



North Carolina Healthcare Information
and Communications Alliance, Inc.



North Carolina Health Information
Security & Privacy Collaboration

NC HISPC Health Information Exchange Agreement

Submitted to: Linda Dimitropoulos
Project Director
Privacy & Security Solutions for Interoperable HIE
RTI International

Submitted by: Holt Anderson
Executive Director
NCHICA

December 21, 2007
Subcontract No. 37-321-0209825

Health Information Exchange Agreement

This Health Information Exchange Agreement ("Agreement") is made effective this ____ day of _____, 200_ ("Effective Date"), by and between _____, a _____ [type of entity] organized under the laws of the State of _____ and having its principal place of business at _____, ("A"); and _____, a _____ [type of entity] organized under the laws of the State of _____ and having its principal place of business at _____ ("B") (each, a "Network" and together, "Networks").

WITNESSETH:

WHEREAS, Networks have established secure, electronic patient data exchange systems (the "Exchanges") to allow Authorized Users (as defined below) to electronically access patient information from other Authorized Users; and

WHEREAS, Networks have entered into agreements with health care entities under which each Authorized User has agreed to provide the Networks' designated "Registered Users" with access to an Exchange in order to view patient information generated by participating Authorized Users; and

WHEREAS, Networks desire to participate in each other's Exchange in order to allow Authorized Users to contribute and access patient information for the continuing care and treatment of patients and beneficiaries; and

WHEREAS, each Network desires the other to have the same privileges to the Exchange as a "Registered User" has pursuant to the agreement between an Authorized User and a Network; and

NOW, THEREFORE, in consideration of the foregoing premises and the mutual covenants and agreements set forth below, the parties agree as follows:

1. Definitions

"Documentation" means the user documentation, manuals, and user guides, whether in paper, electronic, or other form, furnished to a Network by the other for use with the Exchanges.

"Data" means any data or information accessible via an Exchange by or on behalf of a Network or its registered users, including, without limitation, personally identifying information and protected health information.

"Registered User" means employees, contractors and staff of an Authorized User who are allowed access to the Exchanges or to generate Data on an Exchange pursuant to this Agreement.

2. Network License and Restrictions. Subject to the terms and conditions of this Agreement and during the term of this Agreement, each Network is hereby granted a limited license to allow its Authorized Users via their Registered Users to remotely access and use the Exchanges and Documentation for the sole purpose of accessing and viewing Data in the Exchange as authorized by the Networks. **[Authorized Users shall use such Data solely for purposes of payment, treatment and healthcare operations as each of those terms is defined in the HIPAA Regulations.]** Any access to or use of the Exchange not expressly permitted in this Agreement is prohibited. Except as expressly permitted in this Agreement, neither Network shall, nor allow or authorize any third party to: (i) use or access an Exchange; (ii) alter, enhance or otherwise modify, or create derivative works of an Exchange, or reverse

engineer, disassemble, or decompile an Exchange or any of its components; or (iii) sublicense, transfer, or assign its rights to access and use an Exchange, in whole or in part, to a third party. Neither Network shall, or allow a registered user to, access, transfer, use, or disclose Data in any manner or for any purpose that is prohibited by any applicable state or federal law, rule, or regulation. Except as expressly set forth in this Agreement, neither Network will obtain any rights in the other's Exchange, Documentation, any of the technology used to create the other's Exchange, including electronic formats and tools that the Network or Authorized User uses in interfacing the Data into the Exchange, or in all related software, hardware, documentation, and methodologies used by the other Network, or its Authorized Users, to develop, maintain, and operate the Exchange and deliver services to a Network.

3. Network Responsibilities.

3.1 Security and Confidentiality. Each Network shall be responsible for ensuring the security and confidentiality of the Data within its Exchange to which the Authorized Users are granted access, including, without limitation, all user IDs and passwords assigned to Authorized Users and Registered Users. Each Network shall assure that Authorized Users shall not disclose their Data User Accounts to any third party.

3.2 Hardware and Software. Each Network shall acquire, install, provide, and properly maintain, at its own cost, the hardware and software including, without limitation, all of each Network's core systems necessary or appropriate to receive, access and utilize its Exchange, as permitted by this Agreement.

3.3 Lack of Guarantee or Warranty. Each Network acknowledges and agrees that the Exchanges: (a) are accessed over the Internet; (b) rely, in part, on the existence and proper operation of equipment and software that is outside of the control of Networks and Authorized Users; and (c) rely on access to information from, and the provision of information controlled by, third-parties and, as a result, access to the Data by a Network may be prevented by events or actions outside of the other Network's or Authorized User's control. The Networks and Authorized Users have made and hereby make no guarantee or warranty to each other as to the availability or accessibility of the Exchanges or Data.

3.4 Authorized User Training. Networks shall assure by contract or otherwise that Authorized Users who are granted Data User Accounts have education and training for Registered Users on HIPAA requirements to maintain the confidentiality of patient information accessed through the Exchanges.

3.5 Insurance. Each Network shall obtain and maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than \$_____ each occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this contract or be no less than two times the occurrence limit.

4. Data. Each Network acknowledges that the information provided through the Exchanges is drawn from numerous sources, and each Network agrees to verify, to the best of its ability, that the Data obtained from an Exchange which Authorized Users rely upon in making treatment decisions about each patient in fact corresponds to that patient. Each Network agrees and understands that the Data accessed through the Exchanges may not include a patient's entire record of treatment in the region.

5. Access.

5.1 Access by Authorized Users, Registered Users, Contractors and Staff. Each Network shall establish and implement appropriate policies and procedures for purposes of preventing unauthorized access to and disclosure of Data. Each Network shall protect the confidentiality of all Data in accordance with applicable laws and the terms and conditions of this Agreement.

5.2 Access by Additional Contractors. Each Network may enroll the following types of entities as Authorized Users:

- a. Hospitals, physicians;
- b. Payors
- c. Clearinghouses; and
- d. Other health care providers subject to HIPPA.

Each Network will be responsible for initiating, updating, monitoring, controlling, and removing or suspending access of its Authorized Users. Each Network shall receive from each Authorized User contractual assurances that it will initiate, update, monitor, control and, where necessary, remove or suspend access of its Registered Users.

Once the enrolling Authorized User provides a Registered User with training to familiarize them with the Exchange, the enrolling Network will assign him or her a unique identifier and password that contains at least 7 digits including at least 2 alpha digits and 2 numeric digits. Authorized Users must change their passwords at least every 180 days and may not re-use a password. Passwords shall be case sensitive.

Each Authorized User shall agree to an Exchange Agreement detailing the permitted uses of the system, HIPAA compliance requirements and the user's roles and responsibilities. Each Authorized User's consent to the agreement will be logged in an audit trail or otherwise documented.

The enrolling Network immediately shall remove an Authorized User's or Registered User's access to the Exchange if the user no longer qualifies as an Authorized User or Registered User.

- a. Each enrolling Network must place appropriate restrictions on each Authorized User upon enrollment, as follows:
 1. Hospitals and other Facilities. Facilities shall, prior to becoming Authorized Users, agree to access or input Data relating solely to patients.
 2. Health Care Licensees. Physicians and other licensed providers may have access to any patient's information when they are the patient's primary, admitting, attending, consulting, or operating physician.
- b. Each Network shall put into place (and assure that each Authorized User puts into place) protections against unauthorized access.

c. Each Network will establish warnings and automatic e-mail alerts to the Authorized User and to the other Network when it detects erratic usage or anomalies by an Authorized User or any other user (e.g., a Registered User overrides the system five times within five minutes).

5.3 Audit Trails.

a. Each Network will record each time an Authorized User accesses the Exchange and will record every item of patient information accessed by the Authorized User.

b. The audit trail will identify whether the Authorized User “override” the system to access information of patients with whom the user does not have a pre-existing relationship.

c. Each Network will review the audit trails of information accessed to identify and investigate any potential abuses or violations of the Exchange Policies and Procedures or applicable federal or state laws or regulations.

d. Upon request, each Network will follow its internal policies and procedures for providing an accounting of disclosures to the patient or patient’s representative requesting the accounting, in order to indicate who has accessed the patient’s information for treatment provided.

5.4 Sanctions of Users

a. Each Network will follow its internal policies and procedures to sanction its Authorized Users who inappropriately access patient information from the Exchange.

b. If a Network, following an investigation of an alleged violation, concludes that a user authorized by another Network inappropriately accessed information of the first Network, the first Network will contact the authorizing Network and request that the authorizing Network follow its internal policies and procedures to investigate the apparent violation and, if appropriate, sanction the user. The authorizing Network thereafter shall notify the first Network in writing that it has concluded its investigation, determined that a violation did or did not occur, and taken appropriate action without specifying the particular action taken. If the first Network concludes that the same user has inappropriately accessed patient information a second time, that Network will request that the authorizing Network revoke the user’s privileges to use the Exchange.

c. Each Network shall require that Authorized Users notify such Network if the Authorized User determines that a breach has occurred. That Network will then notify other Networks of the breach and suggest that they conduct an audit to determine if the breaching party inappropriately accessed their Data.

5.5 Purposes of Access. Authorized Users shall use the Exchange solely to access patient information in the following situations:

[a. Pursuant to the purposes specified in 45 C.F.R. §164.506(c) (the HIPAA regulations):

- **For treatment activities of any health care provider.**

- **If the patient information was created at the covered entity for which the Authorized User works, for the payment or health care operations purposes of that covered entity.**
- **If the patient information was not created at the covered entity for which the Authorized User works, for the payment activities of that covered entity, and for the health care operations activities of that covered entity, if that entity either has or had a relationship with the patient and the information is needed to conduct quality assessment and improvement activities or review the competence or qualifications of healthcare professionals.]**

6. HIPAA.

6.1 Each Network represents and warrants that: (i) its Authorized Users shall access and use the Exchanges solely in their capacity as “covered entities,” as that term is defined in 45 C.F.R. § 160.103; and (ii) each such access and use by an Authorized User shall be made solely for purposes of treatment, payment, and those health care operations specified in 45 C.F.R. § 164.506(c), or pursuant to a valid patient authorization or court order when required under 45 C.F.R. § 164.508, 45 C.F.R. § 2.1, *et seq.*, and/or state law.

6.2 Each Network shall assure that Authorized Users implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the security and integrity of Data on the Authorized User’s computer network, and the confidentiality of all Data displayed, transmitted, or accessed at or from the Authorized User’s location using the Exchange. Each Network shall assure that each Authorized User shall report to the relevant Authorized User and the Network any use or disclosure of Data created at that Authorized User of which the Registered User becomes aware that is not permitted or required by this Agreement or by law.

Each Network shall assure that each Authorized User will include a clause in its Notice of Privacy Practices indicating that patient data may be provided to third parties in various formats. The clause shall be substantially as follows:

“In order to efficiently coordinate the treatment, payment, and health care operations aspects of your care, we may disclose your PHI in any format that we determine is secure and expeditious, *e.g.*, verbally, electronically, via fax, and/or in paper form.”

6.3 Restrictions on Patient Information.

a. If an Authorized User allows its patients the right to prohibit the access of all their data from a particular encounter(s) through an Exchange, and the patient has chosen this option, the Network shall either exclude relevant data or require the Registered User to exclude such data.

b. No exchange will allow any Authorized User access to any patient information from a dedicated acute in-patient or outpatient psychiatric unit or an in-patient or outpatient substance abuse facility, as designated by each Network.

c. If possible, each Network will allow Authorized Users to access patient information from all lab results and medication histories to provide complete information for the continuing care and treatment of the patient.

d. Each Network will allow Authorized Users to access patient information dating as far back as the information is maintained on each Network information system or Authorized User system, as applicable. Each Network or Authorized User shall maintain patient information on its information system for the minimum amount of time required by law but in no event less than six (6) years following a patient's discharge or treatment.

e. Each Network shall notify the other in advance of any planned changes in any legacy system firewalls or VPN of an Authorized User or the Network that may impact the data accessed by an Exchange or the connectivity to an Exchange.

6.4 Response to Patient Requests

a. When responding to requests for release of patient information, Authorized Users shall not release data accessed or obtained through an Exchange unless required by law. Each Authorized User shall only disclose data from its patient medical records. The information provided by Exchange does not constitute the patient's medical record and the system does not maintain patient data. Each Exchange shall simply query and collate patient data from the participating providers.

b. Each Authorized User will follow its internal policies and procedures for responding to patients' or patient representatives' requests for a) access to patient information, b) amendments to the patient's information, and c) restrictions on the access, use, or disclosure of patient information.

c. If an Authorized User receives a request to access or to amend patient information regarding treatment that was provided by another Authorized User, the Authorized User will forward that request to the treating provider and the treating provider shall be responsible for responding to the request for access or amendment.

d. If an Authorized User receives a request to restrict the access, use, or disclosure of patient information regarding treatment that was provided by another provider (but not including requests forwarded from another Authorized User notifying of a restriction), the Authorized User will forward that request to the treating provider and the treating provider shall be responsible for responding to the request for restrictions.

7. Confidential Information. Each Network acknowledges that in accessing and using the Exchanges, it will be exposed to and provided with Network confidential information, including but not limited to the Exchange and all related software, documentation, and services provided by Network in establishing and maintaining the Exchange. Each Network must maintain the confidentiality of such information and materials pursuant to the terms and conditions of this Agreement, and each Network agrees to exercise no less than reasonable care when handling the confidential information. Except as provided in this Agreement, no Network shall disclose the confidential information to a third party without the express written consent of the other Network, unless: (a) a Network is required to do so by law, (b) the confidential information becomes publicly available, or (c) the Network obtained the confidential information prior to the

Effective Date of this Agreement, or obtains that information through another source who had no duty of confidentiality to a Network.

8. Term and Termination. This Agreement shall commence on the Effective Date and shall continue in effect for _____ years. Either party may terminate this Agreement by providing the other party with ninety (90) days written notice of such termination. Upon termination, all licenses granted to a Network relating to access to or use of the Exchange or the accompanying software tools and documentation will cease. Upon termination, each Network promptly shall return all confidential information to the other.

9. Disclaimers. Each Network provides access to its Exchange “as is” and without any warranty of any kind whether express, implied, or statutory. Neither Network warrants that the performance or delivery of the Exchange will be uninterrupted or error-free. Each Network hereby disclaims all implied and express warranties, conditions, and other terms, whether statutory, arising from course of dealing, or otherwise, including without limitation terms as to merchantability or fitness for a particular purpose. Neither Network shall be liable to the other for any consequential, incidental, indirect, punitive, or special damages suffered by a Network or any third party, however caused and regardless of legal theory or foreseeability, including, without limitation, lost profits, business interruptions, or other economic loss, directly or indirectly arising out of this Agreement. No Network shall be liable for any damages arising out of or related to the acts or omissions of a Network in (a) accessing or using the Exchange or (b) disclosing any Data contained therein.

10. Indemnification. Each Network will indemnify and hold the other and its employees, agents, subcontractors, and licensors harmless from and against any and all liability (including reasonable attorneys’ fees), injury, or damages that arise from or are related to: (a) a Network’s use of or inability to use an Exchange; or (b) Network’s breach of this Agreement, including, without limitation, Network’s breach of any obligation, representation, or warranty set forth herein.

11. Miscellaneous. This Agreement sets forth the entire agreement between the parties and supersedes any and all prior agreements or representations, written or oral, of the parties with respect to the subject matter of this Agreement. This Agreement may not be modified, altered, or amended except by a written instrument duly executed by both parties. No failure or delay by either party in exercising any right hereunder will operate as a waiver thereof. No party shall assign this Agreement, or any of the rights or obligations contained herein. This Agreement shall be binding on the parties, their successors and permitted assigns. The parties agree that any breach of a party’s obligations under Sections 2 and 5 will result in irreparable injury to the other party for which there is no adequate remedy at law. Therefore, in the event of any breach or threatened breach of such obligations, the nonbreaching party will be entitled to seek equitable relief in addition to its other available legal remedies in a court of competent jurisdiction. If any provision of this Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remaining portions shall remain in full force and effect. All notices required under this Agreement shall be: (a) in writing; and (b) deemed to have been duly made and received when (i) personally served, (ii) delivered by commercially established courier service, or (iii) ten (10) days after deposit in the mail via certified mail, return receipt requested, to the addresses specified in the first paragraph of this Agreement or to such other address as the parties shall designate in writing from time to time.

12. Business Associate Addendum. Attached hereto is a copy of the Business Associate Agreement executed by the parties hereto **[needed if purposes beyond TPO.]**
IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date first above written.

A

B

By: _____
(Authorized Signature)

By: _____
(Authorized Signature)

Printed Name

Printed Name

Title

Title