District of Columbia Health Information Exchange Policy and Procedure Manual

HIPAA Privacy & Direct Privacy Policies

(Version 1 – November 27, 2012)

Table of Contents

Introduction to the Policy and Procedure Manual

District of Columbia Health Information Exchange (DC-HIE) is the statewide Health Information Exchange (HIE) for the District of Columbia. It provides a secure, confidential, electronic system to support the exchange of protected health information (PHI) and electronic protected health information (ePHI) including patient medical records, among health care providers in the District and beyond. DC HIE is administered and staffed by the District of Columbia Department of Health Care Finance (DHCF).

Direct Secure Messaging is the name of the technical infrastructure that allows providers/authorized users subscribed to the DC HIE to share health information electronically in a method similar to regular email but with the added security required for sensitive health information. Direct Secure Messaging is a 'push' secure messaging system whereby information is sent from one subscribed provider directly to another subscribed provider who is known to the sender. Direct Secure Messaging is based on the National Direct Project, which was launched March 2009 by the Office of the National Coordinator of Health Information Technology (ONC).

This Policy and Procedure Manual contains policies and procedures that implement the policy decisions which underlie DC-HIE. These policies and procedures will inform all subscribers and stakeholders of the "rules of the road" for the HIE, in addition to the trust agreements that each Participant and User signs.

Governing Body Policies and Procedures

The DC-HIE Policy Board is responsible for advising DHCF and the Mayor on the overall strategic direction for DC-HIE as well as providing recommendations on its development and implementation. Working with the Statewide HIE HIT Coordinator and other strategic advisors, the DC-HIE Policy Board will provide feedback on the implementation of technical and policy components that are critical to a successful health information exchange.

The DC-HIE Policies and Procedures describe the ways in which the DC-HIE will operate to maximize its effectiveness and transparency. They include basic organizational policies and procedures. How DC HIE Policy Board Meetings are organized is covered in the DC HIE Bylaws. All meetings will be conducted in compliance with federal and District laws.

HIPAA Privacy and Security Overview

Because DC-HIE is in the business of helping providers securely exchange health information, DC-HIE has written Privacy and Security Policies and Procedures to affirm its commitment to comply with the applicable provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act). DC-HIE is required to comply with certain provisions of the HIPAA Privacy and Security Regulations. The Policies and Procedures included in this Manual provide the framework through which DC-HIE will comply.

HIPAA Privacy Policies and Procedures

The HIPAA Privacy Regulations provide rules regarding the use and disclosure of PHI, as well as specific rules regarding an individual's rights to access PHI about him/herself. DC-HIE is required to follow all requirements of the HIPAA Privacy Regulations. DC-HIE's Privacy Officer will oversee its compliance with the HIPAA Privacy Regulations and its efforts to protect the privacy of all PHI and ePHI that is exchanged through the Direct Secure Messaging. DC-HIE will consistently monitor, and periodically audit, its Privacy practices to ensure compliance with the Privacy Policies and Procedures.

HIPAA Security Policies and Procedures

Under HIPAA Security Regulations, Covered Entities and Business Associates are required to implement administrative, physical, and technical safeguards that ensure the confidentiality, integrity, and availability of ePHI. These safeguards are designed to:

1. Ensure the confidentiality, integrity, and availability of all ePHI it creates, receives, maintains, or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted by the HIPAA Privacy Regulations; and,
4. Ensure compliance with the HIPAA Security Regulations by its workforce.

The Security Policies and Procedures in this Manual address DC-HIE's obligations under the HIPAA Security Regulations. In designing these policies and procedures, DC-HIE has considered:

1. DC-HIE's size, complexity, and capabilities;
2. DC-HIE technical infrastructure, hardware, and software security capabilities;
3. The costs of security measures; and
4. The probability and criticality of potential risks to ePHI.

DC-HIE's Privacy Officer and the HIE/HIT Coordinator will oversee DC-HIE's initiatives to create and maintain appropriate and reasonable policies, procedures, and controls to protect the security of ePHI exchanged through Direct Secure Messaging.

Direct Secure Messaging Operations Policies and Procedures

Direct Secure Messaging is the initial service of the DC-HIE. The Direct Secure Messaging Operations Policies and Procedures include general policies and procedures that describe how the Direct Secure Messaging service will be used, operated and managed.

General HIPAA Policies and Procedures

For the purposes of the DC-HIE general HIPAA Policies, Privacy Policies and Security Policies, the following terms shall have the meaning ascribed to them below.

Addressable: Addressable refers to implementation specifications contained within certain HIPAA Regulations which DC-HIE is not required to implement. DC-HIE must perform an assessment to determine whether the addressable implementation specification is a reasonable and appropriate safeguard for implementation in its efforts to protect unauthorized use, disclosure, and access of PHI or ePHI. If it is not reasonable and appropriate, DC-HIE must document the reasons supporting this conclusion.

Administrative Safeguards: Administrative Safeguards are actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of Users in relation to the protection of ePHI.

Breach: The unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Business Associate: A Business Associate is a person or entity who, on behalf of a Covered Entity, performs, or assists in the performance of, a function or activity involving the use or disclosure of individually identifiable health information, including, but not limited to, facilitation of the exchange of health information; claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; or practice management.

Contingency Event: An unplanned event, such as an emergency or disaster, which may require the activation of DC-HIE's Contingency Plan, Data Back-Up Plan, Disaster Recovery Plan, or Emergency Operations Plan.

Covered Entity: A Covered Entity is (i) a health plan, (ii) a health care clearinghouse, or (iii) a health care provider who transmits any health information in any form, including in electronic form. For purposes of this HIPAA Privacy and Security Policy and Procedures Manual, Covered Entity means a Direct Secure Messaging Subscriber who utilizes Direct Secure Messaging, including health care providers, medical practices, and laboratories.

Direct Secure Messaging: A service provided by DC-HIE to DC-HIE Direct Subscribers that allows the Subscriber to send and receive secure messages utilizing the Direct Project specifications and an internet-based service provided by DC-HIE, through a contracted HISP.

Direct Secure Messaging Subscriber: An individual clinician who is regulated by the District of Columbia Health Licensing and Regulatory Administration (DC HLRA) Board of Licensure and who has successfully subscribed to Direct Secure Messaging.

Direct Subscriber Information: demographic information about Direct Secure Messaging subscribers provided to DC-HIE during the Direct Secure Messaging subscription process or in accordance with the Direct Secure Messaging End Subscriber License Agreement.

Electronic Protected Health Information or ePHI: Electronic PHI means PHI which is either transmitted by electronic media or maintained in electronic media.

HIPAA Regulations: HIPAA Regulations means the Health Insurance Portability and Accountability Act of 1996 and the rules and regulations promulgated thereunder, and the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. §§ 17921-17954) and the rules or regulations promulgated thereunder.

Network: Refers to the technology platform provided by DC HIE's technology vendor.

Physical Safeguards: Physical Safeguards are physical measures, policies, and procedures to protect the Network and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Privacy Officer: Privacy Officer means the individual named in the Assigned Privacy Responsibility Policy (HP-7).

Protected Health Information or PHI: 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.

Required: Required refers to implementation specifications contained within certain HIPAA regulations with which DC-HIE must comply.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations of Direct Secure Messaging.

Security Officer: Security Officer means the individual named in the Assigned Security Responsibility Policy (HS-3).

Technical Safeguards: Technical Safeguards means the technology and the policy and procedures that DC-HIE has in place to protect ePHI and control access to it.

User: A person or entity with authorized access to Direct Secure Messaging. Users include workforce members, Direct Secure Messaging Subscribers, employees and agents of DC-HIE who are authorized to use Direct Secure Messaging and Vendors.

Vendor: Vendor means a vendor, consultant, contractor or other non-DC-HIE third party who may have access to the Network for any reason or purpose (other than those who may have incidental access) or who may have access to any DC-HIE facilities housing the information technology assets that support the Network or related infrastructure.

Workforce Member: All persons who are under the control of DC-HIE, including, but not limited to, employees, independent contractors, loaned personnel, interns, and temporary personnel who have access to the Network or any PHI derived from the Network.

Workstation: Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

DC-HIE	General HIPAA Policies	Policy No.: **DC-H-2**
Title: Workforce Member Confidentiality and Compliance	Version: **1**	Effective Date:

Purpose Statement: All Workforce Members are required to certify in writing, by signing the Workforce Member Confidentiality and Compliance Statement provided below, that they have received, read, received training on, understand and agree to follow the policies in the manual that has been provided to them and all applicable provisions of HIPAA and the HITECH Act. Also, as part of their compliance with these Policies and Procedures, Workforce Members must certify that they will protect the confidentiality of PHI, including ePHI, and that they will report any unauthorized disclosures of PHI or ePHI and other Security Incidents to the Privacy Officer or Security Officer, as specified in this manual.

Policy/Procedure:

1. All Workforce Members will sign the Workforce Member Confidentiality and Compliance Statement provided below prior to being given access to PHI, ePHI or the Network and annually thereafter.
2. The Privacy Officer will maintain a record on each Workforce Member that includes the original, signed Workforce Member Confidentiality and Compliance Statements.
3. The Privacy Officer will return a copy of the signed Workforce Member Confidentiality and Compliance Statement to the Workforce Member.
4. Any Workforce Member that refuses to sign the Workforce Member Confidentiality and Compliance Statement will be sanctioned in accordance with the Workforce Member Discipline Policy (H-3).

Responsibility: Privacy Officer; Workforce Member
Regulatory Category: Privacy Regulations; Security Regulations

Workforce Member HIPAA Confidentiality and Compliance Statement

I, _____, acknowledge that I have received, read, received training on, understand and agree to follow the DC-HIE HIPAA Privacy and Security Policies and Procedures that have been given to me for my review. Also, I acknowledge that during the course of performing my assigned duties at DC-HIE, I may have access to, use, or disclose Protected Health Information (PHI) or electronic PHI (ePHI). I agree to handle such information in a confidential manner at all times during and after my employment and commit to the following obligations:

1. I will use and disclose PHI, including ePHI, only in connection with and for the purpose of performing my assigned job functions.
2. I will request, obtain, or communicate PHI, including ePHI, only as necessary to perform my assigned job functions and will refrain from requesting, obtaining or communicating more PHI, including ePHI, than is necessary to accomplish such functions.
3. I will take reasonable care to properly secure PHI, including ePHI, on my Workstation and will take steps to ensure that others cannot view or access such information.
4. I will use and disclose PHI, including ePHI, solely in accordance with the applicable federal and state laws and regulations and all DC-HIE HIPAA Privacy and Security Policies and Procedures. I also agree, in a timely manner, to familiarize myself with any periodic updates or changes to these policies.
5. I will immediately report any unauthorized use or disclosure of PHI, including ePHI, that I become aware of to the appropriate DC-HIE Official.
6. I understand and agree that my failure to fulfill any of the obligations set forth in this Statement and any failure to comply with the DC-HIE's HIPAA Privacy and Security Policies and Procedures will result in my being subject to appropriate disciplinary action, up to and including, the termination of my employment.

Workforce Member	Privacy Officer Signature
Workforce Member Printed Name	Date
Workforce Member Job Function	Date

Responsibility: Privacy Officer; Workforce Member
Regulatory Category: Privacy Regulations; Security Regulations

DC-HIE	General HIPAA Policies	Policy No.: **DC-H-3**
Title: **Workforce Member Discipline**	Version: **1**	Effective Date:

Purpose Statement: DC-HIE will discipline Workforce Members, as necessary, for violations of its HIPAA Privacy and Security Policies and Procedures.

Policy/Procedure:

MINOR OCCURRENCES

If the Privacy Officer determines that a Workforce Member's acts or omissions resulted in a relatively minor violation of these HIPAA Privacy and Security Policies and Procedures and no significant violation of any law or regulation, the Privacy Officer, in collaboration with the HIT Coordinator will determine whether or not further education, clarification, or other corrective actions are needed.

Example: Failing to protect information on a computer screen in an area that has high public access, and not having screen saver time out software set to time out at a reasonable time like after 5-10 minutes of inactive use.

SIGNIFICANT VIOLATIONS

If the Privacy Officer determines that a Workforce Member's acts or omissions resulted in a significant violation of these HIPAA Privacy and Security Policies and Procedures or a violation of any law or regulation, the Privacy Officer will report the findings to the District of Columbia HIT Coordinator. The HIT Coordinator will notify the appropriate representative or DC agency, who will then determine the scope of any disciplinary steps to be taken.

Example: The agency (DHCF) not having Continuity of Operations Plans (COOP) plans or Disaster Recovery Plans in place for bringing your IT services back on line after a disaster or emergency event.

DISCIPLINARY ACTION

1. Disciplinary action should be commensurate with the seriousness of the security or privacy violation. Discipline shall be consistent with:

    a. any and all District laws and rules governing sanctions for District government employees, including but not limited to the DC Personnel Regulations, 6-B D.C. Mun. Regs. §§1600 et seq.;
    b. the terms and conditions set forth in the contract in which a contractor secured with DHCF and any and all District laws and rules governing DC government contracts and procurement, including but not limited the Procurement Practices Reform Act of 2010, DC Official Code §§ 2-351.01 et seq. (2010); and
    c. the Business Associate Agreement and all federal and District laws applicable to Business Associates of DC HIE/DHCF

2. The HIE/HIT Coordinator will consult with DC Human Resources, DHCF Contracting Officer, Office of Contracting and Procurement, the Business Associate Agreement, or legal counsel to determine the appropriate disciplinary action.

Responsibility: Privacy Officer; HIT Coordinator, Human Resources representative.
Regulatory Category: Privacy Regulations
Regulatory Reference:

- 45 C.F.R. §164.308(a)(1)(ii)(C), Sanction Policy [Implementation Specification; Required]

HITECH Act Language

"A business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach."

"For purposes of this section, a breach shall be treated as discovered by a covered entity by a business associate as of the first day on which such breach is known to such entity or associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred."

"Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate involved in the case of a notification required under subsection (b))."

HIPAA Security Rule Language: "Implement policies and procedures to address security incidents."

Purpose Statement: Despite taking all reasonable and appropriate steps to protect the confidentiality, integrity and availability of ePHI transmitted through Direct Secure Messaging, DC-HIE may experience Security Incidents and/or Breaches. DC-HIE will promptly identify, report, track, and respond to Security Incidents and potential Breaches. Awareness of, response to, and creation of reports about Security Incidents and Breaches are integral parts of DC-HIE's efforts to comply with the HIPAA Regulations.

Policy/Procedure:

SECURITY INCIDENTS

1. A "Security Incident" is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations through the Network.

2. The following incidents are examples of potential Security Incidents. This list is not exclusive. The Security Officer will determine when a Security Incident has or is likely to have occurred.

    a. Stolen or otherwise inappropriately obtained passwords that are used to access the Network;
    b. Corrupted backup tapes that do not allow restoration of ePHI through the Network
    c. Virus attacks that interfere with the operations of the Network;

d. Physical break-ins to DC-HIE's facilities which may lead to the theft of electronic media containing ePHI;
e. DC-HIE's failure to terminate the account of a former DC-HIE Direct User that is then used by an unauthorized individual to access the Network; and/or
f. Allowing electronic media containing ePHI, such as a computer hard drive or laptop, to be accessed by a User who is not authorized to access such ePHI prior to removing the ePHI stored on the media.
g. Allowing electronic media containing ePHI, such as a computer hard drive or laptop, to be accessed by a User who is not authorized to access such ePHI prior to removing the ePHI stored on the media.

BREACHES

1. A Breach is defined as the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to obtain such information.

2. The HITECH Act Breach notification requirements only apply to PHI that is "unsecured." "Unsecured" PHI is that PHI which is not secured through a technology or methodology that the Department of Health and Human Services (HHS) has stated renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals.

3. According to guidance issued by HHS in August 2009 (the most recent guidance issued by HHS on this topic as of the creation date of this Policy), PHI is secured through encryption (for ePHI) or destruction (for PHI in all other formats).

4. DC-HIE will take all measures necessary to secure PHI in accordance with the Device and Media Controls (HS-18), Technical Access Controls (HS-19), and Transmission Security (HS-22) Policies included in this Manual.

5. In addition, the following occurrences are not Breaches:

    a. Any unintentional acquisition, access, or use of PHI by a Workforce Member or individual acting under the authority of DC-HIE if:

        i. Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such Workforce Member or individual, respectively, with DC-HIE; and
        ii. Such information is not further acquired, accessed, used, or disclosed by any person.

    b. Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility under the authority of DC-HIE to another similarly situated individual at the same facility and any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

IDENTIFYING POTENTIAL BREACHES AND SECURITY INCIDENTS

1. DC-HIE will be responsible for monitoring and auditing activities. DC-HIE will, on a regular basis, review audit reports which provide a summary of all uses of the Network.
2. The following findings in the audit reports will signal a potential Breach or Security Incident:

    a. A single Direct Secure Messaging User sending more than five messages through DC-HIE Direct Messaging between the hours of 12:00 am – 5:00 am
    b. Failed authentication attempts after five (5) unsuccessful attempts
    c. Activity originating from an I/P address outside of the country

REPORTING POTENTIAL BREACHES AND SECURITY INCIDENTS

1. Any Workforce Member, including DC-HIE management, must report any potential Breach or Security Incident that he or she discovers, or any other potential threat to the confidentiality, integrity, or availability of ePHI exchanged through the Network, to the Privacy Officer immediately upon discovery of the potential Breach, Security Incident or threat.
2. Any Direct Secure Messaging User, other than a Workforce Member, must 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, its own covered entity, and its own Privacy Officer.
3. The individual providing notice of the potential Breach, Security Incident or other threat may provide such notice in writing.
4. Any Direct Secure Messaging Subscriber shall 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.
5. The Privacy Officer will document the report of a potential Breach or Security Incident or threat along with the date and time that he or she was notified of such event.
6. DC-HIE will not take any retaliatory measures against an individual who reports a potential Breach or Security Incident or threat. If the Breach or Security Incident was created by the neglect, or deliberate action, of a User, then DC-HIE may impose sanctions as set forth in other Policies.
7. No DC-HIE Exchange Participant or User will prohibit or otherwise attempt to hinder or prevent another DC-HIE Exchange Participant or User from reporting a potential Breach, Security Incident or threat.

RESPONSE TO POTENTIAL BREACHES AND SECURITY INCIDENTS

1. Upon becoming aware of a potential or suspected Breach or Security Incident, the DC-HIE Privacy Officer will immediately activate the Incident Response Team. The Incident Response Team shall be composed of the District HIT Coordinator, the DC-HIE Privacy Officer, DC-HIE Technology Provider (could be a technology contractor), DC-HIE Policy Analyst, District-wide Privacy and Security Official, and the Chairperson of the Legal/Policy/Privacy Committee. The HIT Coordinator will be the Incident Response Leader.

2. The Incident Response Team will promptly conduct an initial review of the facts surrounding the potential Breach or Security Incident to determine whether a Breach or Security Incident occurred. The Incident Response Team will strive to make an initial determination within 48 hours of becoming aware of the potential Breach or Security Incident.

3. If the Incident Response Team determines that a Breach or Security Incident did not occur, the DC-HIE Privacy Officer will document this along with all of the information that supports such conclusion and no further investigations are required. The Privacy Officer will present a summary of the Incident Response Team's findings at the next meeting of the DC-HIE Policy Board.

4. If the Incident Response Team determines that a Breach or Security Incident did occur or is likely to have occurred, then:

    a. The Incident Response Team will determine the scope, magnitude and severity of the Breach or Security Incident; mechanisms for containing the Breach or Security Incident if it is on-going; mechanisms for mitigating the harmful effects of the Breach or Security Incident; and, ways to remediate the vulnerability that led to the Breach or Security Incident. The Incident Response Team will prepare these initial findings within 72 hours of becoming aware of the potential Breach or Security Incident and will update those findings as more information becomes available.
    b. The Incident Response Team will determine which Direct Secure Messaging Users, if any, should be involved in the investigation and mitigation activities and involve such Participants and Users as the Committee deems appropriate.
    c. The Incident Response Team will officially notify all affected Direct Secure Messaging Users of a Breach or Security Incident within ten (10) business days of becoming aware of such Breach or Security Incident. The notification will include the following information:

        i. The date of the Breach or Security Incident.
        ii. The identity of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such Breach or Security Incident, if it can be determined.
        iii. A description of the roles of the people involved in the Breach or Security Incident such as, but not limited to, Users, Workforce Members, Vendors or unauthorized persons.
        iv. The type of information that was Breached or involved in the Security Incident, if it can be determined.
        v. A brief description of the circumstances involved in the Breach or Security Incident.

    d. District-wide Privacy and Security Officer will determine whether DC-HIE is required to make any additional notifications pursuant to applicable breach notification laws and discuss such notifications with the Incident Response Team and the affected Direct Secure Messaging Users.
    e. If DC-HIE has determined that a Direct Secure Messaging User's noncompliant behavior caused a Breach or Security Incident, DC-HIE will determine the appropriate corrective action to pursue, including termination of the Direct Secure Messaging

User's authorization to use the service. The Direct Secure Messaging User must abide by whatever corrective action DC-HIE decides to pursue regarding the noncompliant behavior.

f. The HIT Coordinator will notify the DC-HIE Policy Board of the results of the Incident Response Team's findings. The DC HIE Policy Board will provide guidance to the HIT Coordinator regarding how to communicate the findings more widely if necessary.

g. The Security Officer will retain all documentation regarding the Breach or Security Incident for ten years.

OTHER MEASURES REGARDING BREACHES AND SECURITY INCIDENTS

1. DC-HIE will provide training and awareness materials to Users, as appropriate, regarding the process for promptly identifying, reporting, tracking, and responding to potential Breaches and Security Incidents in accordance with this Policy.

2. DC-HIE will report significant violations by Workforce Members in accordance with the Workforce Member Discipline Policy (H-3) against Workforce Members whose actions lead to or cause Breaches or Security Incidents.

3. No User who reports a suspected Breach or Security Incident that is caused by another User will face retaliation from DC-HIE.

Responsibility: Privacy Officer, Direct Secure Messaging User, Workforce Member, Human Resources representative
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 42 U.S.C.A. §17932 (b)-(d)
- 45 C.F.R. §164.308(a)(6)(i), Security Incident Procedures [Standard; Required]
- 45 C.F.R. §164.308(a)(6)(ii), Response and Reporting (of Security Incidents) [Implementation Specification; Required]

HITECH Act Language: "In the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract with such covered entity, the business associate may use and disclose such protected health information only if such use or disclosure, respectively, is in compliance with each applicable requirement of section 164.504(e)."

HIPAA Privacy Rule Language:
"A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information."

"The contract or other arrangement between the covered entity and the business associate required by §164.502(e) must meet the requirements of paragraph (e)(2) or (e)(3) [governmental agencies], as applicable.

(ii) A covered entity is not in compliance with the standards of §164.502(e) and paragraph (e) of this subsection, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful:

(a) Terminated the contract or arrangement, if feasible; or
(b) If termination is not feasible, reported the problem to the Secretary."

"(2) *Implementation specifications: Business associate contracts*. A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;

(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with §164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information to provide an accounting of disclosures in accordance with §164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(I) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information, or if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible."

HIPAA Security Rule Language:

"A covered entity, in accordance with § 164.306 (the Security Rule; General Standards), may permit a business associate to create, receive, maintain, or transmit electronic PHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) (the Organizational Requirements) that the business associate will appropriately safeguard the information."

"Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a)."

Purpose Statement: DC-HIE is a Business Associate under the HIPAA Privacy Regulations because it facilitates the exchange of health information on behalf of Covered Entities. Under both the HITECH Act and its Business Associate Agreements with Covered Entities, DC-HIE is required to comply with the HIPAA Privacy Regulations. These Privacy Policies and Procedures document such compliance.

Policy/Procedure:

CONTRACTS WITH VENDORS

1. DHCF, on behalf of DC-HIE may enter into agreements with Vendors, as permitted by its Business Associate Agreements, for services related to the Network.

2. In its agreements with Vendors, DC-HIE will require that Vendors:

    a. Appropriately safeguard ePHI and access to the Network through privacy and security policies and procedures that are fully compliant with the HIPAA Privacy and Security Regulations;
    b. Ensure that any agent, including subcontractors, to whom it provides ePHI agrees to implement reasonable and appropriate safeguards to protect it; and
    c. Report to DC-HIE any Security Incident of which it becomes aware.

3. Agreements with Vendors must authorize the termination of the contract by DHCF if DHCF determines that the Vendor has violated a material term of the contract.

4. DHCF will terminate a contract with a Vendor if DHCF/DC-HIE becomes aware of a pattern of activity or practice of the Vendor that constitutes a material breach or violation of the Vendor's privacy or security obligations unless the Vendor cures the breach or ends the violation. If termination of the contract is not feasible, DC-HIE will report the breach to the Secretary of Health and Human Services.

AGREEMENTS WITH DC-HIE DIRECT USERS

1. DC-HIE will enter into agreements with Direct Secure Messaging Subscribers pursuant to the Agreements with DC-HIE Direct Secure Messaging Agreement Policy (DM-5).

Responsibility: Privacy and Security Officers; Direct Secure Messaging Users; Vendors
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 42 U.S.C.A. §17934, Application of privacy provisions and penalties to business associates of covered entities
- 45 C.F.R. §164.502(e), Uses and Disclosures of Protected Health Information: General Rules
- 45 C.F.R. §164.314(a)(1), Organizational Requirements
- 45 C.F.R. § 164.504(e)(2), Uses and Disclosures: Organizational Requirements
- 45 C.F.R. §§164.308(b)(1)-(b)(4), Business Associate Contracts and Other Arrangements [Standard; Required]

HIPAA Privacy Policies and Procedures

DC-HIE	HIPAA Privacy	Policy No.: **DC-HP-1**
Title: **Uses and Disclosures of PHI**	Version: **1**	Effective Date:

Purpose Statement: DC-HIE will only use or disclose PHI as permitted by its Direct Secure Messaging Subscription Agreements.

HIPAA Privacy Language Rule

Permitted Uses and Disclosures – 45 C.F.R. §164.506(a)

"Except with respect to uses or disclosures that require an authorization under §164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations…provided that such use or disclosure is consistent with other applicable requirements of this subpart."

Uses and Disclosures for Which an Authorization Is Required— §164.508(a)

"Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization."

Policy/Procedure:

1. DC-HIE may only use or disclose PHI to fulfill its responsibilities under the Direct Secure Messaging Subscription Agreement. This includes, but is not limited to, performing proper management and administrative functions.

2. DC-HIE's uses and disclosures of PHI in connection with Direct Secure Messaging are more fully described in DC-HIE's Use and Disclosure of PHI in DC-HIE Direct Messaging Policy (DM-6).

3. DC HIE's technology vendor uses the highest level of encryption technology available to ensure the security of messages transmitted on its system.

Responsibility: Privacy Officer; DC-HIE Direct Secure Messaging User

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.506(a), Uses and Disclosures to Carry Out Treatment, Payment, or Health care Operations [Standard; Required]
- 45 C.F.R. §164.508(a), Uses and Disclosures for which an Authorization is Required [Standard; Required]

DC-HIE	HIPAA Privacy	Policy No.: **DC-HP-2**
Title: **Minimum Necessary Standard**	Version: **1**	Effective Date:

Purpose Statement: DC-HIE will use reasonable efforts to limit PHI or ePHI that it uses or discloses as part of its management and administration of the Network to the least amount necessary (the "minimum necessary") to accomplish the intended purpose of the disclosure. This policy encompasses PHI in any format, such as oral, electronic, or written.

HIPAA Privacy Rule Language: "A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

"For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

"For all other requests, a covered entity must: (A) develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and (B) review requests for disclosure on an individual basis in accordance with such criteria."

Policy/Procedure:

DC-HIE will limit all uses and disclosures of or requests for PHI to the minimum necessary to achieve the purpose of the use, disclosure or request, except for:

a. Disclosures made to the Secretary of Health and Human Services
b. Uses or disclosures required by law
c. Uses or disclosures required for compliance with HIPAA

INTERNAL USES

1. The Privacy Officer will assess and determine, on a yearly basis, those Workforce Members who require access to PHI in order to carry out their job functions.

2. DC-HIE will document its Workforce Members' access to PHI in accordance with the Information Access Management Policy (HS-5).

3. The Privacy Officer will ensure that reasonable efforts are used to limit the access to the persons identified and for only the types of PHI which are needed to carry out their job functions.

4. For PHI that DC-HIE uses to perform certain management and administrative functions, DC-HIE will limit all uses of PHI to the minimum necessary to achieve the purpose of the particular management or administrative function.

EXTERNAL DISCLOSURES

1. For any disclosure DC-HIE makes on a routine and recurring basis, DC-HIE will implement protocols that establish the minimum necessary amount of PHI that may be disclosed to achieve the purpose of the disclosure. On an annual basis, the Privacy Officer will:

    a. Assess and determine all routine and recurring disclosures requested or made by DC-HIE.
    b. Compose and complete a disclosure survey that identifies all routine and recurring disclosures.
    c. Assess and determine the types of PHI that are disclosed for the disclosures identified on the disclosure survey.
    d. For all recurring disclosures identified in the disclosure survey, the PHI disclosed will be limited to the amount reasonably necessary to achieve the purpose of the disclosure, but each disclosure does not require independent review by the Privacy Officer.

2. For all disclosures not specifically listed on the annual disclosure survey, the disclosure request must be sent to the Privacy Officer for review and determination for compliance with the minimum necessary standard.

3. Disclosures made to public officials as required by or in accordance with the law, if the public official represents that the information requested is the minimum necessary for the stated purpose(s), do not have to be reviewed by the Privacy Officer since they are deemed to be the minimum necessary for the requested disclosure.

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations
Regulatory Reference:

- 45 C.F.R. §164.514(d)(4)(i)-(d)(iii), Other Requirements Relating to Uses and Disclosures of PHI: Minimum Necessary Requirements

DC-HIE	HIPAA Privacy	Policy No.: **DC-HP-3**
Title: **De-Identification of PHI**	Version: **1**	Effective Date:

Purpose Statement: If permitted by the applicable Direct Secure Messaging Subscription Agreement DC-HIE may use and disclose an individual's health information that has been de-identified. After health information is de- identified, it is no longer subject to the requirements of the HIPAA Privacy Regulations.

HIPAA Privacy Rule Language: "Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information."

Policy/Procedure:

1. All de-identification of health information will be performed at the direction and under the supervision of the Privacy Officer and in accordance with the applicable Business Associate Agreement and Direct Secure Messaging Subscription Agreement.

2. The reason for the de-identification will be documented and maintained by the Privacy Officer.

3. DC-HIE may de-identify an individual's health information in either of the following ways:

    a. Remove all of the following identifiers from the individual's health information, as set forth in 45 CFR § 164.514(b)(2)(i):
        i. Names.
        ii. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes.
        iii. All elements of dates (except year) for dates directly related to anindividual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
        iv. Telephone numbers.
        v. Fax numbers.
        vi. Social Security numbers.
        vii. Electronic mail address.
        viii. Medical record numbers.
        ix. Health plan beneficiary numbers.
        x. Account numbers.
        xi. Certificate/license numbers.
        xii. Vehicle identifiers and serial numbers, including license plate numbers.
        xiii. Device identifiers and serial numbers.
        xiv. Web Universal Resource Locators (URLs).
        xv. Internet Protocol (IP) address numbers.

xvi. Biometric identifiers, including finger and voice prints.
xvii. Full face photographic images and any comparable images.
xviii. Any other unique identifying number, characteristic, or code, except

b. If any of the above 18 identifiers are not removed, DC-HIE may utilize a qualified person to determine that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify a subject of the information.

i. A "qualified person" is person:

1) One with appropriate knowledge and experience applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable;
2) One who applies such methods and principles to determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
3) One who documents the methods and results of the analysis that justify such determination.

c. No de-identified information will be disclosed if DC-HIE has knowledge that the information could be used alone or in combination to identify a subject of the information.

d. DC-HIE may assign a code or other means of record identification to allow information that has been de-identified to be re-identified by DC-HIE, as long as:

i. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual.
ii. DC-HIE does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations
Regulatory Reference:

- 45 C.F.R. §164.514(a)-(c), De-Identification

DC-HIE	HIPAA Privacy	Policy No.: **DC-HP-4**
Title: **Access of Individuals to PHI**	Version: **1**	Effective Date:

Purpose Statement: DC-HIE does not create nor maintain designated record sets on behalf of its Direct Secure Messaging Users. Therefore, DC-HIE cannot, on behalf of its Direct Secure Messaging Users, grant an individual access to PHI. This policy sets forth how DC-HIE shall comply with requests from an individual to inspect or obtain a copy of his or her protected health information.

HIPAA Privacy Rule Language: "Except as otherwise provided in paragraph [45 C.F.R. § 164.524](a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set."

Policy/Procedure:

1. An individual who inquires about requesting his or her PHI will be provided a letter which indicates that DC-HIE does not maintain the individual's designated record set and cannot comply with the request.

2. The individual will be instructed to contact his or her health care provider(s) to request access to PHI contained within his or her medical record.

The following is template language for a response letter:

On [*insert date*], DC-HIE received a request from you for [*a copy of or the right to access*] protected health information about you that may have been exchanged through DC-HIE. DC-HIE is not a custodian of records nor does it maintain a designated record set.

As a result, DC-HIE cannot provide you with the requested information. If would like to access or obtain a copy of your health information, you should contact your health care providers directly and they will gladly assist you.

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations
Regulatory Reference:

- 45 C.F.R. §164.524, Access of Individuals to PHI [Standard; Required]

DC-HIE	HIPAA Privacy	Policy No.: **DC-HP-5**
Title: **Amendment of PHI**	Version: **1**	Effective Date:

Purpose Statement: DC-HIE does not create nor maintain designated record sets on behalf of its DC-HIE Direct Users. Therefore, DC-HIE cannot, on behalf of its DC-HIE Direct Users, amend any protected health information. This policy sets forth how DC-HIE shall comply with requests from an individual to amend his or her protected health information.

HIPAA Privacy Rule Language: "An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set."

Policy/Procedure:

1. In the event that DC-HIE receives a request from an individual to amend PHI exchanged through the Network, the individual will be provided with a letter which indicates that DC-HIE does not maintain medical records and cannot comply with the request to amend his or her medical record.

2. The individual will be instructed to contact his or her health care provider to request an amendment of his or her PHI.

The following is template language for a response letter:

On [*insert date*], DC-HIE received a request from you to amend protected health information about you that may have been exchanged through DC-HIE. DC-HIE is not a custodian of records nor does it maintain a designated record set. As a result, DC-HIE cannot make the requested amendment. If would like to amend your protected health information, you should contact your health care providers directly and they will gladly assist you.

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations
Regulatory Reference:

- 45 C.F.R. §164.526, Amendment of Protected Health Information [Standard; Required]

DC-HIE	HIPAA Privacy	Policy No.: **DC-HP-6**
Title: **Accounting of Disclosures of PHI**	Version: **1**	Effective Date:

Purpose Statement: Individuals have a right to receive an accounting of disclosures of their protected health information made for the six years prior to their request. Pursuant to the Direct Secure Messaging Subscription Agreement, Direct Secure Messaging Users are responsible for maintaining all information related to disclosures that the Direct Secure Messaging User makes through Direct Secure Messaging that will be needed to respond to a request for an accounting of disclosures. DC-HIE will only be responsible for providing information in response to a request for an accounting of disclosures for disclosures that DC-HIE makes, as permitted by the Direct Secure Messaging Subscription Agreement.

HIPAA Privacy Rule Language: "An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested."

HITEACH Act Language: "In applying section 164.528 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information –

"(A) the exception under paragraph (a)(1)(i) of such section *treatment, payment, and health care operations] shall not apply to disclosures through an electronic health record made by such entity of such information; and

"(B) an individual shall have a right to receive an accounting of disclosures described in such paragraph of such information made by such covered entity during only the three years prior to the date on which the accounting is requested."

Requests for Accounting Made to Covered Entities

1. Within 21 days of receiving the accounting request from the Direct Secure Messaging User, DC HIE will provide the User with an accounting of all disclosures of that individual's PHI made by DC HIE during the six years (or shorter time period as requested by the individual) prior to the request.

2. If DC-HIE is unable to act on the accounting request within 21 days, DC-HIE may extend the deadline by no more than 30 additional days if, prior to the expiration of the initial 30 days, DC-HIE provides the DC-HIE Direct User with an explanation for the delay and an estimated date of completion. The Direct Secure Messaging User will then notify the individual of the reason for the delay. DC-HIE may exercise only one such extension.

3. The content of the accounting provided to the DC-HIE Direct User will consist of the same information as provided below for accounting requests made directly to DC-HIE. In addition, the procedures regarding Exceptions and Suspensions provided below apply regardless of

whether the DC-HIE Direct User submits the accounting request to DC-HIE or the individual submits the request directly to DC-HIE.

Request for Accounting Made by Individuals Directly to DC-HIE

1. An individual may request an accounting of all disclosures pertaining to the individual's PHI made by DC-HIE to a third party during the six years prior to the request with the exception of those disclosures identified below. The individual may request an accounting for a period less than six years.

2. DC-HIE must act on an individual's request for an accounting within sixty (60) days of receiving the request. If DC-HIE is unable to act on the request within 60 days, DC-HIE may extend the deadline by no more than thirty (30) additional days if, prior to the expiration of the initial 60 days, DC-HIE provides the individual with an explanation for the delay and an estimated date of completion. DC-HIE may exercise only one such extension.

3. Accounting requests will be delivered to the Privacy Officer who may designate another DC-HIE Workforce Member to process the request.

4. DC-HIE must provide the first accounting that an individual requests in a twelve (12) month period at no cost. DC-HIE, through future legislative authority, may charge a reasonable cost-based fee for subsequent accountings requested in the same 12-month period. DC-HIE must notify the individual of the cost requirement and allow the individual to withdraw or narrow the scope of his or her request to limit the cost of a subsequent accounting.

Required Information

1. The accounting must include all disclosures pertaining to the individual's PHI made by DC-HIE to a third party during the six years (or such shorter time period as requested by the individual) prior to the request, unless an exception applies.

2. For each disclosure, the following information must be included:

    a. The date of the disclosure.
    b. The name and address, if known, of the recipient of the PHI.
    c. A brief description of the PHI disclosed.
    d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure. Alternatively, DC-HIE may include a written request from the third party for the information disclosed.

Exceptions

1. Pursuant to in 45 C.F.R. § 164.528, the following disclosures of PHI are not required to be included in a requested accounting:

    a. Disclosures made to carry out treatment, payment, and health care operations as provided in 45 C.F.R. § 164.506;

b. Disclosures made to individuals of PHI about them as provided in 45 C.F.R. § 164.502;
c. Disclosures made incident to a use or disclosure otherwise permitted or required by HIPAA as provided in 45 C.F.R. § 164.502;
d. Disclosures made pursuant to an authorization as provided in 45 C.F.R. § 164.508;
e. Disclosures made for the Covered Entity's facility directory or to persons involved in the individual's care as provided in 45 C.F.R. § 164.510;
f. Disclosures made for national security or intelligence purposes as provided in 45 C.F.R. § 164.512(k)(2);
g. Disclosures made to correctional institutions or law enforcement officials as provided in 45 C.F.R. § 164.512(k)(5);
h. Disclosures made as part of a limited data set in accordance with 45 C.F.R. § 164.514(e); and
i. Disclosures that occurred prior to the compliance date for the covered entity.

Suspensions of an Individual's Right to an Accounting

1. DC-HIE must suspend an individual's right to receive an accounting of disclosures made to a health oversight or law enforcement agency if that agency requests that DC-HIE do so.

    a. The agency requesting suspension must submit a written statement that DC-HIE's provision of a requested accounting to an individual would be reasonably likely to impede the activities of the agency. The statement must also state the duration of the requested suspension.

    b. If the agency requesting suspension does not submit a written statement, but rather requests the suspension orally, DC-HIE must:

        i. Document the identity of the agent and agency requesting the suspension and the reason for it. DC-HIE will include the badge number or a copy of the agent's credentials in the documented record.
        ii. Effect a temporary suspension of the individual's right to an accounting of disclosures made to that agency.
        iii. Limit the duration of the suspension to 30 days or less from the time of the oral request, unless a written request is provided during that time.

Document and Retention

DC-HIE must retain the following documents for at least ten years:

a. The information required to be included in a requested accounting.
b. Copies of written accountings provided to individuals.
c. Designation of persons responsible for processing requests for accountings made by individuals.

Responsibility: Privacy Officer; DC-HIE Direct User
Regulatory Category: Privacy Regulations
Regulatory Reference:

- 45 C.F.R. §164.528, Accounting of Disclosures of Protected Health Information [Standard; Required]

DC-HIE	HIPAA Privacy	Policy No.: **DC-HP-7**
Title: **Assigned Privacy Responsibility**	Version: **1**	Effective Date:

Purpose Statement: DC-HIE will designate a Privacy Officer who will be responsible for the implementation and day-to-day administration and oversight of DC-HIE's compliance with the HIPAA Privacy Regulations. The Privacy Officer will also develop Workforce Member and User training programs regarding the privacy of PHI, update and implement these Privacy Policies and Procedures, and serve as the designated decision-maker for issues and questions involving interpretation of the HIPAA Privacy Regulations.

HIPAA Privacy Rule Language: "A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity."

Policy/Procedure:

1. The Privacy Officer is responsible for the following tasks:
   a. Inventorying the uses and disclosures of all PHI;
   b. Ensuring that legal issues in drafting compliance documents are addressed or engage competent legal counsel to draft such documents;
   c. Determining whether a Workforce Member's acts or omissions resulted in a violation of the HIPAA Privacy and Security Policies and Procedures in accordance with DC-H-3;
   d. Developing, updating, and revising these Privacy Policies and Procedures as necessary to comply with the HIPAA Privacy Regulations;
   e. Developing a privacy training program for Workforce Members and Users;
   f. Establishing procedures to monitor internal privacy compliance;
   g. Keeping up to date on the latest privacy developments and federal and state laws and regulations;
   h. Coordinating with the Security Officer in evaluating and monitoring operations and systems development for Privacy and Security requirements;
   i. Serving as DC-HIE's liaison to regulatory bodies for matters relating to
   j. Privacy
   k. Coordinating any audits of the Secretary of HHS or any other governmental or accrediting organization regarding DC-HIE's compliance with state or federal privacy laws or regulations; and
   l. Other tasks necessary to ensure the privacy of PHI.

2. DC-HIE's Privacy Officer's name and contact information is:

   Name: LaRah Payne, Sc.D.
   Email: larah.payne@dc.gov
   Phone: 202-442-9116

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations

HIPAA Security Policies and Procedures

DC-HIE	HIPAA Security	Policy No.: **DC-HS-1**
Title: **Security Risk Management, Evaluation & Updates**	Version: **1**	Effective Date:

Purpose Statement: DC HIE, under the HIPAA Security Regulations, is required to periodically evaluate its security safeguards and implement a security management process. Implementation of this security management process will assist DC HIE in ensuring the confidentiality, integrity, and availability of ePHI and the Network. DC HIE will create and maintain appropriate and reasonable policies, procedures, and controls to prevent, detect, contain, and correct security violations.

HIPAA Security Rule Language

"Implement policies and procedures to prevent, detect, contain, and correct security violations."

"Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic PHI that establishes the extent to which an entity's security and procedures meet the requirements of this subpart."

"Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information."

Policy/Procedure:

Evaluation and Risk Analysis

1. At least once per year, DC HIE will convene a workgroup of at least four (4) individuals to conduct an accurate and thorough evaluation of DC HIE's security safeguards and an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI accessed through the Network.

2. The workgroup will consist of at least the Security Officer, individuals representing DC HIE's information technology department or DC HIE's technology vendor, individuals familiar with the Network and the District-wide Privacy and Security Official.

3. The workgroup will conduct the following activities:

    a. Review of DC HIE's Security Policies and Procedures to evaluate their appropriateness and effectiveness in protecting against any reasonably anticipated threats or hazards to the privacy and security of ePHI exchanged through the Network.
    b. A gap analysis to compare DC HIE's Security Policies and Procedures against actual practices.
    c. An identification of threats and risks to the Network ("Risk Analysis"), including the following:

i. Potential security risks to the Network, including those Security Incidents specifically identified in the Breach and Security Incident and Response Procedures Policy (H-4);
ii. The probability of the occurrence of risks which may affect the Network;
iii. The magnitude of the identified risk to the Network;
iv. The criticality of each Network function to DC HIE's operations during or after an emergency or disaster pursuant to the Applications and Data Criticality Analysis Policy (HS-15);
v. The frequency of reviews and audits of the Network pursuant to the Information System Activity Review Policy (HS-2);
vi. The training, and the frequency of such training, to be offered to DC HIE Direct Users and Workforce Members regarding the security of ePHI;
vii. The need to do penetration testing of the security of the Network; and
viii. The need to engage third parties to evaluate the risks and vulnerabilities to the Network.

d. An assessment of whether established security controls reasonably and appropriately protect against the risks identified for the Network.

4. The evaluation and risk analysis process will be documented and the findings will be reported to the DC HIE Policy Board.

Risk Management

1. In an effort to reduce risks and vulnerabilities to ePHI exchanged through the Network, DC HIE will update its Security Policies and Procedures if the results of the evaluation show that such updates are needed and will create a Risk Management Plan to address risks identified in the annual Risk Analysis.

2. In addition to updating the Security Policies and Procedures and Risk Management Plan after each Risk Analysis, DC HIE will also update the Policies and Procedures and Plan as needed:

   a. After any Security Incident to minimize the likelihood of a similar Security Incident occurring in the future;
   b. After a new use of the Network is authorized;
   c. In response to the addition of any new Network functionality
   d. In response to environmental or operational changes (e.g. significant new threats or risks to the security of ePHI; changes to DC HIE's organizational or technical infrastructure; changes to information security requirements or responsibilities; or availability of new security technologies or recommendations).

3. In developing each Risk Management Plan, DC HIE will consider the following:

   a. The security measures that are already in place to address the risk;
   b. Additional security measures that can reasonably and appropriately be put in place to address the risk;

c. Communication of the security measures and Risk Management Plan to Workforce Members, DC HIE Participants, DC HIE Direct Secure Messaging Users, and Vendors; and
d. The need to engage other resources to assist in the implementation of the Risk Management Plan.

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(1)(i), Security Management Process [Standard; Required]
- 45 C.F.R. §164.308(a)(1)(ii)(A), Risk Analysis [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(1)(ii)(B), Risk Management [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(8), Evaluation [Standard; Required]
- 45 C.F.R. §164.316(b)(2)(iii), Updates [Implementation Specification; Required]

DC HIE	HIPAA Security	Policy No.: **HS-2**
Title: **Information System Activity Review**	Version: **1**	Effective Date:

Purpose Statement: DC HIE will implement hardware, software, and/or procedural mechanisms that record and examine the activity of Users in the Network to enable DC HIE to detect potentially problematic activity in the Network. These audit controls will allow DC HIE to:

1. Identify questionable access to and exchange activities in the Network;
2. Investigate Breaches and Security Incidents;
3. Respond to potential weaknesses in the Network's architecture; and
4. Assess the effectiveness of DC HIE Security Policies and Procedures.

HIPAA Security Rule Language: "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

Frequency of the Network Activity Review

1. DC HIE will conduct monthly audits, and create audit reports, which provide a summary of all uses of the Network.

2. DC HIE will identify and document the names of Workforce Members who will review monthly audit reports.

3. DC HIE will retain monthly audit reports for ten years after the date they are created.

Audit Report Content

1. DC HIE will identify the data to be captured in the monthly audit reports. The data to be captured in monthly audit reports related to Direct Secure Messaging is set forth in DC HIE Direct Messaging Auditing and Monitoring Policy (DM-7).

2. Within two weeks of receiving the monthly audit report, a designated DC HIE Workforce Member will review the report.

3. If DC HIE uncovers any indications of improper use of Direct Secure Messaging, it will follow the Breach and Security Incident Response Procedures Policy (H-4).

4. As patterns are identified and anomalous behavior becomes more apparent in the monthly audit reports, DC HIE may establish thresholds for each type of activity captured in the audit report. The thresholds will signify the level at which certain behavior warrants further inspection and may signal a Breach or Security Incident or failure to comply with DC HIE's policies and procedures. As thresholds are established or revised, this Policy or other related Policies will be revised accordingly.

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164308(a)(1)(ii)(D), Information System Activity Review [Implementation Specification; Required]
- 45 C.F.R. §164.312(b), Audit Controls [Standard; Required]

DC HIE	HIPAA Security	Policy No.: **HS-3**
Title: **Assigned Security Responsibility**	Version: **1**	Effective Date:

Purpose Statement: Under the HIPAA Security Regulations and the HITECH Act, DC HIE is required to designate a Security Official who is responsible for the development and implementation of its Security Policies and Procedures. This policy reflects DC HIE's commitment to comply with such regulations. In addition, the appointment of the Security Officer will provide organizational focus to, and highlight the importance of, DC HIE's efforts to protect the confidentiality, privacy and security of the ePHI.

HIPAA Security Rule Language: "Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."

Policy/Procedure:

1. The Security Officer will perform the following duties, including taking all reasonable and appropriate measures to:

    a. Ensure and confirm that DC HIE is compliant with applicable federal, state, and local laws pertaining to the security of ePHI;
    b. Guide the development, documentation, and dissemination of appropriate security policies and procedures that govern the use of the Network;
    c. Ensure that any updates to the Network have options that support required and/or addressable implementations of the HIPAA Security Regulations and DC HIE's internal security requirements;
    d. Approve and oversee the administration, implementation, and selection of DC HIE's security controls for the Network;
    e. Implement and oversee the security training of Users, and ensure that Users receive such training on a periodic basis as deemed necessary pursuant to DC HIE's Security Risk Management, Evaluation and Updates Policy (HS-1);
    f. Facilitate the yearly Risk Analysis and creation of a Risk Management Plan under DC HIE's Security Risk Management, Evaluation and Updates Policy (HS-1);
    g. Ensure that the Network activity is monitored and audited to identify Security Incidents and malicious activity as set forth in the Information System Activity Review Policy (H-2);
    h. Ensure that the threats and risks to the confidentiality, integrity, and availability of ePHI are monitored and evaluated; and
    i. Oversee the development and implementation of an effective Security Incident response policy and related procedures as set forth in the Breach and Security Incident Management Response Procedures Policy (H-4).

2. DC HIE's Security Officer is

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(2), Assigned Security Responsibility [Standard; Required]

DC HIE	HIPAA Security	Policy No.: **HS-4**
Title: **Workforce Member Security**	Version: **1**	Effective Date:

Purpose Statement: To protect the confidentiality, integrity, and availability of ePHI, DC HIE will implement reasonable and appropriate safeguards to prevent unauthorized access to ePHI while ensuring that properly authorized Workforce Members can exchange ePHI through the Network.

HIPAA Security Rule Language: "Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic PHI, as provided under paragraph (a)(4) [information access management] of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic PHI."

Policy/Procedure:

Workforce Clearance

1. Security privileges will be identified and defined for each Workforce Member who is granted access to the Network.
2. Based on the level of privileges to be granted to candidates for employment, Human Resources personnel will perform appropriate and reasonable verifications checks on the candidate.
3. Verification checks may include, but are not limited to:
    a. Character references;
    b. Confirmation of claimed academic and professional qualifications;
    c. Credit checks; or
    d. Criminal background checks.

Supervision of Workforce Members

1. Workforce Members who have the ability to access the Network, or those who work in areas where ePHI might be accessed, will be properly supervised. DC HIE will ensure that Workforce Members only access the ePHI that they are authorized to access pursuant to their job responsibilities.

2. DC HIE will ensure that appropriate sanctions are taken against Workforce Members who improperly access ePHI, or who inappropriately grant access to ePHI to others. Sanctions will be instituted in accordance with the DC HIE Workforce Member Discipline Policy (H-2).

Access to PHI

DC HIE will authorize, establish and modify, as appropriate, each Workforce Member's access to ePHI in accordance with the Information Access Management Policy (HS-5).

Termination of Access to PHI

DC HIE will terminate a Workforce Member's access to ePHI, either in the event of a Workforce Member's resignation or a Workforce Member's termination by DC HIE, in accordance with the Suspension and Termination Procedures Policy (HS-6).

Responsibility: Security Officer; Human Resources; Workforce Members
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(3)(i), Workforce Security [Standard; Required]
- 45 C.F.R. §164.308(a)(3)(ii)(A), Authorization and/or Supervision [Implementation Specification; Addressable]
- 45 C.F.R. §164.308(a)(3)(ii)(B), Workforce Clearance Procedure [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-5**
Title: **Information Access Management**	Version: **1**	Effective Date:

Purpose Statement: DC HIE strives to protect the confidentiality, integrity, and availability of ePHI by taking reasonable steps to appropriately manage access to the Network. Safeguarding access to the Network by taking reasonable and appropriate steps integral to DC HIE's compliance efforts under the HIPAA Security Regulations.

HIPAA Security Rule Language: "Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of subpart E of this part." Subpart E refers to the HIPAA Privacy rules, located at 45 C.F.R. §164.500 et seq.

Policy/Procedure:

Establishing Access to ePHI for DC HIE Workforce Members

1. DC HIE will ensure that only authorized Workforce Members will have access to Direct Secure Messaging.

2. DC HIE will document the various levels of access to Direct Secure Messaging that each Workforce Member will have based upon the job function requirements of each position.

3. Workforce Members will not be granted access to, and must not attempt to access, the Network until the Workforce Member has been properly cleared in accordance with the Workforce Member Security Policy (HS-4).

4. Once a Workforce Member has been granted access to Direct Secure Messaging, the Security Officer or his/her designee will give notice of such access to the DC HIE Technical Administrator, or her designee.

5. The Technical Administrator, or designee, will then assign the Workforce Member a unique username and temporary password to activate the Workforce Member's level of access to the Network.

6. Once the Workforce Member receives his or her temporary password, the Workforce Member will change his or her password in accordance with the Password Management Policy (HS-11).

Review and Modification of Workforce Members' Access to EPHI

- 45 C.F.R. §164.308(a)(4)(ii)(C), Access Establishment and Modification [Implementation Specification; Addressable] "Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."

Access to DC Direct Secure Messaging for DC HIE Direct Secure Messaging Users

1. Individuals will be provided with access to Direct Secure Messaging in accordance with Direct Secure Messaging Subscription Agreement.

Responsibility: Security Officer; Technical Administrator (or designee); Direct Secure Messaging Users

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(4)(i), Information Access Management [Standard; Required]
- 45 C.F.R. §164.308(a)(4)(ii)(B), Access Authorization [Implementation Specification; Addressable]
- 45 C.F.R. §164.308(a)(4)(ii)(C), Access Establishment and Modification [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-6**
Title: **Suspension and Termination Procedures**	Version: **1**	Effective Date:

Purpose Statement: When a Workforce Member's employment ends or he/she provides notice of their intention to cease participation in DC HIE, the Workforce Member's access to ePHI is no longer appropriate and DC HIE will terminate the Workforce Member's access to ePHI.

HIPAA Security Rule Language: "Implement procedures for terminating access to electronic PHI when the employment of a workforce member ends or as required by determinations as specified in paragraph (a)(3)(ii)(B) *workforce clearance+ of this section."

Policy/Procedure:

1. When a Workforce Member provides notice of his or her intention to end employment with DC HIE or their job duties no longer require transmission of ePHI, the Human Resources Manager and the Workforce Member's supervisor will give reasonable notice to the DC HIE's Technical Administrator (or his/her designee), so that the departing Workforce Member's access to the Network can be terminated when he or she ends employment or changes job duties.

2. DC HIE will document the following information regarding the departing Workforce Member:

    a. Date and time of receiving the Workforce Member's notice to end employment at DC HIE or change in job duties;
    b. Date of the Workforce Member's planned departure or job change;
    c. Description of the Workforce Member's access to the Network that must be terminated; and
    d. Date, time, and description of the actions taken to terminate the departing Workforce Member's access to the Network.

<u>DC HIE Workforce Member Termination Procedures/Change in Job Duties</u>

1. When a Workforce Member is terminated or their job duties change and they are no longer required to transmit ePHI, DC HIE will immediately remove or disable the Workforce Member's access privileges to the Network before the Workforce Member is notified of his or her termination, when feasible.

2. Such Network access privileges include, but are not limited to:

    a. Workstations and server access;
    b. Access to data contained within or available through the Network;
    c. Access to any network that DC HIE uses;
    d. Email accounts; and/or
    e. Inclusion on group email lists.

General Resignation and Termination Procedures

1. DC HIE will terminate, as appropriate, a departing or terminated Workforce Member's physical access to areas where ePHI is located within DC HIE's facilities.

2. DC HIE will collect, and document the collection of, equipment and property that contains ePHI, which were used by the terminated or departing Workforce Member.

    a. Such documentation will include:

        i. The Workforce Member's name;
        ii. The date and time the equipment and property were returned; and
        iii. The identification of the returned property and equipment.

    b. DC HIE will securely maintain such documentation.

3. Equipment that may contain, allow, or enable the Workforce Member to access ePHI, and which must be returned upon the workforce member's termination or departure, include, but is not limited to:

    a. Portable computers;
    b. Personal Digital Assistants (PDAs);
    c. Name tags or name identification badges;
    d. Security tokens;
    e. Facility access cards; and/or
    f. Building, desk, or office keys.

Suspension and Termination Procedures for DC HIE Direct Secure Messaging Users

1. DC HIE Direct Users may be suspended or terminated in accordance with the DC HIE Direct Messaging End User License Agreement and the DC HIE Direct User Suspension and Termination Policy (DSM-9).

Responsibility: Security Officer; Technical Administrator (or designee); Human Resources Manager.
Regulatory Category: Administrative Safeguards. **Regulatory Reference:**

- 45 C.F.R. §164.308(a)(3)(ii)(C), Termination Procedures [Implementation Specification; Addressable.

DC HIE	HIPAA Security	Policy No.: **HS-7**
Title: **Security Awareness and Training**	Version: **1**	Effective Date:

Purpose Statement: DC HIE has the responsibility under the HIPAA Security Regulations for providing and documenting security awareness and training for DC HIE Workforce Members in order that those persons can properly carry out their functions while appropriately safeguarding ePHI. This policy reflects DC HIE's commitment to comply with such Regulations.

HIPAA Security Rule Language: "Implement a security awareness and training program for members of its workforce (including management)."

Policy/Procedure:

Training for Workforce Members

1. DC HIE will provide training and supporting reference materials to its Workforce Members, as appropriate, to carry out their functions with respect to the security of ePHI. As part of its risk analysis, pursuant to its Security Risk Management, Evaluation and Updates Policy (HS-1), DC HIE will determine how often such training will be required for its Workforce members and the method of such training.

2. DC HIE will maintain sufficient records that document and confirm a Workforce Member's completion of security awareness training, such as a document signed by each Workforce member and the Security Officer acknowledging receipt of such training.

3. Security awareness training should include information to make Workforce Members aware of and familiar with DC HIE's HIPAA Security Policies and Procedures.

4. DC HIE will provide security information reminders and updates to its Workforce Members, in accordance with the Security Reminders Policy (HS-8).

5. DC HIE will make its Security Policies and Procedures available for reference and review by its Workforce Members who have access to ePHI.

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(5)(i), Security Awareness and Training [Standard; Required]

DC HIE	HIPAA Security	Policy No.: **HS-8**
Title: Security Reminders	Version: **1**	Effective Date:

Purpose Statement: DC HIE, through its technology vendor, will periodically provide information and reminders to Users on a variety of topics designed to increase the security of the services offered by DC HIE.

HIPAA Security Rule Language: "Implement periodic security updates."

Policy/Procedure:

1. DC HIE's Security Officer will periodically, as needed, issue security information and awareness reminders to Users. Such security reminders could include:

    a. Information regarding general security risks and how to follow DC HIE's HIPAA Security Policies and Procedures;

    b. Information regarding how to use DC HIE services in a manner that reduces security risks; and/or

    c. Legal and business responsibilities of DC HIE for protecting the ePHI exchanged through the Network.

2. DC HIE will issue security reminders immediately upon, or within a reasonable time following the occurrence of any of the following events:

    a. Making substantial revisions to DC HIE's Security Policies and Procedures;
    b. Implementing new, or significantly changing existing, security controls;
    c. Making substantial changes to DC HIE's legal or business responsibilities;
    d. Identifying substantial threats or new risks against the services offered by DC HIE; or
    e. Introducing new functions or making significant changes to existing service (ex: Direct) functionalities.

3. Means of providing security information and awareness reminders and updates may include, but are not limited to:

    a. Email reminders;
    b. Posters;
    c. Letters;
    d. Meetings;
    e. Information system sign-on messages;
    f. Newsletter articles; and/or

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(5)(ii)(B), Security Reminders [Implementation Specification; Addressable

DC HIE	HIPAA Security	Policy No.: **HS-9**
Title: **Malicious Software**	Version: **1**	Effective Date:

Purpose Statement: DC HIE will implement and periodically review its processes and safeguards for guarding against, detecting, and reporting malicious software that pose risks to privacy and security ePHI, or the integrity or operation of the Network. Though DC HIE's technology vendor, DC HIE is taking appropriate precautions to secure the services it offers and DC HIE encourages users to take similar precautions.

HIPAA Security Rule Language: "Implement procedures for guarding against, detecting, and reporting malicious software."

Policy/Procedure:

1. DC HIE will take all necessary and reasonable measures to protect the services offered through its network, and all media that DC HIE uses upon which ePHI is contained, from malicious software, including:

    a. Ensuring that anti-virus software is installed on all media devices and hardware, either owned by or used by DC HIE containing ePHI or which have connection to the Network;
    b. Mitigating the harm of malicious software attacks by recovering ePHI and other data contained on all media devices and hardware that has been attacked by malicious software;
    c. Requiring all Workforce Members to scan email attachments and downloads before they are opened.
    d. DC HIE will conduct a weekly virus scan of its network server and Workstations.
    e. DC HIE Workforce Members must not bypass or disable anti-virus software installed on Workstations unless they are properly authorized to do so.
    f. DC HIE will provide periodic training and awareness to its Workforce Members about guarding against, detecting, and reporting malicious software, including:

        i. How to discover malicious software;
        ii. How to report malicious software;
        iii. How to scan for malicious software that may be contained in email attachments; and/or
        iv. How to use anti-virus software.

    g. Workforce Members must pass electronic files through virus protection programs prior to use, pursuant to the Malicious Software Policy (HS-9).
    h. Workforce Members must immediately report suspected or confirmed malicious software to the Security Officer.

Responsibility: Security Officer; Technical Administrator; Workforce Members
Regulatory Category: Administrative Safeguards.
Regulatory Reference:

- 45 C.F.R. §164.308(a)(5)(ii)(B), Protection from Malicious Software [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-10**
Title: **Log-in Monitoring and Automatic Log-Off**	Version: **1**	Effective Date:

Purpose Statement: DC HIE will control access to its Workstations through the use of log-in procedures and automatic log-off functionality. DC HIE will use similar log-in monitoring and automatic log-off functionality for those components of the Network that are accessed through a web-based user interface.

HIPAA Security Rule Language: "Implement procedures for monitoring log-in attempts and reporting discrepancies."

Policy/Procedure:

1. After a five (5) consecutive, unsuccessful attempts to log-on to a DC HIE Workstation, the Workforce Member's password will be disabled. All such events will be logged as part of the monthly activity report pursuant to the Information System Activity Review Policy (HS-2).

2. If a Workforce Member's password is disabled due to unsuccessful log-on attempts, the Workforce Member should contact the DC HIE's Technical Administrator.

3. The Technical Administrator will verify the Workforce Member's identity and determine whether the Workforce Member's access was disabled because of five consecutive, unsuccessful attempts to log-on or for another reason.

4. After verifying the Workforce Member's identity and that such Member's access was disabled because of unsuccessful log-on attempts, the Technical Administrator will issue the Workforce Member a new, temporary password. The Workforce Member will then use the temporary password to log-on to the Workstation and re-set his or her own individual password in accordance with the Password Management Policy (HS-11).

Automatic Log Off

1. A Workforce Member will be automatically logged-off of a DC HIE Workstation 5-10 minutes of inactivity.

2. To activate a new session, a Workforce Member will have to log-on to the Workstation using his or her user name and password.

Responsibility: Security Officer; Workforce Members

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(5)(ii)(C), Log-In Monitoring [Implementation Specification; Addressable

DC HIE	HIPAA Security	Policy No.: **HS-11**
Title: **Password Management**	Version: **1**	Effective Date:

Purpose Statement: Where DC HIE requires the use of a password to access or exchange information through Direct Secure Messaging, Users will be required to take appropriate measures to select and secure such passwords.

HIPAA Security Rule Language: "Implement procedures for creating, changing, and safeguarding passwords."

Policy/Procedure:

1. Passwords are case sensitive. The minimum length is eight (8) alpha-numeric characters.

2. Users may not, under any circumstances, share their passwords or second method of authentication, if applicable, with anyone. If a User does share his/her password with another person, he/she must notify DC HIE immediately so that the password can be re-set.

3. Users should refrain from recording or using passwords where they may be obtained or observed by others.

Responsibility: Security Officer; Technical Administrator; Users

Regulatory Category: Administrative Safeguards

Regulatory Reference:

- 45 C.F.R. §164.308(a)(5)(ii)(D), Password Management [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-12**
Title: **Contingency Plan**	Version: **1**	Effective Date:

Purpose Statement: The DC HIE Contingency Plan establishes procedures to recover the Network following a disruption. DC HIE has established the following objectives for this Contingency Plan:

1. Maximize the effectiveness of DC HIE's contingency operations through an established plan that consists of the following phases:

    a. Notification and Activation Phase to detect and assess damage and to activate the plan;
    b. Recovery phase to restore temporary Network operations and to recover damage done to the Network; and
    c. Reconstitution phase to restore the Network's functional capabilities to normal operations.

2. Identify the activities, resources, and procedures needed to carry out Network requirements during prolonged interruptions to normal operations.

3. Assign responsibilities to designated Workforce Members who will participate in the contingency planning strategies, and provide guidance for recovering the Network during prolonged periods of interruption to normal operations.

4. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

Policy/Procedure:

Contingency Plan Triggers

1. This Contingency Plan will be activated upon the occurrence of one or more of the following triggers:

    a. DC HIE Direct Secure Messaging will be completely unavailable for more than 5 business hours due to an unplanned outage; and
    b. Other triggers, as appropriate.

Mitigation Measures

1. DC HIE's technology vendor will use at least a Tier 3 data center to house its servers. Because of the robust protections offered by a Tier 3 data center, the likelihood of damage to the Network is very low. If there is damage to the Network, DC HIE will be able to recover exact copies of ePHI, to the extent that it is maintained within the Network, pursuant to the Data Back-Up and Disaster Recovery Plan Policy (HS-13). Tier 3 data centers have dual powered equipment and multiple uplinks and there are multiple identity checkpoints to prevent unauthorized access to the Network.

2. DC HIE will take various steps to mitigate any damage to the Network caused by an emergency or disaster and to continue operations after such an event. DC HIE may perform these measures itself or may require that other third parties to whom DC HIE has outsourced certain activities, perform these measures.

    a. Ensure that preventative controls, such as generators, waterproof tarps, sprinkler systems, and fire extinguishers will be fully operational at the time of an emergency or disaster.
    b. Ensure that its electronic media and hardware containing ePHI, including component supporting such devices, are connected to an uninterruptible, redundant power supply.
    c. Ensure that DC HIE will maintain service agreements with its hardware, software, and communications providers to support Network recovery.

Notification Procedures

1. 1. DC HIE personnel or a third party representative who discover that DC HIE's facilities, the third party facilities or the Network has been affected by an emergency or disaster, must notify the DC HIE official named below:

    Michael C. Tietjen
    Management Analyst
    District of Columbia Health Information Exchange
    609 H Street, NE, 1st Floor
    Washington, DC 20002
    Office 202.442.9055
    E-Mail: michael.tietjen2@dc.gov

2. When notified the DC HIE official will notify all others within DC HIE or a third party vendor who will be part of the contingency and recovery activities.

Damage Assessment Procedures

1. The Risk Officer or other DC HIE official, upon his/her initial review of the situation will assess the following:

    a. The cause of the disruption;
    b. The potential for additional disruption or damage;
    c. The affected physical area and the status of physical infrastructure;
    d. The status of the Network server's functionality and inventory, including items that may need to be replaced; and
    e. The estimated time to repair services to normal operations.

Activation of Contingency Plan

Based on the damage assessment from the Risk Management Officer, or other DC HIE Official, DC HIE senior management will determine what contingency operations and recovery activities are necessary to repair and sustain operations of the Network.

Recovery Operations

DC HIE will restore the Network and recover any ePHI that was maintained within the Network in accordance with the following Policies and Procedures:

a. Data Backup Plan and Disaster Recovery Plan Policy (HS-13); and
b. Emergency Mode Operations Plan Policy (HS-14).

Other Contingency Plan Procedures

1. DC HIE will perform a criticality analysis of each Network function to determine its importance to DC HIE's operations during or after a disaster in accordance with the Security Risk Management, Evaluation and Updates Policy (HS-1) and as outlined in the Applications and Data Criticality Analysis Policy (HS-15).

2. DC HIE will provide periodic training materials regarding its disaster and emergency response procedures to Workforce Members, as appropriate.

3. DC HIE will periodically test its Contingency Plan to ensure that critical business processes can continue in a satisfactory manner. If necessary, DC HIE may revise the Contingency Plan, and the occurrence of any of the following events may result in a revision of the Contingency Plan:

    a. Disaster recovery role and responsibility changes, including changes to contact information;
    b. Changes to DC HIE's physical or technical infrastructure or operating systems;
    c. Changes in threats to the Network; or
    d. Results of testing that indicate that the plan needs to be modified to ensure that it is sufficient, accurate, and up-to-date.

Responsibility: Risk Management Officer, other DC HIE Officials as deemed necessary
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(7)(i), Contingency Plan [Standard; Required]

DC HIE	HIPAA Security	Policy No.: **HS-13**
Title: **Data Backup Plan and Disaster Recovery Plan**	Version: **1**	Effective Date:

Purpose Statement: To the extent that DC HIE's technology vendor maintains ePHI within its systems/servers, the vendor will implement plans to create, maintain, and recover exact copies of such ePHI. The ability to recover exact copies of this ePHI will enable DC HIE to restore or recover any loss of ePHI and to restore the Direct Secure Messaging service after damage caused by an emergency or disaster, such as fire, vandalism, terrorism, system failure, or natural disaster.

HIPAA Security Rule Language: "Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI." "Establish (and implement as needed) procedures to restore any loss of data."

Policy/Procedure:

1. DC HIE's technology vendor will backup data, including, but not limited to Direct, transmitted over its Network to the extent that Subscribers/Users can access their messaging data for one year after sending/delivery. DC HIE's technology vendor will archive such data for ten (10) years.

2. DC HIE will ensure that its technology vendor will implement and maintain policies and procedures regarding data backup and disaster recovery. Also, DC HIE will ensure that the vendor's testing and revision plan will be incorporated into its contingency plan.

Responsibility: Security Officer; Technical Vendor
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(7)(ii)(A), Data Backup Plan [Implementation Specification; Required]
- 45 C.F.R. §164.310(d)(2)(iv), Data backup and storage [Implementation Specification; Addressable]
- 45 C.F.R. §164.308(a)(7)(ii)(B), Disaster Recovery Plan [Implementation Specification; Required]
- 45 C.F.R.§164.308(a)(7)(ii)(D), Testing and Revision Procedures [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-14**
Title: **Emergency Mode Operation Plan**	Version: **1**	Effective Date:

Purpose Statement: DC HIE's technology vendor will develop and implement an Emergency Mode Operation Plan to enable the continuation of its critical business processes and to protect the security of ePHI while DC HIE operates in emergency mode. DC HIE will oversee this plan. The vendor's Emergency Mode Operation Plan will permit authorized Users to access and use the service during and immediately following an emergency or disaster. Emergency mode operation procedures detailed in the Emergency Mode Operation Plan must be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while DC HIE operates in emergency mode.

HIPAA Security Rule Language: "Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode."

Policy/Procedure:

1. The vendor's Emergency Mode Operation Plan will:

    a. Define and categorize reasonably foreseeable emergencies and/or disasters that could have an impact on the confidentiality, integrity, and availability of ePHI that is exchanged through the Network.
    b. Include a procedure that specifies how the vendor will react to emergencies and disasters.
    c. Include a procedure that outlines how DC HIE will maintain security processes and controls during and immediately following an emergency or disaster.
    d. Authorize designated Workforce Members to enter DC HIE's offices and facilities and any offsite location where backup media are stored to maintain the security process and controls of the Network.
    e. Identify the roles that particular DC HIE Workforce Members will serve while DC HIE is operating in emergency mode.
    f. Identify the roles of designated Workforce Members who will be permitted to administer or modify processes and controls that protect the security of ePHI while DC HIE is operating in emergency mode.

2. DC HIE will make the vendor's Emergency Mode Operations Plan easily available to its Workforce Members at all times.

3. The vendor will periodically test its Emergency Mode Operations Plan to ensure that critical business processes can continue in a satisfactory manner. If necessary, the vendor may revise the Emergency Mode Operations Plan, and the occurrence of any of the following events may result in a revision of the Emergency Mode Operations Plan:

    a. Disaster recovery role and responsibility changes, including changes to contact information.
    b. Changes to DC HIE's physical or technical infrastructure or operating systems.

c. Changes in threats to the Network
d. Results of testing that indicate the plan needs to be modified to ensure that it is sufficient and up to date.

Responsibility: Security Officer; Risk Management Officer, DC HIE Technology Vendor
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(7)(ii)(C), Emergency Mode Operation Plan, [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(7)(ii)(D), Testing and Version Procedures, [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-15**
Title: **Applications and Data Criticality Analysis**	Version: **1**	Effective Date:

HIPAA Security Rule Language: "Assess the relative criticality of specific applications and data in support of other contingency plan components."

Purpose Statement: The purpose of the criticality analysis is for DC HIE to document the impact to its services, processes, and operating objectives if a disaster or other emergency causes any or all of the Network's functions to become unavailable for a documented period of time. The criticality analysis will serve as the basis for the prioritization of each Network function and the importance of the function to DC HIE's business operations during a disaster.

Policy/Procedure:

1. To prioritize functions within the Network for disaster recovery, the Contract Administrator, in collaboration with the HIT Coordinator and Risk Management Officer will develop a matrix, which:

    a. Inventories all the Network functions; and
    b. Determines the necessity of each Network function to DC HIE's operations.

2. The matrix will be used to determine which of the Network functions are most important to the operation of DC HIE's critical business operation and thereby determine how disaster recovery efforts will be focused during a Contingency Event or other disaster.

3. The matrix may direct:

    a. Which Network functions will be restored first; and/or
    b. Which Network functions will receive the first line of assistance during a disaster.

4. DC HIE will conduct a yearly data criticality analysis as part of its risk assessment in accordance with the Security Risk Management, Evaluation and Updates Policy (HS-1).
5. The Contract Administrator, in collaboration with the HIT Coordinator and Risk Management Officer, will be responsible for documenting all activities relating to the data criticality analysis and providing such documentation to any Vendor that needs this information in connection with the Emergency Mode Operations Plan Policy (HS-14). Such documentation will be maintained and retained by the to-be-named Security Officer for six years from the date of creation.

Responsibility: Contract Administrator, HIT Coordinator, Risk Management Officer; Vendor
Regulatory Category: Administrative Safeguards
Regulatory Reference: 93 HIPAA Security Policies and Procedures

- 45 C.F.R. §164.308(a)(7)(ii)(E), Applications and Data Criticality Analysis [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-16**
Title: **Facility Access and Security**	Version: **1**	Effective Date:

Purpose Statement: DC HIE and its Vendor(s), to the extent applicable, will ensure that physical access to the servers that host Direct Secure Messaging is limited.

HIPAA Security Rule Language: "Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."

Policy/Procedure:

Facility Access and Security Controls

1. The server that maintains all of the ePHI exchanged through the Network is housed in a Tier 3 data center. DC HIE's technology vendor, in its discretion, may relocate its servers to another Tier 3 or higher data center.

2. All DC HIE servers are contained within DC HIE's designated, locked cage at the data center.

3. The data center is locked at all times, and only grants authorized personnel limited physical access through the use of biometric security measures. In addition, the following security controls are utilized in the data center to protect the facility, and DC HIE's servers, from unauthorized access, tampering and theft:

    a. Signs and warnings stating that access to an area is restricted
    b. Surveillance cameras
    c. Alarms

4. DC HIE, in its discretion, may evaluate, from time to time, the need for additional security controls to be put into place by its Vendors to protect the physical security of its servers.

5. Designated Workforce Members and/or Vendor personnel will personally supervise all visitors and vendors while they are physically present at the data center in the secured cabinet that houses the servers.

Facility Repairs and Modification

1. The data center is responsible for conducting all necessary repairs and modifications to its facility to either repair or enhance its security features.
2. The data center will notify the Security Officer if any repairs or modifications are required for the cabinet containing DC HIE's server and backup server. DC HIE will document and maintain such notifications.

Responsibility: Security Officer; Vendor

Regulatory Category: Physical Safeguards

Regulatory Reference:

- 45 C.F.R. §164.310(a)(1), Facility Access Controls [Standard; Required]
- 45 C.F.R. §164.310(a)(2)(i), Contingency Operations [Implementation Specification; Addressable]
- 45 C.F.R. §164.310(a)(2)(ii), Facility Security Plan [Implementation Specification; Addressable]
- 45 C.F.R. §164.310(a)(2)(iii), Access Control and Validation Procedures [Implementation Specification; Addressable]
- 45C.F.R. §164.310(a)(2)(iv), Maintenance Records [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-17**
Title: **Workstation Use and Security**	Version: **1**	Effective Date:

Purpose Statement: Workstations will be used in a manner that is consistent with DC HIE's business purposes. DC HIE requires the implementation of reasonable physical safeguards to protect all Workstations and other electronic devices that access, store or transmit ePHI from theft or unauthorized use. DC HIE will periodically review, and may modify, as appropriate, the permitted and prohibited uses of Workstations and the security controls implemented to protect Workstations in accordance with the Security Risk Management, Evaluation and Updates Policy (HS-1). DC HIE will periodically distribute training and education materials to Workforce Members regarding the use and security of Workstations used to access the Network.

HIPAA Security Rule Language:
"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI."
"Implement physical safeguards.

Policy/Procedure:

1. DC HIE's Workstations will only be used for business purposes.

2. DC HIE will locate Workstations in physically secure areas and will physically position Workstations in ways that minimize unauthorized viewing of ePHI.
3. Workstations will not be located in any of the following locations:

    a. Public walkways
    b. Hallways
    c. Waiting areas
    d. Any other area where unauthorized viewing of ePHI may occur

4. In the event that unauthorized viewing of ePHI cannot be minimized by positioning the Workstation, DC HIE will install a screen filter on the Workstation.
5. DC HIE will require Workforce Members to have unique user identifiers and passwords to gain access to their Workstations.
6. Workforce Members must activate workstation locking software upon leaving a Workstation for more than five (5) minutes.
7. Workforce Members must log off from their Workstations when their work-day shift is complete.
8. DC HIE will ensure that anti-virus software, which is configured to receive anti-virus updates are installed on all Workstations that its Workforce Members use in accordance with the Malicious Software Policy (HS-9).

9. These same Workstation security procedures apply to all Workstations regardless of the Workstation's location.
10. Portable Workstations must be physically secured at all times when not in the Workforce Member's immediate possession while such Workstations are off-site.

Responsibility: Security Officer; Technical Domain Manager; Workforce Members
Regulatory Category: Physical Safeguards
Regulatory Reference:

- 45 C.F.R. §164.310(b), Workstation Use [Standard; Required]
- 45 C.F.R. §164.310(c), Workstation Security [Standard; Required]

DC HIE	HIPAA Security	Policy No.: **HS-18**
Title: **Device and Media Controls**	Version: **1**	Effective Date:

Purpose Statement: DC HIE will take reasonable and appropriate steps to control its hardware and electronic media throughout the media's entire lifecycle, from initial receipt to final removal. Such control includes reasonably and appropriately protecting, accounting for, storing, backing up, and disposing of its hardware and electronic media in accordance with specific control procedures and tracking all incoming hardware and electronic media and transfers of hardware and electronic media as they are moved into and out of DC HIE's direct control and premises.

HIPAA Security Rule Language: "Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility."

Policy/Procedure:

Inventory and Movement of Hardware and Electronic Media

1. DC HIE will periodically take an inventory of hardware and electronic media that contain ePHI. Workforce Members will be advised that they should not save any ePHI to electronic media unless required to perform their job functions.
2. If a Workforce Member is required to save ePHI to electronic media to perform his job functions, it may only be saved to hard drives and approved USB drives. No other media may be used to store ePHI.
3. Prior to moving hardware or other electronic media that contain ePHI outside of DC HIE's facilities and out of the direct control of DC HIE, the Security Officer must be notified of and grant authorization for such movement.
4. DC HIE will maintain documented records regarding the movement outside of DC HIE's facilities and direct control of hardware and electronic media that contains ePHI. Documentation regarding the movement of hardware or electronic media will be required only for desktop computers, laptops, and other media storage devices that can be tracked. The following information must be documented in each record regarding the movement of hardware or electronic media:

    a. Date of movement
    b. Method of movement
    c. Description of the moved medium
    d. Dates indicating the time period that the moved medium was used at DC HIE
    e. Dated signatures of the Security Officer and all Workforce Members supervising the movement.

Disposal of ePHI Hardware and Electronic Media

1. DC HIE will take all reasonable and appropriate steps to remove ePHI from hardware and electronic media prior to the final disposal of the hardware or electronic media.
2. The Security Officer or designee will determine which sanitization method is appropriate for the removal of ePHI from hardware and/or electronic media.
3. The following sanitization methods may be used to remove ePHI from hardware and/or electronic media:

    a. Clearing

    - Overwrites storage space on the hardware or electronic media with non-sensitive data.
    - The hardware and/or electronic media type and size may influence whether overwriting is a suitable sanitization method.
    - DC HIE will consult the National Institute of Standards and Technology (NIST) *Guidelines for Media Sanitization*, Publication 800-88 regarding recommendations for clearing different media types.

    b. Purging

    - Degaussing is an acceptable method of purging.
    - Degaussing exposes the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains.
    - Degaussing cannot be used to purge nonmagnetic media, such as optical media or compact discs (CDs).
    - DC HIE will consult the National Institute of Standards and Technology (NIST) *Guidelines for Media Sanitization*, Publication 800-88 regarding its recommendations for purging different media types.

4. If hardware and/or electronic media cannot be cleared or purged, the only method of disposal is to physically destroy the hardware and/or electronic media. Acceptable methods of destroying hardware and/or electronic media include:

    a. Disintegration
    b. Incineration
    c. Pulverization
    d. Melting
    e. Shredding

5. DC HIE will document the disposal of all hardware and electronic media 100 HIPAA Security Policies and Procedures disposal and the steps taken to remove ePHI prior to the disposal of such hardware and electronic media.

6. The Security Officer or his or her designee will inspect all hardware and electronic media to ensure that all ePHI has been removed from the hardware or electronic media prior to disposal.

Media Re-Use

1. For the internal re-use of hardware and/or electronic media, such as the re-deployment of a computer to another Workforce Member, DC HIE will reformat all files on the hardware and/or electronic media so that such files are not accessible.
2. For external re-use of hardware and/or electronic media (e.g. donation or return of leased hardware), DC HIE will completely and permanently remove ePHI from the hardware and/or electronic media in accordance with the Disposal procedures of this Policy.

Responsibility: Security Officer; Technical Domain Manager; Workforce Members
Regulatory Category: Physical Safeguards
Regulatory Reference:

- 45 C.F.R. §164.310(d)(1), Device and Media Controls [Standard; Required]
- 45 C.F.R. §164.310(d)(2)(i), Disposal [Implementation Specification; Required]
- 45 C.F.R. §164.310(d)(2)(ii), Media Re-Use [Implementation Specification; Required]
- 45 C.F.R. §164.310(d)(2)(iii), Maintenance of Records regarding Movements of Hardware and Media [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-19**
Title: **Technical Access Controls**	Version: **1**	Effective Date:

Purpose Statement: To protect the confidentiality, integrity, and availability of ePHI, DC HIE has taken reasonable and appropriate steps to ensure that there are technical safeguards to control and restrict access to the Network to persons who are authorized to have such access in accordance with the Information Access Management Policy (HS-5).

HIPAA Security Rule Language:
"Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified in 45 C.F.R. §164.308(a)(4)." 45 C.F.R. §164.308(a)(4) states, "Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of subpart E of this part."

Policy/Procedure:

1. DC HIE will implement appropriate technical security controls and methods that permit only authorized persons to access the Network. Such controls and methods may include, but are not limited to, the following:

    a. When appropriate, issuance of unique user identifications (user IDs) for each User to be used in conjunction with passwords and a second authentication method as part of DC HIE's dual-factor authentication measures.
    b. Emergency access procedures that enable authorized Workforce Members to obtain access to the Network during a disaster or other emergency.
    c. Activation of password protected screensaver on internal Workstations after a designated period of inactivity.
    d. Automatic log-off after a designated period of inactivity in accordance with the Log-in Monitoring and Automatic Log-Off Policy (HS-10).
    e. Requiring Workforce Members to logoff or lock Workstations upon leaving their work areas.
    f. Encryption, when appropriate, of ePHI exchanged through the Network.

Emergency Access Procedure

DC HIE may not need to access the Network during an emergency or disaster. However, if DC HIE does require such access during an emergency or disaster, DC HIE will follow the procedures outlined in its Contingency Plan Policy (HS-12) and Emergency Mode Operations Plan Policy (HS-14) regarding who has access to the Network.

Workstation Screen Savers for DC HIE Workforce Members

1. All DC HIE Workstations will be equipped with screensavers that will automatically activate after 10 minutes of inactivity.

2. Workforce Members can only deactivate the Workstation screensaver by entering his or her confidential password when prompted.

Encryption and Decryption

1. Based on its risk analysis in accordance with the Security Risk Management, Evaluation and Updates Policy (HS-1), DC HIE will determine when to implement encryption for ePHI exchanged through the Network and the type and quality of the encryption algorithm and cryptographic key length for data that DC HIE controls and maintains.
2. The Security Officer will approve the encryption mechanism that DC HIE will use.
3. When encryption is used, DC HIE will:

    a. Protect its cryptographic keys against modification and destruction, and protect its private keys against unauthorized disclosure.
    b. Manage the cryptographic keys used to encrypt ePHI exchanged through the Network.
    c. Periodically determine activation and deactivation dates for its cryptographic keys.

Responsibility: Security Officer; Technical Domain Manager; Vendors
Regulatory Category: Technical Safeguards
Regulatory Reference:

- 45 C.F.R. §164.312(a)(1), Access Control [Standard; Required]
- 45 C.F.R. §164.312(a)(a)(2)(i), Unique User Identification [Implementation Specification; Required]
- 45 C.F.R. §164.312(a)(2)(ii), Emergency Access Procedure [Implementation Specification; Required]
- 45 C.F.R. §164.312(a)(a)(2)(iii), Automatic Logoff [Implementation Specification; Addressable]
- 45 C.F.R. §164.312(a)(a)(2)(iv), Encryption and Decryption [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-20**
Title: **Integrity**	Version: **1**	Effective Date:

Purpose Statement: To safeguard ePHI, it is important to ensure that ePHI has not been altered or destroyed in an unauthorized manner. Therefore, DC HIE's technology vendor will take reasonable and appropriate steps to protect the integrity of ePHI exchanged through the Network.

HIPAA Security Rule Language: "Implement policies and procedures to protect electronic PHI from improper alteration or destruction."

Policy/Procedure:

1. Under no circumstances are Workforce Members permitted to modify or alter clinical information exchanged through the Network.

2. Except as set forth in this Policy or Deletion of Direct Secure Messages Policy (DM-13), ePHI exchanged through the Direct Secure Messaging service will not be destroyed without first providing notice to and receiving authorization from the Security Officer.

3. DC HIE has sufficient policies and procedures in place that minimize the need to authenticate ePHI; therefore, it is not reasonable or appropriate to implement additional mechanisms to authenticate ePHI.

Responsibility: Security Officer

Regulatory Reference:

- 45 C.F.R. §164.310(c)(1), Integrity [Standard; Required]
- 45 C.F.R. §164.310(c)(2), Mechanisms to Authenticate Electronic PHI [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-21**
Title: **Person or Entity Authentication**	Version: **1**	Effective Date:

HIPAA Security Rule Language: "Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed."

Purpose Statement: To protect the confidentiality, integrity, and availability of ePHI, DC HIE will maintain a documented process for verifying the identity of any person or entity prior to granting access to the Network.

Policy/Procedure:

1. DC HIE requires the use of authentication before access to the Network is granted.

    a. User IDs are assigned in accordance with the Technical Access Controls Policy (HS-19).
    b. All passwords must be complex and confidential in accordance with the Password Management Policy (HS-11).

2. DC HIE will not allow redundant authentication credentials.

3. When feasible, DC HIE will mask, suppress, or otherwise obscure the passwords of persons and entities seeking access to Direct Secure Messaging so that unauthorized persons are not able to observe such passwords.

4. DC HIE will limit the authentication attempts of persons seeking access to the Network at a predetermined number of consecutive inaccurate attempts. Authentication attempts that exceed this limit shall result in:

    a. Logging of the event for review;
    b. Disabling of the User's password; and
    c. Notifying the Security Officer or other appropriate DC HIE official.

5. The credentials of each User will be verified pursuant to the Information Access Management Policy (HS-5).

Responsibility: Security Officer
Regulatory Category: Technical Safeguards
Regulatory Reference:

- 45 C.F.R. §164.312(d), Person or Entity Authentication [Standard; Required]

DC HIE	HIPAA Security	Policy No.: **HS-22**
Title: **Transmission Security**	Version: **1**	Effective Date:

HIPAA Security Rule Language: "Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network."

Purpose Statement: To ensure the confidentiality, integrity, and availability of ePHI, DC HIE will implement technical security measures to guard against unauthorized access to ePHI while it is transmitted over electronic communications networks.

Policy/Procedure:

1. DC HIE will implement secure protocols, which encrypt data while such data is being electronically transmitted. In addition, these secure protocols allow decrypted data to be presented to the User upon its arrival to his or her Workstation.

2. Unauthorized access to ePHI transmitted through Direct Secure Messaging is prevented through the use of the administrative, technical and physical safeguards for the Network described in the Policies and Procedures.

Responsibility: Security Officer; Technical Domain Manager

Regulatory Category: Technical Safeguards

Regulatory Reference:

- 45 C.F.R. §312(e)(1), Transmission Security [Standard; Required]
- 45 C.F.R. §312(e)(2)(i), Integrity Controls [Implementation Specification; Addressable]
- 45 C.F.R. §312(e)(2)(ii), Encryption During Transmission [Implementation Specification; Addressable]

DC HIE	HIPAA Security	Policy No.: **HS-23**
Title: **Availability**	Version: **1**	Effective Date:

HIPAA Security Rule Language: "Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains."

Purpose Statement: DC HIE will make all documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Policy/Procedure:

1. DC HIE will make the following documentation available to those persons responsible for implementing these Policies and Procedures:

    a. Policies and procedures regarding the security of ePHI and the Network.
    b. All documentation that records any updates, revisions, modifications, or deletions made to existing Privacy and Security Policies and Procedures.
    c. All policies and procedures no longer in effect for a certain Security Regulation requirement or implementation specification.
    d. Any other documentation that the Security Officer deems appropriate to retain and to make available to Users regarding DC HIE's Policies and Procedures.

2. The Security Officer will be responsible for ensuring that such documentation as required by the HIPAA Security Regulations is made available to Users.

3. All documentation specified in this policy will be available on the Network.

Responsibility: Security Officer
Regulatory Category: Policies, Procedures, and Documentation
Regulatory Reference:

- 45 C.F.R. §164.316(b)(2)(ii), Availability [Implementation Specification; Required]

Operational Policies

DC HIE	HIPAA Security	Policy No.: **O-1**
Title: **Policy Board Structure, Procedures Amendment Process**	Version: **1**	Effective Date:

Purpose Statement: It is important that subscribers to Direct Secure Messaging and/or the DC HIE understand how DC HIE is governed, how it develops its policies and procedures and amendments.

1. The District of Columbia Health Information Exchange Policy Board (DC HIE), hereafter Board, is the governing body assembled in response to the District of Columbia Mayor's Order regarding establishment of a Health Information Exchange Policy Board.

2. The purpose, functions and membership of the Board shall be designated by virtue of the authority vested by the Mayor the District of Columbia by section 422 (11) of the District of Columbia Home Rule Act, approved December 24, 1973. (Pub. L. 93-198, 87 Stat. 790; D.C. Official Code Sec. 1-204.22(11) (2010 Supp).

    a. The purpose of the Board is to advise the Mayor, the Director of the Department of Health Care Finance (DHCF) and other District leadership regarding the implementation of secure, protected health information exchange benefiting District stakeholders in accordance with the DHCF HIE Action Plan.

    b. The functions of the Board shall consist of the following:

        i. Make recommendations regarding the development of policies essential to broad implementation of secure, protected health information exchange benefiting District stakeholders.
        ii. Make recommendations to DHCF regarding improving HIE operations, including vision, mission, geographic and functional scope.
        iii. Make recommendations on establishing the roles, responsibilities, and relationships between parties to organize, promulgate, and oversee activities among stakeholders and across state, regional, and local levels, and implementation of associated accountability mechanisms.

3. The DC HIE Policy Board will approve all new, amended, or replaced DC HIE Policies and Procedures and repeal any existing DC HIE Policies and Procedures. However, any Policy Board member or Direct Secure Messaging Subscriber may submit in writing to DC HIE a request for the development of a new Policy and Procedure, or a request for the amendment or repeal of an existing Policy and Procedure.

4. All such requests shall identify (i) the Policy and Procedure that is the subject of the requested change (if any), (ii) the type of Policy and Procedure sought (if it is a request for a new Policy and Procedure), (iii) a thorough description of why the request is necessary, and

(iv) an analysis of the expected impact of adopting the new Policy and Procedure or modifying/repealing an existing Policy and Procedure.

5. The DC HIE Policy Board Chair will consider any requests that meet the submission criteria set forth within thirty (30) days following receipt of such request.

    a. If, after considering the request, the Board Chair determines that the request does not have merit or lacks sufficient detail, it will communicate this determination to the requestor.
    b. If after considering the request, the Board Chair determines that the request has merit, it will forward the request to a subcommittee or to staff to review the request and make a recommendation for action to the Policy Board.

6. If the Board Chair approves a recommendation of a subcommittee or staff to adopt of a new, amended, or replaced Policy and Procedure or repeal a Policy and Procedure, the Board Chair will forward such recommendation to the DC HIE Policy Board.

7. The DC HIE Policy Board will then vote on whether to approve the recommended Policy and Procedure. If it is approved, the DC HIE Policy Board will determine the effective date of such Policy and Procedure.

8. Recommendations and motions passed by the Board or suggestions and advice to the Chair shall be utilized, and if not utilized, the reason for rejections shall be stated.

9. DC HIE will use its best efforts to provide notice of such new, amended, repealed or replaced Policies and Procedures to DC HIE Exchange Participants and DC HIE Direct Users prior to the effective date of any such changes.

10. Documentation recording any changes or modifications to the Privacy and Security Policies and Procedures will be maintained for at least ten years.

DC HIE	HIPAA Security	Policy No.: **O-2**
Title: **Availability**	Version: **1**	Effective Date:

Purpose Statement: It is important that DC HIE be responsive to a subpoena request but not disclose ePHI in an inappropriate manner.

Policy/Procedure:

1. Immediately upon receipt of any subpoena, DC HIE will forward said subpoena to its legal counsel.
2. DC HIE will follow advice of legal counsel regarding a response to a subpoena.
3. If the subpoena is requesting the health information of a specific person or persons whose ePHI was exchanged using the Network, counsel should be advised that DC HIE takes the position that it is not the custodian of medical records and, therefore, is not the proper party to respond to the subpoena.

Responsibility: DC HIE

DC HIE Operational Policies and Procedures for DC HIE Direct Messaging

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-1**
Title: **DC-HIE Direct User Information Confidentiality**	Version: **1**	Effective Date:

Purpose Statement: DC-HIE will protect the confidentiality of all Direct Secure Messaging User Information.

Policy/Procedure:

1. DC-HIE will not use or share DC-HIE Direct User Information with any person except as set forth in this Policy.

2. DC-HIE may access all Direct Secure Messaging User Information submitted to DC-HIE and allow third parties who are performing services for DC-HIE to use this information for the benefit of DC-HIE.

3. DC-HIE may use a Direct Secure Messaging User's name, email address, physical address, or other data to communicate with the User and to populate a Direct Secure Messaging Provider Directory.

4. DC-HIE may use the Direct Secure Messaging Provider Directory to facilitate communication between Subscribers.

5. Direct Secure Messaging Users may only access their personal Direct Secure Messaging User Information. They may not access another Direct Secure Messaging User's Information except as available through the Provider Directory.

6. DC-HIE will maintain a list of user passwords after their initial set-up, but only for the purpose of transmitting those passwords to its technology vendor for Direct account set up. The user passwords will be kept on a password protected computer.

Responsibility: DC-HIE, DC-HIE Direct Users

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-2**
Title: **Certificate Validation**	Version: **1**	Effective Date:

Purpose Statement: To ensure that only authorized DC-HIE Direct Secure Messaging Users are sending messages using DC-HIE's Direct Secure Messaging, DC-HIE will validate the certificate for each message.

Policy/Procedure:

1. For each message a DC-HIE Direct Secure Messaging User sends using DC-HIE Direct Secure Messaging, DC-HIE will check the validity of the certificate by verifying that:

    a. The certificate has not expired;
    b. The message has a valid signature;
    c. The certificate has not been revoked;
    d. The certificate is binding to the expected entity and
    e. The certificate has a trusted certificate path.

2. DC HIE will perform certificate validation for the exchange of health information within the District. In the future and for exchanges from/to DC HIE to another HIE, DC HIE will pursue a contract with an external and established certificate validation vendor.

Responsibility: DC-HIE

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-3**
Title: **Direct Addresses**	Version: **1**	Effective Date:

Purpose Statement: To send and receive messages using DC-HIE Direct Messaging, each Direct Secure Messaging User will choose a unique DC-HIE Direct Messaging address.

Policy/Procedure:

1. Prior to an individual being accepted as a Direct Secure Messaging User pursuant to the DC-HIE Direct Secure Messaging Subscription Agreement, he/she will choose a DC-HIE Direct Messaging address.

2. An individual DC-HIE Direct Secure Messaging address will be structured as follows: firstname.lastname@direct.dc-hie.org.

3. A facility-based individual's DC-HIE Direct Secure Messaging address will be structured as follows: facility.firstname.lastname@direct.dc-hie.org.

   For Users at large hospitals, health systems and/or health plans based in or with significant operations in the District, Users will use utilize a specific naming convention that will be available via drop-down menu on the Create Your Direct Secure Messaging account section of the HIE webpage.

4. A DC-HIE Direct Secure Messaging User may share his DC-HIE Direct Secure Messaging address with any other DC-HIE Direct User with whom he/she would like to exchange messages.

5. DC-HIE may list each DC-HIE Direct User's DC-HIE Direct Messaging address in a directory in accordance with the DC-HIE Direct User Information Confidentiality Policy (DC-DSM-1).

Responsibility: DC-HIE; DC-HIE Direct Messaging User

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-4**
Title: Trusted HISPS	Version: **1**	Effective Date:

Purpose Statement: DC-HIE only allows Direct Secure Messaging Users to send messages to and receive messages from individuals who exchange such messages through a trusted health information service provider (HISP). This policy will set forth the procedure that DC-HIE uses to determine whether a HISP is trusted and a list of trusted HISPs.

Policy/Procedure:

1. During the first quarter of 2013, DC-HIE will develop a process by which it determines whether to admit a HISP into its circle of trust.

2. Until such a process is developed and DC-HIE expands its circle of trust to include other HISPs, DC-HIE Direct Secure Messaging Users may only send messages to and receive messages from other DC-HIE Direct Secure Messaging Users.

Responsibility: DC-HIE; DC-HIE Direct Users

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-5**
Title: **Agreements with Direct Secure Messaging Subscriber/Users**	Version: **1**	Effective Date:

Purpose Statement: Each Direct Secure Messaging Subscriber User must agree to be legally obligated to protect the privacy, security and integrity of the information exchanged through Direct Secure Messaging. Furthermore, DC-HIE must agree to be legally obligated to fulfill its responsibilities as a Business Associate of each Direct Secure Messaging User. Each party's legal obligations are set forth in the DC-HIE Direct Messaging End User License Agreement and Business Associate Addendum.

Policy/Procedure:

1. All individuals that are Direct Secure Messaging Subscribers/Users must agree to the Direct Secure Messaging Subscription Agreement before the individual can access or use Direct Secure Messaging.

2. Each Direct Secure Messaging Subscriber/User, if it is a Covered Entity, must also enter into a Business Associate Agreement with DC-HIE where the User is the Covered Entity and DC-HIE is the Business Associate. The Business Associate Agreement is an addendum to the DC-HIE Direct Messaging End User License Agreement.

Responsibility: DC-HIE; DC-HIE Direct Users

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-6**
Title: **DC-HIE's Use and Disclosure of PHI in DC-HIE Direct Messaging**	Version: **1**	Effective Date:

Purpose Statement: Pursuant to the Direct Secure Messaging Subscription Agreement, Direct Secure Messaging Users are permitted to use DC-HIE Direct Secure Messaging to send PHI to other DC-HIE Direct Secure Messaging Users for any purpose allowed by law. DC HIE's technology contractor, on behalf of DC-HIE, delivers the information to the receiving Direct Secure Messaging User. Pursuant to the Business Associate Agreement between DC-HIE and each Direct Secure Messaging User, DC-HIE may also use and disclose PHI, as needed, for its proper management and administration and to fulfill any other obligations described in the Direct Secure Messaging Subscription Agreement.

Policy/Procedure

1. DC-HIE's technology contractor may only use information provided by a Direct Secure Messaging User, as needed, to perform certain proper management and administrative functions and fulfill its obligations under the Direct Secure Messaging Subscription Agreement. This includes, but is not limited to, encrypting messages sent by a Direct User, delivering messages to the DC-HIE Direct User recipient identified by the sending DC-HIE Direct User, and auditing and monitoring use of DC-HIE Direct Secure Messaging as described in the DC-HIE Direct Messaging Auditing and Monitoring Policy (DC-DSM-7).

2. Each DC-HIE Direct Secure Messaging User is responsible for making sure that all of the information he sends through DC-HIE Direct Messaging complies with applicable law. This includes obtaining any consents or authorizations required by applicable law prior to sending such information.

Responsibility: DC-HIE; DC-HIE Direct Users

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-7**
Title: **DC-HIE Direct Messaging Auditing and Monitoring**	Version: **1**	Effective Date:

Purpose Statement: In accordance with the Information System Activity Review Policy (HS-2), DC-HIE's technology contractor may implement auditing and monitoring mechanisms to record and examine the activity of Direct Secure Messaging Users to enable DC-HIE to detect potentially problematic activity.

Policy/Procedure:

Audit Report Content

1. DC-HIE's technology contractor will create monthly audit reports that capture DC-HIE Direct User-level data associated with at least the following activities:

    a. User sign-ons to the DC-HIE Direct Secure Messaging Service;
    b. Messages sent by a DC-HIE Direct Secure Messaging User using DC-HIE Direct Messaging; and
    c. Failed authentication attempts after a pre-determined number of unsuccessful attempts to log-in to the DC-HIE Direct Messaging Service.

2. The monthly audit reports may generate the following information for each activity logged:

    a. Date and time of activity;
    b. Descriptions of each attempted or completed activity;
    c. Identification of the DC-HIE Direct User performing the activity; and/or
    d. Origin of the activity, such as the I/P address or workstation identification number.

DC HIE Direct User Requests for Audit Reports

1. If a DC-HIE Direct User desires an audit report of his/her activity within DC-HIE Direct Secure Messaging, he/she will submit a request to DC-HIE with a brief explanation of the reason for the request.

2. Within one week of receiving the request from the DC-HIE Direct User, DC-HIE will decide whether to accept or deny the request and transmit such decision to the DC-HIE Direct User.

3. If DC-HIE deny a request, DC-HIE will provide a brief explanation of the denial.

4. If DC-HIE accepts a request, DC-HIE will provide the DC-HIE Direct User with the requested report as soon as feasible.

Responsibility: DC-HIE, DC-HIE Direct Users

DC-HIE	Operational Policy for Direct Secure Messaging	Policy No: **DC-DSM-8**
Title: **Direct Secure Messaging User Subscriptions**	Version: **1**	Effective Date:

Purpose Statement: To protect the confidentiality, integrity, and availability of ePHI exchanged through Direct Secure Messaging, DC-HIE has implemented a strict subscription process to verify the identity and appropriateness of those who seek a Direct Secure Messaging address. DC HIE offers the following subscription types:

A. **Individual Subscriber**: an individual healthcare provider who registers as an employee or who is affiliated with an organization, or 2) a provider with a solo practice that is not affiliated with an organization with other providers. Requires the Subscriber organization or individual, as a solo practitioner to already have a Direct Secure Messaging account.

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). Requires the Subscriber's organization to already have a Direct Secure Messaging account.

D. **Delegate**: for a non-licensed individual such as an office manager or administrative support person, authorized to use a Subscriber's Direct Secure Messaging account on behalf of an organization or Subscriber. Requires the organization or Subscriber to have an active Direct Secure Messaging Account. Non-licensed, non-clinical District of Columbia Government employees who wish to register as a Delegate must submit a District-developed job description along with a letter of authorization from their supervisor.

Health care professionals who are licensed and credentialed in DHCF's Medicaid Management Information System or by the Department of Health's Health Professional License Database will be able to register for a Direct Secure Messaging account.

Non-licensed, non-clinical individuals will also be able to register for a Direct Secure Messaging account. DC HIE refers to this group as delegates and they are described in letter D above. The identity of delegates will be verified by a telephone call from DC HIE to the Human Resources representative at the prospective Subscriber's organization or agency. DC HIE may permit additional verifiable subscribers beyond this group at a later time.

Policy/Procedure:

1. Each individual who desires to use Direct Secure Messaging will be responsible for completing the subscription processes and the DC HIE Subscription Agreement available at the Direct Secure Messaging webpage.

2. To subscribe, an individual must complete and submit the following:

a. The Subscription Agreement, which is available on the HIE/Subscribe to Direct webpage of DHCF.
b. DC HIE Identity Verification Form. This form requires the individual to submit a valid form of identification such a state-issued driver license or U.S. Passport. The Identity Verification Form must be notarized.

The Subscription Agreement will require the individual to attest to the following:

a. he/she has completely and accurately represented his identity,
b. he/she is a health care provider with a valid license, certificate or registration issued by the Department of Health Professional License Database to practice his/her clinical occupation, and
c. that such license, certificate or registration is currently in effect and in good standing.
d. DC HIE recognizes that non-licensed, non-clinical individuals (Delegates) who currently transmit PHI via facsimile or via another paper-based method as a part of their job responsibilities may benefit from and be interested in obtaining a Direct Secure Messaging address. Delegates must also complete the subscription processes and the DC HIE Subscription Agreement and the Identity Verification Form. The appropriateness of Delegates to transmit ePHI via Direct Secure Messaging will be verified by a telephone call from DC HIE to the Human Resources representative at the prospective Delegate's organization or agency. Non-licensed, non-clinical District of Columbia Government employees who wish to register as a Delegate must submit a District-developed job description along with a letter of authorization from their supervisor.

3. The Subscription Agreement must be signed and forwarded to DC-HIE via one of the following methods: a) email at info.dc-hie@dc.gov b) facsimile at 202-442-4790 or c) postal mail at DHCF, 899 North Capitol Street, NE Suite 6037, Washington, DC 20002-4210 Attn: Direct Secure Messaging Subscription. In addition, the Identity Verification Form must be completed, signed, notarized and forwarded to DC HIE via one of the above methods.

4. The Direct Secure Messaging User is responsible for maintaining accurate subscription information and notifying DC-HIE of changes to such information so long as the individual remains a Direct Secure Messaging User.

5. Beginning September 1, 2013, through future legislation, DC HIE will begin to charge a nominal monthly fee to cover basic costs for use of Direct Secure Messaging. Details will be forwarded to providers in advance of imposition of the monthly fee. DC HIE reserves the right to terminate a Subscription Agreement for non-payment of fees. Subscribers/Users may terminate their subscription to Direct Secure Messaging at any time for any reason.

6. Once the individual, organization or Delegate submits all required subscription information to DC-HIE, DC-HIE will verify the identity and appropriateness of the prospective subscriber.

7. For licensed clinical professionals, once DC-HIE has verified the status of the individual's professional license, certificate or registration and confirmed that it is in effect and in good standing, he/she will be issued Direct Secure Messaging login instructions via email. For non-

licensed, non-clinical individuals, once DC HIE has verified user identity and appropriateness, DC HIE will issue the user Direct Secure Messaging login instructions via email. Once login instructions are issued, the individual/organization will then be able to send and receive Messages through Direct Secure Messaging.

8. DC-HIE will regularly confirm that each Direct Secure Messaging User has a valid license, certificate or registration by checking each DC-HIE Direct User's license, certificate or registration against reports of suspended or terminated licenses, certificates and registrations issued by the DC Department of Health's Health Professional License Database. DC HIE will also regularly confirm that non-licensed, non-clinical Direct Secure Messaging users continue to be valid that their use of Direct Secure Messaging is appropriate.

9. If DC-HIE discovers that a DC-HIE Direct Secure Messaging User's professional license, certificate or registration has been suspended or terminated, DC-HIE will suspend or terminate such User in accordance with the DC-HIE Direct Secure Messaging User Suspension and Termination Policy (DC-DSM-9). If DC HIE discovers that a non-licensed, non-clinical DC HIE Direct Secure Messaging user is no longer employed with the organization that authorized his/her Direct Secure Messaging account or that his/her job responsibilities no longer require the transmission of PHI via Direct Secure Messaging, DC HIE will with advance notice suspend or terminate such User in accordance with the DC HIE Direct Secure Messaging Suspension and Termination Policy.

Responsibility: DC-HIE; DC-HIE Direct Secure Messaging User

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-9**
Title: **DC-HIE Direct User Suspension and Termination**	Version: **1**	Effective Date:

Purpose Statement: DC-HIE will suspend or terminate a Direct Secure Messenger's access to Direct Secure Messaging for the reasons set forth in Subscription Agreement.

Policy/Procedure

Suspension Procedures for Direct Secure Messaging Users

1. In accordance with Direct Secure Messaging Subscription Agreement, DC-HIE can suspend a Direct Secure's Messaging user account under the following circumstances:

    a. the Direct Secure Messaging User's license, certificate or registration to practice his/her health care profession in the District of Columbia is suspended;
    b. the Direct Secure Messaging User violates any provision of the Subscription Agreement or any DC-HIE Policy and Procedure;
    c. the DC-HIE Direct User fails to pay his/her membership fee within sixty days of the date of the invoice; or
    d. upon discovering any material error or omission in the information that the Direct Secure Messaging User provided during the Subscription process.

2. To suspend a Direct Secure Messaging User, DC-HIE will de-activate the id and password that the Direct Secure Messaging User uses to access the DC-HIE Direct Messaging Service.

3. DC-HIE will provide notice of the suspension by email to a suspended Direct Secure Messaging User as soon as possible. Such notice will contain an explanation of the reason(s) that the User was suspended.

4. The DC-HIE Direct User will have ten (10) business days in which to respond to the notice of suspension by providing DC-HIE with a plan of correction to address the reason(s) for the suspension.

    a. If the DC-HIE Direct Secure Messaging User fails to provide DC-HIE with a plan of correction, DC-HIE will terminate the DC-HIE Direct User.
    b. If the DC-HIE Direct User provided DC-HIE with a plan of correction, DC-HIE will have ten (10) business days in which to notify the DC-HIE Direct User whether the plan of correction is acceptable. If the plan of correction is not acceptable, then DC-HIE will inform the DC-HIE Direct User of the defects in the plan.

5. If, in DC-HIE's opinion, the reason(s) leading to the suspension of the DC-HIE Direct User is addressed, DC-HIE will re-activate the id of the DC-HIE Direct User and issue such

User a new, temporary password. The DC-HIE Direct User will then use the temporary password to access to the DC-HIE Direct Messaging Service and change his password in accordance with the Password Management Policy (HS-11).

Termination Procedures for Direct Secure Messaging Users

1. In accordance with the DC-HIE Direct Secure Messaging Subscription Agreement, DC-HIE can terminate a DC-HIE Direct User under the following circumstances:

    a. The DC-HIE Direct User's license, certificate or registration to practice his/her health care profession in the District of Columbia is suspended or revoked or otherwise terminated;
    b. The DC-HIE Direct User violates any provision of the DC-HIE Direct Secure Messaging Subscription Agreement or any DC-HIE Policy and Procedure and the violation is so serious that suspension is not an appropriate response;
    c. Upon discovering any material error or omission in the information that the DC-HIE Direct User provided during the Subscription process that is so serious that suspension is not an appropriate response;
    d. The DC-HIE Direct User fails to pay his/her membership fee within ninety days of the date of the invoice; or
    e. The DC-HIE Direct User has, in the opinion of DC-HIE, failed to adequately address the reason(s) leading to a suspension of the DC-HIE Direct User in accordance with the DC-HIE Direct Messaging End User License Agreement and this Policy.
    f. Uncured breach of the DC HIE Direct Secure Messaging Subscription Agreement
    g. Parties each have the right to terminate the Subscriber's use of Direct Secure Messaging without cause, with at least thirty (30) days prior written notice.
    h. Parties may terminate the DC HIE Direct Secure Messaging Subscription 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.
    i. Subject to restrictions imposed by law, the Parties may terminate use of DC HIE Direct Secure Messaging 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.
    j. DC HIE may immediately terminate the Subscriber's use of DC HIE Direct Secure Messaging 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.

2. To terminate a DC-HIE Direct User, DC-HIE will:

    a. De-activate the ID and password that the DC-HIE Direct User uses to access the DC-HIE Direct Messaging Service; and
    b. Revoke the certificate issued to the DC-HIE Direct User.

3. DC-HIE will provide notice of termination to a terminated DC-HIE Direct User as soon as possible.

Responsibility: DC-HIE; DC-HIE Direct Users

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-10**
Title: **DC-HIE Direct Secure Messaging Training**	Version: **1**	Effective Date:

Purpose Statement: DC HIE will provide, at no additional cost, web-based training information to Direct Secure Messaging users to optimize their experience and help to ensure that users will safeguard ePHI exchanged through DC HIE.

Policy/Procedure:

1. DC HIE will provide training to DC HIE users to teach them how to use Direct Secure Messaging and the DC HIE.

2. As part of the training, DC HIE will provide information on methods to protect the confidentiality and integrity of ePHI.

Responsibility: DC HIE

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-11**
Title: **DC-HIE Direct Messaging Service Log-in and Log-off**	Version: **1**	Effective Date:

Purpose Statement: To regularly track the identification and authentication of those accessing Direct Secure Messaging**,** DC-HIE will monitor log-in attempts to the DC-HIE Direct Secure Messaging Service. DC-HIE will also enhance the security of DC-HIE Direct Messaging by automatically logging-off inactive DC-HIE Direct Users from the DC-HIE Direct Messaging Service.

Policy/Procedure:

Unique User IDs

1. DC-HIE will control access to Direct Secure Messaging by assigning each Direct Secure Messaging User who is granted access to DC-HIE Direct Messaging a unique user ID that:

    a. Identifies the individual; and
    b. Permits activities performed on Direct Secure Messaging to be traced to the individual.

2. User IDs may consist of, but are not limited to:

    a. DC-HIE Direct User's name
    b. Organization

Log-In Procedures

1. A Direct Secure Messaging Subscriber/User may only access the Direct Secure Messaging Service after successfully entering his/her User ID, password. This process allows DC-HIE to verify the identity the DC-HIE Direct User.

2. After five (5) consecutive, unsuccessful attempts to log-on to the Direct Secure Messaging Service, the DC-HIE Direct User's password will be disabled. All such events will be logged as part of the monthly activity report pursuant to the DC-HIE Direct Messaging Auditing and Monitoring Policy (DC-DSM-7).

3. If a DC-HIE Direct User's password is disabled due to unsuccessful log-on attempts, the DC-HIE Direct User should contact the DC HIE Technical Administrator at 202-442-4623.

4. DC HIE will verify the Direct Secure Messaging User's identity and determine whether the User's access to Direct Secure Messaging Service was disabled because of consecutive, unsuccessful attempts to log-on or by DC-HIE for another reason.

5. After verifying the DC-HIE Direct User's identity and that such User's access was disabled because of unsuccessful log-on attempts, DC HIE will issue the DC-HIE Direct Secure User a new, temporary password. The DC-HIE Direct User will then use the temporary password to log-on to the DC-HIE Direct Messaging Service and re-set his or her own individual password in accordance with the Password Management Policy (HS-11).

Automatic Log-Off

1. A DC-HIE Direct User will be automatically logged-off of the DC-HIE Direct Messaging Service after 30 minutes of inactivity.

2. To activate a new session, a DC-HIE Direct User will have to log-on to the DC-HIE Direct Messaging Service using his or her user name, password and second method of authentication.

Responsibility: Security Officer; DC-HIE Direct User; Technical Administrator

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-12**
Title: **DC-HIE Direct Messaging Password Management**	Version: **1**	Effective Date:

Purpose Statement: To prevent unauthorized access to and use of Direct Secure Messaging, DC-HIE requires Direct Secure Messaging Subscribers/Users to take appropriate measures to select and secure passwords that allow such access to DC-HIE Direct Messaging.

Policy/Procedure:

1. All Direct Secure Messaging Users will select a user name and password that will allow them to access Direct Secure Messaging.

2. When a DC-HIE Direct User or Workforce Member logs-on to the DC-HIE Direct Messaging Service for the first time, he/she will be prompted to change the initial, temporary password provided to him/her by DC-HIE.

3. All passwords must comply with the Password Management Policy (HS-11).

Responsibility: DC-HIE Direct Users

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-13**
Title: **Deletion of DC-HIE Direct Messages**	Version: **1**	Effective Date:

Purpose Statement: DC-HIE allows Direct Secure Messaging Users to retain messages that they receive through Direct Secure Messaging in their Direct Inbox. For proper system administration and management, DC-HIE's technology vendor (HISP) contractor may periodically limit the aggregate size of a Subscriber/User's Inbox.

Policy/Procedure:

1. A DC-HIE Direct User will be able to delete a message that he/she has received in the DC-HIE Direct Messaging Service. DC-HIE Direct Users are encouraged to delete messages after the message has been read and either printed or downloaded for the User's records.

2. DC-HIE's technology vendor may automatically delete messages from a DC-HIE Direct Secure Messaging Subscriber's Inbox if the receiving Subscriber has read the message and the message is more than 90 days old. DC HIE's technology vendor will retain messages (not attachments) in its systems for one (1) year and it allows for backup and archiving of messages for ten (10) years.

3. DC-HIE's technology vendor will monitor the number and size of messages retained by each Direct Secure Messaging Subscriber/User. If the technology vendor finds that the number or size of messages retained are excessive, the vendor may contact such User to request that he/she delete his/her messages.

Responsibility: DC-HIE; DC-HIE Direct User

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-14**
Title: **DC-HIE Direct Messaging Encryption and Decryption**	Version: **1**	Effective Date:

Purpose Statement: To ensure the confidentiality, integrity, and availability of ePHI, DC-HIE's technology vendor has implemented technical security measures, including encryption, to guard against unauthorized access to ePHI while it is transmitted through DC-HIE Direct Messaging.

Policy/Procedure

1. DC-HIE's technology vendor will encrypt the content of all messages sent by a DC-HIE Direct User through DC-HIE Direct Messaging.

2. The content of the message will be encrypted using industry standard message encryption mechanisms and Secure Socket Layer (SSL) communications.

3. The subject line information in a message will be encrypted.

4. DC-HIE will decrypt the content of the message for the Direct Secure Messaging User receiving the message.

5. DC-HIE and its Vendor(s), to the extent applicable, will:

    a. Protect its cryptographic keys against modification and destruction, and protect its private keys against unauthorized disclosure.
    b. Manage the cryptographic keys used to encrypt ePHI exchanged through DC-HIE Direct Messaging.
    c. Periodically determine activation and deactivation dates for its cryptographic keys.

Responsibility: DC-HIE; Direct Secure Messaging Users; Vendors

DC-HIE	Operational Policy for DC-HIE Direct Messaging	Policy No: **DC-DSM-15**
Title: **Restriction on Disclosure of Sensitive Information**	Version: **1**	Effective Date:

Purpose Statement: DC HIE recognizes that certain information is given additional protections under federal and DC laws. Such information must comply with the use, disclosure, and confidentiality requirements set forth by applicable federal and DC laws.

Policy/Procedure:

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 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:

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

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

   i. The patient has given written consent to the person seeking access for the release of the records for a specific use; or
   ii. 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.

c. 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.

Responsibility: DC HIE Direct Secure Messaging Users, DC HIE
Regulatory Reference:

- DC Code § 44-211