DEPARTMENT OF HEALTH CARE FINANCE

NOTICE OF FINAL RULEMAKING

The Director of the Department of Health Care Finance ("DHCF"), pursuant to the authority set forth in Section 6(6) of the Department of Health Care Finance Establishment Act of 2007 ("Establishment Act"), effective February 27, 2008 (D.C. Law 17-109; D.C. Official Code § 7-771.05(6) (2018 Repl.)), hereby gives notice of the adoption of a new Chapter 87 (District of Columbia Health Information Exchange) of Title 29 (Public Welfare) of the District of Columbia Municipal Regulations ("DCMR").

As set forth in Section 4 of the Establishment Act (D.C. Official Code § 7-771.03(2)) (2018 Repl.)), DHCF was established with the purpose of developing a comprehensive, efficient, and cost-effective health-care system for the District's uninsured, under-insured, and low-income residents. Further, as set forth in Section 8 of the Establishment Act (D.C. Official Code § 7-771.07(8) (2018 Repl.)), DHCF's duties include the development and maintenance of comprehensive information-technology infrastructure that accurately and efficiently processes claims, interfaces with other necessary public, private, and nonprofit information-technology systems, and collects information for data analysis of trending, cost measurement, performance management, policy development, and strategic planning.

DHCF leads the District's health information technology ("HIT") and health information exchange ("HIE") policy development effort and serves as the State Health IT Coordinator for the District. In its capacity as the State Health IT Coordinator, DHCF fulfills several complementary roles: DHCF administers the Medicaid Electronic Health Record Incentive Program; DHCF facilitates federal and local funding to support health IT projects that directly support Medicaid providers while building infrastructure to serve all District residents; DHCF develops health IT strategies for the District that are responsive to the complex health care needs of a diverse population; and DHCF coordinates ongoing, District-wide public input through the DC HIE Policy Board and stakeholder outreach activities.

The effective use of health information, especially when exchanged among organizations via HIE, is a fundamental component of DHCF's short term and long term health system reform efforts and a vital component of efficient health care delivery. At the recommendation of the DC HIE Policy Board and the State Innovation Model HIE Workgroup, the District committed to undertake several initiatives aimed at bolstering the District's HIE capacities in the District's 2016 State Health Innovation Plan. Among those initiatives was DHCF's commitment to the creation of a District-wide HIE and the development of thresholds and standards for participation in that exchange.

To meet its commitment to the promotion of HIE in the District and in accordance with the purposes and duties set forth under the Establishment Act, DHCF is proposing regulations to establish the District of Columbia Health Information Exchange ("DC HIE"), govern the registration and designation of HIE entities in the District of Columbia, and set out guidance to regulate the efficient and secure transmission of health information according to nationally

recognized standards. The Health Information Technology for Economic and Clinical Health Act (Pub. L. No. 111-5, Title XIII, 123 Stat. 226 (2009)), guides the establishment of the DC HIE.

The DC HIE is proposed as a statewide, interoperable system of registered and designated HIE entities. Under the proposed framework, HIE entities operating in the District are eligible to apply for registration and designation by DHCF. Registered and designated HIE entities will work collaboratively within the DC HIE framework to facilitate person-centered care through the secure electronic exchange of health information among participating organizations. Registered and designated HIE entities participating in the DC HIE will work with DHCF to implement the District's health information exchange initiatives as outlined under the District's State Medicaid Health Information Technology Plan ("SMHP") in support of a District-wide health data infrastructure and service.

An initial Notice of Proposed Rulemaking was published in the *D.C. Register* on December 14, 2018, at 65 DCR 013545. One (1) set of comments was received from the Kaiser Foundation Health Plan of Mid-Atlantic States (KP). DHCF carefully considered all comments received and made some technical changes in response to the comments received, as outlined below.

Protected Health Information

KP recommended a number of amendments to Section 8703 to indicate that Section 8703 governs "protected health information," which is individually identifiable, rather than all health information even if it is not identifiable. KP added that aggregated information that is not identifiable should not be unnecessarily limited in its ability to be shared beyond existing law. DHCF agrees and is proposing technical corrections to the title of the Section and Subsections 8703.1 through 8703.4 and a corresponding amendment to the cross reference in Subsection 8707.2(c) to clarify intent.

Authentication Protocols

To assure that only authorized users access, use, or disclose PHI through or from a registered HIE entity, Subsection 8703.5 requires registered HIE entities use and ensure that participating organizations are using authentication methodology that meets minimum requirements set forth in the latest version National Institute of Standards and Technology ("NIST"), Special Publication 800-63. NIST publication 800-63 identifies four levels of authentication. KP stated that the rule could be interpreted to require registered HIE entities adhere to the requirements of NIST Level 1, which does not require identity proofing. KP recommended that the rulemaking clearly require adherence to the requirements of NIST Level 2, which requires single-factor authentication.

DHCF agrees that the reference to "minimum technical requirements" in Subsection 8703.5 creates potential ambiguity. NIST Level 2 requirements referenced by KP are currently the industry standard and the standard to which DHCF will require registered HIE entities to adhere. However, NIST guidance may be updated in the future and industry standards for user authentication will continue to evolve. In order to ensure registered HIE entities take affirmative steps to keep pace with evolving standards, DHCF will publish guidance on its website that

identifies the minimum technical requirements that registered HIE entities should use and ensure are in use by its participating organizations. DHCF is proposing a technical amendment to Subsections 8703.5 and 8703.6 to clarify its intent to maintain guidance on NIST minimum technical authentication requirements on its website.

Termination of Authorized Users

Subsection 8703.8 sets forth requirements for registered HIE entities with regard to the termination of an authorized user's access to PHI disclosed through the HIE entity. KP commented that the thirty (30) day timeframe established in Subsection 8703.8 is an inordinate amount of time to terminate access to PHI, particularly if the individual has been identified as a security risk. KP recommended that DHCF require "prompt" termination of access to PHI; aligning with the requirements of Subsection 8703.6.

The thirty (30) day timeframe set forth in Subsection 8703.8 is proposed as a maximum threshold. However, DHCF expects registered HIE entities to quickly address any potential threat to the security of PHI. DHCF is proposing technical amendments to Subsection 8703.8 to require prompt termination of access to PHI, no later than thirty (30) days, to users identified in in Subsection 8703.8.

Privacy Breach and Non-HIPAA Violation

In the initial Notice of Proposed Rulemaking, a non-HIPAA violation is defined as an inappropriate use, access, maintenance, or disclosure of health information that is not a HIPAA violation, but is inconsistent with State or federal law. KP offers that the definition of non-HIPAA violation is vague. KP stated that the proposed definition would find a "non-HIPAA violation" for acts that are "inconsistent" with other non-specified laws, whether or not that amounts to a violation of those laws. To clarify the standard, KP recommended removing references to non-HIPAA violations and expanding the definition of "privacy breach" to include access, use, or disclosure of health information in a manner not permitted by under HIPAA or other privacy laws.

In a related comment, KP stated that DHCF regulations should not include restatements of federal law and DHCF should limit potentially confusing cross references to federal notice requirements. KP offered that the rulemaking should focus on stating District requirements specific to exchange of information through an HIE entity. KP recommended removal of Subsections 8706.1 and 8706.2 and recommended minor edits to Subsections 8706.3, 8706.5 - 8706.6, 8705.5 – 8705.6, and 8709.6 to incorporate "privacy breach," as defined above, into the rule.

DHCF distinguishes breaches and non-HIPAA violations to achieve clarity between federal HIPAA requirements and the requirements of this Chapter. DHCF agrees, that as drafted the definition of non-HIPAA violation creates potential ambiguity. DHCF is proposing technical amendments to the definition of non-HIPAA violation to clarify that a non-HIPAA violation includes the acquisition, access, use, maintenance, or disclosure of health information in a manner not permitted under District or federal law. DHCF is not adopting the offered term

"privacy breach," as defined above. Therefore, DHCF is not proposing further amendments to Subsections 8706.1 - 8706.3, 8706.5 -8706.6, 8705.5 – 8705.6, and 8709.6 at this time.

Notice to Health Care Consumers

Subsection 8707.2 sets forth requirements for participating organizations to notify health care consumers no later than the first medical encounter following enrollment of the organization in a registered HIE entity. To ensure that a participating organization can use their website or mobile applications to more broadly reach health care consumers, KP recommended amendments to Subsection 8707.2 to include electronic notice.

Written notice to health care consumers does not preclude the use of electronic means. DHCF's goal and the intent of Subsection 8707.2 is to ensure that organizations take affirmative steps to inform health care consumers of their participation with HIE entities. DHCF expects that participating organizations will use available online and electronic resources to deliver notice to health care consumers. Therefore, DHCF is not recommending amendments at this time.

Further, KP stated that Subsection 8702.2(a) will ultimately require many provider organizations modify their Notice of Privacy Practices (NPP) to specifically identify the HIE entities, with which, the provider organization participates. KP reasoned that Subsection 8707.2(a) will place an undue burden on participating organizations and prefers that participating organization have the ability to maintain a generic reference in their NPPs that indicates the organization's participation in one or more HIE networks.

Health care consumers need information in order to make informed choices about their care. A generic reference to participation with one or more registered HIE entities will not convey important information. To preserve a health care consumers ability to opt out of participation with individual or all HIE entities, the consumer will need to know which specific HIE entities are exchanging their information.

DHCF understand that HIE entities create their own procedures and there will be variation in NPPs across participating organizations. DHCF is proposing technical amendments to Subsection 8707.2(a) to clarify that DHCF will provide further policy guidance on NPPs on its website to assist HIE entities and participating organizations with regard to providing this information to health care consumers.

Opt Out

Subsection 8710.1(b) requires designated HIE entities and their participating organizations to take affirmative steps to ensure consumers have the ability to opt out of participation in health information exchange. KP requested an amendment to clarify that consumers have the right to opt out of having their PHI through an HIE, not the ability to have their information otherwise disclosed in accordance with applicable law. As set forth in Subsection 8710.1(b), the ability to opt out of health information exchange is not absolute and exceptions are outlined in Subsection 8710.2. DHCF is proposing a technical amendment to 8710.1(b) to clarify that consumers can refuse access to PHI disclosed through an HIE entity.

Further, KP requested amendment to Subsection 8710.2(d) to specifically identify reports and queries needed to comply with prescription drug monitoring programs. DHCF believes that the exceptions identified in Subsection 8710.2 are sufficiently broad and would include any mandatory reporting required under District or federal law. DHCF does not intend for the requirements of these Subsections to interfere with consumer consent or provider disclosure requirements otherwise set forth in District or federal law. For these reasons, DHCF is not proposing further amendments at this time.

Health Information Exchange and HIE Entities

KP commented that the definition of "Health Information Exchange" and "HIE entity" are confusing and potentially inconsistent with the proposed structure that an HIE is a system of health data infrastructure to facilitate exchange, and HIE entity is an organization that maintains such a system. Further, KP recommended minor changes to the definitions of "authorized user" and "participating organization" to clarify references to HIE versus HIE entities.

The definitions for "health information exchange" and "HIE Entity" were developed in collaboration with the DC HIE Policy Board with input from other industry stakeholders. The definitions are reflective of this deliberative process and align with the conceptual framework set forth in this Chapter. Therefore, DHCF is not proposing substantive amendments to these definitions at this time. DHCF agrees with the KP's recommended edits to "authorized user" and participating organization" and is proposing technical corrections to Section 8799 to clarify the meaning of these terms consistent with KP's recommendations.

Defining Key Terms

KP commented that the definition of "disclosure" is overly broad and could be interpreted to include an HIE entity's or participating organization's acknowledgment that a medical record on a particular health care consumer or recipient exists. KP reasoned that this broad definition would allow a patient to opt out of having the very existence of a medical record disclosed through an HIE entity. KP proposed that the definition of disclosure limit the inclusion of acknowledgment of the existence of a medical record to only those records subject to the requirements of 42 CFR Part 2. A health care consumer's ability to opt out of health information exchange is limited and exceptions are identified in Subsection 8710.2. DHCF believes exceptions in Subsection 8710.2 are sufficiently broad to address these concerns without making substantive changes to the definition of "disclosure."

KP recommended use of consistent terms inside the definitions of key items, suggesting that DHCF use "health information" or "protected health information" and remove references to the undefined term "health-related information" within the definition section. DHCF agrees and is proposing technical corrections to Section 8799 in accordance with KP's recommendation.

Finally, KP commented that DHCF should only define terms that are used elsewhere in the regulation. The term "registered agent" is defined but not otherwise used. DHCF agrees and is

proposing a technical correction to identify the term "registered resident agent," as it appears in Subsection 8702.2(i).

These rules were adopted as final on July 10, 2019, and shall become effective upon publication in the *D.C. Register*.

A new Chapter 87, DISTRICT OF COLUMBIA HEALTH INFORMATION EXCHANGE, of Title 29 DCMR, PUBLIC WELFARE, is added to read as follows:

CHAPTER 87 DISTRICT OF COLUMBIA HEALTH INFORMATION EXCHANGE

8700 GENERAL PROVISIONS

8700.1 This chapter governs the establishment of the District of Columbia's Health Information Exchange ("HIE"), the registration and designation of HIE entities in the District by the Department of Health Care Finance ("DHCF") that opt to participate in the DC HIE and sets forth requirements to maintain the privacy and security of health information exchanged by a registered or designated HIE entity.

8700.2 This chapter sets forth requirements for participation in the DC HIE by registered and designated HIE entities, in order to:

(a) Ensure the privacy and security of protected health information ("PHI")

accessed, used, or disclosed through a registered or designated HIE entity, including protections for the Secondary Use of PHI obtained, accessed, or released through a registered or designated HIE entity;

(b) Govern the access, use, maintenance, and disclosure of PHI through or by a registered or designated HIE entity;

(c) Improve access to clinical records by treating providers and participating organizations in the District;

(d) Promote interoperable exchange of health information;

(e) Ensure registered and designated HIE entities in the District adhere to District requirements and nationally recognized operating standards; and

(f) Govern the DC HIE infrastructure and consumer services developed for implementation by registered and designated HIE entities participating in the DC HIE.

8700.3 DHCF shall provide ongoing monitoring to ensure compliance with criteria for registration and designation of HIE entities in a manner consistent with this chapter.

8700.4 Registered and designated HIE entities are subject to the following requirements:

(a) The Health Insurance Portability and Accountability Act of 1996, including all pertinent regulations (45 CFR Parts 160 and 164) issued by the U.S. Department of Health and Human Services, as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), (Pub. L. No. 111-5, Title XIII, 123 Stat. 226 (2009));

(b) The Health Breach Notification Rule, 16 CFR Part 318, adopted by the Federal Trade Commission pursuant to the HITECH Act;

(c) The District's "Consumer Protection Procedures Act," effective July 22, 1976 (D.C. Law 1-76; D.C. Official Code §§ 28-3901 *et seq.*);

(d) Federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records under 42 CFR Part 2;

(e) The District's "Mental Health Information Act of 1978," effective March 3, 1979 (D.C. Law 2-136; D.C. Official Code §§ 7-1201.01 *et seq.*); and

(f) All other applicable District and federal laws and regulations governing the use, access, maintenance, and disclosure of health information.

8701 THE DISTRICT OF COLUMBIA'S HEALTH INFORMATION EXCHANGE (DC HIE)

8701.1 The DC HIE shall be a privately-operated interoperable system of registered and designated HIE entities that facilitates person-centered care through the secure electronic exchange of health information among participating organizations in support of a District-wide health data infrastructure.

8701.2 DHCF shall provide governance and oversight of the DC HIE to enable the secure and efficient exchange of health information, as well as implement the District's health information exchange initiatives as outlined under the District's State Medicaid Health Information Technology Plan and otherwise set forth by DHCF.

8701.3 DHCF may issue grants, contracts, or agreements to design, develop, implement or maintain shared HIE infrastructure and consumer services for the DC HIE in accordance with the HITECH Act, Chapter 18 (Health Care Benefit Grants) of Title 29 (Public Welfare) of the District of Columbia Municipal Regulations, the Procurement Practices Reform Act of 2010, effective April 8, 2011 (D.C. Law 18-371; D.C. Official Code §§ 2–351.00 *et seq.*) and the Grant Administration Act of 2013, effective December 24, 2013 (D.C. Law 20-61; D.C. Official Code §§ 1-328.11 *et seq.*), as amended by the Grant Administration Amendment Act of 2015, effective October 22, 2015 (D.C. Law 21-36; 62 DCR 10905 (August 14, 2015)).

8702 HIE REGISTRATION REQUIREMENTS AND APPLICATION

8702.1 An HIE entity wishing to participate in the DC HIE must apply for registration in a form and manner consistent with this section and policy guidance provided by DHCF. Application materials and guidance will be published by DHCF on its website at www.dhcf.dc.gov.

8702.2 HIE entities applying for registration shall comply with the requirements of the chapter and demonstrate they meet the following minimum criteria:

(a) The HIE entity or its managing business organization, is a business organization established under District or applicable state laws;

(b) The HIE entity or its managing business organization maintains a general business liability insurance and cyber liability insurance for the operation of the HIE entity;

(c) The HIE entity maintains a professional staff responsible to a governing body that has the capacity to ensure accountability to the organization's mission;

(d) The HIE entity can query health care consumer information in accordance with the requirements for accessing, using or disclosing health information through an HIE set forth under this chapter;

(e) The HIE entity submits the results of its latest third-party privacy and security audit;

(f) The HIE entity submits a policy that ensures reasonable notice will be provided to its participating organizations if the HIE entity ceases its operations or dissolves its services in the District of Columbia. The HIE entity's policy submission shall be consistent with requirements set forth in guidance provided by DHCF and published on DHCF's website at www.dhcf.dc.gov;

(g) The HIE entity shall provide a report for each of the past three (3) years, from a third-party auditor which shows no expression of doubt to the entity's ability to continue as a going concern and resulting in an unqualified opinion with regard to the HIE entity's financial statements;

(h) The HIE entity attests that no disciplinary actions were taken by federal, District, or state agencies against the entity, its principals, or officers in the two (2) years prior to applying for registration;

(i) If the HIE entity is not domiciled in the District of Columbia, the HIE entity shall provide the contact information of registered resident agent who shall accept service in the District of Columbia on behalf of the HIE entity;

(j) The HIE entity provides DHCF with a copy of its user access control policy;

(k) The HIE entity provides DHCF with a copy of its Notice of Privacy Practices and consumer opt-out form;

(l) The HIE entity submits its Incident Response Plan to DHCF;

(m) At the time of application, an HIE entity operating in the District of Columbia that applies for registration, shall meet or exceed the access, use, and disclosure requirements set forth in this chapter; and

(n) The HIE entity complies with any other requirements or requests for information made by DHCF, either directly or through policy guidance published on its website at www.dhcf.dc.gov.

8702.3 DHCF retains the right to waive certain application requirements or exempt an HIE entity from certain application requirements set forth in § 8702.2 in

accordance with the provisions set forth in § 8712.

8702.4 Within ninety (90) calendar days after receipt of complete information from an applicant seeking to register as an HIE entity in the District of Columbia, DHCF shall take one of the following actions:

(a) Approve the registration application;

(b) Deny the registration application for failure to meet requirements for registration set forth in § 8702.2 to the applicant in writing; or

(c) Request additional information from the applicant, in writing, to determine an HIE entity's eligibility for registration.

8702.5 HIE entities that are denied registration, in accordance with § 8702.4, shall have the opportunity to appeal DHCF's determination in accordance with the procedure for appeals and administrative review as set forth in § 8713.

8702.6 As a condition of participation in the DC HIE, registered HIE entities shall:

(a) Submit operational information, as requested by DHCF.

(b) Comply with requirements for participation in the DC HIE set forth in this chapter or established by DHCF in policy guidance published on its website at www.dhcf.dc.gov.

8702.7 An HIE entity's registration shall be awarded in three (3) year terms. DHCF shall review an HIE entity's registration every three (3) years from the date of registration in accordance with requirements in § 8702.8 to determine whether the entity will be renewed for an additional three (3) year term.

8702.8 In order to renew their registration HIE entities must demonstrate continued compliance with § 8702 by providing the following information in a form and manner specified by DHCF:

(a) Any changes to information submitted with regard to the items set forth in § 8702.2 that affect the veracity of a prior submission;

(b) Results of a scheduled audit performed in compliance with § 8704; and

(c) Documentation of compliance with additional requirements as set forth by DHCF in policy guidance.

8703 REGISTERED HIE ENTITY PROTECTED HEALTH INFORMATION ACCESS, USE, AND DISCLOSURE REQUIREMENTS

8703.1 A registered HIE entity shall only disclose PHI for an authorized purpose, as set forth in §§ 8703.2 and 8703.3.

8703.2 An authorized user may use, access, or disclose PHI for Primary Use. Primary Use of PHI is the use, access, and disclosure of data through or by a registered HIE entity for the purpose of:

(a) Treatment;

(b) Payment of claims and billing;

(c) Health care operations for conducting case management, conduct of quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that obtaining generalized knowledge is not the primary purpose of any studies resulting from such activities;

(d) Reporting to public health authorities in compliance with reporting requirements; or

(e) Other uses or disclosures required by District or federal law.

8703.3 A registered HIE entity shall only disclose PHI for a Primary Use in accordance with the requirements below:

(a) The disclosure shall only be to an authorized user for the specific purpose for which that authorized user is given access to the HIE; and

(b) All disclosures shall be in full compliance with this chapter, federal and District requirements indicated in § 8700.4.

8703.4 Secondary Use of health information is the use, access, or disclosure of health information through the registered HIE entity that is not for a Primary Use; subject to any limitations under HIPAA or federal law. A registered HIE entity shall provide DHCF with policies governing disclosure for Secondary Use in accordance with policy guidance published to the DHCF website.

8703.5 To assure that only an authorized user accesses, uses, or discloses PHI through or from a registered HIE entity, a registered HIE entity shall:

(a) Use and ensure that its participating organizations are using an authentication methodology that meets the minimum technical requirements set forth in the latest edition of the National Institute of

Standards and Technology ("NIST"), Special Publication 800-63. DHCF shall maintain additional information on minimum technical requirements in policy guidance published to the DHCF website; and

(b) Take appropriate actions to mitigate the risk of unauthorized use, access, or disclosure of PHI when the registered HIE entity learns or has reason to believe that a participating organization's system or third-party system is not compliant with NIST guidelines, as set forth in guidance published to the DHCF website. Appropriate actions include but are not limited to ceasing acceptance of the system's authentication of authorized users until the system demonstrates compliance with NIST guidelines to the satisfaction of the registered HIE entity.

8703.6 To assure that only an authorized user accesses, uses, or discloses PHI through or from a registered HIE entity, a registered HIE entity shall ensure that its enrolled participating organizations comply with all of the following requirements:

(a) Appoint a system administrator who is capable of carrying out the requirements set forth in § 8703.5 on behalf of the participating organization prior to exchanging any PHI;

(b) Promptly inform the registered HIE entity system administrator of any circumstances that require termination of an authorized users access as described under § 8703.8;

(c) Ensure that any third-party system it uses authenticates an authorized user in accordance with NIST guidelines, as set forth in guidance published to the DHCF website, prior to allowing that person's access to the HIE through the third-party system; and

(d) Inform the registered HIE entity concerning the following:

(1) The appointment of the system administrator, or any change in such an appointment, within a timely manner of any such appointment or change;

(2) A breach, as defined in 45 CFR § 164.402, or non-HIPAA violation by a person who had or has access to the HIE through the participating organization; or

(3) Any unusual finding, act, or event that it has a basis to believe is or may be a violation of this chapter.

8703.7 A registered HIE entity shall require that the participating organization's system administrator carries out each of the following measures on behalf of the participating organization:

(a) Identify each authorized user within the participating organization and note the user's assigned unique user name in accordance with the most recent applicable guidelines issued by NIST, or other nationally recognized standards identified by DHCF in policy guidance published to its website at www.dhcf.dc.gov;

(b) Coordinate with the registered HIE entity to determine a methodology for assigning each authorized user access to PHI;

(c) Assign to each authorized user an access level that appropriately corresponds to that person's role within the participating organization and the permitted access to PHI;

(d) Modify, in a timely manner, an authorized user's access level as appropriate to reflect any change in that user's role within the participating organization;

(e) Immediately inform the registered HIE entity of changes in an authorized user's role within the participating organization; and

(f) Confirm to the registered HIE entity the appropriateness of a staff member to be an authorized user and that the HIE access level assigned to that staff member corresponds to the authorized user's role within the participating organization.

8703.8 The registered HIE entity shall promptly, but no later than thirty (30) calendar days, terminate access to PHI by any authorized user:

(a) Who is suspended by the participating organization;

(b) Who is no longer associated with the participating organization; or

(c) Who no longer requires access to the PHI.

8703.9 To mitigate the risks of improper access or disclosure of electronic PHI the registered HIE entity shall undergo annual assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI conducted in accordance with guidance published on the DHCF website. The registered HIE entity shall provide the DHCF Privacy and Security Officer with a copy of their risk assessment on an annual basis.

8703.10 Based on the findings of the assessment conducted in accordance with § 8703.9, the registered HIE entity shall implement security measures to reduce risks and vulnerabilities to:

(a) Protect against anticipated threats to the security or integrity of PHI; and

(b) Protect against any unauthorized uses or disclosures of such PHI in accordance with applicable District or federal laws.

8704 AUDITING REQUIREMENTS FOR REGISTERED HIE ENTITIES

8704.1 In order to ensure that only an authorized user, who is appropriately authenticated, is granted access and has access to health information, a registered HIE entity shall:

(a) Develop and implement protocols, methodologies, and a monitoring approach designed to discover any unusual finding, which may be identified within an audit of the user access logs, including conducting ongoing electronic monitoring of user access logs and investigate any unusual findings in accordance with this chapter;

(b) Conduct each audit under this section in accordance with nationally recognized standards and methodologies as identified by DHCF in policy guidance published on its website at www.dhcf.dc.gov;

(c) Conduct random audits of the user access logs to identify any unusual finding; and, if the registered HIE entity has been notified about an unusual finding or has reason to believe that inappropriate access has occurred;

(d) Investigate each unusual finding identified in the access log audit to determine if there has been a violation of § 8703;

(e) Resolve the matter surrounding an unusual finding by taking remedial actions under § 8705 of this chapter;

(f) Report any unusual finding to each participating organization involved in the unusual finding in a manner consistent with policy guidance set forth by DHCF and published on its website at www.dhcf.dc.gov; and

(g) Maintain an audit trail of user access logs in a retrievable storage medium in accordance with the requirements set forth below:

(1) The registered HIE entity shall perform periodic testing to ensure that the storage medium being used to maintain the user access logs shall allow the data to be recovered; and

(2) Maintenance and storage of the audit trail of user access log data shall comply with the most stringent requirements outlined in applicable District and federal requirements, including ensuring

data storage for the longest duration of time identified in applicable District and federal requirements.

8704.2 When a registered HIE entity has identified a potential violation of this chapter, the registered HIE entity shall conduct an unscheduled audit that shall:

(a) Determine whether there is a violation;

(b) Identify the size and scope of the potential violation; and

(c) Identify and complete remedial actions required under § 8705 of this chapter.

8705 REMEDIAL ACTIONS TO BE TAKEN BY A REGISTERED HIE ENTITY

8705.1 A registered HIE entity shall immediately suspend an authorized user's access when it is necessary to avoid a HIPAA privacy breach, non-HIPAA violation, or a threat to the security of health information accessed, used, or disclosed through or from a registered HIE entity.

8705.2 If the registered HIE entity determines that harm to the privacy of persons or security of health information or an ongoing risk of improper use, access, maintenance, or disclosure of PHI may occur prior to conclusion of an investigation, it shall suspend an authorized user's access pursuant to this section before an investigation is complete. Such suspension shall continue until the underlying threat to the privacy of persons or security of health information is contained.

8705.3 A registered HIE entity shall conduct an investigation in accordance with the requirements set forth below if there is reason to believe that a HIPAA breach or non-HIPAA violation has occurred:

(a) The registered HIE entity shall begin the investigation, no later than sixty (60) calendar days after learning of the allegations giving rise to a potential breach or violation;

(b) The registered HIE entity shall conduct the investigation in a thorough, timely, professional manner and take all necessary actions to gather information concerning the potential breach or violation that reflects the size and scope of such potential breach or violation;

(c) If appropriate, an investigation shall include an audit under the § 8704;

(d) Upon the completion of an investigation, a registered HIE entity shall:

(1) Make a written finding describing the results of the investigation

and provide a copy to DHCF and the District of Columbia Office of the Attorney General within thirty (30) calendar days; and

(2) Maintain records of each investigation for at least five (5) years from the date of completion of such investigation or five (5) years from the date a minor health care consumer becomes an adult, whichever is longer.

8705.4 If a registered HIE entity has a reasonable belief that a HIPAA breach or a non-HIPAA violation has occurred, as a result of an audit conducted in accordance with § 8704 or investigation conducted in accordance with § 8705.3, the registered HIE entity shall carry out the following actions within ten (10) business days after acquiring the reasonable belief unless another time period is set forth below:

(a) The registered HIE entity shall determine any remedial action necessary to address the breach or violation as described below;

(1) The registered HIE entity may require that a remedial action include steps to correct an underlying problem; and

(2) The registered HIE entity shall provide a time frame for implementing the remedial action that is consistent with policy guidance set forth by DHCF and published on its website at www.dhcf.dc.gov; and

(b) Within thirty (30) calendar days, the registered HIE entity shall provide the following to DHCF and the District-wide Privacy and Security Official to the participating organization, and to each authorized user whom the investigation indicates may have committed a breach or violation:

(1) A copy of the findings of the investigation, excluding any sensitive health information;

(2) A list of the remedial actions to be taken by each person and the associated time frame of the remedial action;

(3) A description of the actions necessary to mitigate the harm that may be caused by the breach or the non-HIPAA violation;

(4) A list of the authorized users that are responsible for carrying out the actions to mitigate harm; and

(5) A description of any future action that the HIE entity may take, including suspension, if the authorized user does not comply with the remedial action.

8705.5 Upon completion of the investigation, the registered HIE entity shall immediately suspend access for an authorized user or participating organization when available information indicates one of the following has occurred:

(a) An actual HIPAA breach;

(b) An actual non-HIPAA violation;

(c) An actual violation of District or federal law relevant to privacy or security;

(d) An authorized user or participating organization has sold health information in violation of these regulations; or

(e) An authorized user or participating organization has failed to carry out the remedial actions identified by the registered HIE entity.

8705.6 After the registered HIE entity verifies that the remedial action is complete, a registered HIE entity may reinstate a user's authorization to access information provided that the registered HIE entity modifies the authorized user's access as needed to ensure compliance with this chapter.

8706 NOTICE OF HIPAA BREACH AND NON-HIPAA VIOLATION BY A REGISTERED HIE ENTITY

8706.1 Notification of a HIPAA breach and non-HIPAA violation by a registered HIE entity shall be consistent with notification requirements under applicable federal and District laws and regulations, including HIPAA, the HITECH Act, and under 42 CFR Part 2.

8706.2 When federal or District law does not require a registered HIE entity to provide notification to a participating organization or to an affected health care consumer, or when 42 CFR Part 2 does not mandate other notification requirements, a registered HIE entity shall provide notification of a HIPAA breach and, if applicable, non-HIPAA violations in accordance to the requirements with this section.

8706.3 If an investigation under § 8705 of this chapter concluded that there was a HIPAA breach or non-HIPAA violation, in addition to applicable HIPAA notification requirements, the HIE entity shall notify:

(a) The person who notified the registered HIE entity of the potential HIPAA breach or non-HIPAA violation, if applicable, and to the extent permitted by HIPAA and other federal and District privacy laws;

(b) Any participating organization that has provided health information regarding the health care consumer involved;

(c) Each health care consumer whose PHI or sensitive health information was inappropriately accessed or disclosed due to a HIPAA breach or non-HIPAA violation; and

(d) The DHCF Privacy Officer and the District of Columbia Office of the Attorney General.

8706.4 The registered HIE entity shall include in its notification the contact information for the registered HIE entity, including the registered HIE entity's address, telephone number, website where the health care consumer can learn more information, and a description of the breach or the violation.

8706.5 A registered HIE entity, its enrolled participating organization, or its representative shall provide notification to a health care consumer following a HIPAA breach or non-HIPAA violation subject to the following requirements:

(a) If the registered HIE entity providing the notification under this Subsection has knowledge that another person is acting as the authorized representative for the health care consumer, the registered HIE entity shall provide the notification to that authorized representative instead of the health care consumer;

(b) Notice to the health care consumer required under this Subsection shall be provided in writing by first-class mail to the last known address of the health care consumer, if the health care consumer has made no prior election to method of notice;

(c) If there is insufficient or out-of-date contact information that precludes notice consistent with this chapter, a substitute form of notice shall be provided in accordance with the criteria set forth below:

(1) In the case in which there is insufficient or out-of-date contact information for fewer than ten (10) individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means; or

(2) In the case in which there is insufficient or out-of-date contact information for ten (10) or more individuals, then such substitute notice shall be posted on the home page of the registered HIE entity's website for a period of ninety (90) calendar days on the website or be conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. The notice shall include a phone number that remains

active for at least ninety (90) calendar days where a health care consumer can learn whether their health information may be included in the HIPAA breach or non-HIPAA violation;

(d) When notice about a HIPAA breach or non-HIPAA violation is required pursuant to this chapter, a registered HIE entity and its enrolled participating organization, as required, shall provide notice in writing within a reasonable time frame, but not later than sixty (60) days from the discovery of the breach or from the date that the registered HIE entity should have reasonably discovered the breach;

(e) If the HIPAA breach or non-HIPAA violation affects more than five hundred (500) health care consumers, in addition to providing individual notice to the affected health care consumers, a registered HIE entity shall provide notice to prominent media outlets serving the District without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of a breach; and

(f) If the participating organization providing the notification keeps a medical record for the health care consumer, the notification shall be placed within the health care consumer's medical record.

8706.6 A registered HIE entity, its participating organizations, or its representative shall provide notification to appropriate authorities following HIPAA breach or non-HIPAA violation as follows:

(a) Report all violations of federal or District privacy or security law to those federal or District authorities to which reporting such violation is required by applicable law; and

(b) Send a copy of such report to the DHCF Privacy Officer and the District of Columbia Office of the Attorney General.

8706.7 If DHCF is notified of a breach under § 8706.6, DHCF shall forward such notification to the District of Columbia Office of the Attorney General within thirty (30) calendar days after receipt of the notification.

8707 REGISTERED HIE ENTITY CONSUMER PARTICIPATION, ACCESS, AND EDUCATION REQUIREMENTS

8707.1 A registered HIE entity shall require its enrolled participating organization to comply with the consumer participation, access, and education requirements set forth in this section.

8707.2 A participating organization shall provide written notice to each health care consumer no later than the first medical encounter following enrollment of the

organization in a registered HIE entity, of:

(a) Such organization's participation with a registered HIE entity, including in such organization's Notice of Privacy Practices under HIPAA. DHCF will provide further policy guidance on Notice of Privacy Practices on its website at www.dhcf.dc.gov;

(b) Information concerning the health care consumer's ability to opt out from participation in the registered HIE entity and the process of opting out; and

(c) The types of information the participating organization shall disclose to the registered HIE entity and the extent that information accessed through the HIE entity may be used for treatment, payment, health care operations, and Secondary Use, as defined in § 8703.4.

8707.3 A registered HIE entity shall provide written information to health care consumers concerning the process, means, and methods of accessing their PHI as follows:

(a) If the health care consumer's PHI is directly available electronically to the health care consumer, the registered HIE entity shall advise the health care consumer how to obtain the PHI electronically; and

(b) If the health care consumer's PHI is not directly available electronically to the health care consumer, the registered HIE entity shall, within seven (7) business days of receipt of a health care consumer's written notice or request, provide the health care consumer with the contact information for each participating organization that has access to the consumer's PHI, so that the health care consumer may gain access to the health care consumer's health information directly from each participating organization.

8708 HIE DESIGNATION REQUIREMENTS AND APPLICATION

8708.1 Registered HIE entities that meet additional requirements and are selected by DHCF through a competitive application process shall become designated HIE entities. Designated HIE entities are partners with DHCF that operate or maintain DC HIE infrastructure or services in order to facilitate the secure, electronic exchange of health information among registered HIE entities and participating organizations in the District.

8708.2 To be eligible to apply for designation, an HIE entity must meet the requirements set forth below:

(a) Be a registered HIE entity;

(b) Meet or exceed the consumer education and auditing requirements as set forth in §§ 8709 and 8710; and

(c) Be organized in accordance with the District of Columbia Nonprofit Corporation Act of 2010, effective July 2, 2011 (D.C. Law 18-378; D.C. Official Code §§ 29-401.01 *et seq.*) or organized as a nonprofit corporation in the jurisdiction where the entity is incorporated.

8708.3 An HIE entity must apply for designation in a form and manner consistent with this section and policy guidance provided by DHCF. Application materials and guidance will be published by DHCF on its website at www.dhcf.dc.gov. DHCF shall accept applications for designation on a time-limited and periodic basis.

8708.4 DHCF shall provide notice of the designation application period by publishing the opening and closing dates of the period to the DHCF website at least thirty (30) calendar days before the application period begins.

8708.5 To be eligible to be selected as a designated HIE entity, registered HIE entities shall demonstrate compliance with the following requirements:

(a) Develop and submit strategic and operational plans to address the needs of health providers (including but not limited to community health providers, individual and small group practices, and public health agencies) in achieving HIE capabilities;

(b) Attest to a commitment to interoperability and connectivity with registered HIE entities in the District to allow for the proliferation of DC HIE infrastructure and services and with national health information networks, if appropriate;

(c) Demonstrate necessary technical capacity to operate and implement publicly funded DC HIE infrastructure and tools;

(d) Detail the HIE entity's approach for maintaining financial sustainability, including public and private financing strategies, projected utilization, and rate structures;

(e) Provide DHCF with a copy of the HIE entity's most recently filed Internal Revenue Service Form 990;

(f) Demonstrate accreditation by a nationally recognized accreditation and certification organization for entities that electronically exchange health care data;

(g) Attest to having a plan or process in place to provide technical assistance and guidance to the system administrator of each participating organization in assigning the appropriate access to the HIE for each of its authorized users;

(h) Provide DHCF with a copy of its access and auditing plan as defined in §§ 8709.4 through 8709.6;

(i) Provide DHCF with a copy of its consumer education plan as set forth in § 8710.4; and

(j) Provide additional information requested by DHCF or required under policy guidance provided by DHCF and published on its website at www.dhcf.dc.gov.

8708.6 HIE entities may apply for registration and designation concurrently.

8708.7 Within ninety (90) calendar days after receipt of complete information from an applicant seeking to become a designated HIE entity in the District of Columbia, DHCF shall take one of the following actions:

(a) Approve or deny the designation application in writing based on the relative strength of the application, as determined by DHCF;

(b) Deny the designation application in writing for failure to meet requirements for designation set forth in § 8708.5; or

(c) Request additional information from the applicant, in writing, to determine eligibility for designation.

8708.8 Registered HIE entities that are denied designation, in accordance with § 8708.7, shall have the opportunity to appeal DHCF's determination in accordance with the procedure for appeals and administrative review as set forth in § 8713.

8708.9 An HIE entity's designation shall be awarded in five (5) year terms. DHCF shall review an HIE entity's designation every five (5) years from the date of designation to determine whether the HIE entity will be renewed for an additional five (5) year term. DHCF may request an HIE entity submit updated information related to the requirements set forth in § 8708.5 during review of an HIE entity's designation.

8708.10 The designated HIE entity must comply with additional requirements as set forth in this chapter or otherwise established by DHCF through policy guidance published on its website at www.dhcf.dc.gov.

8708.11 A designated HIE entity must submit an annual report for review by DHCF that

addresses:

(a) Updates to the Strategic and Operational plans developed and submitted in § 8705.5(a), including plans for ensuring the necessary capacity to support clinical transactions;

(b) Rates of adoption, utilization, and transaction volume, and mechanisms to support health information exchange; and

(c) And other information as requested by DHCF.

8709 DESIGNATED HIE ENTITY AUDITING REQUIREMENTS

8709.1 A designated HIE entity shall conduct an annual privacy and security audit performed by a qualified third-party auditor, that:

(a) Detects inappropriate access, use, maintenance, and disclosure of information that are in violation of this chapter;

(b) Assesses security measures, related to the technical, physical and administrative safeguards of PHI.

8709.2 At the request of DHCF and consistent with the specifications in such request, a designated HIE entity shall:

(a) Provide the results of any audit that is required under this section, and any supporting documentation to DHCF; and

(b) Conduct an additional unscheduled audit and provide the results of such an audit to DHCF within the time frame specified by the agency.

8709.3 If a designated HIE entity's annual privacy and security audit reveals information that demonstrates inappropriate access, use, maintenance, or disclosure of information that constitutes a breach or violation of this chapter, or if the health information of more than ten (10) health care consumers was improperly used, accessed, maintained, or disclosed during the twelve (12) months prior to the audit, then:

(a) The designated HIE entity shall use the findings from the audit to:

(1) Educate and train a participating organization or an authorized user on proper access, use, and disclosure of information through or from the HIE; or

(2) Evaluate and implement new control measures, including policies, procedures, or technology, to ensure proper use and access of the

HIE;

(b) The designated HIE entity shall take the appropriate measures specified in § 8705; and

(c) The designated HIE entity shall post a publicly available summary report of the audit on its website within thirty (30) calendar days after completion of the audit and DHCF shall also post the report on its website.

8709.4 A designated HIE entity shall adopt and implement an access and auditing plan that requires the designated HIE entity and each participating organization, as applicable, to conduct a random audit of the HIE access logs on a periodic basis in accordance with the requirements set forth in §§ 8709.5 and 8709.6.

8709.5 The access and auditing plan shall prescribe responsibility for conducting random audits to either the designated HIE entity or its participating organizations according to the designated HIE entity's or participating organizations' technological capabilities.

8709.6 The access and auditing plan required under § 8709.4 shall include:

(a) The manner used to identify a non-HIPAA violation of this chapter or a HIPAA breach;

(b) The method used to report a non-HIPAA violation of this chapter or a HIPAA breach;

(c) The reasonable steps that shall be taken to promptly mitigate a non-HIPAA violation of this chapter or a HIPAA breach;

(d) A review of the designated HIE entity's access logs to ensure that only an authorized user is granted access to HIE information and is meeting the requirements of this rule; and

(e) A plan to ensure that the designated HIE entity's participating organization conduct its own audit or review of the HIE access logs within ten (10) business days of receipt of the access logs from the designated HIE entity, if the designated HIE entity chooses to hold its participating organizations responsible for implementing the plan, as per § 8709.5.

8710 DESIGNATED HIE ENTITY REQUIREMENTS TO PROMOTE CONSUMER PARTICIPATION, ACCESS, AND EDUCATION

8710.1 A designated HIE entity and its participating organizations shall take affirmative steps to ensure health care consumers have:

(a) Information regarding the health care consumer's access and participation options under these regulations is readily available to assist the health care consumer in making an informed decision concerning:

(1) The accessibility of a health care consumer's PHI electronically through a designated HIE entity; and

(2) The risks and benefits of health information exchange;

(b) The ability to opt out of health information exchange at any time and refuse access to the health care consumer's PHI through an HIE entity, except when a disclosure meets conditions identified in § 8710.2; and

(c) The ability to resume participation in an HIE entity at any point after the health care consumer has elected to opt out of participation. Any such resumption of participation shall be upon written notice or request to the designated HIE entity by the health care consumer.

8710.2 Designated HIE entity disclosures that meet one of the following criteria set forth below are not subject to consumer opt out:

(a) Information making up the designated HIE entity's or participating organization's core elements of the master patient index;

(b) A disclosure that a person is required to make under federal or State law requirements;

(c) Results of a diagnostic procedure sent to the health care provider who ordered the procedure or another provider as designated by the ordering provider;

(d) Information regarding prescription medications dispensed or filled by a pharmacy, sent to the health care provider who ordered the prescriptions or another health care provider as designated by the ordering health care provider;

(e) Public health authorities for reporting purposes required, authorized, or otherwise compliant with applicable law; or

(f) Communications permitted under HIPAA or District law without a health care consumer's consent or authorization when using point-to-point transmission.

8710.3 A designated HIE entity shall provide information about the HIE to a health care consumer whose PHI is maintained by the designated HIE entity, or may be accessed, used, or disclosed through the HIE in accordance with the requirements

set forth in §§ 8710.4 and 8710.5:

8710.4 A designated HIE entity shall make health care consumer educational materials available to participating organizations and their users. A designated HIE entity shall develop, adopt, implement, keep current, and make available to health care consumers a health care consumer education plan that includes:

(a) Definitions of the key terms and concepts underlying health information technology, including electronic health records and the exchange of electronic health information;

(b) Health information privacy and security laws;

(c) The general overview of individual benefits and risks to health care consumers of exchanging health information through an HIE entity as compared to opting- out and exchanging health information through a paper-based system; and

(d) Information on how the designated HIE entity shall make the following information available to health care consumers:

(1) A description of each type of PHI that is accessed or disclosed through the designated HIE entity;

(2) The health information maintained by the designated HIE entity;

(3) The specific details concerning who may access, use, or disclose a health care consumer's health information and for what purpose;

(4) The privacy and security measures that the designated HIE entity has implemented to protect health information, and a detailed explanation of what happens if there is a breach that results in unauthorized access to PHI;

(5) A health care consumer's access and participation options regarding health information exchange and the control over, protection of, use of, and correction of each type of health information;

(6) The process provided for a health care consumer to exercise the health care consumer's access and participation options, including a detailed description of the steps a health care consumer can to opt out of participation in health information exchange;

(7) The implications of a health care consumer's decision to opt out of participation in health information exchange and not permit the

disclosure of that consumer's PHI to authorized users, except as otherwise permitted under applicable law; and

(8) The designated HIE entity's policies and procedures, including without limitation, policies and procedures consistent with these regulations regarding how the health care consumer may gain access to the health care consumer's health information.

8710.5 The health care consumer education materials required under § 8710.4 must:

(a) Provide a balanced perspective, outlining the various points of view concerning each subject matter set forth in § 8710.4 and set forth in policy guidance by DHCF and published on its website at http://dhcf.dc.gov, including the risks and benefits associated with sharing PHI electronically;

(b) Present accurate, and not misleading information;

(c) Minimize the use of technical terms and, when such terms are necessary, clearly define the technical terms;

(d) Use plain language that is easily understandable to each health care consumer population served, taking into account the various levels of education, understanding, and interest across that population;

(e) Use text and illustrations that are culturally sensitive, language appropriate, and that recognize user diversity including ethnicity, age, race, sexual orientation, and gender;

(f) Update material to include and incorporate new information; and

(g) Specify the time sensitivity of any material included.

8710.6 A designated HIE entity shall allow a health care consumer to obtain or correct information concerning the consumer's PHI by meeting the requirements set forth below:

(a) A designated HIE entity shall provide the following information to the health care consumer, upon written notice or request by the health care consumer, describing what PHI is available through the HIE concerning the specified health care consumer:

(1) The participating organization that disclosed the PHI to the designated HIE entity;

(2) The date the PHI was disclosed to the designated HIE entity; and

(3) The type of PHI disclosed to the designated HIE entity, if known by the designated HIE entity;

(b) A designated HIE entity shall inform the health care consumer how to correct perceived inaccurate information consistent with the requirements below:

(1) A designated HIE entity shall send information regarding the process for petitioning a participating organization or provider regarding the correction of inaccurate health information within twenty (20) calendar days of receiving notice from a health care consumer of a potential inaccuracy in the health care consumer's health information available through the HIE. The information shall include the contact information of relevant participating organizations that provided the perceived inaccurate information; and

(2) This process shall be in accordance with the requirements specified under federal HIPAA requirements, including but not limited to 45 CFR § 164.526.

8710.7 Upon receipt of written notice or request, a designated HIE entity shall provide each health care consumer with a report detailing any disclosure for a time period specified by the health care consumer, of the health care consumer's PHI. In instances where a health care consumer requests recurring disclosures to the same HIE entity for the same purpose, a summary report may be provided by the designated HIE entity.

8710.8 If the health care consumer requests the details of the summary report as described in § 8710.7, the designated HIE entity shall provide the health care consumer information consistent with the requirements set forth below:

(a) The time period specified by the health care consumer shall not exceed the data retention period as specified by HIPAA and federal regulations at 45 CFR § 164.528;

(b) Except as otherwise permissible under 45 CFR § 164.528(b)(3) through (4), the report shall specify the following for each instance that the health care consumer's PHI was disclosed during the time frame reflected in the report:

(1) The name of each authorized user;

(2) The name of the participating organization to which the authorized user is affiliated, if such information is kept by the

HIE entity in the ordinary course of business;

(3) The date and time of the disclosure;

(4) The type of PHI disclosed, if known by the designated HIE entity; and

(5) The name of the participating organization that made the PHI available to the designated HIE entity.

8710.9 A designated HIE entity shall acknowledge a health care consumer's written notice or request, as described in § 8710.7, within ten (10) business days of receipt of the request.

8710.10 A designated HIE entity shall respond to a health care consumer's written notice or request, described in § 8710.7, with either the requested report or with a written explanation why such report is unavailable, when it shall be available, or where the health care consumer may obtain the requested information.

8710.11 The designated HIE entity shall respond within a reasonable time frame, but not later than thirty (30) calendar days after the initial written notice or request, as described § 8710.7, by the health care consumer:

(a) A designated HIE entity shall provide a summary report, as described in § 8710.7, upon request by the health care consumer, at least twice per calendar year at no cost to the health care consumer. If the summary report is available in an electronic format, it shall be provided to the consumer in a generally available electronic format, if so requested, at no additional charge; and

(b) For any additional report, the designated HIE entity may charge a reasonable fee not to exceed the cost to provide the additional report, but no more than the allowable amount in accordance 45 CFR § 164.524(c)(4).

8710.12 A designated HIE entity shall implement a process to manage and enable consumer choice regarding the consumer's participation in an HIE, opting out from such participation, or opting to resume participation in the HIE system, in accordance with the requirements set forth below:

(a) A designated HIE entity shall maintain a log that records each health care consumer's participation status over time in accordance with the requirements set forth in paragraphs (a)(1) and (2) below;

(1) A designated HIE entity shall retain the log for the duration required by State or federal law, whichever requires a longer

retention; and

(2) A designated HIE entity shall keep the log in a retrievable storage medium;

(b) A designated HIE entity shall not disclose a health care consumer's PHI if the health care consumer has submitted a written notice or request to opt-out of health information exchange in accordance with § 8710.1(b) except as otherwise permitted under applicable law and in accordance with this chapter; and

(c) A designated HIE entity shall not disclose information derived from a health care consumer's PHI, including for Secondary Use, if the health care consumer has submitted a written notice or request to opt-out of health information exchange, except as otherwise permitted under applicable law.

8710.13 The requirements set forth in §§ 8710.14 through 8710.19 shall apply to all communications between a designated HIE entity and a health care consumer.

8710.14 A designated HIE entity or its participating organizations shall implement a process to allow a health care consumer to communicate with a designated HIE entity about the health care consumer's participation status through an appropriate medium of the health care consumer's choice, including:

(a) By telephone, via a phone number;

(b) By mail, via a standardized form;

(c) By fax, via a standardized form;

(d) Online, via a secure website;

(e) Secure email or text message; and

(f) In-person at the designated HIE entity's offices during business hours.

8710.15 A health care consumer's communication opting out (or opting in if the consumer has already opted out) of health information exchange shall be made in:

(a) Writing;

(b) Online;

(c) Fax;

(d) Secure email or text message; or

(e) By telephone, if the designated HIE entity confirms the action with a written communication to the health care consumer in accordance with § 8710.18;

8710.16 A designated HIE entity shall take appropriate measures to assure that an individual who communicates with the designated HIE entity is authorized to act on behalf of the participating health care consumer.

8710.17 A designated HIE entity shall implement the health care consumer's requested action within five (5) business days of receipt of the health care consumer's written or online request concerning:

(a) Opting-out of the HIE; and

(b) Resuming participation in the HIE after previously opting-out.

8710.18 A designated HIE entity shall provide each health care consumer the option to receive confirmation of any change in the health care consumer's participation status. If a health care consumer requests confirmation in writing, the designated HIE entity shall:

(a) Send the confirmation of participation status change within three (3) business days of the effective date of change of the health care consumer's participation status; and

(b) If consistent with all applicable privacy and security law and regulations, including HIPAA and applicable District laws and regulations, send the confirmation of status change through one of the following methods as specified by the health care consumer:

(1) An email sent to the email address specified by the health care consumer;

(2) A letter to an address specified by the health care consumer;

(3) A letter by fax to a fax number specified by the health care consumer;

(4) A letter given to the health care consumer at the designated HIE entity during normal business hours; or

(5) A text message sent to the number specified by the health care consumer.

8710.19 When a health care consumer changes their participation status, the designated HIE entity shall provide the following to the health care consumer:

(a) Information concerning when the status change will become effective; and

(b) Information concerning what information shall be excluded from health information exchange regarding a health care consumer who opts out.

8711 OVERSIGHT AND ENFORCEMENT

8711.1 DHCF shall take enforcement actions as necessary, including the suspension or revocation of registration or designation in accordance with the requirements set forth below:

(a) When DHCF is considering suspension or revocation of an HIE entity's registration or designation as set forth in this section, all investigatory data that are collected, created, or maintained related to the suspension or revocation are classified as confidential data on persons and as protected nonpublic data; and

(b) DHCF may disclose data classified as protected nonpublic or confidential under § 8711.1 (a) if disclosing the data, as permissible under 45 CFR § 164.512(j), will protect the health, privacy, or safety of health care consumers.

8711.2 DHCF may take action as necessary to address violations of this chapter by requiring corrective action or suspending or revoking an HIE entity's registration or designation. DHCF shall notify the HIE entity in writing stating the grounds for the action taken. Notice shall include:

(a) A reference to the regulatory or statutory authority, including policy and program manuals, for the action;

(b) A description of the findings of fact regarding the violations with respect to which the action is proposed;

(c) The nature of the action;

(d) Any circumstances that were considered in determining the amount of the proposed action;

(e) Instructions for responding to the notice, including a statement of the HIE entity's ability to request administrative review; and

(f) The address to which the request for review must be sent.

8711.3 If DHCF suspends or revokes the registration or designation of a HIE entity, the HIE entity shall not, during the period of suspension or revocation, engage in any new advertising or solicitation or hold itself out as a registered or designated HIE entity.

8711.4 All suspensions of registration or designation shall be accompanied by a requirement for corrective action.

8711.5 A DHCF written request for corrective action shall include:

(a) Nature and scope of corrective action requested;

(b) Date by which corrective action must be completed by the registered or designated HIE entity; and

(c) Details on how DHCF will evaluate the registered or designated HIE entity's correction of underlying issues.

8711.6 DHCF may suspend or revoke a registration or designation issued to an HIE entity or issue a requirement for corrective action if the DHCF finds that:

(a) The HIE entity is operating outside of nationally recognized standards identified by DHCF in policy guidance, or in a manner contrary to that described in any other information submitted under §§ 8702.2 and 8708.5, unless amendments to the submissions have been filed with and approved by DHCF;

(b) The HIE entity is unable to fulfill its obligations to furnish comprehensive HIE services as required under its agreements with DHCF or with its participating organizations;

(c) The HIE entity is no longer financially solvent or is not reasonably expected to meet its obligations to DHCF or its participating organizations;

(d) The HIE entity, or any person acting with its sanction, has advertised or merchandised its services in an untrue, misleading, deceptive, or unfair manner;

(e) The continued operation of the HIE would pose risks to its participating organizations or the privacy and security of health care consumers served by the participating organizations;

(f) The HIE entity improperly discloses any PHI, or health information derived from PHI, that is available through the registered or designated

HIE entity's infrastructure, except as consistent with or otherwise permitted by this chapter and applicable federal or District law; and

(g) The HIE entity has otherwise failed to substantially comply with the requirements of this chapter or other applicable federal or District law.

8711.7 Within thirty (30) calendar days of receipt of notice of enforcement action from DHCF pursuant to this section, an HIE entity may request an administrative review of the action taken by DHCF in accordance with the procedures set forth in § 8713.

8711.8 DHCF shall publish and maintain guidance on nationally recognized standards for the secure access, use, and disclosure of health information on the DHCF website at www.dhcf.dc.gov.

8711.9 All other Medicaid requirements outlined in District laws and regulations, are applicable to HIE entities.

8712 EXEMPTIONS

8712.1 DHCF may exempt a registered or designated HIE entity from certain requirements if such an exemption does not pose substantial risks to the privacy or security of health care consumers and:

(a) The HIE entity's infrastructure does not allow the registered or designated HIE entity to maintain compliance with this chapter; or

(b) The requirements of this chapter would cause an undue burden or hardship on the registered or designated HIE entity.

8712.2 A registered or designated HIE entity may request a one (1) year exemption from specific requirements set forth in this rule. An exemption request must:

(a) Be made in writing;

(b) Identify each specific requirement of this chapter from which the HIE entity is requesting an exemption;

(c) Identify the requested time period of the exemption;

(d) State the reason for each exemption request; and

(e) Include information that justifies the exemption request.

8712.3 Within forty-five (45) days after receipt of complete information from a registered or designated HIE entity requesting an exemption, DHCF shall take one of the following actions:

(a) Grant the exemption by providing written notification; or

(b) Deny the exemption request by providing written notification that enumerates the reasons for the denial to the registered or designated HIE entity.

8712.4 An exemption may not be made for any requirement within this rule that is required of a registered or designated HIE entity by federal or other District law.

8712.5 For good cause shown, DHCF may renew a one (1)-year exemption for up to an additional one (1) year period, upon request by the registered or designated HIE entity.

8713 APPEALS AND ADMINISTRATIVE REVIEW

8713.1 Within thirty (30) calendar days of receipt of notice of a DHCF enforcement action in accordance with § 8711 or notice from DHCF denying an HIE entity's application for registration or designation pursuant to §§ 8702.5 and 8708.8, an HIE entity may request an administrative review of the action taken by DHCF.

8713.2 The request for administrative review shall be made in writing to the Health Care Reform and Innovation Administration at DHCF.

8713.3 The request for administrative review shall identify the specific action for review, a written explanation of the HIE entity's cause for requesting administrative review, the requested relief, and any supporting documentation.

8713.4 DHCF shall review the submitted request for administrative review and shall issue a final notice to the HIE entity upon completion of the administrative review. DHCF shall reserve the right to request additional documentation from the HIE entity during its administrative review.

8713.5 DHCF shall mail its final notice to the HIE entity no later than forty-five (45) calendar days from the date of receipt of the written request for administrative review and all supporting documentation, including any additional documentation requested by DHCF.

8713.6 The final notice shall include DHCF's decision to approve or deny the requested relief and detail the basis for the determination.

8713.7 Determinations made by DHCF and communicated in the final notice to an HIE entity may be appealed to the Office of Administrative Hearings (OAH) within thirty (30) calendar days of the date of issuance of the final notice.

8713.8 The filing of an appeal with OAH shall not stay any enforcement action taken by DHCF related to the request for administrative review or determinations communicated in the final notice to an HIE entity.

8799 DEFINITIONS

8799.1 When used in this this chapter, the following terms shall have the meanings ascribed:

Authentication - The process of establishing confidence in user identities electronically presented to an information system.

Authorization - Has the meaning provided in 45 CFR § 164.508.

Authorized user – A person identified by a participating organization or a HIE entity, including a health care consumer, who may use, access, or disclose protected health information through or from a health information exchange for a specific authorized purpose and whose HIE access is not currently suspended or revoked.

Breach – The meaning provided in 45 CFR § 164.402.

Business associate - The meaning provided in 45 CFR § 160.103.

Core elements of the Master Patient Index (MPI) - The minimum elements that are:

(a) Required for an HIE entity to identify a particular patient across separate clinical, financial, and administrative systems; and

(b) Needed to exchange health information electronically.

DC HIE - The District's statewide health information exchange, an interoperable system of registered and designated HIE entities that facilitates person-centered care through the secure, electronic exchange of health information among participating organizations supported by a District-wide health data infrastructure.

Designated HIE - An HIE entity that has applied for and received designation from the Department of Health Care Finance in accordance with Chapter 87, District of Columbia Health Information Exchange, of Title 29, Public Welfare, of District of Columbia Municipal Regulations.

DHCF - The District of Columbia's Department of Health Care Finance.

Disclosure - The release, re-disclosure, transfer, provision, access, transmission, communication, or divulgence in any other manner of information in a medical record, including an acknowledgment that a medical record on a particular health care consumer or recipient exists, outside the entity holding such information.

Electronic Health Record - An electronic record of health information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Health care consumer - Any actual or potential recipient of health care services, such as a patient in a hospital.

Health care provider –

(a) A person who is licensed, certified, or otherwise authorized under District law to provide health care in the ordinary course of business or practice of a profession or in an approved education or training program;

(b) Government agencies involved in the provision of health or social services;

(c) A facility where health care is provided to health care consumers or recipients; or

(d) An agent, employee, officer, or director of a health care facility, or an agent or employee of a health care provider.

Health information - Any information, whether oral or recorded in any form or medium, that:

(a) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(b) Relates to the past, present, or future physical or mental health or condition of a person, the provision of health care to a person, or the past, present, or future payment for the provision of health care to a person.

Health Information Exchange (HIE) - A system that facilitates person-centered care through the secure electronic exchange of health

information among approved, qualifying partners in support of health data infrastructure according to nationally recognized standards.

HIE Entity - An entity that creates or maintains an infrastructure that provides organizational and technical capabilities in a system to enable the secure, electronic exchange of health information among participating organizations not under common ownership.

HIPAA - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub.L. No. 104-191, 110 Stat. 1938 (1996)).

HITECH Act - The Health Information Technology for Economic and Clinical Health Act (Pub. L. No. 111-5, Title XIII, 123 Stat. 226 (2009)).

Incident Response Plan - The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information system(s).

Master patient index - A database that maintains a unique index identifier for each patient whose protected health information may be accessible through an HIE entity and is used to cross reference patient identifiers across multiple participating organizations to allow for patient search, patient matching, and consolidation of duplicate records.

Non-HIPAA violation - The acquisition, access, use, maintenance, or disclosure of health information in a manner not permitted under District or federal law:

(a) Which compromises the security or privacy of the health information; and

(b) Is not a HIPAA violation.

Opt-out – A health care consumer's election not to participate in the HIE, so that the HIE entity shall not disclose such health care consumer's protected health information, or data derived from such health care consumer's health information, except as consistent with this chapter.

Participating organization - An entity that enters into an agreement with an HIE entity that governs the terms and conditions under which its authorized users may use, access, or disclose protected health information by the HIE entity.

Point-to-point transmission - A secure electronic transmission of PHI, including, but not limited to, records sent via facsimile or secure clinical

messaging service, sent by a single entity that can be read only by the single receiving entity designated by the sender.

Protected health information (PHI) - A subset of health information that has the same meaning as given in 45 CFR § 160.103, and includes sensitive health information.

Registered Resident Agent - An agent of an entity who is authorized to receive service of any process, notice, or demand required or permitted by law to be served on the entity.

Registered HIE - An HIE entity that has applied for and received registration from the Department of Health Care Finance in accordance with Chapter 87, District of Columbia Health Information Exchange, of Title 29, Public Welfare, of District of Columbia Municipal Regulations.

Sensitive health information - A subset of PHI, which consists of:

(a) 42 CFR Part 2 information; or

(b) Any other information that has specific legal protections in addition to those required under HIPAA, as implemented and amended in federal regulations.

System administrator - An individual employee within a participating organization (or an individual employed by a contractor to the participating organization) who is designated by the participating organization to manage the user accounts of specified persons within the participating organization in coordination with an HIE entity.

Third-party system - Hardware or software provided by an external entity to a participating organization, which interoperates with an HIE entity to allow an authorized user access to information through the HIE entity and may include an electronic health record system.

Unqualified opinion – A written statement by an auditor that financial statements fairly reflect the results of the business organization's operations and its financial position according to generally accepted accounting principles.

Unusual finding – A finding that there was an irregularity in the manner in which use, access, maintenance, disclosure, or modification of health information or sensitive health information transmitted to or through an HIE entity should occur that could give rise to a breach, a violation under this chapter or a violation of other applicable privacy or security laws.