SERCH/Florida CONNECT HISP-HISP Agreement

This HISP-HISP Agreement ("Agreement") effective as of _____ (the "Effective Date") by and between **Harris Corporation**, under contract with the Agency for Health Care Administration for operation of the **Florida Health Information Exchange** and [**Name of HISP Partner**], a [**State**] [**Type of company**] ("HISP"). Hereinafter, HISP will be referred to individually as "Party" and collectively as the "Parties."

Recitals

WHEREAS, the Office of the National Coordinator for Health Information Technology has sponsored the Direct Project, which has developed technical specifications for a secure, scalable, standards-based way to establish universal health addressing and transport for participants (including providers, laboratories, hospitals, and pharmacies) to send 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 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 Parties.

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. *Encryption*. Each Party agrees to use at least 2048 (RSA) bit SSL keys.

c. *Message Size Limits*. Parties will inform each other of their respective message size limits, including attachments, or any changes in limits at least thirty (30) days prior to such changes.

d. *Accounting of Disclosures*. As between the Parties, each Party is responsible for maintaining records for accounting of disclosures purposes under C.F.R. § 164.528(a). Each Party may fulfill its responsibility by contractually requiring its respective Users to maintain such records.

e. *Service Levels*. Each Party will provide 24/7 availability with 99.9% monthly service levels excluding planned maintenance windows.

3. Party Users.

a. *Identification*. Each Party employs a process 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 4(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 purposes related to the provision of health care; 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.

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.

4. Permitted Purposes.

a. *Provision of Health Care*. Each Party will only permit its respective Users to send Direct Messages to the other Party's Users related to the provision of health care.

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.

5. Prohibited Use.

a. *Audit Trails*. Unless required by law, each Party will not disclose to any third party data about when, to whom or from whom, or size of Direct Messages are sent and received by Users.

b. *Content of Transactions*. Each Party will not collect information from the content of Direct Messages.

c. *Referral Patterns*. Each Party agrees to not use information obtained from Users to compare referral or practice patterns, or make any other comparison of Users without the User's written permission.

6. Patient Confidentiality; Compliance with Laws.

a. *Agents*. Each Party has all necessary terms in its contract with its Users to permit it to function as an agent for transporting Direct messages. Each Party acknowledges and agrees that it is a Business Associate, as the term is defined in the Health Insurance Portability and Accountability Act ("HIPAA"), of its Users as applicable. As such, each Party has entered into a Business Associate Agreements (BAA) with each of the Users. Each Party acknowledges and agrees that it is a Qualified Service Organization, as the term is defined in the Confidentiality of Alcohol and Drug Abuse Patient Records Regulation, of its Users as applicable. As such, each Party has entered into a Qualified Service Organization Agreement with each of the Users.

b. *HIPAA and Confidentiality of Alcohol and Drug Abuse Patient Records Regulation Policies*. Each Party 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.

6. 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.

7. Liability. Each Party expressly releases and holds harmless the other Party, its officers, directors, employees, members, agents, licensors, shareholders, and Users from any and all claims, liabilities, demands, causes of action, costs, expenses and damages of every kind and nature, in law, equity, or otherwise, arising of or in any way related to this Agreement.

8. 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.

9. Term and Termination. This Agreement will commence on the Effective Date and expire on December 31st of the second calendar year following the Effective Date (the "Initial Term"). Upon the expiration of the Initial Term, this Agreement will automatically renew for successive one (1) year terms unless either Party provides the other Party with notice of its intent not to renew at least sixty (60) days prior to the expiration of the then current term. Either Party may terminate this Agreement if the other Party has breached this Agreement and failed to cure such breach within thirty (30) days of receiving written notice of the breach from the non-breaching Party.

10. 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. Litigation between the Parties concerning this Agreement or its subject matter shall be conducted exclusively in state or federal court in the state where the Party being sued is located. The Parties consent to such jurisdiction and venue.

b. *Amendment*. 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.

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

Party A, **Harris Corporation**	Party B, _____
By:_____	By:_____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date Signed: _____	Date Signed: _____