

Florida Health Information Exchange Trust Service Agreement For the Exchange of Direct Messages

This Agreement for the Exchange of Direct Messages (“Agreement”) is a multi-party agreement by and between the undersigned vendor, Harris Corporation (“Vendor”) a Delaware Corporation, under contract with the Agency for Health Care Administration (Agency), statutorily created in Florida Statutes Chapter 20, for the operation of the Florida Health Information Exchange (Florida HIE) and the other undersigned party (hereinafter referred to as Participant), and all other signatories who have executed the same Agreement. Hereinafter, each Party will be referred to individually as “each Party” or collectively the “Parties” unless the Vendor or Participant is specified. This Agreement is effective when fully executed.

Recitals

WHEREAS, the Office of the National Coordinator for Health Information Technology (ONC) has sponsored the Direct Project, which has developed technical specifications as set forth in the Applicability Statement for Secure Health Transport for universal health addressing and transport to enable the sending of encrypted health information directly to known, trusted recipients over the Internet (the “Direct Specifications”).

WHEREAS, each Party provides services that allow authorized individuals and organizations (“Users”) to send encrypted health information (“Direct Messages”) directly to and receive Direct Messages from known, trusted recipients using the Direct Specifications (the “Direct Messaging Service”).

WHEREAS, each Party desires to enable its Users to (1) send encrypted messages using the Direct Specifications to Users of the other Party; and (2) receive encrypted messages sent using the Direct Specifications by Users of the other Party.

NOW THEREFORE, in consideration of the mutual terms, covenants and conditions established in this Agreement, the Parties agree as follows:

1. Purpose. The purpose of this Agreement is to enable the Parties to permit their respective Users to (1) send Direct Messages to Users of the other Party; and (2) receive Direct Messages from Users of the other Party.

2. Responsibilities of Vendor. The Vendor will establish and maintain a website to enable the exchange of trust anchor security certificates among the Parties to facilitate the collective ability to exchange Direct Messages among Parties consistent with the terms of this Agreement. The Vendor will publish Direct Messaging addresses and other information as made available by the Parties to facilitate exchange of Direct Messages among the Parties. Vendor will provide reasonable support to participants in complying with the Trust Agreement including maintaining, updating and distributing a trust bundle of participant trust anchors or maintaining dedicated connections to the Florida HIE Direct Secure Messaging (DSM) service as applicable.

Vendor will provide the Trust Services for the Participant to utilize as indicated below:

- a. Trust Bundle exclusive of DSM _____
- b. Trust Bundle with DSM _____
- c. Dedicated DSM connection _____

3. Responsibilities of Parties.

2.15.2014

a. *Minimum Technical Requirements.* Each Party agrees that, at a minimum, it has implemented the Direct Specifications and currently offers a Direct Messaging Service to its Users. Each Party agrees that it will remain in compliance with the Direct Specifications, as amended from time to time, throughout the term of this Agreement.

b. *Message Size Limits.* Parties agree to message size limits including attachments of no greater than 20 megabytes.

c. *Maintenance of Records.* As between the Parties, each Party is responsible for maintaining records for accounting of disclosures purposes under 45 C.F.R. § 164.528(a) or other purposes required by applicable law. Each Party may fulfill its responsibility by contractually requiring its respective Users to maintain such records.

d. *Message Content.* The Parties agree to exchange Direct Messages of Users. With the exception of routine maintenance and other transient outages, each Party shall not intentionally prevent or delay the incoming or outgoing transmission or receipt of any message to its intended recipient under this Agreement, and each Party shall not alter the content of any such message except as required for software compatibility. The Parties do not validate or enforce clinical document standards on the content enclosed in Direct Messages.

e. *Addresses Shared.* Participants agree to provide a listing of their Users' Direct Messaging addresses and User contact information in a format specified by the Vendor within 10 days of execution of this Agreement and update as specified by the Vendor every 90 days thereafter. User content information shall include User's organization, first name, last name, national provider identifier, address, and phone number. The Parties agree that the Direct Messaging listing will be posted on a public website as made available by Participants "as is" without any warranty of any kind, express or implied.

4. Party Users.

a. *Identification.* Each Party employs a process for identity proofing that meets or exceeds National Institute of Standards and Technology (NIST) Level 2 requirements in effect as of the date of execution of this Agreement by which the Party, or its designee, validates sufficient information to uniquely identify each person or entity seeking to become a User prior to issuing such person or entity a Direct Messaging address and credentials that would grant the person access to the Party's Direct Messaging Service.

b. *Authentication Requirements.* Each Party employs a process by which it, or its designee, uses the credentials issued pursuant to Section 3(a) to verify the identity of each User prior to enabling such User to access the Party's Direct Messaging Service. Such process must include a method for determining and effecting termination of access as appropriate.

c. *User Agreements.* Each Party will ensure that each of its Users is legally obligated to, at a minimum: (i) comply with all applicable law; (ii) send Direct Messages only for the Permitted Purposes as defined below; and (iii) refrain from disclosing to any other person any credentials, passwords or other security measures issued to the User by the Party.

d. *Changes in User Access.* Each Party must be able to suspend or terminate an individual User's access to the Party's Direct Messaging Service without affecting the access of any of the Party's other Users.

2.15.2014

e. *Mobile Devices.* If access to the Party's Direct Messaging Service is permitted through a mobile device, then such Party will require its respective Users to only access the Party's Direct Messaging Service through mobile devices that have appropriate security protections as determined by the Party based on the functionality and capability of the Party's Direct Messaging Service.

f. *Prohibited Users.* Each Party agrees that it will not allow individual patients or consumers to be a User.

5. Permitted Purposes.

a. *Exchange of Health Information.* Each Party will enable its respective Users to send Direct Messages to the other Party's Users that may contain information about a specific patient for the provision of health care or other exchange of health care related data permitted by applicable law.

b. *Future Use.* Each Party's respective Users may retain, use and re-disclose Direct Messages that they receive from the other Party's Users in accordance with applicable law and the receiving User's record retention policies and procedures. Each Party may retain, use and re-disclose Direct Messages only in accordance with applicable law and the agreements between the Party and its Users.

6. Proprietary Information.

a. *Protection of Proprietary Information.* Each Party agrees that, except in performing under this Agreement or with the written consent of the other Party or as required by applicable law, it will not use or disclose the other Party's Proprietary Information. For purposes of this Agreement, "Proprietary Information" means information, materials, processes, ideas, and techniques (whether or not reduced to writing) (i) which are not generally known in the relevant industry; (ii) which afford possessors of the information a commercial advantage over others; (iii) which are considered trade secrets under applicable law (as that term is defined in Section 8(c) of this Agreement); and/or (iv) which, if utilized or disclosed by a Party receiving such information, would place the Party disclosing such information at a competitive disadvantage.

b. *Names, Logos, Marks.* Neither Party shall use the name, logos, or marks of the other Party without prior written consent, except that each Party may use the name, logo, or mark of the other Party to indicate that they have a connection for exchange of Direct Messages. Either Party may disclose the existence and terms of this Agreement as necessary in order to pursue its business goals.

c. *Survival.* The provisions of this Section 5 shall survive termination of this Agreement.

7. Patient Confidentiality; Compliance with Laws.

a. *Business Associate Agreements.* Each Party acknowledges and agrees that it is in a Business Associate role, as the term is defined in the Health Insurance Portability and Accountability Act ("HIPAA"), with each of its Users with respect to the provision of the Direct Messaging Service. As such, each Party has or will enter into a Business Associate Agreements (BAA) with Users as appropriate.

b. *HIPAA and Confidentiality of Alcohol and Drug Abuse Patient Records Regulation Policies.* Each Party warrants that it has policies and procedures to ensure on-going compliance with all applicable requirements of the HIPAA Privacy and Security Rules and the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, and all applicable regulations and guidance issued pursuant to HIPAA, HITECH and the Confidentiality of Alcohol and Drug Abuse Patient Records Regulation as well as applicable state privacy and security laws.

c. *Notification of Compromised Security.* Each Party agrees to notify the other Party if it believes that the security of either Party’s Direct Messaging Service has been compromised that would potentially impact the other Party. Following notification, each Party may take whatever steps it deems necessary, in its sole discretion, to address the identified vulnerability.

8. Malicious Software. Each Party will employ commercially reasonable security controls so that the Direct Messages being sent by the Party’s Users will not introduce any viruses, worms, unauthorized cookies, Trojans, malicious software, “malware,” or other program, routine, subroutine, or data designed to disrupt the proper operation of a system or any part thereof or any hardware or software used by a Party or its Users in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause a system or any part thereof or any hardware, software, or data used by a Party or its Users in connection therewith, to be improperly accessed, destroyed, damaged or otherwise made inoperable.

9. Liability. Neither Party shall be liable for any claims, demands, expenses, liabilities and losses (including reasonable attorney’s fees) which may arise out of any acts or failures to act by the other party, its employees or agents, in connection with the performance of services pursuant to this Agreement.

10. Representations and Warranties.

a. Each Party represents and warrants that it is a valid legal entity or instrumentality of government with the power and authority to enter into and perform this Agreement.

b. Each Party represents and warrants that it is in compliance with its User agreements, Business Associate Agreements, and Qualified Service Organization Agreements.

c. Each Party represents and warrants that it complies with all applicable statutes and regulations of the state(s) in which it does business, as well as all applicable Federal statutes, regulations, standards and policy requirements relating to this Agreement and to the use and exchange of electronic health information, including but not limited to HIPAA, HITECH, and the Confidentiality of Alcohol and Drug Abuse Patient Records Regulation.

d. This Agreement must be signed by a representative of each Party that is authorized to commit the Party to all of the terms of this Agreement. By signing this Agreement, the person signing represents and warrants that he or she has been authorized by the respective Party to enter into the obligations set forth in this Agreement and has read and understood this Agreement.

11. Term and Termination. The Agreement will continue in perpetuity until and unless either Party terminates it by providing the other Party with a least thirty (30) days written notice of its intent to terminate, which notice either Party may provide at any time with or without cause.

2.15.2014

12. Miscellaneous

a. *Governing Law and Jurisdiction.* In the event of a dispute between the Parties arising out of this Agreement, the applicable Federal and state conflicts of law provisions that govern the operations of the Parties shall determine governing law.

b. *Amendment.* Except as set forth herein, this Agreement may not be changed, modified or amended in any respect except by a written instrument signed by the Parties.

c. *Counterparts.* This Agreement may be executed in any number of counterparts, each of which shall be deemed an original as against the Party whose signature appears thereon, but all of which taken together shall constitute but one and the same instrument.

d. *Severability.* In the event that a court of competent jurisdiction holds any section, or any part or portion of any section of this Agreement, invalid, void or otherwise unenforceable, each and every remaining section or part or portion thereof will remain in full force and effect.

e. *Incorporation of Recitals.* The recitals set forth above are hereby incorporated into this Agreement in their entirety and shall be given full force and effect as if set forth in the body of this Agreement.

f. *No Third-Party Beneficiaries.* This Agreement is entered into for the benefit of the Parties and not for the benefit of any third party. This Agreement creates no third-party beneficiary rights.

g. *Notices.* Notices shall be addressed to the Party representative signing this Agreement and effective on the date received: (i) per written proof of receipt from delivery service, or (ii) per facsimile confirmation.

13. Fees and other Costs

a. *Connection Related Service Fees.* If applicable, Participant agrees to pay Vendor fees for the services provided by Vendor to enable the exchanging of messages among the Parties' Users as specified in the Florida HIE Pricing Policies attached hereto and invoiced by Vendor. The fee may be changed upon ninety (90) days written notice to Participant except for a fee reduction which can go into effect immediately consistent with the most current Florida HIE Pricing Policies posted on the Florida HIE website (<https://www.florida-hie.net/>). The fee schedule as of February 1, 2014 is displayed in Exhibit 1.

b. *Other Costs.* Each Party agrees to pay their own respective costs for security certificates or other costs the Party incurs as necessary to prepare for or perform the requirements of this Agreement. For purposes of illustration, these costs may include but are not limited to costs for performing and testing the enabling technology for the exchange, testing compliance with operating policies and procedures of the Agreement, and reviewing the Agreement.

IN WITNESS WHEREOF, this Agreement has been entered into and executed by officials duly authorized to bind their respective parties.

Vendor, _____

Participant, _____

By: _____

By: _____

2.15.2014

Printed Name: _____

Printed Name: _____

Title: _____

Title: _____

Date Signed: _____

Date Signed: _____

Exhibit 1
Florida HIE Trust Service Fee Schedule
2014*

For Florida HIE Trust Services, fees are charged as follows:

- Participants are charged an annual service fee of \$7,500 for trust services exclusive of the Florida HIE Direct Secure Messaging (DSM) service
- Trust service participants are charged \$25,000 for up to 15,000 DSM transactions
- Participants may elect a DSM dedicated connection for \$25,000 for up to 15,000 transactions with an annual \$7,500 trust service fee

*Fees are subject to change upon ninety (90) days written notice to Participants.