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, effective February 27, 2008 (D.C. Law 17-109; D.C. Official Code § 7-771.05(6)) ("Establishment Act"), and in An Act To enable the District of Columbia to receive Federal financial assistance under title XIX of the Social Security Act for a medical assistance program, and for other purposes, approved December 27, 1967 (81 Stat. 744; D.C. Official Code § 1-307.02) ("Social Security Act"), and Mayor's Order 2024-115, dated July 1, 2024, hereby gives notice of his adoption of the following amendments to Chapter 87 (District of Columbia Health Information Exchange) of Title 29 (Public Welfare) of the District of Columbia Municipal Regulations ("DCMR").

DHCF is the single state agency responsible for the administration of the State Medicaid program under Title XIX of the Social Security Act and Children's Health Insurance Program under Title XXI of the Act in the District. Pursuant to Section 8 of the Establishment Act (D.C. Official Code § 7-771.07(8)), DHCF developed and maintains a comprehensive information-technology ("IT") 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 trends, cost measurement, performance management, policy development, and strategic planning.

DHCF leads health IT and health information exchange ("HIE") policy 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 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 its Policy Subcommittee, the District committed to undertaking activities aimed at further strengthening the DC HIE in the District's 2022 State Medicaid Health IT Plan (SMHP). These initiatives include integrating diverse health data that is relevant to aiding decision-making, supporting person-centered care coordination, and generating change in health outcomes and care delivery. This includes population health and social needs data, which in turn can better inform the District's health system's ability to address health disparities.

To meet its commitment to a holistic and integrative approach to promoting the HIE in the District and in accordance with the purposes and duties set forth under the Establishment Act, DHCF is updating regulations for the efficient and secure transmission of health information. The goal of the changes is to move the DC HIE from the HIE model to the Health Data Utility ("HDU") model. An HIE facilitates data exchange primarily for clinical care - sharing patient information between

hospitals, providers, and other healthcare organizations. An HDU enhances these entities' ability to share health data timely and securely, for purposes beyond individual treatment, such as the required reporting of aggregate and anonymized data for public health efforts, population health management, and community health initiatives. As an HDU, the DC HIE will act as a more robust, efficient, centralized hub for data sharing.

The rulemaking also makes changes to:

- Align policy more closely with definitions established in the Health Information Portability and Accountability Act of 1996 (Pub. L. 104-191; 110 Stat. 1936);
- Facilitate data sharing with public health authorities;
- Update language on the use and maintenance of information;
- Change the HIE entity designation period from five (5) years to six (6) years;
- Extend the reporting period for third-party audits and disciplinary action lookbacks from two (2) years to three (3) years;
- Establish reporting requirements for registered HIEs to provide detailed descriptions of primary uses of HIE data on a rolling thirty (30) day basis and require secondary uses of HIE data be submitted to DHCF for review and approval;
- Update all timeframes associated with reporting requirements to be measured in calendar days; and
- Clarify renewal application requirements and documentation timelines.

These changes improve procedural efficiency and oversight of the HIE. The changes were shared with and reviewed by the HIE Policy Board's policy subcommittee to help inform the rulemaking.

DHCF projects no fiscal impact in Medicaid expenditures to implement the Health Information Exchange rule.

A Notice of Proposed Rulemaking was published in the *District of Columbia Register* at 72 DCR 014066 on December 19, 2025. Comments were received from two stakeholder organizations. Each comment is addressed below:

Nationally Recognized Standards

Comment: One commentor recommended amending the language "nationally recognized standards" and "standards and methodologies". Additionally, the commenter recommended adding explicit cross references to certain standards and guidelines and publishing a non-regulatory mapping guidance appendix that shows how DC HIE requirements align to the frameworks.

Response: DHCF acknowledges the stakeholder's concern and will update its sub-regulatory guidance on nationally recognized standards for designation and registration, no later than September 30, 2026, and post them to the DC HIE webpage at: www.dhcf.dc.gov/page/dc-hie. No changes to the text of the rule have been made at this time.

Primary/Secondary Use and Reporting Cadence

Comment: One commentor recommended 1) adopting a risk tiering schema for DHCF's reporting based on data identifiability (de-identified, limited dataset, identifiable) where each tier would be held to a certain risk threshold and 2) publishing pre-approved templates for routine public health reporting, which they believe would support HDU objectives and focus DHCF oversight where risk is greatest.

Response: DHCF acknowledges the commenter's concerns and notes that DHCF currently has an internal use case form with sections that are used to inform what the HDU reports to DHCF. DHCF believes these existing case forms supports both HDU objectives and DHCF's oversight activities because this standardized internal use case documentation already functions effectively as a template for HIE reporting. DHCF will, however, remember the commenter's recommendation for future updates regarding HDU reporting.

No changes to the text of the rule have been made at this time.

Comment: One commentor recommended 1) permitting reporting to reference existing publicly posted use case documentation and 2) only allowing DHCF to suspend data use if it finds the use to be inconsistent with the law or regulation. The commentor believes these changes would avoid unintended delays to critical data uses and preserve the independence of the HDU.

Response: DHCF acknowledges this comment and intends to update its guidance on reporting to reference existing publicly posted use case documentation. DHCF believes it is unnecessary to add language regarding the suspension of data use, as this is already addressed in § 8703.5(c).

No changes to the text of the rule have been made at this time.

Authentication

Comment: One commentor recommended that DHCF specify identity functions by role and connection method and acceptable MFA (multi-factor authentication) patterns and provide a phased compliance timeline aligned with EHR capabilities to "reduce[] uneven enforcement, align[] with evolving identity standards, and support[] scalable adoption."

Response: DHCF acknowledges this comment, but does not believe that it is necessary to provide that level of detail in these regulations. In its review of future sub-regulatory guidance, DHCF will consider this additional information, if it is determined necessary.

No changes to the text of the rule have been made at this time.

Annual Risk Assessments and Audit Content

Comment: One commentor recommended that DHCF permit an up-to-date and validated HITRUST assessment report to satisfy the annual risk assessment submission and reference, in guidance, the Office of National Coordinator for Health Information Technology's ("ONC") audit expectations and ASTM International's E2147-18 Standard Specification for Audit and Disclosure Longs for Use in Health Information Systems for audit log content and retention. The commentor

believes leveraging established and independently validated assessments reduce burden while enhancing rigor and consistency with ONC/ASTM standards.

Response: DHCF notes that HIEs are already submitting HITRUST assessments as part of existing audit requirements. DHCF will consider the utility of independently validated assessments in its future review of regulatory and sub-regulatory guidance.

No changes to the text of the rule have been made at this time.

Comment: One commentor recommended adding a method, more secure than email, to submit information and assessments.

Response: DHCF appreciates the concern raised, but notes that existing email mechanisms, such as encryption, are secure for conveying information and assessments.

No changes to the text of the rule have been made at this time.

Breach Notification

Comment: One commentor recommended that DHCF clarify the hierarchy of local and federal timelines for providing notification of a breach and provide a limited safe harbor for good faith multi system investigations to prevent premature or incomplete notices. The commentor believes this would avoid conflicting deadlines and maintain strong consumer protection.

Response: DHCF notes that §§ 8706.1 and 8706.2 state the order of applicable timelines. Under these provisions, the default timelines are those required under federal law first (HIPAA/HITECH and 42 CFR Part 2).

No changes to the text of the rule have been made at this time.

Designation

Comment: HITRUST, the stakeholder organization, recommended replacing the language "Health Information Trust Alliance" with "HITRUST CSF-based certification (HITRUST il or r2)." The commentor believes that the current language may be misread as an organizational reference rather than a certifiable program. The organization operates exclusively as HITRUST and is recognized as such in the health IT and cybersecurity sectors.

Response: DHCF acknowledges this comment and has revised the language in § 8708.5(g) to reflect the recommended HITRUST CSF-based certification terminology.

Consumer Access and Evaluation

Comment: One commentor recommended 1) referencing ONC's HTI 1 (Health Data, Technology, and Interoperability) final rule information sharing updates and consumer facing expectations and 2) pre-approving standardized consumer notices and templates.

Response: DHCF acknowledges this comment and will update its sub-regulatory guidance with specific references, no later than September 30, 2026, and post them to the DC HIE webpage at: www.dhcf.dc.gov/page/dc-hie.

No changes to the text of the rule have been made at this time.

The Director of DHCF took final action to adopt this rulemaking on April 21, 2026, and the rules shall become effective upon publication of this notice in the *District of Columbia Register*.

Chapter 87, DISTRICT OF COLUMBIA HEALTH INFORMATION EXCHANGE, of Title 29 DCMR, PUBLIC WELFARE, is amended as follows:

Section 8700, GENERAL PROVISIONS, is amended as follows:

Paragraphs (a), (e), and (f) of Subsection 8700.2 are amended to read as follows:

(a) Ensure the privacy and security of protected health information ("PHI") accessed, used, or disclosed through a registered or designated HIE entity;

…

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

…

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

A new paragraph (g) is added to Subsection 8700.2 to read as follows:

(g) Provide lawful access to data for public health authorities.

Section 8701, THE DISTRICT OF COLUMBIA'S HEALTH INFORMATION EXCHANGE (DC HIE), is amended as follows:

Subsection 8701.1 is amended to read as follows.

8701.1 The DC HIE shall be a privately-operated interoperable system of registered and designated HIE entities that shall facilitate person-centered care through the secure electronic exchange of health information among participating organizations in support of a District-wide health data infrastructure that functions as a Health Data Utility (HDU).

Section 8702, HIE REGISTRATION REQUIREMENTS AND APPLICATION, is amended as follows:

Paragraphs (g) and (h) of Subsection 8702.2 are amended to read as follows:

(g) The HIE entity shall provide a report for each of the past three (3) years, from a third-party auditor that expresses no doubt about the entity's ability to continue as a going concern and resulting in an unqualified opinion concerning 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 three (3) years prior to applying for registration;

Paragraph (a) of Subsection 8702.6 is amended to read as follows:

(a) Submit operational information, as requested by DHCF, and ensure it is publicly posted on a DC-registered HIE's website; and

Subsection 8702.8 is amended to read as follows:

8702.8 In order to renew their registration HIE entities shall demonstrate continued compliance with § 8702 by providing the following information no later than ninety (90) calendar days prior to the end of the three (3) year term and 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; and

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

Section 8703, REGISTERED HIE ENTITY PROTECTED HEALTH INFORMATION ACCESS, USE, AND DISCLOSURE REQUIREMENTS, is amended as follows:

Paragraph (d) of Subsection 8703.2 is amended to read as follows:

(d) Reporting to public health authorities for the purpose of disease prevention, control, surveillance, and improving community health in accordance with 45 CFR § 164.512(b) and other District or federal law; or

Subsection 8703.4 is amended to read as follows:

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. A registered HIE entity may engage in data use for Secondary Use Purposes, subject to any limitations under District or federal law.

Subsection 8703.5 is deleted and replaced to read as follows:

8703.5 Beginning October 1, 2025, DHCF shall review and keep a record of Primary Uses and Secondary Uses proposed by HIE's, submitted electronically as described by DHCF guidance, prior to implementation. The registered HIE entity shall:

(a) Provide DHCF with its policies governing the disclosure and use of health information for Secondary Use, in accordance with the policy guidance published on the DHCF website, and notify DHCF of any amendments or updates to these policies;

(b) Report Primary and Secondary Uses of health information to DHCF on the last business day of every month, including detailed descriptions of each use to ensure transparency and accountability; and

(c) Suspend any Primary or Secondary Use DHCF deems inconsistent with the definition of HDU set forth in this chapter.

Existing Subsections 8703.5, 8703.6, 8703.7, 8703.8, 8703.9, and 8703.10 are renumbered and amended to read as follows:

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:

(a) Use and ensure that its participating organizations are using an authentication methodology that meets the minimum technical requirements set forth in the National Institute of Standards and Technology ("NIST"), Special Publication 800-63 Revision 4, and other standards identified by DHCF in its policy guidance. 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 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.

8703.7 To assure that only an authorized user accesses, uses, or discloses PHI through or from a registered HIE entity, a registered HIE entity shall require 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 § 8703.9;

(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 thirty (30) calendar days, of any such appointment or change;

(2) A breach, as defined in 45 CFR § 164.402; or

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

8703.8 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 username in accordance with the most recent applicable guidelines issued by NIST, or other 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 an authorized user's access level as appropriate to reflect any change in that user's role within the participating organization within thirty (30) days;

(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.

8703.9 The registered HIE entity shall ensure that access to PHI is terminated for any authorized user within seven (7) calendar days of the user's disassociation from the participating organization. This requirement applies to users who:

(a) Are suspended by the participating organization;

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

(c) No longer require access to the PHI to perform their duties.

8703.10 To mitigate the risks of improper access or disclosure of electronic PHI the registered HIE entity shall conduct 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's Information and Privacy Officer with a copy of their risk assessment on an annual basis by email at DHCFprivacy@dc.gov.

8703.11 Based on the findings of the assessment conducted in accordance with § 8703.10, 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.

A new Subsection 8703.12 is added to read as follows:

8703.12 The Department may, upon request, extend deadlines in this Section when a delay is caused by circumstances beyond the HIE's control such as:

(a) A natural disaster or other emergency that could not be reasonably controlled by the HIE or the Department, or

(b) A circumstance where the HIE can demonstrate good cause for an extension.

Section 8704, AUDITING REQUIREMENTS FOR REGISTERED HIE ENTITIES, is amended as follows:

Paragraph (b) of Subsection 8704.1 is amended to read as follows:

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

Section 8705, REMEDIAL ACTIONS TO BE TAKEN BY A REGISTERED HIE ENTITY, is amended as follows:

Subsection 8705.1 is amended to read as follows:

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

Subsections 8705.3, 8705.4, and 8705.5 are amended to read as follows:

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 any unusual finding, act, or event that it has a basis to believe is or may be a violation under § 8703, occurred:

(a) The registered HIE entity shall begin the investigation immediately 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 § 8704; and

(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 of the finding to DHCF's Information and Privacy Officer within thirty (30) calendar days of the conclusion of the investigation; 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 an affected 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 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 twelve (12) calendar 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 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.

(b) Within thirty (30) calendar days, the registered HIE entity shall provide the following to DHCF, the participating organization, and 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 any unusual finding, act, or event that it has a basis to believe is or may be a violation under § 8703;

(4) A list of the authorized user roles 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) A HIPAA breach or violation;

(b) A violation of District or federal law relevant to privacy or security;

(c) An authorized user or participating organization has sold health information in violation of this chapter; or

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

Section 8706, NOTICE OF HIPAA BREACH AND NON-HIPAA VIOLATION BY A REGISTERED HIE ENTITY, is renamed and amended to read as follows:

8706 NOTICE OF HIPAA BREACH OR OTHER VIOLATION BY A REGISTERED HIE ENTITY

8706.1 Notification of a HIPAA breach 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 42 CFR Part 2.

8706.2 When federal or District law, other than this chapter, 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, violations of other federal or District law in accordance with the requirements of this section.

8706.3 If an investigation under § 8705 concluded that there was a HIPAA breach or other violation of federal or District law, 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 other violation under § 8703, 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 other violation under § 8703; and

(d) The DHCF Privacy Officer.

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, email address, and website where the health care consumer can learn more information, and a description of the breach or other 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 violation under § 8703 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, reasonably calculated to reach each affected health care consumer, shall be provided in accordance with the criteria set forth below:

(1) If 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) If 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 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 violation under § 8703.

(d) When notice about a HIPAA breach or violation under § 8703 is required pursuant to this chapter, a registered HIE entity and its enrolled participating organization, shall provide notice in writing to DHCF no 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 violation under § 8703 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 no 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 violation under § 8703 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 (DHCFPrivacy@dc.gov).

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 and pursue enforcement actions as necessary in accordance with § 8711.

Section 8707, REGISTERED HIE ENTITY CONSUMER PARTICIPATION, ACCESS, AND EDUCATION REQUIREMENTS, is amended as follows:

Paragraph (b) of Subsection 8707.3 is amended to read as follows:

(b) If the health care consumer's PHI is not directly available electronically to the health care consumer, the registered HIE entity shall, within nine (9) calendar 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.

Section 8708, HIE DESIGNATION REQUIREMENTS AND APPLICATION, is amended as follows:

Paragraphs (a) of Subsection 8708.5 is amended to read as follows:

(a) Develop and submit strategic and operational plans to serve as an HDU that addresses the needs of health providers, public health agencies, Medicaid managed care organizations, health care consumers, and any other stakeholders identified by DHCF in policy guidance in achieving HIE capabilities;

Paragraph (g) of Subsection 8708.5 is deleted and replaced to read as follows:

(g) Demonstrate HITRUST CSF-based certification, the System and Organizational Controls 2 framework of the American Institute of Certified Public Accountants, or another program that is widely adopted across the cybersecurity industry, developed and maintained by established bodies, and subject to third-party independent validation;

Existing paragraphs (g), (h), (i), and (j) of Subsection 8708.5 are renumbered to read as follows:

(h) 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;

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

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

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

Subsection 8708.9 is amended to read as follows:

8708.9 An HIE entity's designation shall be awarded in six (6) year terms, effective immediately. DHCF shall review an HIE entity's designation every six (6) years from the date of designation to determine whether the HIE entity will be renewed for an additional six (6) 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.

Subsection 8708.11 is amended to read as follows:

8708.11 A designated HIE entity shall submit an annual report for review by DHCF that addresses:

(a) Updates to all strategic and operational plans developed and submitted in accordance with § 8708.5(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) Additional information as requested by DHCF.

Section 8709, DESIGNATED HIE ENTITY AUDITING REQUIREMENTS, is amended as follows:

Paragraph (a) of Subsection 8709.1 is amended to read as follows:

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

Subsection 8709.6 is amended to read as follows:

8709.6 The access and auditing plan required under § 8708.4 shall include:

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

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

(c) The reasonable steps that shall be taken to promptly mitigate a 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 chapter; 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 twelve (12) calendar 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, pursuant to § 8709.5.

Section 8710, DESIGNATED HIE ENTITY REQUIREMENTS TO PROMOTE CONSUMER PARTICIPATION, ACCESS, AND EDUCATION, is amended as follows:

Paragraph (e) of Subsection 8710.2 is amended to read as follows:

(e) Public health authorities for purposes required by applicable law; or

Paragraph (d) of Subsection 8710.4 is amended to read as follows:

(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 take to opt out of participation in the designated HIE entity;

(7) The implications of a health care consumer's decision to opt out of participation in the HIE 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 policies and procedures consistent with this chapter regarding how the health care consumer may gain access to the health care consumer's health information.

Paragraph (e) of Subsection 8710.5 is amended to read as follows:

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

Subsection 8710.9 is amended to read as follows:

8710.9 A designated HIE entity shall acknowledge a health care consumer's written notice or request, as described in § 8710.7, within twelve (12) calendar days of receipt of the request.

Paragraph (c) of Subsection 8710.12 is amended to read as follows:

(c) A designated HIE entity shall not disclose information derived from 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, except as otherwise permitted under applicable law.

Subsection 8710.17 is amended to read as follows:

8710.17 A designated HIE entity shall implement the health care consumer's requested action within seven (7) calendar 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.

Paragraph (a) of Subsection 8710.18 is amended to read as follows:

(a) Send the confirmation of participation status change within five (5) calendar days of the effective date of change of the health care consumer's participation status; and

Section 8712, EXEMPTIONS, is amended as follows:

Subsection 8712.3 is amended to read as follows:

8712.3 Within forty-five (45) calendar 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;

(b) Request additional documentation from the HIE entity regarding the need for an exemption; or

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

Section 8799, DEFINITIONS, is amended as follows:

Subsection 8799.1 is amended as follows:

The following new definition of "Health care operations" is added after the existing definition of "Health care consumer":

Health care operations – The meaning provided in 45 C.F.R. § 164.501.

The following new definition of "Health Data Utility" is added after the existing definition of "Health care provider":

Health Data Utility - A Health Data Utility (HDU) is a model with cooperative

leadership, designated authority, and advanced technical capabilities to combine, enhance, and exchange electronic health data across care and service settings for treatment, care coordination, quality improvement, and community and public health purposes. The HDU facilitates the secure, bidirectional communication of health data between public health authorities and healthcare providers, enhancing the ability to control disease outbreaks, improve public health outcomes, and promote health equity.

The definition of "Non-HIPAA violation" is repealed.

The following new definition of "Payment" is added after the existing definition of "Participating organization":

Payment - The meaning provided in 45 C.F.R. § 164.501.

The definition of "Protected health information (PHI)" is amended to read as follows:

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.