Direct Secure Messaging Subscription Form

The District of Columbia Department of Health Care Finance (DHCF) was awarded funds from the U.S Department of Health and Human Services Office of the National Coordinator for Health Information Technology to facilitate health information exchange in the District of Columbia. DHCF administers the District of Columbia Health Information Exchange (DC HIE) whose principal offices are located at 899 North Capitol Street, N.E., Washington, D.C. 20002.

DHCF contracted with a vendor to build the technical infrastructure for Direct Secure Messaging. By using Direct Secure Messaging, Subscribers may send and/or receive PHI on an individual patient with whom Subscriber has a treatment relationship, to or from another Subscriber who also has a treatment relationship with the individual. The District may also issue authorized public health alerts through Direct Secure Messaging.

DC HIE's responsibility is to facilitate the exchange of secure PHI between covered entities who/which are legally authorized to transmit such information through the System, in accordance with federal and District laws and this Subscription Agreement. DC HIE has no role in verifying the accuracy of any messages. DC HIE shall not be liable for any claims and/or damages arising from Subscriber's use of Direct Secure Messaging. The following types of individuals/organizations may be eligible for Direct Secure Messaging subscription through the DC HIE.

A. **Individual Subscriber/Delegate**: an individual healthcare provider/qualified health care professional who registers as an employee or who is affiliated with an organization (i.e., pharmacist), or a provider with a solo practice that is not affiliated with an organization with other providers. Individual subscribers may also be non-licensed individuals who work for organizations in the District that have a clinical license and who regularly exchange PHI as part of their job duties. This could be an office manager or administrative support person. Non-licensed District of Columbia Government employees who desire a Direct address may be required to submit a District-developed job description along with a letter of authorization from their supervisor.

B. **Organization**: healthcare organizations (i.e., medical practice, hospital or health system) and for an individual practitioner with a solo practice.

C. **Sub-Organization**: for a healthcare organization's different functions or departments (i.e., hospital radiology or emergency).

Definitions

DC HIE – District of Columbia Health Information Exchange (DC HIE). DC HIE was established by Mayor's Order under the auspices of the Department of Health Care Finance (DHCF). DHCF received funding from the U.S. Department of Health and Human Services (DHHS), Office of the National Coordinator for Health Information Technology (ONC) to plan and implement a statewide Health Information Exchange (HIE).

DHCF – Department of Health Care Finance. A cabinet-level agency of the Government of the District of Columbia (District) primarily responsible for administering the Medicaid program in the District. DHCF is also responsible for implementing and operating several elements of the Patient Protection and Affordable Care Act of 2009 including health information exchange, health information technology and health benefit exchange.

Direct Secure Messaging – a secure point-to-point messaging service for clinical providers. Direct Secure Messaging is the basic service HIEs must provide.

ePHI – Electronic PHI means PHI which is either transmitted by electronic media or maintained in electronic media.

Health Information Exchange – Health Information Exchange (HIE) is the act of transferring health information electronically between two or more entities. HIE is also often referred to as a noun or an entity that is responsible for facilitating the exchange of health information between providers.

Health Care Operations – Health Care Operations as defined in 45 CFR 164.501 and the requesting Participant or Participant User is requesting/accessing PHI for its own use. Participant shall only use the Minimum Necessary PHI for such Health Care Operations purposes.

HITECH Act – Health Information Technology for Economic and Clinical Health Act (HITECH Act) is legislation created to stimulate the adoption of electronic health records (EHR) and supporting technology in the United States. President Obama signed HITECH into law on February 17, 2009 as part of the American Recovery and Reinvestment Act of 2009 (ARRA), an economic stimulus bill.

HIPAA – Health Insurance Portability and Accountability Act of 1996. There are two sections to the Act. HIPAA Title I deals with protecting health insurance coverage for people who lose or change jobs. HIPAA Title II includes an administrative simplification section which deals with the standardization of healthcare-related information systems. In the information technology industries, this section is what most people mean when they refer to HIPAA. HIPAA establishes mandatory regulations that require extensive changes to the way that health providers conduct business.

Meaningful Use – Any purpose to demonstrate meaningful use of certified electronic health record technology and the purpose is permitted by Applicable Law, including but not limited to the HIPAA regulations. "Meaningful use of certified electronic health record technology" shall have the meaning assigned to it in the regulations promulgated by the Department of Health and Human Services.

Definitions (continued)

Payment – Payment as defined in 45 CFR 164.501 and permitted by Applicable Law.

Provider Directory – a database accessible to Subscribers containing email addresses of Subscribers, attributes of the Subscriber and entities (Participant) with which the Subscriber is associated. The Provider Directory includes, but is not limited to, licensed health care providers, Medicaid providers, other state contracted health care providers, federal health care providers, administrators of state health programs, health plans, and providers in other States that have executed an agreement for Direct Secure Messaging.

Public Health – Public Health activities and reporting, but only to the extent permitted by Applicable Law.

Protected Health Information – Personal health information (PHI), also referred to as protected health information, generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that is collected by a health care professional to identify an individual and determine appropriate care.

Subscriber – The person who registers and provides verifiable demographic information for the purpose of obtaining a Direct Secure Messaging account in his/her name.

Treatment – Treatment of the Individual who is the subject of the Protected Health Information ("PHI") requested or received by the Participant or Participant User.

Direct Secure Messaging Subscription Agreement

This Direct Secure Messaging Subscription Agreement is entered into between Subscriber and District of Columbia Health Information Exchange (DC HIE), acting by and through the Department of Health Care Finance (DHCF). DHCF manages, operates and staffs DC HIE. DHCF is located at 899 North Capitol Street, N.E., 6th Floor, Washington, D.C. 20002.

Subscriber desires to participate in the DC HIE's Direct Secure Messaging for the purpose of exchanging patient data a.k.a. Protected Health Information (PHI) with other providers/qualified health care professionals whose identity has been approved and have been verified by DHCF. DHCF agrees to allow such participation under the terms and conditions set out in this Agreement.

I. Permitted Purposes for this Secure Messaging Service

Subscriber shall:

Subscriber agrees to send PHI and/or health data, or use the same received by it from other Subscriber, in a manner which complies with the Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936, 45 CFR 164 *et al* ("HIPAA") and for the following purposes:

A. **Treatment.** Treatment of the Individual patient who is the subject of the Protected Health Information (PHI) requested or received by the Subscriber, and

B. **Health Care Operations.** Health Care Operations, as defined by HIPAA, provided that:

i. the requesting Subscriber has an established treatment relationship with the individual who is the subject of the PHI;

ii. the purpose of the request is for those Health Care Operations listed in paragraphs (1) and (2) of the definition of Health Care Operations in 45 CFR § 164.501 or health care fraud and abuse detection with respect to use of the Service or compliance with this Agreement's requirements; and

iii. Subscriber is requesting/accessing PHI for its own use. Subscriber must only request and use the Minimum Necessary PHI for such Health Care Operations purposes.

C. **Public Health.** Public Health activities and reporting, but only to the extent permitted by the HIPAA and applicable law.

D. **Reporting on Clinical and Quality Measures.** Reporting on such clinical quality measures and such other measures to demonstrate "meaningful use," as specified in regulations promulgated by the U.S. Department of Health and Human Services under the American Recovery and Reinvestment Act of 2009, Sections 4101 and 4102, or other payer incentive or accreditation programs, but only to the extent permitted by applicable law.

E. **Compliance and Investigations**. Complying with internal investigations to ensure compliance with HIPAA and expanded requirements for privacy and security under the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as Subtitle D of the American Recovery and Reinvestment Act of 2009.

II. Subscriber Responsibilities

Subscriber shall:

A. Meet and comply with the District of Columbia Health Information Exchange Policy and Procedure Manual for the DC HIE Direct Secure Messaging Agreement.

B. Ensure that Subscriber's current Medicaid Provider Number and/or Professional License Information are correctly reflected and current in both the Medicaid Management and Information System and the Department of Health licensed provider/qualified health care professional database.

C. Request from other Subscribers and transmit only the amount of PHI that is the **MINIMUM NECESSARY** required for a particular task.

D. DC HIE Direct Secure Messaging Subscribers shall not include (1) Alcohol or Drug Abuse Patient Records, (2) Mental Health Information, (3) Psychotherapy Notes, (4) Communicable Diseases Records, and (5) HIV and AIDS Medical Records and Information unless otherwise prescribed in accordance with applicable federal and DC laws, including but not limited to obtaining specific client authorization for such disclosures.

a. **Alcohol or Drug Abuse Patient Records.** Subscribers must comply with the requirements and restrictions set forth in 42 CFR Part 2 and any other District or Federal law governing this information with respect to disclosures, use, and confidentiality of information for individuals seeking or obtaining diagnosis, treatment or referrals in federally assisted substance abuse programs.

b. **Mental Health Information.** Disclosures of mental health information must comply with the requirements and restrictions, including but not limited to obtaining written permission from the individual, as set forth in DC Official Code D.C. Code §§ 7-1201.01 to 7-1208.07 and any other District or Federal law governing this information.

c. **Psychotherapy Notes**. Subscribers must not disclose psychotherapy notes unless given authorization and subject to the exceptions prescribed in 45 CFR §164.508(a)(2) and any other District or Federal law governing this information.

d. **Communicable Diseases Records**. Disclosures and use of records incident to the case of a disease or medical condition reported under DC Official Code §§7-131 to 7-144, must comply with the requirements set forth in DC Official Code §§7-131 to 7-144 and any other District or Federal law governing this information.

e. **HIV and AIDS Medical Records and Information**. Disclosure of information related to HIV and AIDS shall comply with the requirements and restrictions set forth in DC Official Code §7-1605 and any other District or Federal law governing this information.

f. **Laboratory Services**. Transmission of laboratory results via Direct is a use case encouraged by ONC. In addition, the security incorporated into Direct, DC HIE and its Direct Secure Messaging subscribers will follow DC Code to ensure that:

i. All requests for clinical laboratory services, the results of all clinical laboratory tests, and the contents of patient specimens shall be confidential.

ii. Persons other than the patient or the patient's physician may have access to the results of the patient's laboratory tests if:

(a) The patient has given written consent to the person seeking access for the release of the records for a specific use; or
(b) The court has issued a subpoena for the results of the patient's laboratory tests, and except in a law enforcement investigation, the person seeking access has given the patient notice and an opportunity to contest the subpoena.

iii. All clinical laboratory results shall be reported to the requesting physician. When there is no requesting physician, the clinical laboratory shall report the test results to the patient and shall recommend that the patient forward the laboratory results to the patient's personal physician as soon as possible.

E. Limit use or disclosure of PHI only to that permitted by this Agreement or required by law.

F. Comply with administrative, physical, and technical safeguards requirements in 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316 as required by § 13401 of the HITECH ACT (February 18, 2010), to maintain the security of the PHI and to prevent use or disclosure of such PHI other than as provided for by this Agreement. Such safeguards shall include:

i. Administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that Subscriber receives, maintains or transmits.

ii. Immediately report to its covered entity any privacy or security incident of which it becomes aware, including any attempts to access ePHI, whether those attempts were successful or not.

iii. Implementing reasonable security measures necessary to protect the security of PHI known as ePHI as defined by HIPAA Security Standards at 45 C.F.R.

Parts 160 and 164, subparts A and C (the "Security Rule") of all such computer systems, networks, files, data and software, and ensure that its business associates agree to the same.

iv. Not to further electronically transmit or permit access to PHI unless such transmission or access is authorized by this Agreement, and further agrees to only transmit or permit such access if such information is secured in a manner that is consistent with applicable law (i.e., encrypted), including the HIPAA Security Rule. For purposes of this Agreement, "encrypted" shall mean the reversible conversion of readable information into unreadable, protected form so that only a recipient who has the appropriate "key" can convert the information back into original readable form.

G. Have in place and abide by procedures for mitigating, and to mitigate to the extent practicable, any known deleterious effects of a use or disclosure of PHI by itself or its Business Associates in violation of HIPAA.

H. Immediately report any potential Breach or Security Incident that he or she discovers, or any other potential threat to the confidentiality, integrity, or availability of PHI exchanged through Direct Secure Messaging to the DC HIE Privacy Officer.

I. Report to its own Privacy Officer and another Subscriber from whom it received PHI any use or disclosure which is not permitted or required by HIPAA when the Recipient Subscriber becomes aware of such unauthorized use or disclosure. Such reports must be made immediately and in writing.

J. Ensure that any workforce member or any agent, including a subcontractor, agrees to the same restrictions and conditions that apply through this Agreement with respect to PHI received from another Subscriber.

K. Retain all information related to disclosures of PHI that the Subscriber makes through Direct Secure Messaging that will be needed to respond to a request for an accounting of disclosures in accordance with the DC HIE Policies and Procedures Manual.

L. Agree to amendments to this Agreement to comply with changes to HIPAA mandates, as well as applicable federal and District law.

III. DC HIE Responsibilities

DC HIE shall:

A. Provide Direct Secure Messaging as a web-mail client via web browser for Subscriber to utilize.

B. Provide for availability of technical infrastructure during reasonable business hours.

C. Retain audit trail data of transactions for ten years from the date of transaction.

D. Establish file size and mailbox limits, and will send alerts to Subscriber's mailbox when Subscriber approaches that limit, along with an explanation of what happens when limits are exceeded.

E. Facilitate the exchange of secure PHI and/or health information between covered entities which are legally authorized to transmit such information through the operation of the System, in accordance with federal and District laws, the DC HIE Policy and Procedure Manual, and this Subscription Agreement. DC HIE has no role in verifying the accuracy of any messages.

F. Verify whether a Subscriber is authorized to send or receive information and/or patient data through the System.

G. DC HIE reserves the right to amend the Agreement to comply with changes to HIPAA mandates, as well as applicable federal and District law. DHCF will notify Subscriber of any required changes via the System.

IV. Fees

There shall be no initial charge for the Direct Secure Messaging service through August 2013. DC HIE reserves the right to begin charging a nominal fee to cover basic costs. DC HIE will provide written notice to Subscriber prior to the imposition of such fee. DC HIE reserves the right to terminate this Agreement for non-payment of fees. A Subscriber may terminate his/her Direct Secure Messaging subscription at any time for any reason.

V. Sanctions

Subscriber agrees that its workforce members, agents and subcontractor who violate the provisions of HIPAA or other applicable federal or state privacy law, will be subject to discipline in accordance with Subscriber's personnel policies and applicable collective bargaining agreements. Subscriber agrees to impose sanctions consistent with its personnel policies and procedures and applicable collective bargaining agreements with respect to persons employed by it. Members of the Subscriber's workforce who are not employed by Subscriber are subject to the policies and applicable sanctions for violation of this Agreement.

VI. Effective Date of Subscription Agreement

Effective on the date executed, Subscriber accepts this Agreement through the Direct Secure Messaging Service registration process.

VII. Duly Authorization to Enter Agreement

This Subscription Agreement has been entered into and executed by the individual Subscriber or an official who is duly authorized to bind their organization. Subscriber acknowledges that he/she has read and fully understands this Agreement. Subscriber has been given the risks and benefits of secure messaging and understands the risks associated with online communications between health care providers/qualified health care professionals and other providers/qualified health care professionals, and between

health care providers/qualified health care professionals and patients, and consents to the conditions outlined herein. In addition, Subscriber agrees to adhere to the policies set forth herein. By agreeing to these terms below, the Subscriber hereby gives informed consent to participate in Direct Secure Messaging service, and hereby agrees to and accept all of the provisions contained above.

VIII. Miscellaneous Provisions

A. **Successors and Assigns.** The provisions of this Agreement shall be binding upon and shall inure to the benefit of the parties hereto and their respective successors and permitted assigns, if any.

B. **No Third-Party Beneficiaries.** The Parties to this Agreement are the only parties entitled to enforce its terms. Except for the enforcement of individual rights provided under HIPAA and HITECH, nothing in this Agreement gives, is intended to give, or shall be construed to give or provide any benefit or right, whether directly, indirectly, or otherwise, to third persons.

C. **Severance.** In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event the Subscriber believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of HIPAA or HITECH, the Subscriber shall notify, in writing, both the DC HIE at its headquarters and the District–wide Privacy and Security Official at the Office of the Attorney General, Office of Healthcare Privacy and Confidentiality, 441 4th Street, NW Washington, DC 20001 in writing and such concerns will be addressed as soon as practicable.

D. **Injunctive Relief.** Notwithstanding any rights or remedies under this Agreement, or provided by law, Subscriber retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of Protected Health Information by another Subscriber, its workforce, any of its subcontractors, agents, or any third party who has received Protected Health Information from the Subscriber.

E. **Assistance in Litigation or Administrative Proceedings.** Subscriber shall make itself and any agents, affiliates, subsidiaries, subcontractors or its workforce assisting the Subscriber in the fulfillment of its obligations under this Agreement, available to the DC HIE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the DC HIE, its directors, officers or employees based upon claimed violation of HIPAA, the Privacy Rule or other laws relating to security and privacy, except where the Subscriber or its agents, affiliates, subsidiaries, subcontractors or its workforce are a named adverse party.

F. **Waiver and Release from Liability and Indemnification.**

i. DC HIE is not liable for any claims and/or damages arising from the following:

(a) Inaccurate or incomplete information provided by Subscribers through the System;

(b) Interruption in the ability to access the Network due to technical difficulties, technical maintenance, or system failure;

(c) Access of protected health information through the System due to Subscribers' negligent sharing or loss of User IDs and password or leaving the System accessible when unattended. Any protected health information accessed through Subscriber in this manner may be available to others and is no longer protected by DC HIE's privacy practices;

(d) Any and all claims due to access by anyone else to any and all PHI printed and/or downloaded by Subscriber from the Service.

ii. Subscriber shall indemnify, hold harmless and defend the DC HIE from and against any and all claims, losses, liabilities, costs, and other expenses incurred as a result or arising directly or indirectly out of or in connection with (a) any misrepresentation, breach of warranty or non-fulfillment of any undertaking of the Subscriber under this Agreement.

IX. Survival

The respective rights and obligations of the Subscriber to comply with federal and District laws with respect to PHI that it received through Direct Secure Messaging Service shall survive termination of the Subscriber's subscription to Direct Secure Messaging.

X. Force Majeure

Parties will not be liable for nonperformance or delay in performance (other than obligations of payment or adherence to federal and District laws) caused by any event reasonably beyond the control of the Parties including, but not limited to wars, hostilities, revolutions, foreign or domestic terrorism, riots, civil commotion, national emergency, strikes, lockouts, unavailability of supplies, epidemics, fire, flood, earthquake, force of nature, explosion, embargo, or any other Act of God, internet, electric power or communications outage, or any law, proclamation, regulation, ordinance or any court, government or government agency.

XI. Term and Termination

A. **Term.** This Agreement will commence on the date when the Subscriber is certified to use the Direct Secure Messaging Service and will be in effect until terminated in accordance with this Agreement.

B. **Termination.** This Agreement may terminate as follows:

i. Uncured Breach or failure to comply with the Policies and Procedures governing DC HIE.

ii. Termination Without Cause. Parties each have the right to terminate this Agreement without cause, with at least thirty (30) days prior written notice.

iii. Privacy/Security Breach. Parties may terminate this Agreement immediately, in writing if either breaches a material obligation under this Agreement if the security of Direct Secure Messaging or the system of DC HIE, Subscriber, or agents of either Party, has been or is likely to be seriously compromised by such breach, or such breach has been or is likely to result in a serious violation of the legal obligations of either Party to protect the privacy and confidentiality of patient data. DC HIE may elect to suspend Subscriber's access to the Direct Secure Messaging system in lieu of termination, in accordance with the DC HIE Policies and Procedures.

iv. Cessation of Operation. Subject to restrictions imposed by law, the Parties may terminate this Agreement in writing if performance is impossible because of cessation of business operations, DC-HIE non-appropriation, or if Subscriber is the subject of proceedings for bankruptcy or insolvency, receivership, or dissolution or makes an assignment for the benefit of creditors.

v. Failure of Infrastructure of DC HIE. DC HIE may immediately terminate this Agreement upon written notice if anything required for the DC HIE to continue lawful operations becomes unavailable. Alternatively¸ DC HIE may temporarily suspend the access of Subscriber until such time as DC HIE is able to resume lawful operation of the Direct Secure Messaging Service.

vi. DC HIE reserves the right to deactivate Subscriber account if Subscriber's clinical license is suspended or revoked or if Subscriber is dis-enrolled from the Medicaid Program or if the Delegate is no longer employed in a capacity that requires transmission of PHI/ePHI.

vii. DC HIE reserves the right to deactivate Subscriber's account if the Subscriber violates any provision of this agreement or any Policy and Procedure governing DC HIE, and the violation is so serious that suspension is not an appropriate response.

viii. DC HIE reserves the right to deactivate Subscriber's account upon discovering any material error or omission in the information that the DC HIE Subscriber provided during the Enrollment process that is so serious that suspension is not an appropriate response.