This Agreement is made the _____ day of _____, 20__

VENDOR PARTICIPATION AGREEMENT

FOR ELECTRONIC HEALTH INFORMATION EXCHANGE

BETWEEN:

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, represented by the Minister of Health (the **"Province"**)

AND:

_____ (the **"Software Support Organization"** or **"SSO"**) at the following address:

_____
_____
_____
Facsimile: _____
Email: _____

WHEREAS:

A. The Province owns and is responsible for the operation of the Province Systems.

B. The Province Systems contain highly sensitive confidential information, including Personal Information, and it is in the public interest to ensure that appropriate measures are in place to protect the confidentiality and integrity of such information.

C. The Province permits Authorized Users to access one or more Province Systems to provide health services to, or to facilitate the care of, the individual whose personal information is being accessed..

D. This Agreement sets out the terms by which SSO may make an Interface Implementation available to SSO Customers for the purpose of enabling access to one or more Province Systems by Authorized Users.

E. The Province is also prepared to grant the SSO limited access to non-production instances of a Province System for the SSO's development and testing of an Interface Implementation, on the terms and conditions set out herein.

NOW THEREFORE in consideration of the promises and the covenants, agreements, representations and warranties set out in this Agreement (the receipt and sufficiency of which is hereby acknowledged by each party), the parties agree as follows:

ARTICLE 1 – INTERPRETATION

1.1 Definitions.

In this Agreement, unless the context otherwise requires, the following definitions will apply:

(a) "**Access Subcontractor**" means a Subcontractor that provides any part of the Interface Access Services;

(b) **"Applicable Laws"** means all applicable laws of Canada, British Columbia, or another province or territory in Canada which is binding on the parties (or one party as applicable), and in effect from time to time, but does not include any law, statute, regulation or by-law, treaty, directive, policy having the force of law, order, judgement, injunction, award or decree of a foreign jurisdiction outside of Canada;

(c) **"Authorized User"** means a person permitted by the Province to access one or more Province Systems, to provide health services to, or to facilitate the care of, the individual whose personal information is being accessed;

(d) "**Canadian Access Personnel**" has the meaning given in Section 4.6;

(e) "**Canadian Entity**" means a corporation, partnership, limited partnership, or other similar entity (i) that is incorporated or created under the laws of Canada or under the laws of any province of Canada, and (ii) all of whose directors if a corporation, or persons acting in a similar capacity if a partnership, limited partnership, or other similar entity, are Canadian residents;

(f) "**Confidential Information**" has the meaning given in Section 4.13;

(g) "**Conformance Initiation Notice**" has the meaning given in Section 3.5;

(h) "**Conformance Standards**" means the various volumes of the "Professional and Software Conformance Standards" documents published by the Province, as such documents are amended and supplemented by the Province from time to time and made available in accordance with Section 2.3;

(i) "**Conformance Evaluation**" means the conformance evaluation process for an Interface Implementation set out in Article 3;

(j) "**Data Centre Location(s)**" means the physical location(s) where the SSO or an Access Subcontractor will store Disclosed Data in connection with the provision of Interface Access Services, as disclosed to the Province in accordance with Section 3.5(c) or otherwise by written notice from the SSO. For greater certainty, all such Data Centre Location(s) must be located within Canada;

(k) "**Disclosed Data**" means any Personal Information obtained from a Province System in connection with the use, by any person (including Authorized Users), of an Interface Implementation, and specifically includes any copies of the foregoing that are in the possession of SSO or its Subcontractors;

(l) "**Disclosure Order**" has the meaning given in Section 4.5;

(m) "**Foreign Access**" has the meaning given in Section 4.7;

(n) "**Foreign Access Conditions**" means:

(i) the SSO will ensure that Foreign Access is controlled, monitored and mediated by Canadian Access Personnel,
(ii) the SSO will ensure that Foreign Access is limited to temporary access and storage for the minimum time necessary for the Permitted Purpose, and
(iii) if Foreign Access is for the Permitted Purpose of data recovery, the SSO will ensure that Foreign Access is limited to access and storage only after the system failure has occurred;

(o) "**Interface Access Services**", "**Interface Application**", and "**Interface Application Training**" have the meanings given in the definition of "Interface Implementation" below;

(p) **"Interface Implementation"** means:

(i) any computer application, software service, website or similar functionality, that is created, adapted, owned, licensed or maintained by the SSO and that enables user access to a Province System (an "**Interface Application**"),
(ii) any services, including software support, hardware, data hosting, application service provider (ASP), disaster recovery and backup services, that the SSO provides in relation to the Interface Application described in (i) above, that in any way results in the SSO or an Access Subcontractor accessing, possessing, transmitting, collecting, retaining, using or disclosing Disclosed Data (the "**Interface Access Services**"), and
(iii) any training program or educational or training materials that the SSO provides to SSO Customers and Authorized Users in relation to the

Interface Application described in (i) above (the "**Interface Application Training**");

(q) **"Material Breach"** has the meaning given in Section 9.4;

(r) **"Permitted Purpose"** means access to Personal Information (including when stored at the facilities from where the SSO or an Access Subcontractor provides Interface Access Services) that is necessary for: (i) installing, implementing, maintaining, repairing, trouble-shooting or upgrading an electronic system or equipment used by a SSO Customer or the SSO for or in connection with the SSO providing an Interface Implementation to a SSO Customer, or (ii) recovery of data (including Personal Information) undertaking following the failure of an electronic system used by a SSO Customer or the SSO for or in connection with the SSO providing an Interface Implementation to SSO Customer;

(s) **"Personal Information"** means all recorded information that is about an identifiable individual or is defined or deemed as "personal information" or "personal health information" pursuant to any laws or regulations related to privacy or data protection that are applicable to the Province, SSO Customers, Authorized Users or to the SSO or an Access Subcontractor (including without limitation any information that constitutes "personal information" pursuant to the *Freedom of Information and Protection of Privacy Act* (British Columbia), the *Personal Information Protection Act* (British Columbia) or the *Pharmaceutical Services Act* (British Columbia) , or that constitutes "personal health information" pursuant to the *E-Health (Personal Health Information and Protection of Privacy) Act* (British Columbia));

(t) **"Personnel"** means, in relation to the SSO, the employees and independent contractors of the SSO or any Subcontractor;

(u) "**Province Data**" means any Personal Information contained in a Province System that is made available to, or that is otherwise accessible by, the SSO in any manner (whether authorized or not) in respect of this Agreement or the performance of any services in relation to an Interface Implementation;

(v) **"Province Proprietary Materials"** means the Province Proprietary Software and Province Training Materials;

(w) **"Province Proprietary Software"** means any software owned by or licensed to the Province, including object and source code versions, and any records, documentation and any modifications or interfaces relating to the foregoing, which the Province, in its sole discretion, permits the SSO to access (including via remote online access) or use in connection with an Interface Implementation or the development, testing or evaluation thereof. For greater certainty, Province Proprietary Software includes any non-production instance(s) (i.e. dev, test, sandbox, conformance) that the Province

makes available to the SSO for the development, testing or evaluation of an Interface Implementation;

(x) "**Province System**" means the production and training instance(s) of any electronic health record (EHR) or other information systems (including networks) reasonably identified by the Province (in the Conformance Standards or otherwise) as a Province System for the purposes of this Agreement, and any replacement or successor to any such system. For greater certainty, unless otherwise directed by the Province the Province Systems include all production and training instance(s) of the information systems of the Province identified by the SSO in a Conformance Initiation Notice as being an information system that an Interface Implementation interfaces with;

(y) **"Province Training Materials"** means any education or training documentation, data or other materials owned by or licensed to the Province, which the Province, in its discretion, permits the SSO to access or use in connection with an Interface Implementation;

(z) "**SSO Customer**" means:

(i) in relation to an SSO that is is a commercial software support organization, a customer of SSO that has acquired or licensed an Interface Implementation for the purpose of enabling Authorized User access to one or more Province Systems; or
(ii) in relation to an SSO that is a health authority, an Authorized User;

(aa) **"Subcontractor"** means any third party person engaged by the SSO or a Subcontractor to perform any part of the SSO's obligations under this Agreement or any part of an Interface Implementation on behalf of the SSO, and includes an Access Subcontractor.

1.2 Interpretation.

In this Agreement:

(a) "includes" and "including" are not intended to be limiting;
(b) unless otherwise specified, whenever the words "discretion", "option", "determine" and other similar words and variations thereof are used with respect to a party, they will be deemed to mean such party's sole and absolute discretion, option, determination or other such similar act;
(c) unless otherwise specified, a reference to a statute by name means the statute of British Columbia of that name, as amended or replaced from time to time; and includes any regulations or orders made under the authority of that statute; and
(d) unless the context otherwise requires, words expressed in the singular include the plural and *vice versa*.

1.3 Headings.

The division of this Agreement into Articles, Sections, paragraphs and clauses, and the insertion of headings, are for convenience of reference only and will not affect the construction or interpretation of this Agreement.

1.4 Schedules.

The following are the Schedules attached to this Agreement, which are incorporated into this Agreement by reference and are deemed to be an integral part of this Agreement:

Schedule A – Restrictions, Terms, Policies re: Province Proprietary Materials

- Acceptable Use Policy for Non-Production IT Resources

1.5 Conflicts.

Conflicts among provisions of this Agreement will be resolved as follows:

(a) a provision in the main body of this Agreement will prevail over any conflicting provision in a Schedule, unless that conflicting provision expressly states otherwise; and

(b) a provision in the main body of this Agreement or a Schedule will prevail over any conflicting provision in a document attached to or incorporated by reference into the main body or Schedule, as applicable, unless the main body or Schedule expressly states otherwise.

ARTICLE 2 – APPLICABLE LAW AND CONFORMANCE STANDARDS

2.1 Compliance with Applicable Laws.

The SSO will comply with all Applicable Laws in the performance of the SSO's obligations under this Agreement.

2.2 Compliance with Conformance Standards.

The SSO will comply with Conformance Standards as follows:

(a) when creating or updating the Interface Application associated with an Interface Implementation, the SSO will comply with all requirements set out in the Conformance Standards at the time of such creation or update;

(b) when providing the Interface Access Services associated with an Interface Implementation, the SSO will comply with all requirements set out in the Conformance Standards at the time such Interface Access Services are provided; and

(c) the SSO will make commercially reasonable efforts, on an ongoing basis during the term of this Agreement, to make all Authorized Users that use an Interface

Implementation aware of the standards identified in the Conformance Standards that apply to such use.

2.3 Changes to Conformance Standards.

The Province reserves the right to amend the Conformance Standards from time to time during the term of this Agreement in its discretion. The Province will provide the SSO with written notice of such amendment, and the date upon which it becomes effective in advance of the amendment's effective date. Generally, such notice will be provided at least three months in advance of its effective date, however the Province reserves the right to amend the Conformance Standards upon shorter notice if the Province determines that a shorter notice period is required in the circumstances. The Province will make the Conformance Standards, and any amendments thereto, available on the following website (or such other website as the Province may reasonably specify from time to time for the purposes of this Agreement):

http://gov.bc.ca/healthinformationexchange

In the event that the SSO does not agree to an amendment to the Conformance Standards made by the Province under this Section, the SSO must promptly deliver notice to the Province terminating this Agreement pursuant to Section 9.2, and any such termination by the SSO must be effective no later than the effective date of the amendment to the Conformance Standards that the SSO does not agree to.

ARTICLE 3 – CONFORMANCE EVALUATION

3.1 New Interface Implementations.

The SSO will not provide, license or otherwise make any Interface Implementation available to a SSO Customer or other third-party person except as specifically contemplated in Section 3.9.

3.2 Existing Interface Implementations.

Where an Interface Implementation has previously passed Conformance Evaluation and its Interface Application, Interface Access Services or Interface Application Training program or materials are subsequently changed, updated, enhanced or modified in a material manner (an "**Updated Interface Implementation**"), the SSO will not provide, license or otherwise make such Updated Interface Implementation available to a SSO Customer or other third-party person unless the SSO has notified the Province, in writing and in the form and manner required by the Province, of the Updated Interface Implementation and the Province has approved such Updated Interface Implementation in writing.

Prior to providing any such approval the Province, at its discretion: (a) may require that the SSO provide further information respecting the nature of the changes to the Updated Interface Implementation, or (b) may require that the Updated Interface Implementation undergo

Conformance Evaluation. Subject to Section 3.6, the Province will not unreasonably delay or withhold the Conformance Evaluation of an Updated Interface Implementation.

For greater certainty, the obligations in this Section do not apply to the SSO where an Interface Implementation is changed or updated solely to correct bugs or other deficiencies in the operation of the Interface Application or to maintain service levels or other contractual obligations that the SSO may have with the Province or a SSO Customer who is an existing customer of the SSO.

3.3 Acceptance Criteria.

For the purposes of this Article 3, the "**Acceptance Criteria**" for an Interface Implementation means confirmation that:

(a) the Interface Application associated with the Interface Implementation complies with the requirements set out in the Conformance Standards and all other requirements of this Agreement,

(b) the Interface Access Services associated with the Interface Implementation complies with the requirements set out in the Conformance Standards and all other requirements of this Agreement, and

(c) the Interface Application Training associated with the Interface Implementation complies with the requirements set out in the Conformance Standards and all other requirements of this Agreement.

3.4 Internal Testing.

Before submitting an Interface Implementation for Conformance Evaluation, the SSO will conduct thorough internal testing of the Interface Implementation to verify that it meets the Acceptance Criteria to the reasonable satisfaction of the SSO.

3.5 Initiation of Conformance Evaluation.

The SSO must submit an Interface Implementation for Conformance Evaluation by notifying the Province in writing (a "**Conformance Initiation Notice**") at least four (4) weeks in advance of the date that the applicable Interface Implementation will be ready for Conformance Evaluation. The Conformance Initiation Notice must be delivered in the form and manner required by the Province, and must include the following information:

(a) notice of the Province System(s) that the Interface Implementation interfaces with,

(b) a description of the Interface Access Services that the SSO or an Access Subcontractor will provide in connection with the Interface Implementation,

(c) if the Interface Access Services described under paragraph (b) above include data hosting, disaster recovery, backup or similar data storage services, the address of all physical location(s) where Personal Information will be stored in connection with such data storage services (all of which must be located within Canada),

(d) a description of the Interface Application Training programs and materials that the SSO or a Subcontractor will provide in relation to the Interface Implementation, and

(e) any other information respecting the Interface Implementation that may required by the Province.

The SSO acknowledges and agrees that, upon submitting a Conformance Initiation Notice to the Province, the Interface Implementation to which that Conformance Initiation Notice relates will be governed by the terms and conditions of this Agreement.

3.6 Scheduling.

Upon receipt of a Conformance Initiation Notice, the Province will contact the SSO to schedule a mutually agreeable time and location to conduct Conformance Evaluation.

All dates and times for Conformance Evaluation will be subject to the approval of the Province. Without limiting the foregoing, the Province reserves the right to schedule any Conformance Evaluation in its discretion, including based on the availability of its resources, its plans and priorities for the adoption of Province Systems and the order that software support organizations present themselves to the Province for Conformance Evaluation.

3.7 Access for Evaluation.

Upon the Province's request, the SSO will provide the Province with: (a) access to the SSO's facilities, equipment, software, logs, screen shots, training and other materials to allow the Province to observe and direct the conduct of tests, examine test results and otherwise determine whether the Interface Implementation meets the Acceptance Criteria to the satisfaction of the Province, and (b) any further information requested by the Province in relation to the Interface Implementation.

3.8 Non-Conformance.

The Province will determine what Acceptance Criteria to test during Conformance Evaluation. If the Province determines that the Interface Implementation does not meet the Acceptance Criteria ("**Non-Conformance**"), the Province will notify the SSO of such Non-Conformance and will provide the SSO with information reasonably available to the Province with respect to the Non-Conformance. The Province, at its discretion, may do one of the following with respect to any such Non-Conformance:

(a) schedule other date(s) and time(s) for further Conformance Testing, provided that, unless otherwise agreed by the Parties, any such further testing is at least one month after the Province's delivery of notice to the SSO of Non-Conformance. The SSO will use its best efforts to promptly correct all Non-Conformance issues identified by the Province prior to any such further Conformance Testing of the Interface Implementation; or

(b) notify the SSO that the Interface Implementation has failed Conformance Evaluation, in which case the Conformance Evaluation process in relation to the Interface Implementation will end. Subject to any limitations imposed by the Province respecting how often an Interface Implementation may be submitted for Conformance Evaluation and any further direction of the Province, the SSO may resubmit the Interface Implementation for Conformance Evaluation after correcting all Non-Conformance issues.

3.9 Interface Approval Notice.

If the Province determines that the Interface Implementation meets the Acceptance Criteria and that it otherwise approves of the Interface Implementation, the Province will sign and deliver a written notice to the SSO stating that the Interface Implementation has passed Conformance Evaluation (an "**Interface Approval Notice**"). Unless otherwise provided in the Interface Approval Notice, upon delivery of the Interface Approval Notice to the SSO the Interface Implementation, as described by the SSO in the Initiation Notice, will be deemed to have passed Conformance Evaluation for the purposes of this Agreement. From and after the date that the Interface Approval Notice is delivered to the SSO but subject to Section 3.10, the SSO will be eligible, upon the terms and conditions set forth in the Interface Approval Notice and in this Agreement, to supply the approved Interface Implementation to SSO Customers.

3.10 End of Life.

If the Province reasonably determines that:

(a) SSO has stopped marketing and sustaining an approved Interface Implementation, such that it has reached its commercial end of life, or

(b) an Interface Application or a component of an Interface Application associated with an approved Interface Implementation has become obsolete,

the Province may deliver written notice to the SSO withdrawing the SSO's eligibility to supply that Interface Implementation to SSO Customers, with such notice being effective as of the effective date set forth in such notice.

ARTICLE 4 – PRIVACY, SECURITY AND CONFIDENTIALITY

4.1 Privacy and Security Obligations.

The SSO will at all times, and will ensure that its Personnel, its Subcontractors and its Subcontractor's Personnel, comply with the obligations and requirements set forth in this Article 4.

4.2 Acknowledgement.

The SSO acknowledges that, in connection with its provision of an Interface Implementation to SSO Customers, the SSO may be given access to and possession of highly confidential and sensitive information, including Personal Information contained in or obtained from one or more of the Province Systems, and that the confidentiality, integrity, privacy and security of such information is of paramount importance.

4.3 Access to and use of Data.

Except as expressly permitted in this Section 4.3, the SSO expressly acknowledges that it and its Subcontractors have no obligation or right to access or use any Province Data or Disclosed Data in respect of this Agreement or the performance of any activity in relation to an Interface Implementation, notwithstanding that Disclosed Data may be accessed, transmitted and stored by Authorized Users using the services, systems, networks and facilities of the SSO and/or its Access Subcontractors.

Notwithstanding Section 4.15 and 4.16 but otherwise subject to the other terms of this Article 4, SSO agrees as follows:

(a) Except as expressly set out in paragraph (b) below, the SSO will not take any action or fail to take any action, that in either case results in the SSO or its Subcontractors intercepting, accessing or using any Province Data or Disclosed Data;

(b) The SSO or an Access Subcontractor may:

(i) access PharmaNet in accordance with section 6 of the *Information Management Regulation*, B.C. Reg. 74/2015,

(ii) access a Province System other than PharmaNet for a Permitted Purpose, but only if the specific instance of such access has been authorized in advance by an express and lawful written direction of the Province, and

(iii) access Disclosed Data for a Permitted Purpose;

(c) The SSO will take appropriate measures and have policies and procedures in place to ensure that its Personnel and Subcontractors do not access or use Province Data or Disclosed Data except as expressly permitted by this Agreement, including taking

measures and having policies and procedures in place to prevent unauthorized access, collection, use, retention, disclosure, copying, modification or disposal;

(d) Without limiting paragraph (a) above, the SSO:

(i) may only collect, create, access, use, hold and copy Disclosed Data on behalf of Authorized Users and to the extent necessary for the performance of the Interface Access Services in relation to such Authorized Users;
(ii) will not, in respect of Disclosed Data, engage in data sharing, data mining, data matching, de-identification, anonymization or similar activities, except as expressly permitted in the Conformance Standards;
(iii) will not permit any third-party (other than Authorized Users) to: (A) use any user IDs, passwords or other credential (whether physical or logical) that is issued by the Province and permits access to a Province System (a "**System Credential**"), or (B) access a Province System;
(iv) will not divulge, share or compromise a System Credential;
(v) will not test or examine the security related to a system or network of the Province that is used to store or transmit Province Data or Disclosed Data.

4.4 Unauthorized Storage, Access to, Disclosure or Use.

The SSO will immediately report and provide particulars to the Province in writing: (a) of any storage, access to, disclosure or use of Province Data or Disclosed Data contrary to the provisions of this Agreement and any Applicable Laws related to privacy and the collection, use and disclosure of such information, or (b) if it has knowledge of any circumstances, incidents or events which have or may jeopardize the security, confidentiality, integrity or availability of information in a Province System, including any unauthorized attempt to access a Province System.

The SSO will treat any such matter as a priority, and will immediately take containment steps and limit further loss or damage, investigate the matter and implement measures to correct the matter and to prevent a recurrence of the matter, including such measures as may be required by the Province. The Province may in its discretion publicly disclose, on its website or otherwise, the occurrence of any such matter and the corrective measures required and taken as contemplated by this Section.

4.5 Foreign Disclosures.

The SSO will immediately inform the Province if the SSO receives any subpoena, warrant, order, demand or request that is from a foreign court, an agency of a foreign state or another authority outside of Canada, or any directions or requests from any affiliates (as defined in the *Business Corporations Act* (British Columbia)) of the SSO in respect of the same, and in each case, related to any Province Data or Disclosed Data that is in the possession of the SSO (each a "**Disclosure Order**"). Upon receipt of a Disclosure Order, the SSO will not disclose any

Province Data or Disclosed Data in response thereto and the SSO will at all times act in accordance with the terms and conditions of this Agreement.

4.6 Storage at Specified Location(s), Only Canadian Entities May Store, Access or Use.

Except as expressly provided in Section 4.7, the SSO will arrange its affairs to ensure that:

(a) Disclosed Data is only stored by the SSO and its Access Subcontractors at the Data Centre Location(s), unless the Province approves otherwise in writing, and

(b) all storage of, access to, and use of Disclosed Data by the SSO and its Access Subcontractors in the course of providing an Interface Implementation to SSO Customers will be: (i) from within Canada, and (ii) performed by employees of Canadian Entities or, in the case of Access Subcontractors who are individuals, by Canadian residents ("**Canadian Access Personnel**").

4.7 Foreign Access to Disclosed Data.

The SSO may access Disclosed Data from a location outside of Canada ("**Foreign Access**") and by employees and contractors who are not Canadian Access Personnel only for a Permitted Purpose and then in accordance with the Foreign Access Conditions. Without limiting the foregoing, the SSO will ensure that, except for a Permitted Purpose and then only in accordance with the Foreign Access Conditions: (a) the SSO will not make Disclosed Data available to any SSO Personnel, Access Subcontractors or Access Subcontractor Personnel while any such persons are physically located outside of Canada, on either a temporary or permanent basis, and (b) no Interface Access Services will be provided or performed by the SSO in any location outside of Canada.

4.8 Foreign SSO.

If the SSO itself is not, or ceases to be a Canadian Entity (a "**Foreign SSO**"), then the Foreign SSO will use Access Subcontractors that are Canadian Entities, or, in the case of Access Subcontractors who are individuals, who are Canadian residents ("**Canadian Access Subcontractors**"), to ensure its compliance with Sections 4.6 and 4.7. Further, the Foreign SSO will not include any terms in its agreements with its Canadian Access Subcontractors permitting the Foreign SSO to access or use Province Data or Disclosed Data, except as provided in Section 4.7.

4.9 Disclosure of Data.

Notwithstanding Section 4.15, 4.16 and any other term of this Agreement or any other obligation or right of the SSO, the SSO will not disclose to any person (other than Access Subcontractors in accordance with and subject to the terms of this Agreement, the Province, and Authorized Users) or allow any such person to access or use Province Data or Disclosed Data (including when

stored at the facilities from where the SSO or an Access Subcontractor provides Interface Access Services), except as required to satisfy Applicable Law (provided that the SSO first notifies the Province within a reasonable time prior to any such disclosure of the terms and circumstances of the disclosure requirement).

4.10 Flow through of Terms to Access Subcontractors.

The SSO will flow through the requirements of Sections 4.3, 4.4, 4.5, 4.6, 4.7, 4.8 and 4.9 to any Access Subcontractors to apply to the Access Subcontractors, *mutatis mutandis*.

4.11 Non-Disclosure Documents.

If requested to do so by the Province, the SSO will ensure that its Personnel, Subcontractors and Subcontractor Personnel (including Personnel of Access Subcontractors) enter into direct agreements with the Province binding those persons to privacy, confidentiality, and non-disclosure obligations as required by the Province and in a form approved by the Province, substantially the same as the privacy, confidentiality and non-disclosure obligations of this Agreement in whole or in part with regard to the particular circumstances, as determined by the Province.

4.12 Specific Privacy and Security Measures.

Without limiting any other requirement of this Article 4, and solely as it relates to matters within the control of the SSO and its Subcontractors, the SSO must:

(a) take all reasonable measures to ensure that all access to a Province System through an Interface Implementation appropriately uses the secure network or security technology that the Province certifies or makes available for that purpose, such as the Private Physician Network or any replacement or additional secure network or secure transport protocol. Unless otherwise agreed by the parties in writing, the use of any such network or technology by the SSO will be at its own cost and in accordance with the terms and conditions of use, including acceptable use policies, (if any) established by the Province and published in the Conformance Standards or otherwise communicated to the SSO from time to time by the Province in writing;
(b) have defined roles and responsibilities with respect to privacy and security for all Personnel and Access Subcontractors engaged in the provision of Interface Access Services;
(c) have audit and control procedures to monitor and enforce compliance with the privacy, security and confidentiality obligations of this Agreement;
(d) reasonably cooperate with the Province in the investigation or review of any privacy or security incident involving a Province System that, in the Province's reasonable opinion, was connected to an Interface Implementation or the use thereof by any person, including

by promptly providing copies of any applicable access logs or other relevant records to the Province, upon request;

(e) in relation to a privacy or security incident involving a specific Authorized User, comply with any reasonable direction of the Province regarding the suspension, restriction or logging of any further access by that Authorized User to a Province System through an Interface Implementation;

(f) on the Province's request not more than once per calendar year, sign and deliver to the Province a compliance certificate in a form provided by the Province, certifying that the SSO and its Subcontractors are in compliance with the requirements of this Article 4.

4.13 Definition of Confidential Information.

In this Agreement,

(a) "**Confidential Information**" of the Province means any technical, business, financial, personal, employee, operational, scientific or other information or data (including without limitation, the terms of this Agreement) of the Province or any person that has disclosed such information to the Province or its agents that, at the time of disclosure (i) is designated as confidential (or like designation) (ii) is disclosed in circumstances of confidence, or (iii) would be understood by a person exercising reasonable business judgement to be confidential. Province Confidential Information includes all such information or data in whatsoever form or media, whether in writing, in electronic form or communicated orally or visually. The Province Confidential Information specifically includes all Province Data, Disclosed Data, Province Proprietary Materials and any information of the Province or a third party person that is designated in the Conformance Standards as confidential (or similar designation). For greater certainty, the SSO will have no right in, and will have no right to restrict the use or disclosure by the Province, of any Province Confidential Information.

(b) "**Confidential Information**" of the SSO means any technical, business, financial, personal, employee, operational, scientific or other information or data of the SSO that is supplied to, obtained by, or that comes to the knowledge of the Province as a result of this Agreement and that is, at the time of disclosure (i) designated as confidential (or like designation) (ii) is disclosed in circumstances of confidence, or (iii) would be understood by a person exercising reasonable business judgement to be confidential. SSO Confidential Information specifically excludes any Province Confidential Information.

4.14 Safeguarding Confidential Information.

Each of the parties acknowledges and agrees that all Confidential Information of the other party, whether received or created before or after the effective date of this Agreement, will be received

in strictest confidence and held in accordance with and subject to the terms of this Agreement. The party receiving Confidential Information will retain such information in confidence and will treat it in accordance with the terms of this Agreement and with a degree of care no less than the degree of care that the receiving party employs for the protection of its own Confidential Information of a similar nature, provided that in any event the SSO will use no less than a reasonable degree of care to protect such Confidential Information.

4.15 Permitted Disclosure and Use of Confidential Information.

Subject to Sections 4.3 and 4.9 and all other obligations set forth in this Agreement, a Party may use and disclose relevant aspects of another party's Confidential Information to the extent reasonably necessary to perform its obligations and exercise its rights under this Agreement.

4.16 Exceptions to Obligation of Confidentiality.

Subject to Sections 4.3 and 4.9, the obligations of confidentiality contained in this Article 4 will not apply to any information to the extent that a party can reasonably demonstrate that such information:

(a) was, at the time of disclosure to the receiving party, in the public domain;
(b) after disclosure to the receiving party, is published or otherwise becomes part of the public domain through no fault of the receiving party;
(c) was in the possession of the receiving party at the time of disclosure to it and was not the subject of a pre-existing confidentiality obligation;
(d) was disclosed independently to the receiving party by a third party without any confidentiality obligations, provided such third party, or any other party from whom such third party receives such information, is not in breach of any confidentiality obligations in respect of such information;
(e) was independently developed by the receiving party without use of any Confidential Information of the other party;
(f) is disclosed with the prior written approval of the other party, but only to the extent approved by the other party; or
(g) is required to be disclosed by applicable law.

4.17 Notification of Unauthorized Use of Confidential Information.

Subject to 4.4, each party will promptly notify the other party of any unauthorized possession, use, access or disclosure, or attempt to effect the same, of the other party's Confidential Information by any person that may become known to such party.

4.18 Breach of Confidentiality.

In the event of a breach of this Article 4, and to the extent available pursuant to Applicable Laws (including, without limitation, the *Crown Proceeding Act* (British Columbia)), the non-defaulting

party will be entitled to preliminary and permanent injunctive relief, as well as an equitable accounting of all profits and benefits arising out of such breach, which remedy will be in addition to any other rights or remedies to which a party may be entitled under this Agreement or otherwise under any Applicable Laws.

4.19 No Rights to Confidential Information.

Nothing contained in this Article 4 will be construed as obligating a party to disclose its Confidential Information to the other party, or as granting or conferring on a party, expressly or implied, any right, title or interest or any license in or to the Confidential Information of the other Party.

ARTICLE 5 – AUDIT

5.1 Audit.

At the request of the Province, the SSO will:

(a) disclose to the Province the location of all premises from which the SSO or its Access Subcontractors provide Interface Access Services in relation to an Interface Implementation; and

(b) permit the Province and/or its representatives and agents to conduct periodic audits related to performance by the SSO of the SSO's obligations under this Agreement. Any such audit will be conducted on reasonable notice to the SSO and subject to the Province and its representatives agreeing to comply at all times with the SSO's or its Access Subcontractor's reasonable rules and regulations regarding safety, security, and conduct, while on the SSO's or its Access Subcontractor's premises.

ARTICLE 6 – INTELLECTUAL PROPERTY

6.1 Ownership of Province Proprietary Materials.

The Province (or its licensors, as the case may be) will be and remain the exclusive owner of all rights, title and interest, including all intellectual property rights, in and to:

(a) Province Proprietary Materials,
(b) Province Data, and
(c) Disclosed Data.

6.2 Ownership of Interface Implementation.

Subject to Section 6.1 and any written agreement between the parties to the contrary, the SSO (or its licensors, as the case may be) will be and remain the exclusive owner of all rights, title and interest, including all intellectual property rights, in and to an Interface Implementation.

6.3 Use of Province Training Materials and Province Proprietary Software by SSO.

Subject to the provisions of this Agreement, the SSO will have the non-exclusive, non-transferable right during the term of this Agreement, without cost or charge but subject to any third party rights as notified by the Province to the SSO, to: (i) use the Province Training Materials (if any) which the Province in its discretion makes available to the SSO for Interface Application Training, and (ii) use the Province Proprietary Software (if any) which the Province in its discretion makes available to the SSO for development or testing purposes (including Conformance Testing) or to enable Access to a Province System. All such use will be for the purposes of this Agreement and will be in accordance with the terms of this Agreement and the Conformance Standards, and will be subject to any restrictions, license terms or policies (including acceptable use policies) as reasonably determined by the Province, and any third party rights therein, all as may be notified in writing by the Province to the SSO, including as may be attached in Schedule A of this Agreement, as such Schedule may be updated or supplemented from time to time by notice from the Province to the SSO. In connection therewith, the following provisions will apply:

(a) the foregoing rights granted to the SSO do not give the SSO the right, and the SSO is not authorized, to (i) reverse engineer, disassemble, or decompile, alter, modify or create derivative works from the Province Proprietary Materials (other than to modify the Province Training Materials as expressly permitted by the Province), (ii) copy the Province Training Materials (except as required to distribute those training materials to SSO Customers and Authorized Users) (iii) copy the Province Proprietary Software (except that the SSO may make one copy in machine-readable form solely for backup purposes of the Province Proprietary Software components, if any, that are installed on the SSO systems, provided that the SSO reproduces on such copy the copyright notice and any other proprietary legends that were on the original), (iv) market the Province Proprietary Materials, (v) remove, obscure or modify any markings, labels or any notice of proprietary rights, including copyright, patent and trademark notices of the Province or its licensors from the Province Proprietary Materials, (vi) release the results of any testing or benchmarking of the Province Proprietary Materials without the prior written consent of the Province, or (vii) authorize any other Person to access or use the services of the Province Proprietary Software other than as may be expressly permitted in this Agreement;

(b) the foregoing rights are granted on an “as is” basis without representation, warranties or condition of any kind, whether oral or written or express or implied, and the Province specifically disclaims any warranties or conditions of fitness for a particular purpose, merchantability, merchantable quality, durability, satisfactory quality and non-infringement; and

(c) the foregoing rights will terminate upon the expiry or termination of this Agreement.

6.4 Other Access, Data Sharing and Third Party Agreements.

Notwithstanding Section 6.3, the Province reserves the right to require the SSO to enter into such separate license and other agreements as the Province may require with regard to access to and use of any Province Proprietary Materials or the access to and sharing of any data held or made available by the Province, including Province Data. The license granted by the Province to the SSO in Section 6.3 (i) will not extend to any matter referred to in the preceding sentence, and (ii) will not apply to any person (such as health authorities) other than the Province that may hold data or have software that the SSO may need to access or use in connection with the SSO providing software and/or services to SSO Customers.

ARTICLE 7 – REPRESENTATIONS AND WARRANTIES

7.1 SSO Representations and Warranties.

As of the date of this Agreement and throughout its term, the SSO represents and warrants to the Province as follows:

(a) the SSO has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement, and this Agreement has been duly executed and delivered by the SSO, and constitutes a legal, valid and binding obligation of the SSO enforceable against the SSO in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction;

(b) neither the execution and delivery of this Agreement, nor the compliance with the terms of this Agreement by the SSO:
   a. has resulted or will result in a violation of any Applicable Laws,
   b. has resulted or will result in a breach of, or constitute a default under, the SSO's constating documents, any shareholders' agreement to which it is a party, or any shareholder or directors' resolutions,
   c. has resulted or will result in a breach of, or constitute a default under, any instrument or agreement to which the SSO is a party or by which the SSO is bound, or
   d. requires the approval or any consent of any person or any governmental authority, except such as has been obtained as of the date of this Agreement.

ARTICLE 8 – DISCLAIMER, LIMITATION OF LIABILITY AND INDEMNITY

8.1 Disclaimer.

Access to a Province System is provided "as is", without warranty or condition of any kind, whether oral or written or express or implied, and the Province specifically disclaims any warranties or conditions of fitness for a particular purpose, merchantability, merchantable quality, durability, satisfactory quality and non-infringement. The Province does not warrant the

accuracy or the completeness of any information provided by the Province to the SSO under this Agreement, or that Access to a Province System will function without error, failure or interruption.

8.2 Information and Materials at SSO's Own Risk.

The SSO agrees that any information, or materials received or otherwise obtained by the SSO in connection with this Agreement is at the SSO's own risk. The Province is not responsible for the SSO's computer systems or loss of data that may result from Conformance Testing or any Access to a Province System.

8.3 Indemnity by SSO.

(a) The SSO will indemnify and save harmless the Province and the Province's employees and agents from any loss, claim (including any claim of infringement of third-party intellectual property rights), damage award, action, cause of action, cost or expense that the Province or any of the Province's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, (each a "**Loss**") to the extent the Loss is directly or indirectly caused or contributed to by: (i) any act or omission by the SSO or by any of the SSO's agents, employees, officers, directors or Subcontractors in connection with this Agreement; or (ii) any representation or warranty of the SSO being or becoming untrue or incorrect.

(b) The indemnification by the SSO pursuant to paragraph (a) is limited to:

(i) $2,000,000 per Loss; and

(ii) $4,000,000 in the aggregate for all Losses.

(c) The limitation set out in paragraph (b) does not apply to a Loss resulting from or relating to any of the following: (i) bodily injury or damage to real property or tangible personal property; (ii) third-party intellectual property rights; or (iii) a breach of Article 4 (*Privacy, Security and Confidentiality*).

(d) If the Province intends to make a claim for a Loss:

(i) then the Province will promptly notify the SSO in writing of the Loss as soon as reasonably practicable after the Province becomes aware of the Loss, provided that a failure by the Province to provide such notification will not invalidate the claim unless the SSO is materially prejudiced by that failure; and

(ii) if the Loss is on the basis of a third party claim that any element of an Interface Implementation infringes the intellectual property rights of any person,

(A) then, without limiting paragraph (a), the SSO will defend the Province against that claim at the SSO's expense and the SSO will pay all

associated costs, damages and legal fees that a court or arbitrator finally awards or are included in a settlement agreed to by the SSO, and

(B) the Province will cooperate with the SSO in the defence of the claim and, where appropriate in the discretion of the Province, will allow the SSO to appoint and instruct counsel and otherwise control the defence and any related settlement negotiations.

ARTICLE 9 – TERM AND TERMINATION

9.1 Five Year Term.

The term of this Agreement begins on the date first written above and will continue for five years after that date.

9.2 Termination by either Party.

Either Party may, on 60 days advance written notice to the other Party, terminate this Agreement for any reason or no reason.

9.3 Renewal.

The Parties may, by mutual written agreement, agree to renew this Agreement. The Province reserves the right to require any Interface Implementation that has previously passed Conformance Evaluation to undergo Conformance Evaluation again upon renewal of this Agreement.

9.4 Material Breach by SSO.

The SSO will be in material breach of its obligations under this Agreement upon the occurrence of any one or more of the following events (each a "**Material Breach**"):

(a) any direct or indirect assignment of this Agreement by the SSO contrary to Section 10.7;
(b) any disclosure of Province Data or Disclosed Data pursuant to a Disclosure Order contrary to Section 4.5;
(c) any breach of Article 4, including repeated minor breaches that have resulted in unauthorized access, collection, use, exposure or disclosure of Disclosed Data or Province Data and any storing, allowing access to, disclosure or use of Personal Information contrary to this Agreement or Applicable Laws, provided that before the Province determines, in its sole discretion, that the occurrence thereof constitutes a "Material Breach" the Province will have regard to all of the surrounding circumstances, including the nature and significance of the breach, the steps taken by the SSO to remedy the breach and the timeliness and effectiveness of such steps (it being understood that such consideration will in no way prevent the Province from determining that such breach constitutes a "Material Breach"); and

(d) if the SSO breaches any other obligation under this Agreement and fails to rectify that breach to the satisfaction of the Province within 30 days (or such longer period as may be agreed to by the Province on a case-by-case basis) of its receipt of written notice from the Province requesting it to do so, or, where such breach is not capable of being rectified within such timeframe, the SSO fails to take or continue to take such steps and actions as may be reasonably necessary to rectify such breach to the satisfaction of the Province.

9.5 Remedies of the Province

Without limiting any other rights or remedies of that the Province may have at law, in equity, or as otherwise set forth in this Agreement, upon the occurrence of a Material Breach the Province may at its option, elect to do any of the following:

(a) publicly disclose the fact and details of the Material Breach on its website or otherwise,

(b) by written notice to the SSO, direct that one or more of the Interface Implementation(s) affected by such breach (as determined by the Province) be immediately suspended, in which case the SSO will immediately stop providing, licensing or otherwise making such Interface Implementation(s) available to SSO Customers or any other third-party person until such time as further directed by the Province in writing, or

(c) by written notice to the SSO, terminate this Agreement, with immediate effect or on a future date specified in the notice.

9.6 Consequence of Expiration or Termination.

Unless the Province agrees otherwise in writing, upon expiration or termination of this Agreement:

(a) the SSO will no longer permit SSO Customers or Authorized Users to use the services, systems, networks and facilities of the SSO and/or its Access Subcontractors to access a Province System;

(b) the SSO will retain Disclosed Data in accordance with the data retention schedules set forth in the Conformance Standards; and

(c) the Province may disable or revoke all user access to a Province System that is made through or in connection with an Interface Implementation of the SSO.

ARTICLE 10 – GENERAL

10.1 Notices.

All notices necessary under this Agreement will be given in writing, and either personally delivered, or sent by registered mail, email or facsimile to the SSO at the address set out on the first page of this Agreement, and to the Province at:

Director, Conformance and Integration Services
Ministry of Health
1483 Douglas Street, 4th floor
PO Box 9635 STN PROV GOV
Victoria, BC V8W 9P1
Facsimile: (250) 356-6012
Email: HLTH.CISSupport@gov.bc.ca

Notices, if personally delivered or sent by facsimile or email, will be deemed to have been received the same day, or, if sent by registered mail, will be deemed to have been received 4 days (excluding Saturdays, Sundays and statutory holidays) after the date of mailing. Either party may give notice to the other of a substitute address from time to time, which from the date such notice is given will supersede for the purposes of this Agreement any previous address specified by the party giving notice.

10.2 Subcontracts.

No subcontract relieves the SSO from any of its obligations under this Agreement. The SSO must ensure that:

(a) any person retained by the SSO to perform obligations under this Agreement, and

(b) any person retained by a person referred to in paragraph (a) to perform these obligations

fully complies with this Agreement in performing the subcontracted obligations.

The terms of this Agreement will in all events be binding upon the SSO regardless of, and without regard to, the existence of any inconsistent or contrary terms in any agreements between the SSO and any Subcontractor, whether or not and without regard to the fact that the Province may have directly or indirectly been given or otherwise received notice of any such inconsistent term.

10.3 Severability.

If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

10.4 Entire Agreement.

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof.

10.5 Amendment.

No term of this Agreement may be amended except by written instrument signed by each of the Parties, or by a unilateral notice of declaration given or made by one Party pursuant to the terms of this Agreement, in respect of a change or amendment that such Party is entitled to make under the terms of this Agreement without the requirement for the approval of the other Party.

10.6 Waiver.

A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

10.7 Assignment.

The SSO must not, either directly or indirectly, assign any of the SSO's rights under this Agreement without the Province's prior written consent, which consent may be given or withheld in the discretion of the Province.

10.8 Survival.

The following provisions will survive the expiration or termination of this Agreement:

(a) Sections 2.1, 3.1, 3.2, 4.3, 4.9, 4.10 and 4.13 to 4.19, Articles 6 and 8 and Section 9.6,

(b) any provisions which by their nature are intended to survive, and

(c) any other provisions of this Agreement which are required for the proper interpretation of the provisions set forth in paragraphs (a) and (b) above.

10.9 Governing Law.

This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

10.10 Agreement not Fetter.

Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Province or its agencies of any statutory, prerogative, executive or legislative power or duty.

10.11 Binding Effect.

This Agreement will be binding upon and enure to the benefit of the parties and their respective successors and permitted assigns.

10.12 Costs.

The Province is not obligated to pay any amounts to the SSO for the performance of an Interface Implementation or the performance of the SSO's obligations under this Agreement, including under Section 4.12. All charges that the SSO wishes to make for, and all costs and expenses that the SSO incurs in, the performance of an Interface Implementation and the performance of the SSO's obligations under this Agreement will be, directly or indirectly, included in the SSO's charges to the SSO Customers.

10.13 Counterparts.

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

IN WITNESS WHEREOF the parties have executed this Agreement as of the date first written above.

SIGNED on behalf of Her Majesty the Queen in right of the Province of British Columbia by a duly authorized representative of the Minister of Health in the presence of:	
_____	_____
(Witness)	For the Minister of Health
SIGNED AND DELIVERED by @NAME-OF-SSO in the presence of:	
_____	_____
(Witness)	@NAME-OF-SSO

SCHEDULE A –ATTACHED RESTRICTIONS, TERMS, POLICIES REGARDING PROVINCE PROPRIETARY MATERIALS

The contents of this Schedule may be updated or supplemented from time to time by the Province on written notice ot the SSO.

[attach applicable restrictions, terms and polices regarding Province Proprietary Materials (i.e. Acceptable Use Policy for Non-Production IT Resources, etc.]

Schedule A: Acceptable Use Policy for Non-Production IT Resources

Table of Contents

1.0 Introduction

1.1 Key to Document Terminology

IT Resources: information and communication technologies that include, but are not limited to: information systems, devices, and the government electronic network.

Non-production environment: IT resources containing non-production data and used by software organizations for:

- development and integration testing (sandbox environment)
- conformance testing (conformance environment)
- training their clients (training environment)
- accessed by end users on an ongoing basis to refresh their understanding of and practice using ministry Health Information Exchange systems (HIE)

1.2 Purpose

This document defines the acceptable use of the Ministry of Health's (the `ministry') non-production environments and outlines the rules for sharing the environments and data with other organizations.

The acceptable use policy is used to protect IT resources from harm caused by the misuse of systems and data. Inappropriate use, either knowingly or unknowingly, exposes the ministry to risks that may compromise the security, stability and performance of its systems.

1.3 Intended Audience

This document is intended for organizations and their users that access ministry IT resources to develop and integrate their points of service (POS) applications with ministry health information exchange systems.

1.4 Ministry Contact

For more information or questions regarding this policy, contact Conformance and Integration Services at: HLTH.CISSupport@gov.bc.ca

2.0 Non-Production Environment Use

Each HIE system and infrastructure (e.g. HIAL, HNI, Client Registry, Provider Registry, PharmaNet and PLIS) has sandbox, conformance and training non-production environments that mirror the functionality of the production environments.

All users of these ministry environments have a duty to protect the security and integrity of ministry environments and the data within.

2.1 Acceptable Use

General:

The following are activities to which organizations and their users must abide:

1. Comply with all applicable ministry policies, regulations, provincial and federal legislation;
2. Use the IT resources for the purpose they are intended;
3. Protect the security, integrity and availability of all electronic information; and

4. Maintain a POS application instance and corresponding environment set up for each of the ministry environments.

Environment Use:

Sandbox may be used by software organizations for testing the development of an interface application and conducting a conformance self-test to validate compliance to the Conformance Standards.

Conformance is used by software organizations to demonstrate their application complies with all the requirements specified in the Conformance Standards.

Training may be used by organizations to demonstrate their interface application's functionality to end users. It may also be used by end users on an ongoing basis to practice tasks without affecting any real health information.

2.2 Unacceptable Use

The following are prohibited activities:

1. Users must not create personally identifiable or inappropriate data;
2. Illegal activities, including but not limited to: malware distribution, contravening copyrights and patents;
3. Activities and practices that have a negative impact on ministry systems and/or jeopardize the performance or availability of the government's network or information technology infrastructure. These include activities that slow down the environments;
4. Performing stress testing or batch updates that may affect performance unless prior approval is obtained from the ministry;
5. Attempting to circumvent or test the network, security systems and protocols; and
6. Using any part of the ministry information technology infrastructure for financial or personal gain.

2.3 Use of Shared Environments and Shared Data

The non-production environments are shared among multiple organizations and care must be taken to use the environments and data as specified.

In some cases, the data is assigned specifically to you for your sole use. In other cases, it is to be shared amongst other organizations.

The following apply to sharing environments and the data within:

1. Some data are identified as 'shared' so that all users of the environment can access this data in a read only context. This data, while not explicitly protected, must not be deleted, overwritten or modified. If it inadvertently has been, the vendor needs to notify the ministry;
2. Data assigned to another organization, while not explicitly protected, must not be deleted, overwritten or modified. If it inadvertently has been, the user needs to notify the ministry; and
3. All data in non-production environments must be fictitious. This pertains to both client and provider information, including identifiers (e.g., PHN, practitioner MSP ID or college ID). Data elements that require valid formats (e.g., postal code or a phone number) should not be related to a person. Refer to **Section 3** for more detailed information.

2.4 Organization Responsibilities

Organizations connecting to ministry IT resources have the following responsibilities:

1. Ensuring their employees are adequately informed and trained on:
    a. the appropriate use of the ministry non-production environments
    b. the privacy and security practices associated with the environment
2. Keeping information, such as connectivity details, network architecture and related information confidential;
3. Granting access only to authorized users of the ministry applications;
4. Not divulging, sharing or compromising their own or another's authentication credentials (e.g., passwords, access cards, etc.). This includes divulging passwords to technical support;
5. Immediately reporting any actual or suspected malware infection to the ministry; and
6. Immediately reporting any suspected or actual breach of this policy to the ministry.

2.5 Consequences

Consequences for violation of this policy may include the ministry:

1. Issuing a written warning;
2. Suspending or terminating system access;
3. Billing for administrative and damage costs incurred by the violation;
4. Billing for legal compensation for damage(s) caused by the violation; and
5. Applying other legal remedies.

The use of ministry IT resources for any illegal activity is cause for permanent disconnection of service. The ministry will cooperate with any criminal investigation and prosecution that may result from such activity.

3.0 Avoiding Introduction of Personally Identifiable (PI) Data

Examples of data considered potentially personally identifiable:

1. **Practitioner Data**
    - Practitioner Identifiers - college-issued IDs, names, birth and death dates
    - Contact information - addresses, telephone numbers, postal code
2. **Patient Data**
    - Patient Identifiers - PHN, names, birth and death dates
    - Contact information

3. **Provincial Data** [1]
    - Facility or point of service identifiers, e.g., facility ID, pharmacy ID and name
    - Facility manager or staff name
    - Contact information
    - MSP Contract Group Numbers

To help avoid introduction of personally identifiable data through vendor-created data, the following processes are implemented.

3.1 PHN Reclaim Process

a. Removal of data in PharmaNet associated with new PHNs assigned by the TPH transaction (e.g. patient information, address, claims, medication history, clinical data).

b. Data in the Software Vendor's local system will be out of synch with PNet.

c. In the event that the number of available new PHNs is trending to be depleted before the next scheduled reclaim, due to a high volume of TPH transactions performed by Vendors, an ad-hoc reclaim of new PHNs may be executed before the next scheduled PHN reclaim process. Vendors will be given notice by the Ministry's Conformance and Integration Services branch (CIS) prior to execution of an ad-hoc reclaim.

d. The initial execution date was **February 1, 2017**.

e. Subsequent PHN reclaims will be scheduled to run at the start of every quarter (i.e., April 1, 2017; July 1, 2017; October 1, 2017; January 1, 2018).

3.2 Automatic Denial of Data Process

a. Associated fields
    i. ZCC Segment
        1. Patient First Name
        2. Patient Last Name
    ii. ZPA Segment
        1. Area Code
        2. Address Prefix 1
        3. Address Prefix 2
        4. City
    iii. ZZZ Segment
        1. New Patient Keyword

b. The fields above will be validated upon receipt by PharmaNet against a list of acceptable values. Non-mandatory fields can continue to be submitted with blank values.

c. Any data entered that are **not** on the lists of acceptable values (including blanks) will be rejected by PharmaNet. This will result in an error with an incident number in the response message. During regular office hours (Monday to Friday, 8am-4pm PST) PharmaCare Operations can assist with diagnosing the issue, but we highly recommend that Vendors review the data

1 All confidential information of or relating to the Province, Province Customers, or Stakeholders other than confidential information that are not obligated to be treated [by vendors] as confidential;

in the request to ensure that it matches the lists of acceptable values provided by CIS.

d. An acceptable value for a patient's area code is *555*.

e. A list of acceptable values for patient first and last names, addresses and keywords is available by contacting Conformance and Integration Services at: HLTH.CISSupport@gov.bc.ca.

3.3 Nightly Cleanse Process

a. The nightly cleansing process started on **February 1, 2017.**

b. Fields cleansed:

iv. Segment ZPB
   1. Patient Condition
   2. Comment Text fields
   3. Directions

v. Segment ZPJ
   1. Directions

vi. Segment ZPP (V70 messages only)
   1. Entered By ID
   2. Drug Device Name
   3. Compound Instructions
   4. Compound Ingredients
   5. Directions
   6. Prescriber Notes
   7. Folio Number
   8. Rationale
   9. Instructions to Patient
   10. Follow Up Plan
   11. Patient Consent Name

c. Drug Device Name in the ZPP segment will be replaced with either the Brand name associated with the DIN/PIN or the Generic name associated with the GCN Sequence number.

d. All other fields will be replaced with a static string of maximum field size (e.g. THIS IS THE ADVERSE REACTION COMMENT TEXT AND IS EXACTLY 80 BYTES IN LENGTH).

e. Read-only data sets (i.e. integrated data and all vendor data sets) are excluded from the nightly cleanse and should never be changed by any Vendor.

f. Data in the Software Vendor's local system will be out of synch with PharmaNet (especially the free-text fields).

For questions, please contact HLTH.CISSupport@gov.bc.ca.