INTEGRATED ASSESSMENT RECORD

DATA SHARING AGREEMENT

Date: October 1, 2012

TABLE OF CONTENTS

DATA SHARING AGREEMENT

THIS AGREEMENT is effective as of the ___day of _____ (the "Effective Date").

B E T W E E N:

THE PARTICIPANTS LISTED HERETO IN SCHEDULE A,
AS AMENDED FROM TIME TO TIME

(each a "Participant" and collectively the "Participants")

and –

SUCH OTHER PARTIES as may from time to time become parties hereto by entering into an Adhesion hereto (hereinafter each called a "New Participant" and collectively the "New Participants")

and –

CONSOLIDATED HEALTH INFORMATION SERVICES ("CHIS"')

(together collectively the "Parties")

WHEREAS:

A. Each of the Participants provides health care to Clients/Patients (as hereinafter defined);

B. In providing such health care, each Participant is a Health Information Custodian (as hereinafter defined) with respect to Personal Health Information (as hereinafter defined) of Clients/Patients;

C. The Participants and CHIS are signatories to Existing Agreements (as hereinafter defined) related to the sharing of Personal Health Information of Clients/Patients from the Integrated Assessment Record (as hereinafter defined) on a regional basis;

D. The Participants and CHIS that are signatories to Existing Agreements wish to terminate the Existing Agreements and, as of the Effective Date, wish for the terms of this Agreement to apply to the sharing of Personal Health Information of Clients/Patients from the Integrated Assessment Record;

E. The Parties wish to implement a Provincial Integrated Assessment Record Solution ("Shared System") (as hereinafter more particularly described in Schedule C, which may be amended from time to time), which will allow Authorized Users of each Participant to access certain Personal Health Information of Clients/Patients by electronic means, in accordance with the *Personal Health Information Protection Act (PH/PA), 2004, Sch. A;*

F. The Parties wish to enter into this Agreement to outline the roles, rights, obligations, privacy, confidentiality and security responsibilities of each of them in relation to the Shared System; and

G. The Parties wish to provide for the expansion of the Shared System to New Participants who agree to become Parties to this Agreement by entering into an Adhesion Agreement (as hereinafter defined).

FOR VALUE RECEIVED, the receipt and sufficiency of which is acknowledged, the Participants and CHIS agree as follows:

ARTICLE 1
DEFINITIONS AND INTERPRETATION

1.1 Definitions

(a) "Adhesion Agreement" means the agreement signed by the New Participants as set out in Schedule "D";

(b) "Agent" means an "agent" as defined in PHIPA;

(c) "Agreement" means this Agreement and includes any amendments. supplements, schedules, exhibits or appendices attached, referencing this agreement or expressly made a part hereof; attached hereto;

(d) "Applicable Legislation" means the legislation and regulations applicable to the Parties in respect of their respective obligations under this Agreement, which includes but is not limited to PHIPA, the *Public Hospitals Act* (Ontario), the *Mental Health Act* (Ontario), the *Long Term Care Homes Act, 2007* (Ontario), the *Personal Information Protection and Electronic Documents Act* (Canada) and the respective regulations thereunder. as amended from time to time;

(e) "Authorized User" shall have the meaning assigned to it in Schedule "C"(V.29);

(t) "Business Day" means any day other than a Saturday, Sunday and statutory holiday observed in the province of Ontario;

(g) "CIDS" means Consolidated Health Information Services;

(h) "Circle of care" means certain defined health information custodians who may assume an individual's implied consent under section 20(2) of PHIPA for the collection, use or disclosure personal health information for the purposes of providing health care or assisting in the provision of health care, subject to the requirements of PHIPA;

(i) "Client/Patient/Consumer/Resident" means an individual who receives health care from a Participant. The term "Client/Patient" will be used in this Agreement to represent "Client/Patient/Consumer/Resident";

(j) "Confidential Information" means any oral, written or electronic data, including business information. personal information or personal health information that a Participant deliberately or inadvertently provides to its Designated IAR HINP which is treated as confidential by the Participant or would reasonably be treated as confidential by the Participant;

(k) "Consent Call Centre Services" shall have the meaning assigned to it in section 5.5;

(l) "Data Access Committee" or its successor shall have the meaning assigned to it in Schedule "J";

(m) "Effective Date" means the date first written above;

(n) "EMPI" means Enterprise Master Patient Index;

(o) "EMPI HINP" shall have the meaning assigned to it in section 3.2(c);

(p) "EMPI Services" shall have the meaning assigned to it in section 5.3;

(q) "Existing Agreements" means the agreements set out in Schedule "B";

(r) "Health Information Custodian" or "HIC" means a "health information custodian", as defined in PHIPA;

(s) "Health Information Network Provider" or "HINP" means a "health information network provider", as defined in the Regulation made under PHIPA;

(t) "HSN" means Health Sciences North;

(u) "IAR" means Integrated Assessment Record;

(v) "IAR HINP" shall have the meaning assigned to it in section 3.2(a);

(w) "IAR Provincial Steering Committee" or its successor is defined in section 5.6;

(x) "IAR Services" shall have the meaning assigned to it in section 5.2;

(y) "New Participant" means a HTC that is not currently a signatory to an Existing Agreement that signs the Adhesion Agreement and becomes a Party to this Agreement as a Participant;

(z) "Organization Privacy Officer" shall have the meaning assigned to it in section 6.1(t);

(aa) "Originating Participant" means, in relation to PHI, the Participant from whose electronic health information system such PHI is disclosed to the other Participants through the Shared System;

(bb) "Participant(s)" are the HICs that are signatories to this Agreement, as listed in Schedule "A", as updated from time to time;

(cc) "Permitted Purpose" shall have the meaning ascribed in section 2.2, as more particularly set out in Schedule "C";

(dd) "Personal Health Information" or "PHI" means "personal health information" as defined in PHIPA;

(ee) "Personal Information" or "PI" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization;

(ff) "PHIPA" means the *Personal Health Information Protection Act, 2004, Sch. A* (Ontario) and regulations thereunder, all as amended from time to time;

(gg) "Privacy and Security Committee" or its successor shall have the meaning assigned to it in Schedule "J";

(hh) "Privacy Impact Assessment" or "PIA" means a process for identifying, assessing. and mitigating privacy risks in respect of PHI belonging to individuals;

(ii) "Privacy/Security Breach" means an unauthorized theft. loss or disclosure of, access to or modification of PHI, whether inadvertent or intentional;

(jj) "Receiving Participant" means, in relation to PHI, the Participant to which PHI is disclosed from another Party through the Shared System;

(kk) "Regulation" means Ontario Regulation 329/04 made under PHIPA;

(II) "Reporting Services" shall have the meaning assigned to it in section 5.4;

(mm) "Shared System" means the Provincial IAR Solution as more particularly described in Schedule "C";

(nn) "Substitute Decision-Maker" or "SDM" means a 'substitute decision-maker" as defined in PHIPA;

(oo) 'Threat Risk Assessment" or "TRA" means a process for identifying, assessing, and mitigating threats, vulnerabilities and risks to the confidentiality, i ntegrity and availability of the PHI;

(pp) "WOHS" means William Osler Health System; and

(qq) The terms "collect', "disclose", "use", "health care", "individual", "information practices" and "record" have the respective meanings as defi ned in PHIPA.

1.2 Schedules

The current Schedules that form part of this Agreement are listed as follows:

Schedule "A" - Schedule "B" - Schedule ..C" - Schedule "D" - Schedule "E" - Schedule "F" -

Schedule "G" - Schedule "H" - Schedule "I" - Schedule "J" -

Parties to the Agreement Existing Agreements

Provincial Integrated Assessment Record Solution Adhesion Agreement

Plain Language Description of IAR Network Services and Security Safeguards Regarding

Confidentiality and Security of the IAR Enterprise Master Patient Index System

Reporting Services

Consent Call Centre Services

The Privacy and Security and Data Access Committees

1.3 Order of Precedence

In the event of any conflict between any of the provisions of the Schedules hereto and the body of this agreement, the provisions in the body of this Agreement shall govern. In the event of any conflict between any of the provisions of any Existing Agreements and this Agreement, the provisions of this Agreement shall govern.

ARTICLE 2
PURPOSE AND APPLICATION OF AGREEMENT

2.1 The purpose of this Agreement is to outline the responsibilities, obligations and rights of each Participant for the sharing of Client/Patient PHI through the Shared System and to outline the role, responsibilities and services to be provided by the HJNPs and Agents of the Participants with respect to PHI.

2.2 The Participants shall share PHI in accordance with the Permitted Purpose.

2.3 Despite section 2.2 above, the Participants may agree to expand the scope of information sharing beyond the Permitted Purpose and/or services as described in this Agreement. The Parties may agree to the provision of additional services or expand the scope of this Agreement by amending Schedule "C" in accordance with the amending provisions of this Agreement in section I 1.6(b).

ARTICLE 3
STATUTORY COMPLIANCE

3.1 Health Information Custodians (HICs)

Each Participant is a HIC and acknowledges and agrees that:

(a) it is a HIC subject to the Applicable Legislation. and it will comply with the Applicable Legislation;

(b) it is authorized by law to collect and upload the data that it collects to the Shared System;

(c) it will permit its Authorized Users to access the Shared System solely in their role as Agents of the HIC for the provision of health care to their Client/Patients;

(d) making PHI available to another Participant through the Shared System constitutes the disclosure of PHI pursuant to PHIPA;

(e) receiving PHI from another Participant through the Shared System constitutes the collection of PHI pursuant to PHIPA;

(f) in collecting PHI through the Shared System and using and disclosing such PHI, in accordance with the terms of the Agreement, each Participant has, pursuant to PHIPA, a reasonable basis on which to assume that it has the consent of the individual to collect, use and disclose the PHI within the Circle of Care; and

(g) it will not collect PHI through the Shared System, nor use or disclose the PHI so collected, if and to the extent that it is aware that the individual to whom the PHI relates has expressly withheld or withdrawn consent to such collection, use or disclosure, unless permitted or required by law.

3.2 Health Information Network Providers (HINPs)

The Parties acknowledge and agree that:

(a) in providing services to two or more HICs through the Shared System to enable the Participants to use electronic means to disclose PHI to one another, CHIS, HSN, and WOHS are each a health information network provider for the Shared System ("IAR HINP") and shall comply with the requirements with respect to a HINP in the Regulation;

(b) each Participant will be assigned one of CHIS, HSN, or WOHS to be its designated IAR HINP ("Designated IAR HINP");

(c) in providing services to two or more HICs through the Shared System to enable the Participants to use electronic means to disclose PHI to one another, CHIS is a HINP for the EMPI system ("EMPI HINP") and shall comply with the requirements with respect to a HINP in the Regulation;

(d) the requirements with respect to a HINP in the Regulation set out that HINPs enter into a written agreement with each HINP concerning the services provided to the HIC, that complies with the requirements of paragraph 7 of subsection 6(3) of the Regulation;

(e) the Parties wish to enter into this Agreement to comply with the said requirement and to provide for their compliance in other respects with PHIPA; and

(f) this Agreement constitutes compliance with the said requirement.

3.3 Agents

Each Participant:

(a) represents and warrants that it has the authority under PHIPA to collect, use and disclose Client/Patient PHI for the purposes of carrying out certain management,

operational and reporting responsibilities in relation to the Shared System (the "IAR Services"), the EMPI (the "EMPI Services"), reporting and data transfer services approved by the IAR Provincial Steering Committee (the "Reporting Services") and the "Consent Call Centre Services";

(b) authorizes its Designated IAR HINP as its Agent to collect, use and disclose Patient/Client PHI on its behalf for the purposes of carrying out the IAR Services and the Reporting Services; and

(c) authorizes CHIS as its Agent to collect, use and disclose Patient/Client PHI on its behalf for the purpose of carrying out the EMPI Services, the Reporting Services and the Consent Call Centre Services.

3.4 The Designated IAR HINPs and CHIS acknowledge and agree that in carrying out their respective responsibilities for IAR Services and EMPI Services they are Agents subject to the Applicable Legislation and will comply with the Applicable Legislation.

3.5 The Parties acknowledge and agree that this Agreement constitutes the agreement to be entered into between a HTC and its Agent.

ARTICLE 4
PERSONAL HEALTH INFORMATION

4.1 If and to the extent that a Participant collects and retains PHI through the Shared System, such Participant shall be deemed to have custody and control of such PHI for purposes of PHIPA, and shall be subject to the requirements of PHIPA. Each Participant shall be subject to the duties and obligations of a HIC in respect of such PHI and to the Client/Patient to whom it relates.

4.2 No Receiving Participant shall have authority to make any correction to any PHI contained in the Shared System related to the PHI of a Client/Patient that has been uploaded to the Shared System by another Participant, and shall so advise any Client/Patient (or Substitute Decision Maker (SOM) of a Client/Patient) who requests any such correction. Any such request for correction shall be directed back to the Originating Participant within a reasonable time frame, not to exceed five (5) Business Days of the receipt of such request, to be responded to by the Originating Participant in accordance with the provisions of PHIPA.

4.3 If any Participant receives a request from a Client/Patient for access to PHI that is contained within the Shared System that has not been uploaded to the Shared System by the Participant receiving the request, it shall direct the Client/Patient's request to the Originating Participant for response in accordance with the provisions of PHIPA.

4.4 If an Originating Participant becomes aware of an error in the PHI of one of its Clients/Patients in the Shared System, it shall, as soon as is reasonably practicable, make the correction in accordance with PHIPA and professional record keeping standards, and upload the corrected PHI to the Shared System as soon as possible.

4.5 If a Participant becomes aware that PHI it has collected from or uploaded to the Shared System has been subject to a Privacy/Security Breach, it shall, within a practical or reasonable time frame not to exceed two (2) Business Days, notify the Designated IAR

HINP and provide particulars of such occurrence, and its Designated IAR HINP will notify the Originating Participant within a practical or reasonable time frame not to exceed two (2) Business Days. The Originating Participant shall deal with such Privacy/Security Breach in accordance with its policies and procedures, and the Receiving Participant shall cooperate fully with the Originating Participant in dealing with such Privacy/Security Breach. The Designated IAR HINP shall also inform the other Parties about the Privacy/Security Breach in accordance with the integrated incident management process established and agreed to by all Parties.

4.6 If any Patty becomes aware that any PHI in the Shared System has been subject to a Privacy/Security Breach that has resulted from a failure of, or problem in the Shared System it shall forthwith notify its Designated IAR HINP thereof and provide reasonable particulars of such occurrence. The Designated IAR HINP shall immediately execute the integrated incident management process established and agreed to by all Parties.

4.7 If any Party receives a complaint from a Client/Patient about the collection, use or disclosure of their PHI, such Party shall forthwith:

(a) forward the complaint to the Originating Participant for response in accordance with the provisions of PHIPA if the complaint relates to the collection, use or disclosure of PHI by the Originating Participant; or

(b) if the Party receiving the complaint holds the opinion that the complaint relates to the management of the Client/Patient PHI within the Shared System, forward the complaint to the Designated IAR HINP, who will consult with any affected Parties. Any notification required of the Client/Patient shall be done by the Originating Participant and the Designated IAR HINP shall provide the particulars to the Originating Participant so that it may notify the Client/Patient.

4.8 If a Participant does not have the consent of the Client/Patient or their SDM to disclose the PHI through the Shared System, or becomes aware that the Client/Patient has withdrawn their consent, then that Participant shall ensure the Client/Patient's consent directive is registered in the Shared System as soon as reasonably practicable.

4.9 Subject to section 4.8, if a Participant does not have the consent of the Client/Patient or their SDM to disclose all PHI that the Participant considers reasonably necessary for the purpose of providing health care to the Client/Patient, the Participant shall notify the other Participants in accordance with PHIPA, that the Participant is not disclosing all of the PHI that it considers reasonably necessary for the purpose of providing health care to the Client/Patient.

4.10 While each Participant shall use reasonable efforts to ensure that PHI of Client/Patients that it uploads to the Shared System is accurate, complete and up-to-date as necessary for its own purposes, no Participant:

(a) warrants or represents to any other Participant the accuracy or the completeness of any PHI contained within the Shared System; or

(b) shall be held liable or responsible in any way for clinical uses of, or decision-making processes of any other Participant relating to the use of, any such PHI.

4.11 Each Participant acknowledges that its access, including access by its Authorized Users to the PHI Shared System is at that Participant's own discretion and risk.

ARTICLE S
MANAGEMENT AND COORDINATION

5.1 Each Party shall designate a member of its management team to be the primary contact ("Primary Contact") with the other Participants in respect of all technical and other issues arising in connection with the Shared System and/or this Agreement, other than for purposes of providing written notices as required under section 11.13.

5.2 IAR Services

(a) Each Participant designates their Designated IAR HINP to undertake certain management and operational responsibilities on its behalf under PHIPA in relation to the Shared System.

(b) The Designated IAR HINPs shall provide the IAR Services set out in Schedule "C"(II), as may be amended from time to time to each Participant for which they are the Designated HINP.

(c) The Designated IAR HINPs agrees with the Participants, to comply with the HINP Privacy Obligations set out in Schedule "C"(III) in the provision of the IAR Services.

(d) All Participants acknowledge and agree that, to the extent that their Designated IAR HINP is providing the IAR Services on behalf of each of them as a HIC, their Designated IAR HINP is acting as their Agent.

5.3 EMPI Services

(a) Each Participant designates CHIS, as HINP, to undertake certain management and operational responsibilities under PHIPA in relation to the EMPI System.

(b) As EMPI HINP, CHIS shall provide the EMPI Services set out in Schedule "G"(II), as may be amended from time to time, to the Participants.

(c) CHIS agrees, with the Participants to comply with the HINP Privacy Obligations set out in Schedule "G"(III).

(d) All Participants acknowledge and agree that, to the extent that CHIS is providing the EMPI Services on behalf of each of them as a HIC, it is acting as their Agent.

5.4 Reporting Services

(a) Each Participant designates CHIS. as its Agent to undertake certain management and operational responsibilities under PHIPA in relation to reporting and data transfer services approved by the IAR Provincial Steering Committee, as set out in Schedule "J".

(b) CHIS shall provide the Reporting Services set out in Schedule "H" as may be amended from time to time to the Participants.

(c) CHIS agrees with the Participants to comply with the privacy and security obligations set out in Schedule "H" in its provision of the Reporting Services.

(d) All Participants acknowledge and agree that, to the extent that CHIS is providing the Reporting Services on behalf of each of them, it is acting as their Agent.

5.5 Consent Call Centre Services

(a) Each Participant designates CHIS as its Agent to undet1ake certain management and operational responsibilities under PHIPA in relation to establishing and operating the Consent Call Centre Services.

(b) CHIS shall provide the Consent Call Centre Services set out in Schedule "I" as may be amended from time to time to the Participants.

(c) CHIS agrees with the Participants to comply with the privacy and security obligations set out in Schedule "I" in its provision of the Consent Call Centre Services.

(d) All Participants acknowledge and agree that, to the extent that CHIS is providing the Consent Call Centre Services on behalf of each of them, it is acting as their Agent.

5.6 IAR Provincial Steering Committee, or its successor

(a) Subject to the authority vested by each Party, an IAR Provincial Steering Committee shall be established to provide a governance structure for and to direct decision-making with respect to the management and operation of the Shared System and related matters as established by the Parties. The IAR Provincial Steering Committee shall be governed in accordance with Terms of Reference to be established and approved by the Parties, consistent with this Agreement.

(b) The IAR Provincial Steering Committee is responsible for approving any application from a New Participant who wishes to participate in this Agreement. Once approved by the IAR Provincial Steering Committee, the New Participant may become a Party to this Agreement by entering into an Adhesion Agreement.

(c) The IAR Provincial Steering Committee shall establish a Privacy and Security Committee and a Data Access Committee with the responsibilities as described in Schedule "J" and any other representative committee(s) to govern the management and operation of the Shared System and related matters as established by the Parties.

ARTICLE 6
PARTICIPANT OBLIGATIONS

6.1 Each Participant acknowledges and agrees that:

(a) it shall take steps in compliance with PHIPA to ensure that Clients/Patients are knowledgeable about the purposes of the collection, use and disclosure of their PHI uploaded to the Shared System and that they may give or withhold their consent to the sharing of their PHI through the Shared System;

(b) it will access PHI through the Shared System only in compliance with this Agreement

and Applicable Laws;

(c) its Authorized Users shall not make any entry on or alter in any way the PHI in the Shared System related to a Client/Patient of another Participant that has been uploaded to the Shared System by that other Participant;

(d) it shall retain PHI which is subject to this Agreement in accordance with applicable retention periods, and in any event, as long as necessary to allow a Client/Patient to exhaust his or her access rights under PHIPA;

(e) it shall take steps in compliance with PHIPA to adhere to jointly adopted policies and procedures for the Shared System;

(f) it has designated a person responsible for the protection of PHI and the privacy of Clients/Patients relative to this Agreement **("Organization Privacy Officer"),** as identified in Schedule "A". It is acknowledged that an Organization Privacy Officer may delegate their responsibilities and authority under this Agreement to another individual within their respective organization; and

(g) it shall take steps in compliance with PHIPA to fulfill the Participant Obligations set out in Schedule "C"(IV).

ARTICLE 7
PARTICIPANT PRIVACY AND SECURITY PRACTICES

7.1 Each Participant acknowledges and agrees that:

(a) it is responsible for ensuring the integrity and good working order of its own infrastructure, hardware and software systems that comply with industry standards as necessary to support access to the Shared System;

(b) it has information practices in place that comply with PHIPA, and that address its practices relating to the collection. use, disclosure, retention and disposal of PHI, and it monitors and enforces compliance with its own information practices:

(c) it shall take reasonable steps to ensure the physical, administrative, and technological security of PHI in its custody or control and to prevent theft, loss and unauthorized access, copying, modification, use. disclosure or disposal of PHI;

(d) it shall maintain such policies, procedures and systems as necessary to prevent unauthorized persons from having access to, collecting, using, disclosing, modifying, disposing, copying, stealing or otherwise committing any other act that could breach or compromise the confidentiality, availability, accessibility, integrity, structure, format or content of the PHI of a Client/Patient that has been uploaded into the Shared System by another Participant, or the privacy of that Client/Patient;

(e) it shall ensure that its Agents, including its Authorized Users, are aware of and comply with the requirements of this Agreement with respect to the sharing of PHI through the Shared System;

(f) it has provided training to its Agents, including its Authorized Users, with respect to

its legal obligations relating to privacy and PHI, generally, and will provide additional training as required with respect to its specific obligations to protect PHI under this Agreement;

(g) it shall conduct a privacy and security self-assessment according to the checklist approved by the Privacy and Security Committee, at its own cost, on an annual basis. The results of the self-assessment shall be signed off by the Participant's senior management and submitted to the Privacy and Security Committee for review; and

(h) for the purposes of ensuring compliance with this Agreement, the Privacy and Security Committee may recommend to the IAR Provincial Steering Committee that specific privacy or security audits, reviews and/or assessments be conducted of the privacy and/or information security practices of one or more Participants at their own cost. Upon approval from the IAR Provincial Steering Committee, the Privacy and Security Committee, upon reasonable notice, will work with the Participant to assess, review and improve the Participant's privacy and/or information security practices as they relate to the obligations of the Participant

under this Agreement. For these purposes, each Participant shall cooperate with any privacy or security review or assessment, which shall be carried out in such a manner as not to interfere unduly with the day-to-day operations of the Participant.

ARTICLE 8
TERM AND TERMINATION

8.1 The Participants and CHIS agree that the Existing Agreements shall terminate on _____and that as of the Effective Date, the terms of this Agreement shall apply to all PHI of Clients/Patients from the Integrated Assessment Record that has been or will be uploaded to the Shared System.

8.2 This Agreement shall commence as of the Effective Date, and shall remain in force and effect until terminated in accordance with this Agreement.

8.3 Withdrawal of a Participant. A Participant ("Withdrawing Participant") shall have the right to withdraw from and terminate its rights and obligations under this Agreement upon providing not less than ninety (90) Days' written notice to the IAR Provincial Steering Committee. The Withdrawing Participant shall, at the time of the provision of notice in accordance with this section, liaise with the IAR Provincial Steering Committee regarding ongoing obligations arising from PHIPA in respect of Client/Patient PHI that the Withdrawing Participant has uploaded to the Shared System.

8.4 Withdrawal of a HINP or Agent. CHIS, WOHS, and HSN acting in the capacity of a HTNP or Agent, shall have the right withdraw from and terminate its rights and obligations under this Agreement upon providing not less than six (6) months written notice to the IAR Provincial Steering Committee.

8.5 Termination of a Participant for Default. If a Participant ("the Defaulting Participant") is in material default of its obligations under this Agreement, the IAR Provincial Steering Committee may give notice of default to the Defaulting Participant, specifying the nature of the default, and if the Defaulting Participant has not within thirty (30) days after receipt of such notice, cured such default, the IAR Provincial Steering Committee may terminate

a Participant for Default. It is the responsibility of the Privacy and Security Committee to determine whether the Participant is in default of its obligations and to recommend to the IAR Provincial Steering Committee the termination of the Participant. Prior to the termination of a Defaulting Participant in accordance with this section, the IAR Provincial Steering Committee shall liaise with the Defaulting Participant regarding ongoing obligations arising from PHIPA in respect of Client/Patient PHI that the Defaulting Participant has uploaded to the Shared System.

8.6 Termination of Agreement. This Agreement will terminate in the following circumstances:

(a) should the withdrawal or termination of Participants under this Agreement leave only one Participant remaining;

(b) should CHIS, WOHS and/or HSN in their role as a HINP and/or Agent withdraw from this Agreement;

(c) upon the agreement of all Parties to terminate this Agreement;

(d) upon an order or direction from the Minister of Health and Long-Term Care for the Province of Ontario, applicable to participating Local Health Integration Networks or regulatory body that is inconsistent with the ability of the Parties to fulfill the terns of this Agreement, or in the event that insufficient funding is available to support the Shared System, the IAR Provincial Steering Committee may terminate this Agreement.

8.7 Upon termination of this Agreement with respect to a Participant, such Participant will immediately take all necessary action to suspend access by its Authorized Users to the Shared System and cease uploading the PHI of its Clients/Patients to the Shared System. Upon the date of termination or withdrawal, the Designated IAR HINP shall ensure that the Participant's access, including all of its Authorized Users except the Organization Privacy Officer to the Shared System is terminated. Any PHI uploaded to the Shared System by the Withdrawing Participant will no longer being updated.

8.8 Upon its termination from this Agreement in accordance with Section 8.3, the Participant shall continue to be bound by its obligations under this Agreement relating to privacy and confidentiality. In particular, the Organization Privacy Officer of the Participant shall continue to participate in the integrated consent management process and the integrated breach management process as required.

8.9 Notwithstanding that a Participant's access to the Shared System has been terminated, the PHI disclosed to such Participant through the Shared System and which part of individual records of PHI shall remain with the Participant, which shall remain subject to all of its duties and obligations in respect thereof under Applicable Legislation.

ARTICLE 9
LIABILITY AND INDEMNIFICATION

9.1 Each Party (an "Indemnitor") shall indemnify, defend and hold harm less each other Participant and its agents, officers, directors, successors and permitted assigns (collectively, "Indemnitees"), from and against all loss, cost and expense, including all legal expense on a full recovery basis, incurred by the Indemnitees or any of them as a result of or arising

from any:

(a) default by the Indemnitor (which term in this and the following clauses shall be read as including its agents. officers and directors) in the performance of any of its duties or obligations hereunder;

(b) breach of privacy or confidentiality by the Indemnitor;

(c) negligent act or omission of the Indemnitor; or

(d) statutory offences committed by the Indemnitor.

9.2 No Party shall be liable to the other Parties for:

(a) A Party's inability to access PHI through the Shared System for any reason. Each Party acknowledges that connectivity, upgrades, routine maintenance, emergencies and other causes may prevent access to the Shared System from time to time; or

(b) Any liability resulting from a Participant's use of its own record of PHI.

9.3 The HINPs shall not be liable to the Participants for failure to provide access to the electronic infrastructure. Each Participant acknowledges that connectivity, upgrades, routine maintenance, emergencies and other causes may prevent access to the Shared System from time to time.

9.4 Each Participant acknowledges that it is accessing PHI through the Shared System on an "as is" basis, at its own risk, and there is no representation, warranty or covenant made or provided by any other Participant that the PHI is accurate, complete or up-to-date.

9.5 The Parties shall cooperate with one another in the defense of any such action, including providing one another with prompt notice of any such action and the provision of all material documentation. The Parties further agree that they have a right to retain their own counsel to conduct a full defense of any such action.

ARTICLE 10
DISPUTE RESOLUTION

10.1 If a dispute arises between any of the Parties to this Agreement, reasonable commercial efforts will be made to resolve the dispute as effectively and quickly as possible. Disputes will be resolved as follows:

(a) Disputes between the Parties will be resolved among the Primary Contacts of the Parties; and

(b) If such disputes cannot be resolved among the Primary Contacts within two weeks, the issues will be discussed and resolved by the Executive Directors/Chief Executive Officers of the Parties.

10.2 Nothing in this Agreement shall interfere with a Party's ability to avail themselves of injunctive or other relief.

10.3 Nothing in this Agreement shall be construed to interfere with a Party's ability to consult

with either its legal counsel or representatives of any professional organization that regulates or accredits health care organizations or health care practitioners.

ARTICLE 11
GENERAL

11.1 Severability - Should any provision of this Agreement be found to be invalid by a court of competent jurisdiction, that provision shall be deemed severed, and the remainder of this Agreement shall remain in full force and effect.

11.2 Governing Laws – This Agreement shall be governed by the laws of Ontario and the federal laws applicable therein. The Parties consent and submit to the exclusive jurisdiction of the courts of the Province of Ontario in any action or proceeding instituted under this Agreement.

11.3 Entire Agreement - This Agreement contains all of the agreements, representations and understanding of the parties and supersedes and replaces any and all previous understandings, commitments or agreements, oral or written, related to the subject matter hereof. Any amendment to this Agreement must be in writing and signed by duly authorized officers of each party.

11.4 Force Majeure - No Party shall be liable for any delay or failure in the performance of this Agreement if caused by an act of God or any factor beyond the reasonable control and not reasonably foreseeable by such Party, or as the result of the failure of a third party to comply with its obligations and responsibilities to provide materials or information as specified within this Agreement. In such event, the affected Party shall notify each other Party as soon as possible of such force majeure condition and the estimated duration of such condition.

11.5 Consent to Breach not Waiver - No provision of this Agreement shall be deemed to be waived and no breach shall be deemed to be excused unless such waiver or consent is in writing and signed by the Party said to have waived or consented. No consent by a Party to, or waiver of, a breach of any provision by another Party shall constitute consent to, or waiver of, any different or subsequent breach.

11.6 Amending Procedure and Schedule Amendments

(a) This Agreement may be amended by the written agreement of the Parties.

(b) Without limiting the generality of subsection 11.6(a), at any time and from time to time during the Term of this Agreement, any of the Parties may request amendment (a **"Schedule Amendment")** to the Schedules hereto. The Party submitting the request shall specify the nature of the proposed Schedule Amendment and the reasons therefore.

(c) The Schedule Amendment shall be reviewed by the IAR Provincial Steering Committee on behalf of all Parties and. if deemed appropriate shall be executed by all Parties and deemed incorporated into this Agreement.

11.7 Changes that Affect the Agreement - The Parties undertake to give one another written notice of any changes in legislation, regulations or policies respecting those Parties and

programs that are likely to affect this Agreement.

11.8 Independent Contractors - This Agreement does not constitute and shall not be construed as constituting a partnership or joint venture between the Parties. Except as expressly set out herein, no Party shall have any right to obligate or bind any other Party in any manner whatsoever. Each Party shall ensure that neither it nor any of its agents represents to any third party that it or they have authority to bind any other Party.

11.9 Survival - The provisions of this Agreement which by their nature extend beyond the expiry or termination of this Agreement shall survive and remain in effect until all obligations are satisfied, including but not limited to Article 9.

11.10 Counterparts - This Agreement may be executed in several counterparts, each of which shall be deemed to be an original and such counterparts together shall constitute one and the same Agreement and notwithstanding their date of execution shall be deemed to be executed on the date first written above. The delivery of an executed counterpart copy of this Agreement by facsimile or by electronic transmission in portable document format (PDF) shall be deemed to be the equivalent of the delivery of an original executed copy thereof.

11.11 Invalidity - Should any provision of this Agreement be held to be invalid by a court of competent jurisdiction, then that provision will be enforced to the extent permissible, and all other provisions will remain in effect and are enforceable by the Parties.

11.12 Assignment - This Agreement shall not be assigned without the consent of IAR Provincial Steering Committee. Subject to this, the Agreement is binding upon the Parties their successors and permitted assigns.

11.13 Notices - Any notice, document or other communication required or permitted to be given under this Agreement shall be in writing and shall be sufficiently given if sent by prepaid mail, if delivered personally or if sent by facsimile transmission to the address and contact person of the other Parties or on such other Party's Adhesion or to such other address, fax number or person that a Party designates. Any notice delivered personally to a Party shall be deemed to have been given and received on the day it is so delivered. Any notice mailed to a Party shall be deemed to have been given and received on the fourth Business Day next following the date of its mailing provided no postal strike is then in effect or comes into effect within three Business Days after such mailing. Any notice transmitted by fax or delivered shall be deemed to be given and received on the day of its transmission or delivery, if on a Business Day, or if not a Business Day, on the next following Business Day.

IN WITNESS WHEREOF each of the Parties has executed and delivered this Agreement by its duly authorized representative who has authority to bind the Party to this Agreement.

Organization: _____

Signature: _____

Name: _____

Title: _____

Date: _____

I/We have the authority to bind the corporation

SCHEDULE A
PARTIES TO THE
AGREEMENT

Participants	**Address and Contact Person for the Notice**	**Privacy Contact Person**
The Corporation of the City of London	300 Dufferin Avenue , London , ON , N6A 4L9 Attention : Cathy Saunders Title – City Clerk Telephone : 519 661 2500 ext 4937 Email : csaunder@london.ca	Name: Angie Heinz Title : Administrator Telephone : 519 661 2500 ext8260 Facsimile: 519 661 0446 Email: aheinz@london.ca
CHIS		

SCHEDULE B

EXISTING AGREEMENTS

Greater Toronto Area LHINS Data Sharing Agreement, effective as of November 15, 201 1

North East Cluster LHIN Integrated Assessment Record Data Sharing Agreement, effective as of June I, 201 1

South Western Cluster LHIN Integrated Assessment Record Data Sharing Agreement, effective as of January 25, 2012

SCHEDULE C
PROVINCIAL INTEGRATED ASSESSMENT RECORD SOLUTION

I. IAR SOLUTION DESCRIPTION

1. The Provincial Integrated Assessment Record ("IAR") solution is a Shared System that enables health care providers to access common assessment data, which will in tum facilitate collaborative Client/Patient care.

2. "Assessment Data" refers to the data elements comprising the:

   (a) Ontario Common Assessment of Need, Staff and Client Version, Staff Comments only or "OCAN";

   (b) Resident Assessment Instrument Mental Health or "RAI-MH©" assessment tools;

   (c) Admission and Discharge Criteria and Assessment Tools or "ADAT';

   (d) interRAI Community Health Assessment or "CHA";

   (e) interRAI Preliminary Screener;

   (f) Resident Assessment Instrument Home Care or "RAI-HC";

   (g) interRAI Contact Assessment or "CA"; and

   (h) other assessment tools as may be approved for inclusion in IAR by the IAR Provincial Steering Committee, as amended from time to time by external entities such as the Canadian Institute for Health Information ("CIHI") and other identified working groups.

3. Clients/Patients of the Participants often seek healthcare services from more than one Participant and the Participants would like to access Assessment Data collected by each of the Participants about such Clients/Patients in order to provide the best possible services to them.

4. The Shared System provides a central repository for Assessment Data collected by the Participants for Clients/Patients and through two secure interfaces, perm its the Participants to upload Assessment Data and perm its Authorized Users from the Participants to view Assessment Data stored on the Shared System.

5. Authorized Users from each of the Participants are authorized to access the Assessment Data of Clients/Patients on a need to know basis. for the purpose of providing health care or assisting in provision of health care (the **"Permitted Purpose")** in accordance with PHIPA.

6. The implementation and operation of the Shared System is managed by CHIS, HSN, and WOHS in accordance with the terms of this Agreement, acting as HINPs.

7. As HICs, HSN, and WOHS shall each also act as a Participant in the Shared System.

II. IAR SERVICES

8. The HINPs shall directly or where authorized, through a contracted third-party, provide

the following IAR Services to each Participant for which they are the Designated IAR HTNP:

(a) establish a pre-production and production environment for the Shared System;

(b) host and maintain the Shared System in a secure environment for submission and transmission of PHI;

(c) manage servers and network, including but not limited to system configurations, patches and upgrades;

(d) provide support for the technology, administration, operation and confidentiality and security of the PHI in the Shared System either through the direct provision of services or a contracted third party;

(e) coordinate access to Assessment Data to the users authorized by the Participants;

(f) establish a disaster recovery plan, including a data backup facility and processes and procedures to ensure the continued availability of the Assessment Data in the event of the disaster;

(g) appoint an individual(s) (the "HINP Privacy Officer") who will have overall responsibility for the privacy and security of the Shared System;

(h) implement, in conjunction with the Participants, an integrated incident management process to deal with Privacy/Security Breaches by the Participants and Privacy/Security Breaches by the HINP and which includes notification to affected individuals;

(i) inform the Participants if there has been a Privacy/Security Breach by the HINP or unauthorized access by a person other than the Authorized Users of Participants, in accordance with the provisions of the integrated privacy and security incident management process;

U) implement, in conjunction with the Participants, an integrated consent management process to deal with Client/Patient's request to withhold/withdraw or reinstate their consent to share their Assessment Data with all of the Participants;

(k) implement, in conjunction with the Participants, an integrated client privacy support process to handle Client/Patient's request for access or correction to the record of PHI or to challenge to the Shared System's privacy practices;

(l) manage data retention within the Shared System. PHI in the Shared System will be retained for a period not exceeding two (2) years;

(m) implement, in conjunction with the Participants, logging, auditing and monitoring policies and procedures including communication of these controls to all Authorized Users and to the Participants;

(n) ensure that all system changes follow the HINP's change control process;

(o) upon direction from the IAR Provincial Steering Committee, terminate Participant access, including the access of all of its Authorized Users, except as set out in

section 8.7, to the Shared Service, within one (I) Business Day of the effective date of the terminate of the Participant from this Agreement;

(p) use reasonable efforts to ensure that the Shared System is available to all Participants on a 24/7 basis, except in accordance with sections (q) and (r) below;

(q) use reasonable efforts to schedule any planned outages or system downtime, at a time when it does not interfere with access by Authorized Users for purposes of Client/Patient services and to provide the Participants with at least ten (10) Business Days' notice of such outage or downtime; and

(r) provide notification to all Participants of any unplanned outage or downtime as soon as reasonably possible.

III. OBLIGATIONS OF THE HEALTH INFORMATION NETWORK PROVIDERS

9. WOHS and HSN, in addition to being a Participant in the Shared System, and CHIS, shall be an IAR HINP and shall comply with all of the obligations of a HINP under PHIPA, subject to the exception that each may collect, use and disclose PHI in the course of executing its other roles as permitted in this Agreement.

10. No HINP shall use any PHI to which it has access except as necessary to provide the HINP Services described in this Agreement or as authorized and directed by the IAR Provincial Steering Committee, and shall not disclose any PHI to which they have access in the course of providing the IAR Services except as required for the provisions of the services.

1 1. No HINP shall allow its Agents to have access to PHI unless such Agent(s) agree(s) to comply with the restrictions that apply to the HINP.

12. The HINPs shall notify the Participants at the first reasonable opportunity if they have accessed, used, disclosed or disposed of PHI other than in accordance with this Agreement or if an unauthorized person accessed the PHI.

13. The HINPs shall provide to each Participant a plain language description of the services that it provides to the Participants as mandated by the Regulation. The Participants can share this description with the individuals to whom the PHI relates. This will include a general description of the safeguards in place to protect against unauthorized use and disclosure, and to protect the integrity of the information. This description will take substantially the same form as set out in Schedule "E".

14. The HINPs shall, as per requirement of the Regulation. make available to the public:

(a) the description referred to above;

(b) any directives, guidelines and policies of the HINPs that apply to the services that they provide to the Participants to the extent that these do not reveal a trade secret or confidential scientific, technical. commercial or labor relations information; and

(c) a general description of the safeguards implemented by the HINP in relation to the security and confidentiality of the information.

15. The HINPs shall to the extent reasonably practical. and in a manner that is reasonably practical, keep and make available to each Participant for which they act as the Designated IAR HINP, on the request of such Participant, an electronic record of:

(a) all accesses to all or part of the PHI that has been uploaded to the Shared System by the Participant being held in equipment controlled by the HINP. The record shall identify the person who accessed the information and the date and time of the access; and

(b) all transfers of all or part of the PHI that has been uploaded to the Shared System by the Participant by means of equipment controlled by the HINP (whether to third party service providers, or otherwise). The record shall identify the person who transferred the information and the person or address to whom it was sent, and the date and time it was sent.

16. Each HINP shall perform, and provide to the satisfaction of Participants for which it acts as the Designated IAR HINP, a written copy of the results of an assessment of the IAR Services with respect to:

(a) threats, vulnerabilities and risks to the security and integrity of the PHI (often called a "Threat and Risk Assessment,, or "TRA"); and

(b) how the IAR Services may affect the privacy of the individuals who are the subject of the information (often called a "Privacy Impact Assessment" or "PIA").

17. Each HINP will review and develop to the satisfaction of all Participants, a mitigation plan for all high priority risks outlined in the PIA and TRA.

18. Each HINP shall ensure that any third party it retains to assist in providing services to the Participants agrees to comply with the restrictions and conditions that are necessary for the HTNP to comply with this Schedule "C"(III).

19. With the exception of the PHI of its own Clients/Patients, WOHS and HSN in their role as HINPs have no responsibility for the accuracy of any PHI within the Shared System. CHIS has no responsibility for the accuracy of any PHI within the Shared System.

20. The HINPs shall have in place information practices that comply with the requirements of PHIPA and the Regulation, and shall comply with their own information practices.

21. The HJNPs will take steps that are reasonable in the circumstances to ensure that:

(a) PHT is protected against theft, loss and unauthorized use or disclosure; and

(b) The records containing the PHI are protected against unauthorized copying, modification or disposal.

22. In addition to the obligations under sections 20 and 21 above, the HINPs will work with the Participants to develop and/or implement and maintain the administrative, technical and physical safeguards set out in Schedule "F" to this Agreement.

23. The HINPs will hold the Participant's Confidential Information in strictest confidence,

and in any case with no less protection and security than they protect their own Confidential Information.

24. In the event that a HINP receives a court order or other lawful requirement of a court or government agency of competent jurisdiction requiring the disclosure of some or all of a Participant's Confidential Information, the HINP shall first advise the HICs for which it acts as the Designated IAR HINP about the receipt of such court order so that the HIC(s) may be given an opportunity to intervene, e.g., to seek a protective order against such disclosure. This obligation survives the termination or expiration of this Agreement.

IV. OBLIGATIONS OF THE PARTICIPANTS

25. Each Participant agrees to:

(a) ensure that it has obtained knowledgeable consent of the Client/Patient or their SOM for the sharing of the Assessment Data of that Client/Patient through the Shared System;

(b) upload the Assessment Data related to its Client/Patients to the Shared System within a practical or reasonable time frame not to exceed two (2) Business Days on which such assessment is completed;

(c) notify its Designated IAR HINP of any Client/Patient consent directives in relation to the sharing of Assessment Data of that Client/Patient through the Shared System as soon as reasonably practicable, and in any event within two (2) Business Days upon receiving the consent directive from the Client/Patient;

(d) use reasonable efforts to ensure that all PHI of its Clients/Patients is accurate, complete and as up-to-date as necessary for its own purposes;

(e) establish User Account Management Procedures as agreed by all Parties and follow it for every Authorized User; provide tier I support for use of the Shared System, including but not limited to, the provision of training and user support to their Authorized Users; and terminate the use by its Authorized Users of the Shared System, if the authorization of the individual has been terminated or if the Agreement in respect of the Party has been terminated;

(f) establish logging, auditing and monitoring policies and procedures including communication of these controls to all Authorized Users;

(g) establish an incident management process to identify, escalate, investigate and report any privacy and security incident relating to the PHI in the Shared System which affects the Participant's Clients/Patients, such process to interface with and support the IAR integrated incident management process;

(h) establish a consent management process to manage Client/Patient requests to withhold/withdraw or reinstate the consent directive for any assessment conducted by the party, which process must interface with and support IAR integrated consent management process;

(i) establish a client privacy support process to handle Client/Patient requests to access, or make correction to their PHI, or challenge the organization's privacy practices, which process must interface with and support the IAR integrated client privacy support process.

(j) establish an EMPI process to manage the issues with the PI and PHI collected and processed in the EMPI system, which process must interface with and support the IAR integrated EMPI support process.

26. Each Participant shall keep the Assessment Data from the Shared System confidential and secure and shall use the same degree of care to protect IAR Assessment Data as the Participant uses to protect its PHI of a like nature, but in any event, it shall not use a standard of care that is less than a reasonable standard of care.

27. Each Participant shall continue to meet or exceed the level of data protection required as HICs within the Shared System, as the case may be, pursuant to the applicable provisions of PHIPA or other Applicable Legislation.

V. ACCESS TO SHARED SYSTEM

28. Access to the Shared System shall be determined by each Participant in accordance with established need and predetermined criteria.

29. A Participant may designate as authorized users of the Shared System ("Authorized Users") employees and agents of such Participant who have. in accordance with such Participant's own internal policy (the "Access Control Policy"), been granted access to the Shared System. The Participants agree that the Access Control Policy will, among other matters require that the Authorized User has:

(a) a need to access Client/Patient PHI in the Shared System to perform his or her employment responsibilities or assigned duties for that Participant;

(b) entered into a written user agreement with the Participant; and

(c) undertaken the requisite training to use the Shared System.

30. No Participant shall grant access to an Authorized User unless such person has met the requirements set out in section 29 above.

31. If a Participant revokes or suspends an Authorized User's right of access to the PHI of its own Clients/Patients, such Party shall:

(a) immediately advise its Designated IAR HINP of the need to revoke or suspend, as the case may be, such Authorized User's access to the Shared System; and

(b) if such suspension or revocation is the result of actual or alleged Privacy/Security Breach by such Authorized User of this Agreement or the Applicable Legislation (including without limitation abuse or misuse of PHI), follow the integrated privacy and security incident management process established and approved by all Parties.

32. Each Participant agrees that it is responsible for the actions of its Authorized Users in connection with the Shared System.

SCHEDULE D
FORM OF ADHESION

INSTRUMENT OF ADHESION dated this ____ day of_____, 2016 (the **"Adhesion Date")** by *The Corporation of the City of London* (the **"New Participant")** to the

Integrated Assessment Record Data Sharing Agreement made as of the 1st day of October, 2012 among the Parties, or as may prior hereto have entered into instruments of adhesion in respect thereof (the **"Agreement").**

NOW THEREFORE in consideration of being accepted as a party to the Agreement, the New Participant agrees with all present and future parties to the Agreement as follows:

I . The New Participant hereby agrees to comply with and be bound by all of the terms and conditions of the Agreement, as from the Adhesion Date, as if the New Participant were a signatory to the Agreement as a Participant subject to all of the obligations of Participants in this Agreement.

2. All capitalized terms used but not defined herein have the meaning set out in the Agreement.

3. The New Participant designates its Continues Quality Improvement (CQI) as the Primary Contact.

4. The contact person, address and fax number for notice of the New Participant, unless and until changed in accordance with such section, is

Kelly Elgie –Manager CQI
710 Southdale Rd East, London, ON, N6E 1R8
519 661 2500 ext 8263
519 661 0446
kelgie@london.ca

5. The Organization Privacy Officer is:

Angie Heinz – Administrator
710 Southdale Rd East, London, ON, N6E 1R8
519 661 2500 ext 8260
519 661 0446
aheinz@london.ca

The Corporation of the City of London

By: _____
I have authority to bind the Party

The foregoing Instrument is hereby accepted by the current Parties to the Agreement and the New Participant has accordingly become a Party to the Agreement, as of the Adhesion Date.

SCHEDULE E

PLAIN LANGUAGE DESCRIPTION OF IAR NETWORK SERVICES AND SECURITY

The following description of the Integrated Assessment Record (IAR) has been created to highlight privacy and security safeguards within IAR. This description provides participating Health Information Custodians (HICs) with information that they can share with Clients/Patients to reassure them that their Personal Health Information (PHI) is protected, secure and that confidentiality remains intact. This description will be summarized and made available to the public through communication vehicles such as the Participants' website, brochures and posters. Communication materials targeted at the public will be made available in plain language.

I. DESCRIPTION OF THE INTEGRATED ASSESSMENT RECORD

I. The IAR is a web-based tool for authorized Participants who are involved in a Client/Patient's care, to access Client/Patient assessment information such as:

(a) Ontario Common Assessment of Need, Staff and Client Version, Staff Comments only or "OCAN";

(b) Resident Assessment Instrument Mental Health or "RAI-MH©" assessment tools;

(c) Admission and Discharge Criteria and Assessment Tools or "ADAT";

(d) interRAI Community Health Assessment or "CHA";

(e) interRAI Preliminary Screener;

(t) Resident Assessment Instrument Home Care or "RAI-HC";

(g) interRAI Contact Assessment or "CA"; and

(h) other assessment tools as may be approved for inclusion in IAR by the IAR Provincial Steering Committee, as amended from time to time by external entities such as the Canadian Institute for Health Information ("CIHI") and other identified working groups.

2. The IAR offers a secure and accurate method of viewing Client/Patient's PHI as part of the client assessment process. Regardless of where a person receives service, Participants will have the ability to view a snapshot or a subset of their assessment information while maintaining access to the full assessment if required.

II.

III. SUMMARY OF PRIVACY AND SECURITY SAFEGUARDS

3. There are numerous controls built into the IAR to protect PHI. Parties are obligated under the Ontario health information privacy legislation, the *Personal Health Information Protection Act, 2004, Sch. A* (PHTPA) to provide the following safeguards:

(a) Secure Hosting

- The IAR is hosted in a secure environment with effective security safeguards in place that are in compliance with industry best practices.

(b) Authorization

- Users' identities are verified before they are granted access to the IAR

- Users' access to the IAR must be authorized by the administration of their health service provider organization in accordance with an established user management process.

(c) Authentication

- All users are authenticated through an enhanced authentication mechanism prior to accessing the IAR
- Strong password policy is enforced in the IAR.

(d) Data Security

- IAR data is encrypted in storage and in transit.
- IAR data cannot be changed or modified by any users.
- Data retention and disposal policies and procedures are in place to ensure the availability and confidentiality of IAR data.

(e) Logging

- All privacy and security related events and activities such as access to PHI and administrative actions are logged.
- Audit logs are reviewed by Participant's privacy officer on a regular basis to detect suspicious activities or potential Privacy/Security Breaches.

(t) Security Assessment

- Threat Risk Assessments (TRAs) are conducted to identify security gaps and deficiencies which are mitigated appropriately to ensure compliance.
- Penetration testing has been performed to prevent any unauthorized access and modification to the IAR and the data.

(g) Privacy

- Privacy Impact Assessments (PIAs) are conducted to identify privacy gaps and deficiencies which are mitigated appropriately to ensure compliance.
- Each Participant, and each HINP have implemented and followed information practices that comply with PHIPA and its regulations regarding the collection, use and disclosure of PHI including:

    i. An integrated consent management process is in place to manage and enforce Client/Patient's consent among Participants.

    ii. An integrated incident management process is in place to detect, investigate and manage incidents collaboratively among participating organizations

iii. An integrated Client/Patient privacy support process is in place to manage Clients/Patients' requests to access and/or correct their PHI in the IAR, and to challenge the privacy compliance of the Participant.

III CONCLUSION

4. Participants that use the IAR service comply with the provisions of PHIPA and relevant industry standards. They use a variety of administrative, physical and technical safeguards to protect PHI. In addition, Participants have policies and procedures in place to ensure that their employees and other authorized users of the IAR understand their obligations with respect to the IAR, privacy and protection of PHI.

SCHEDULE F
SAFEGUARDS REGARDING CONFIDENTIALITY AND SECURITY OF THE IAR

I. ADMINISTRATIVE

1. An individual(s) has been designated as being responsible for privacy and security compliance.

2. An organizational governance framework for privacy, confidentiality, and security is in place which includes clearly defined roles and responsibilities for privacy and security.

3. Organizational policies and procedures for privacy and security management have been developed, implemented and are monitored and enforced. A mechanism is in place for reviewing and updating the policies and procedures.

4. Only "authorized" staff may have access to and use of the Shared System on a 'need-to-know" basis (i.e.. when required to perform their duties).

5. Nondisclosure or confidentiality agreements are in place for all employees, staff, volunteers and contractors which agreements contain appropriate sanctions for breach of privacy, confidentiality, or security up to and including dismissal or termination of the agreement, whatever the case may be.

6. TRA and PIA have been conducted for the Shared System.

7. Mandatory and ongoing privacy, confidentiality, and security training is conducted for all employees, staff, volunteers and contractors working with the Shared System.

8. A "Privacy/Security Breach" protocol with respect to the privacy and security of the Shared System and data has been developed and implemented.

9. An integrated consent management process is in place to manage and enforce Client/Patient's consent among participating organizations.

10. An integrated incident management process is in place to detect, investigate and manage incidents collaboratively among participating organizations.

11. An integrated client privacy support process is in place to manage Clients/Patients' requests to access and/or correct their PHI in the Shared System, and to challenge the privacy compliance of the participating Health Service Provider.

12. Acceptable business recovery plans, including disaster recovery and data backup are in place.

13. Signed agreements have been in place with any third parties who assist in providing HINP services to the HICs pursuant to this Agreement, which agreements require such third parties to implement appropriate privacy and security safeguards in providing such services to HINP.

II. TECHNICAL

14. Strong access control mechanisms, including authorization and authentication measures (such as computer password protection and unique log-on identification) have been implemented to ensure that only authorized personnel can access the Shared System.

15. Shared System data is encrypted in storage and in transit.

16. Shared System data cannot be changed or modified by any users.

17. Remote electronic access to the Shared System hosting environment is prohibited except where required for delivery of support services by those individuals executing these responsibilities on behalf of HINP and who have been assigned the appropriate access rights by the HINP.

18. Vims-checking programs have been implemented.

19. Detailed real-time audit trails have been implemented to record the user name, time stamp, and nature of data access.

III. **PHYSICAL**

20. Computers and files that hold the Shared System are housed in secure settings in rooms protected by such methods as combination lock doors or smart card door entry, with paper files stored in locked storage cabinets.

21. Employees and staff have been provided with photo identification or coded swipe cards.

22. Contractors and volunteers are required to have appropriate photo identification or coded swipe cards limiting their access to those parts of the premises which are required in order for them to provide their services.

23. Visitors to the data center are screened and supervised.

24. Alarm systems are in place.

25. The number of locations in which the Shared System is stored has been minimized and specified in advance.

26. The architectural space of HINP precludes public access to areas where the Shared System is held.

27. Routine surveillance of premises is conducted.

28. Fire suppression systems are in place to protect the Shared System from fire hazards.

SCHEDULE G
ENTERPRISE MASTER PATIENT INDEX SYSTEM

I. ENTERPRISE MASTER PATIENT INDEX SYSTEM DESCRIPTION

I. The Enterprise Master Patient Index ("EMPI") solution is an electronic system to store and

manage Client/Patient information transmitted from multiple source systems through multiple Shared System instances. The main purpose of the EMPI is to serve as a source of truth for patient identity, allowing Participants to uniquely identify client records. The EMPI uses a sophisticated and flexible data model to identify and link records across these source systems.

2. EMPI receives Client/Patient information from source systems through multiple installations of the Shared System, and provides Client/Patient identification, matching, and Client/Patient searching services to all Participants.

3. The implementation and operation of the EMPI System is managed by CHIS in accordance with the terms of this Agreement, acting as the EMPI HINP.

II. EMPI SERVICES

4. CHIS shall directly (or where authorized, through a contracted third-party) provide the following services to the Participants:

(a) provide, in its role as a HINP, Client/Patient identification, Client/Patient matching, and Client/Patient searching services via the EMPI solution to Participants;

(b) accept the PHI and PI uploaded by the Participant from the Shared System, and process and store the data for the purpose of Client/Patient identification, matching and searching;

(c) host the EMPI Hardware and software components;

(d) manage and support the EMPI hosting environment, including, but not limited to, network, servers, operating systems, databases;

(e) provide support for EMPI technology, administration, operation and privacy/security through the operational services or contracted third party;

(t) monitor the availability and performance of the EMPI hardware and software components;

(g) complete the TRA and PIA on the EMPI implementation and operations;

(h) establish and manage the EMPI operational processes, including manual patient matching;

(i) establish adequate physical, technical and administrative controls to safeguard the privacy and security of PI and PHI;

U) establish an incident management process to manage Privacy/Security Breaches relating to the EMPI, and integrate the process with the IAR incident management process;

(k) establish a disaster recovery plan to include a data backup facility, processes and procedures to ensure the continued availability of the EMPI hardware and software and services in the event of a disaster;

(I) refrain from using any data in the EMPI for any purpose other than as required in its role as the EMPI HINP;

(m) comply with its obligations as a HINP as prescribed in PHIPA;

(n) appoint an individual (the **"HINP Privacy Officer")** who will have overall responsibility for the privacy and security of the EMPI system;

(o) implement, in conjunction with the Participants, an integrated incident management process to deal with Privacy/Security Breaches by the HINP and which includes notification to affected Parties;

(p) implement, in conjunction with the Participants, logging, auditing and monitoring policies and procedures, including communication of these controls to all Authorized Users and to the Participants;

(q) implement, in conjunction with the Participants, an integrated EMPI support process to deal with the issues with the personal information and personal health information collected and processed in EMPI system;

(r) ensure that all system changes follow CHIS's change control process;

(s) use reasonable efforts to ensure that the EMPI is available to all Participants on a 24/7 basis, except in accordance with sections (t) and (u) below;

(t) use reasonable efforts to: (i) schedule any planned outages or system downtime at a time when it does not interfere with access by Authorized Users for purposes of Client/Patient services, and; (ii) provide the Participants with at least ten (10) Business Days' notice of such outage or downtime; and

(u) provide notification to all Participants of any unplanned outage or downtime as soon as reasonably possible.

5. Each Participant acknowledges and agrees that:

(a) the EMPI solution hosted in CHIS receives Client/Patient information from (and provides EMPI services to) multiple source systems, through multiple instances of the Shared System in Ontario;

(b) the Client/Patient information in EMPI collected from all Participants will be used for Client/Patient identification, matching, and searching by other HICs participating in other Shared System instances.

(c) in collecting Client/Patient information from EMPI through the Shared System (and using and disclosing such information, in accordance with the terms of this Agreement) each Participant has a reasonable basis on which to assume pursuant to PHIPA that it has the implied consent of the individual to collect, use and disclose PHI for the purposes of providing health care or assisting with the provision of health care: and

(d) each Participant shall comply with the obligations of a HIC under PHIPA.

III. OBLIGATIONS OF CHIS

6. CHIS shall be the HINP for the EMPI and shall comply with all of the obligations of a HINP under PHIPA.

7. CHIS shall not use any PHI to which it has access except as necessary to provide the EMPT Services, and shall not disclose any PHI to which it has access in the course of providing the EMPT Services.

8. CHIS shall notify the Participants at the first reasonable opportunity if it has accessed, used, disclosed or disposed of PHI other than in accordance with this Schedule "G"(III) or if an unauthorized person has accessed the PHI.

9. CHIS shall provide to each Participant a plain language description of the services that it provides to the Participants as mandated by the Regulation. The Participants can share this description with the individuals to whom the PHI relates. This will include a general description of the safeguards in place to protect against unauthorized use and disclosure, and to protect the integrity of the information.

I0. CHIS shall, as per requirements of the Regulation, make available to the public:

(a) the description referred to in paragraph 9 above;

(b) any directives, guidelines and policies of CHIS that apply to the services that CHIS provides to the Participants, to the extent that these do not reveal a trade secret or confidential scientific, technical, commercial or labor relations information; and

(c) a general description of the safeguards implemented by the CHIS in relation to the security and confidentiality of the information.

1 1. CHIS shall to the extent reasonably practical, and in a manner that is reasonably practical, keep and make available to each Participant, on the request of such Participant, an electronic record of:

(a) all accesses to all or part of the PHI associated with the Participant being held in equipment controlled by CHIS. The record shall identify the person who accessed the information and the date and time of the access, and

(b) all transfers of all or part of the information associated with the Participant by means of equipment controlled by CHIS (whether to third party service providers, or otherwise). The record shall identify the person who transferred the information and the person or address to whom it was sent, and the date and time it was sent.

12. CHIS shall perform and provide to the satisfaction of all Participants a written copy of the results of an assessment of the IAR Services with respect to:

(a) threats, vulnerabilities and risks to the security and integrity of the PHI (by means of a TRA). and

(b) how the EMPI Services may affect the privacy of the individuals who are the subject of the information (by means of a PIA).

13. CHIS will review and develop to the satisfaction of all Participants, a mitigation plan for all high priority risks outlined in the PIA and TRA.

14. CHIS shall ensure that any third party it retains to assist in providing services to the Participants agrees to comply with the restrictions and conditions that are necessary for CHIS to comply with this Schedule "G"(III).

15. CHIS shall have in place information practices that comply with the requirements of PHIPA and the Regulation, and shall comply with its own information practices.

16. CHIS will take steps that are reasonable in the circumstances to ensure that:

    (a) PHI is protected against theft, loss and unauthorized use or disclosure; and

    (b) The records containing the PHI are protected against unauthorized copying, modification or disposal.

17. In addition to the obligations under paragraphs 15 and 16 above, CHIS will work with the Participants to develop and/or implement sufficient administrative, technical and physical safeguards.

18. CHIS will hold the Participant's Confidential Information in strictest confidence, and in any case with no less protection and security than it protects its own Confidential Information.

19. In the event that CHIS receives a court order or other lawful requirement of a court or government agency of competent jurisdiction requiring the disclosure of some or all of a Participant's Confidential Information, CHIS shall first advise the HIC about the receipt of such court order so that the HIC may be given an opportunity to intervene, e.g., to seek a protective order against such disclosure. This obligation survives the termination or expiration of this Agreement.

SCHEDULE H

REPORTING SERVICES

I. DEFINITIONS

In this Schedule H, the following definitions apply:

(a) "Reporting Environment" means the information technology infrastructure that

facilitates the provision of the Reporting Services;

(b) "Reporting Services" means the services provided by CHIS to the Participants or other parties including:

i. the implementation and maintenance of the Reporting Environment;

ii. the generation of Reports; and

iii. the transfer of Reports and data sets to Participants or designated other parties as directed by the IAR Provincial Steering Committee; and

(c) "Reports" means reports or data sets that are derived from information contained in the Participants' uploaded records that are generated from the Shared System.

II. ROLES AND RESPONSIBILITIES OF THE PARTIES:

1. As HICs, the Participants have the authority pursuant to PHIPA to collect, use and disclose the PHI contained in the Reports.

2. Under PHIPA, a HIC may permit its Agents to collect, use, disclose, retain or dispose of PHI on the HIC's behalf only if:

(a) the HIC is permitted or required to collect. use, disclose, retain or dispose of the PHI, as the case may be;

(b) the collection, use, disclosure, retention or disposition of the PHI, as the case may be, is in the course of the Agent's duties and not contrary to the limits imposed by the HIC, PHIPA or another law; and

(c) the prescribed requirements under PHIPA, if any, are met.

3. The Parties hereby acknowledge and agree that CHIS:

(a) may collect, use and disclose the PHI related to the Client/Patients of each Participant on behalf of the Participant solely for the purposes of providing the Reporting Services and for no other purpose; and

(b) acts as the Agent of the Participants in its provision of the Reporting Services.

III. COLLECTION, USE AND DISCLOSURE OF PHI FOR THE PROVISION OF THE REPORTING SERVICES

4. Each of the Participants:

(a) authorizes CHIS as its Agent to collect, use and disclose PHI that is in the custody of the Participant;

(b) authorizes CHIS to store the PHI so collected in a single data repository segregated from the data repository in which it maintains PHI in its role as a Designated IAR HINP; and

(c) authorizes its Designated IAR HINP as its Agent to disclose PHI that is in the custody of the Participant to CHIS.

5. CHIS shall not use or disclose any PHI to which it has access in the course of providing the Reporting Services for the Participants, except as required to provide the services.

6. CHIS shall provide access to PHI collected for the purposes of providing the Repotting Services only to those employees, contractors, volunteers or others acting on its behalf ("Sub-Agents") who require such access in order to fulfill its obligations under this Schedule "H".

7. CHIS shall not permit any of its Sub-Agents to access the PHI unless the individual(s) in question agree(s) to comply with the restrictions that apply to CHIS in providing the Reporting Services.

8. CHIS shall not retain PHI in the Reporting Environment for longer than the lesser of:

(a) the time it is retained in the IAR; or

(b) two (2) years.

9. CHIS may manage de-identification of data on behalf of the Participants as directed by the IAR Provincial Steering Committee. De-identified data may be retained indefinitely within the Reporting Environment.

IV. SAFEGUARDS:

I0. Monitoring: CHIS shall implement policies and procedures to ensure that CHIS and its sub-Agents are complying with the terms of this Agreement. In particular, CHIS shall monitor and audit access, use and disclosure of the PHI related to Clients/Patients of the Participants in the Reporting Environment. These reports shall be made available to a Participant upon request.

11. Theft, Loss or Unauthorized Access of Personal Health Information: In the event that CHIS becomes aware that PHI stored in the Reporting Environment has been stolen or lost, or a person has obtained unauthorized access to PHI, or CHIS has used, disclosed or disposed of the PHI other than as contemplated in this Schedule "H", CHIS shall at the first reasonable opportunity (not to exceed two (2) business days) notify the Participant(s)' Privacy Contact(s), as identified on Schedule "A", by telephone followed by written notice.

V. ASSESSMENTS:

12. Completion of a Privacy Impact Assessment: CHIS shall, at its own expense, complete a PIA of the Reporting Environment, and make available a copy of the PIA to the Participants.

13. Completion of a Threat/Risk Impact Assessment: CHIS shall, at its own expense, complete a TRA of the Reporting Environment, and make available a copy of the TRA to the Participants.

VI. ACCOUNTABILITY AND ACCESS TO INFORMATION:

14. Privacy Contact: CHIS shall designate a Privacy Contact Person who shall have the responsibility for compliance with the security and privacy obligations flowing from its receipt, use, disclosure, retention and destruction of PHI for the purposes of the provision of the Reporting Services.

15. Requests for Access: If CHIS receives a request for access to PHI that it has collected in order to provide the IAR Reporting Services under this Agreement, it shall direct the request to the Privacy Contact of the Participant from which CHIS received the PHI.

16. Complaints: If CHIS receives a complaint regarding its receipt, use, or disclosure of PHI it shall direct the complainant to the Privacy Contact of the Participant from which CHIS received the PHI. The Participant shall respond to the complaint in consultation with CHIS.

VII. DESCRIPTION OF IAR REPORTING SERVICES

17. CHIS shall directly or where authorized, through a contracted third-party, provide the following IAR Reporting Services to the Participants:

(a) establish a production environment for Reports;

(b) host and maintain the Reporting Environment in a secure environment for the storage of PHI;

(c) manage servers and network; including but not limited to system configurations, patches and upgrades;

(d) provide support for the Reporting System technology, administration, operation and privacy/security;

(e) co-ordinate and manage provision of access to users as designated by Participants;

(f) appoint an individual(s) who will have overall responsibility for the privacy and security of the Reporting Services;

(g) implement, in conjunction with the Participants, an integrated incident management process to deal with Privacy/Security Breaches, if any, by CHIS and including notification of affected Participants;

(h) inform the Participants if there has been a Privacy/Security Breach by CHIS or unauthorized access by a person other than an Authorized User of the Participants, in accordance with the provisions of the integrated incident management process;

(i) implement, in conjunction with the Participants, logging, auditing, and monitoring policies and procedures including communication of these controls to all Authorized Users;

U) ensure that all system changes follow CHIS's change control process;

(k) establish secure network connections with WOHC and HSN in their roles as

Designated IAR HINPs for the collection of PHI from their respective IAR production systems and its transfer to the Reporting Environment at CHIS;

(l) facilitate the operation of the Reporting Services for the collection of PHI and generation of Reports approved by the IAR Provincial Steering Committee and/or secure transfer of data to designated third parties as approved by the IAR Provincial Steering Committee; and

(m) conduct any de-identification of PHI as directed by the IAR Provincial Steering Committee.

SCHEDULE I

CONSENT CALL CENTRE SERVICES

I . Pursuant to Schedule "C"(II.8U)) of this Agreement, in implementing the integrated consent management process CHIS, will create and operate a Consent Call Centre on behalf of Participants.

2. In order to accept and implement consent directives on behalf of the Participants'

Clients/Patients, CHIS may collect identification information from the Participants' clients including health card numbers.

3. The collection of health card numbers by CHIS for the purposes of administering and operating the Consent Call Centre is a collection of PHI pursuant to s.34 of PHIPA.

4. In collecting PHI through the Consent Call Centre, CHIS is acting as an Agent to the Participants in order to collect and implement their Client/Patient's or SDM's consent directive.

5. In signing this Agreement the Participants authorize CHIS to act as their Agent for the purposes of collecting and processing consent directives on their behalf.

SCHEDULE J

THE PRIVACY AND SECURITY AND DATA ACCESS COMMITTEES

I. RESPONSIBILITIES OF THE PRIVACY AND SECURITY COMMITTEE, OR ITS SUCCESSOR

1. The Privacy and Security Committee shall be established with delegated authority from

the IAR Provincial Steering Committee to assist with privacy and security issues in managing and implementing the Shared System.

2. Subject to the approval of the IAR Provincial Steering Committee, the Privacy and Security Committee may be the delegated authority for the development of a self- assessment checklist, integrated consent management process, integrated incident management process, integrated user account management process, integrated client privacy support process, Log Review Guideline and any other policies and procedures necessary to support the Shared System.

II. RESPONSIBILITIES OF THE DATA ACCESS COMMITTEE, OR ITS SUCCESSOR

3. The Data Access Committee shall be established to review requests and provide recommendations to the IAR Provincial Steering Committee for approval for any permitted or secondary use of the PHI hosted in IAR solution. For greater certainty, permitted or secondary uses may include data for government reporting as permitted by PHIPA and other Acts, reports to be made available to Participants, and healthcare research.

4. Any disclosure of PHI for permitted or secondary uses must be reviewed by the Data Access Committee and comply with the applicable provisions of PHIPA or another Act.

5. The Data Access Committee may also identify and define categories of reports or transfers that are pre-approved, and may be established subject to advance notification to the Data Access Committee.

6. The Data Access Committee shall maintain and make available to the Participants a list of all approved permitted and secondary uses of reports and transfers.

7. Where a permitted or secondary use of PHI is not automatically facilitated by enabling legislation, the Data Access Committee shall notify all Participants of the request prior to the use, and a Participant may notify the Data Access Committee that it does not wish the PHI in the Shared System for which it is a HIC to be subject to the requested use.

8. If the Data Access Committee receives a request for access to PHI for research purposes, the request must be supported by a recommendation to grant it from an appropriate Research Ethics Board made in accordance with the applicable provisions of PHIPA. Such requests for access to PHI for research purposes may only be granted with the approval of the Data Access Committee and the IAR Provincial Steering Committee.

III. **TERMS OF REFERENCE**

9. The Privacy and Security Committee, the Data Access Committee and any other Committees shall develop terms of reference for its composition and operation consistent with this Agreement and direction received from the IAR Provincial Steering Committee.