that the Data transfers to the Custody, and is under the Control, of the Physician/Provider under PIPA once it is collected by the Physician/Provider, the Physician/Provider warrants that it will not store Data obtained from the Systems outside of Canada.

5.7 Foreign Demand for Disclosure

The Physician/Provider will immediately notify IHA if the Physician/Provider:

(a) receives a Foreign Demand for Disclosure of Data from the Systems;

(b) receives any request for disclosure of Data from the Systems that the Physician/Provider knows or has reason to suspect is for the purpose of responding to a Foreign Demand for Disclosure; or

(c) becomes aware of any unauthorized disclosure that the Physician/Provider knows or has reason to suspect has occurred in response to a Foreign Demand for Disclosure of Data from the Systems.

5.8 Procedures on Demand

If the Physician/Provider becomes legally compelled or otherwise receives a demand to disclose Data from the Systems pursuant to a Conflicting Foreign Order, the Physician/Provider will not disclose that Data unless:

(a) IHA has been notified;

(b) in the event that the Data is in the eHealth Viewer System, IHA has notified the contributor of the Data as well as the Ministry of Health;

(c) the Parties have appeared before a Canadian court of law; and

(d) the Canadian court of law has ordered the disclosure.

6. SYSTEM ACCESS

6.1 Access to the Systems and Data

IHA will administer the provisioning and revocation of Access privileges to the Systems, and the Data therein.

6.2 Terms & Conditions of Access

Access to the Systems and the Data therein is provided to the Physician/Provider on the following terms and subject to the other terms and conditions of this Agreement:

(a) the Physician/Provider is permitted to Access the Systems and the Data therein for the sole purpose of providing health care services to Patients, and only

(i) from the Physician/Provider's Office, or
(ii) from outside the Physician/Provider's Office because the access is necessary to provide health care services and the Physician/Provider is temporarily travelling inside or outside Canada;

(b) Supervised Persons are permitted to Access the Systems and the Data therein for the sole purpose of providing health care services to Patients, and only from the Physician/Provider's Office; and

(c) each Physician/Provider who is authorized, and each Supervised Person who is designated by the Physician/Provider, to Access the Systems and Data therein will be identified by a unique user ID and password and may only Access the Systems, and the Data therein using their unique user ID and password.

6.3 Access to the System for Data and Collection and Disclosure

The Physician/Provider will disclose Data into an IHA System and collect Data from the Systems only as permitted by sections 5.3 and 6.2 of this Agreement. Where the Physician/Provider discloses Data into an IHA System or collects Data from the Systems via remote wired or wireless connections and not from its Office, the Physician/Provider warrants and will ensure that it does so in accordance with Section 10.1 and Section 10.2 of the Agreement and in compliance with IHA's Acceptable Use Policy.

6.4 Location of Access

From time to time IHA may request, and the Physician/Provider must immediately provide, details regarding each Office for which Access privileges are requested, including, for each location, the physical address, phone number, facsimile number and email address.

6.5 Change of Location of Access

The Physician/Provider must immediately advise IHA of any changes to each location, including the physical address, phone number, facsimile number or email address, or if the Physician/Provider ceases to practice at the Office to which access has been provided by IHA.

7. SUPERVISED PERSONS

7.1 Physician/Provider Authority

The Physician/Provider may designate one or more Supervised Person(s) to Access the Systems and the Data therein, but only if the Supervised Person(s):

(a) requires Access to the Systems for the purpose of carrying out the Supervised Person's employment duties in the Office and only to the extent necessary to provide health care services to the Patient;

(b) carries out the duties in the Office;

(c) has undergone suitable pre-employment credentials screening prior to employment with the Physician/Provider (e.g., by taking up references, checking career history, checking academic qualifications and confirming identity);

(d) is under the direct employment and supervision of the Physician/Provider; and

(e) has submitted any required agreements related to the respective Data and Systems;

(f) has completed any required training related to Information Privacy & Security and the Systems.

7.2 Physician/Provider Accountability

The Physician/Provider is responsible for ensuring that Supervised Persons do not access the Systems and do not use or disclose the Data therein to any other Person unless:

(a) such access, use or disclosure is for the purposes described in this Agreement; and

(b) the Physician/Provider has directed the Supervised Person to access, use or disclose the Systems and Data in a manner that is consistent with FIPPA and PIPA.

7.3 Requesting Access for Supervised Persons

The Physician/Provider must utilize the IHA AMP to request access for any Supervised Person requiring Access to the Systems and the Data therein.

7.4 Termination and Departure of Supervised Persons

The Physician/Provider will immediately input a removal of access request into the IHA AMP upon the departure, termination or cessation of employment of any Supervised Person to ensure that the Supervised Person's access to the Systems and the Data therein from the Physician/Provider's Office is terminated.

7.5 Designation of Signatory

If more than one Supervised Person is employed by the Physician/Provider, the Physician/Provider may designate one as a Signatory who may act for the Physician/Provider to request and revoke access for other Supervised Person(s) via the IHA AMP.

8. USER ID AND PASSWORD

8.1 Disclosure of IDs and Passwords

The Physician/Provider will not disclose the Physician/Provider's user ID or password, or permit any Supervised Person to disclose their user ID or password to any other Person, including other health care professionals (as defined in the HPA) or Supervised Person(s) for any reason.

8.2 Loss of User IDs and Passwords

The Physician/Provider is responsible for the loss of any user IDs and passwords and any subsequent suspected or actual unauthorized disclosure or misuse of these IDs or passwords.

8.3 Logging Off of the System

The Physician/Provider will ensure that the Physician/Provider and all Supervised Persons adhere to the standard and practice of logging off of the Systems promptly upon completion of an access session to the Systems.

8.4 Accountability for User IDs and Passwords

The Physician/Provider is wholly responsible and accountable for all activity and work done or directed to be done under or using the Physician/Provider's or the Supervised Person's user IDs and passwords.

8.5 Single user for each User ID and Password only

The Physician/Provider will not permit other persons Access to the Systems when they are logged into the Systems nor permit any Supervised Person to permit other Persons Access to the Systems when they are logged into the Systems.

9. ACCURACY OF INFORMATION

9.1 Liability of Physician/Provider

The Physician/Provider is responsible for the accuracy of the Data that they input into the IHA System.

9.2 Accuracy Policies and Procedures

The Physician/Provider will implement appropriate policies and procedures to ensure that the Data they input in the IHA Systems is accurate. Such policies and procedures include but are not limited to:

(a) clearly defining business and other administrative and operational rules and accuracy checks to ensure that Data submitted to the IHA Systems is accurate;

(b) developing a clear and thorough policy and procedure for the documentation of such Data; and

(c) developing a standard education program for appropriate access to and use of the Systems by Supervised Persons.

9.3 Physician/Provider Notification

The Physician/Provider will notify IHA of any material, significant or large-scale errors in Data that it identifies in the Systems.

9.4 IHA Corrections

For material or large-scale errors in Data identified by the Physician/Provider including any errors in Data that are the result of IHA System failure, malfunction or interruption, IHA is responsible for making all reasonable attempts to remedy or correct all material or large-scale errors for IHA Systems

9.5 Data Quality Notice

Each Party will immediately notify the other Party of any perceived problem with the quality of Data in the Systems upon becoming aware of such an issue.

9.6 Disclaimer

Access to the Systems and Data is provided by IHA "as is", without warranty of any kind including warranty of fitness for a particular purpose. IHA does not warrant the accuracy or the completeness of any Data in the Systems or that the Systems or access thereto will function without failure, malfunction or interruption. Data provided by the Systems is not exhaustive and is constantly being updated and therefore cannot be relied upon as complete. Any Data received or otherwise obtained through access to the Systems is used at the Physician/Provider's own discretion and risk. Any such Data is provided as a supplement to, and not a substitute for knowledge, expertise, skill, and professional judgment in providing Patient care.

10. SECURITY AND PROTECTION OF PRIVACY

10.1 Safeguard Security

The Physician/Provider will take all reasonable and appropriate measures to safeguard the security and physical protection of devices used to Access the Systems and the Data therein, including Access to and use of the Systems and Data. The Physician/Provider will protect the Data from Access by any Persons other than the Physician/Provider and Supervised Persons, and will ensure that the Systems, and the Data is accessed, used and disclosed only for the authorized purposes as set out in this Agreement, pursuant and subject to FIPPA and PIPA. The Physician/Provider will ensure that Supervised Persons do not:

(a) permit any other Person to Access or use the Systems or Data therein when the Supervised Person is logged into the System;

(b) divulge, share or compromise their user IDs and passwords;

(c) use or attempt to use the user ID or password of any other Supervised Person;

(d) test, examine or attempt to circumvent the security of the Systems;

(e) take any action that might reasonably be construed as altering, destroying or rendering the Systems' Data ineffective;

(f) alter the format or content of the display of such Data.

Where the Physician/Provider accesses the Systems and Data therein from locations other than its Office, whether such access is via remote wired or wireless network connections, the Physician/Provider will comply with IHA's Acceptable Use Policy, any agreements related to the eHealth Viewer System, and avoid known or suspected security risks which may exist in unsecured locations and from third party devices.

IHA is only responsible for the security of Data in the IHA System while the Data is within its Custody and under its Control.

10.2 eHealth Conformance Standards

The Physician/Provider will take reasonable and appropriate measures to ensure its compliance with eHealth Conformance Standards. As such, the Physician/Provider will ensure that:

(a) there is a designated individual in its Office who has overall responsibility for information security and compliance with eHealth Conformance Standards;

(b) buildings that contain devices used to access the Systems are protected against unauthorized Access by providing locks, bolts (or equivalent) on vulnerable doors and windows;

(c) devices used to access the Systems are not left unattended and that device protections exist and are activated, such as by setting automatic session timeout after a period of inactivity (e.g., password-protected screen saver) or by placing the workstation in a physically secure area;

(d) monitors for devices used to access the Systems are situated and positioned in a manner that limits unauthorized viewing;

(e) appropriate detection, prevention, regular patching and upgrading controls and appropriate user awareness procedures exist to protect against malware (e.g., malicious software such as viruses, worms). This includes the installation of anti-virus and anti-malware software on all devices used to access the Systems; and

(f) devices that access the internet and the Systems are protected by:

(i) using web browsers with a standard, secure configuration;

(ii) preventing users from disabling security options in web browsers;

(iii) applying updating to web browser software quickly and efficiently;

(iv) using firewall controls; and

(v) warning users of the dangers or and restricting the downloading of mobile code (e.g., executable code such as Java applets, MS ActiveX, JavaScript or VBScript, that has been written deliberately to perform unauthorized functions).

10.3 EHealth Conformance Standards – Future Security Technologies

As IHA transitions to meet full compliance with the EHealth Conformance Standards, the Physician/Provider will adopt new security technologies required by the EHealth Conformance Standards as they become available.

10.4 Privacy and Security Breach

The Physician/Provider will, and will ensure that its Supervised Persons will, advise IHA immediately upon learning of any circumstances, incidents or events which, to their knowledge, have jeopardized or may in the future jeopardize the:

(a) privacy of the Patients to whom the Data relates, when such Data is still in the Custody and/or under the Control of IHA or the contributor to the eHealth Viewer; or

(b) security of any computer system in its Custody or under its Control that is used to Access the Systems and the Data therein.

10.5 Investigation

The Physician/Provider will immediately notify IHA of, and will cooperate in the investigation of all reported cases of breach of this Agreement by Supervised Persons or of any wrongful use of or access to the Systems or Data therein by any Person. IHA reserves the right to suspend access to the Systems during the course of any investigation to ensure adequate protection of the Systems and the Data therein.

10.6 Reports

The Physician/Provider will report to IHA the results of any investigative activities undertaken pursuant to Section 10.5 of the Agreement, and will also report to IHA the steps taken to address any issues or concerns about the security of the Systems and the Data therein or the tools and mechanisms used to access the Systems and such Data.

11. PHYSICIAN/PROVIDER SYSTEMS

The Physician/Provider is responsible for its own systems, including mobile devices, used to access the Systems and the Data therein and any costs relating thereto. The Physician/Provider is responsible for ensuring that its own systems, including mobile devices, used to access the Systems and Data meet industry standards for such systems as well as any standards set by IHA.

12. NO ACCESS BY SUPPORT ORGANIZATIONS

The Physician/Provider will not authorize or permit access to the Systems and the Data therein by any Person employed by or contracted to a software or hardware support organization providing services to the Physician/Provider.

13. AUDITING

13.1 Right of Inspection

IHA or its agent may, at any reasonable time and on reasonable notice, enter the Physician/Provider's Office to inspect the Physician/Provider's information management systems or practices relevant to access to the Systems and the Data therein, and/or to verify compliance with this Agreement. IHA or its agent may also, at any reasonable time and on

reasonable notice, inspect the Physician/Provider's mobile devices relevant to access to the Systems and the Data therein, and/or to verify compliance with this Agreement.

13.2 Cooperation

The Physician/Provider agrees that it will permit and provide reasonable assistance to IHA to facilitate an inspection pursuant to Section 13.1.

13.3 Notice to the Regulatory Body

If an inspection reveals that the Physician/Provider is in breach of the terms of this Agreement, then in addition to any action IHA may take against the Physician/Provider under this Agreement or pursuant to other legal remedies, IHA may notify the appropriate regulatory body of the breach.

14. INDEMNITY

The Physician/Provider will defend, indemnify and hold harmless IHA and its directors and officers from and against any Loss, resulting directly or indirectly from any negligence or wilful misconduct or acts or omissions of the Physician/Provider or any Supervised Persons in accessing or using the Systems or any Data therein under this Agreement, or any breach by the Physician/Provider of any of its covenants or obligations under this Agreement.

15. TERM OF AGREEMENT

The term of this Agreement will commence on the date set out on the first page of this Agreement and will continue until terminated in accordance with Section 17. The obligations, representations and warranties of the Physician/Provider as set out in this Agreement will survive the termination of this Agreement or any suspension of rights hereunder.

16. MODIFICATION OF AGREEMENT

Any amendment or modification to the terms and conditions of this Agreement must be approved in writing and duly executed by the Parties.

17. SUSPENSION OF RIGHTS AND TERMINATION OF AGREEMENT

17.1 Suspension or Termination by IHA

Notwithstanding any other provision herein to the contrary, IHA retains the right to:

(a) suspend or terminate the Physician/Provider and/or any Supervised Person's access to the Systems and the Data therein at any time and without notice if IHA, in its sole discretion, determines that it is necessary to do so; and/or

(b) terminate this Agreement in the event of a material breach of this Agreement by Physician/Provider or a Supervised Person that is not the subject of an immediate suspension or termination pursuant to Section 17.1(a) where such

breach has not been remedied to the satisfaction of IHA within the time frame set by IHA.

17.2 Termination by Physician/Provider

This Agreement will automatically terminate upon receipt by IHA of the Physician/Provider's written notice of withdrawal by the Physician/Provider and its Supervised Persons from access to the System.

17.3 Effect of Suspension or Termination

Upon suspension of the Physician/Provider's and/or a Supervised Person's rights or upon termination of this Agreement, the Physician/Provider will and will cause the Supervised Person, as applicable, to cease all access to and use of the Systems and the Data therein.

18 NOTICE

18.1 Notice

If for any reason the Physician/Provider does not comply, or anticipates that it will be unable to comply, with a provision in the Agreement in any respect as it relates to Data under the Control of IHA, the Physician/Provider must promptly notify IHA of the particulars of the non-compliance or anticipated non-compliance, and of the steps it proposes to take to address, or prevent recurrence of the non-compliance or anticipated non-compliance. Nothing in this Section 18.1 will impede IHA's ability to exercise its rights under Section 17.

18.2 Manner of Notice

All notices either Party is required to give or wishes to give under this Agreement will be made in writing to the Agreement Manager for the other Party as set out below and can be given by courier, hand-delivery, regular mail, facsimile, or other electronic means of communication, including e-mail, and will be addressed as follows:

For IHA:

Attention: Norma Janssen
Chief Information Officer
Kelowna Community Health and Services Centre
505 Doyle Avenue, Kelowna, BC V1Y 0C5

For Physician/Provider:

Attention:

18.3 Deemed Receipt

Any notice, document, statement, report, or demand delivered by mail in British Columbia and correctly addressed to the Party to whom it is sent will be deemed given to and received by that Party on the third business day after it is mailed, except in the event of disruption of postal services in British Columbia in which case it will be deemed given to and received by that Party when it is actually delivered. Any notice, document, statement, report, or demand delivered by

facsimile transmission will be deemed given to and received by a Party when successfully transmitted to the facsimile number provided by that Party.

19. GENERAL

19.1 No Assignment

The Physician/Provider may not assign, sublicense or otherwise transfer its rights under this Agreement without the prior written consent of IHA.

19.2 Enurement

This Agreement will enure to the benefit of, and be binding upon, the parties hereto and their respective successors, assigns or approved assigns, as the case may be.

19.3 Entire Agreement

The provisions of this Agreement constitute the entire agreement between the parties and supersede any prior agreements, letters of intent or understanding, whether written or oral, between the parties with respect to the matters contemplated herein. No terms, conditions, warranties, promises or undertakings of any nature whatsoever, express or implied, exist between the parties with respect to this Agreement except as herein set forth.

18.4 Time of Essence

Time will be of the essence in this Agreement.

19.5 Further Assurances

The parties will do and execute such further documents or things as may be necessary or desirable in connection with this Agreement.

1819.6 Governing Law

This Agreement will be governed by the laws of the Province of British Columbia and the laws of Canada applicable therein.

1819.7 Counterparts

This Agreement may be executed in several counterparts, each of which will be deemed to be an original. Such counterparts together will constitute one and the same instrument, notwithstanding that all of the Parties are not signatories to the original or the same counterpart.

19.8 Schedules

The Schedule(s) to this Agreement are part of this Agreement and, if indicated, must be completed prior to the execution of this Agreement. If there is a conflict between a provision in a Schedule and any provision of this Agreement, the provision in the Schedules is inoperative to the extent of the conflict, unless the Schedule states that it operates despite a conflicting provision of this Agreement.

19.9 Headings

The headings in this Agreement are inserted for convenience only and do not form part of the Agreement.

19.10 Legal Relationship

No partnership, joint venture or agency will be created or will be deemed to be created by this Agreement or by any action of any of the Parties under this Agreement.

19.11 Cumulative Rights and Remedies

The rights and remedies of IHA in this Agreement, including its suspension and termination rights, are in addition and without limitation to any and all other remedies available to IHA under this Agreement, at law, in equity or otherwise.

IN WITNESS WHEREOF the parties have executed this Agreement as of the date set out in the first page of this Agreement:

Interior Health Authority	**Insert Physician/Provider/HA Name**
_____ Authorized Signatory **Name**: Norma Janssen **Title**: Chief Information Officer	_____ Authorized Signatory **Name: Insert Physician/Provider Name** **Title**: Physician/Provider

SCHEDULE A – PHYSICIAN/PROVIDER INFORMATION – MUST BE COMPLETED

IHA collects registration information from applicant health care professionals for the purpose of authenticating and authorizing access to the Systems and Data and to monitor all users to ensure integrity of the System and Data.

SECTION 1 – PHYSICIAN/PROVIDER INFORMATION

FIRST NAME	MIDDLE NAME	SURNAME

EMAIL ADDRESS	PRACTITIONER ID #	MSP PRACTITIONER #
USER NAME	**COLLEGE ID # (if applicable)**	

SECTION 2 – OFFICE INFORMATION

**All Phone and Fax numbers must include area code*

OFFICE NAME	PHONE # (###) ###-####	FAX # (###) ###-####

OFFICE STREET ADDRESS / PO BOX	CITY	POSTAL CODE
OFFICE EMAIL		

SECTION 3 - NAME OF EMPLOYED SUPERVISED PERSONS ACCESSING THE SYSTEM ON YOUR BEHALF

FIRST NAME	SURNAME	JOB TITLE	PERSONAL EMAIL*
FIRST NAME	SURNAME	JOB TITLE	PERSONAL EMAIL*
FIRST NAME	SURNAME	JOB TITLE	PERSONAL EMAIL*
FIRST NAME	SURNAME	JOB TITLE	PERSONAL EMAIL*
FIRST NAME	SURNAME	JOB TITLE	PERSONAL EMAIL*

***personal email is required in order to authenticate user when completing annual Data Access & Confidentiality Agreement**

SECTION 4 - NAME OF EMPLOYED SUPERVISED PERSON AUTHORIZED AS YOUR SIGNATORY* FOR PURPOSES OF ACCESS PROVISIONING AND DEPROVISIONING REQUESTS VIA THE IHA AMP

FIRST NAME	SURNAME	JOB TITLE	EMAIL

***If you only employ a single MOA, you cannot authorize them as your Signatory**