GOVERNMENT OF THE DISTRICT OF COLUMBIA
Department of Health Care Finance

Office of the Interim Senior Deputy Director and Medicaid Director **Transmittal 23-55**

TO: Health Information Exchange (HIE) entities that have received Registered HIE entity status pursuant to Chapter 87 of Title 29 DCMR.

FROM: Eugene Simms
Interim Senior Deputy Director and Medicaid Director

DATE: **October 17, 2023**

SUBJECT: **Policy Guidance on Audit Requirements, Notification of Unusual Activity, and Remedial Action Timelines by Registered Entities of the DC Health Information Exchange (HIE)**

Purpose
The purpose of this guidance is to provide additional information in response to §§ 8703.9, 8704.1(b), 8704.1(d), 8704.1(f), 8705.4(a)(2) of the "HIE Rule", Chapter 87 (District of Columbia Health Information Exchange) of Title 29 (Public Welfare) District of Columbia Municipal Regulations (DCMR). This document provides guidelines for Registered Health Information Exchange (HIE) entities on:

- Conducting audits per nationally recognized standards and methodologies;
- Reporting any unusual findings to involved participating organizations; and
- Providing timeframes to involved participating organizations for implementing remedial actions.

The Department of Health Care Finance (DHCF) is committed to supporting HIE's ability to comply with DHCF policy guidance on audit requirements.

Details
HIE entities that have received Registered HIE entity status must comply with the following requirements regarding audits:

Conducting Audits
As outlined in § 8704.1(b), Registered HIE entities must conduct audits in accordance with nationally recognized standards. HIE entities must align with current standards to protect

electronic health information as established at 45 CFR § 170.210. These standards are listed below:

- The current standard for recording disclosures related to treatment, payment, and health care operations (as defined at 45 CFR 164.501) is listed at 45 CFR § 170.210(d), requiring the maintenance of the date, time, patient identification, user identification, and a description of the disclosure.
- The current standard for audit logs and audit log content is listed at 45 CFR § 170.210(h) as **ASTM E2147–18**: Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, approved May 1, 2018.
- The current standard for date and time is listed at 45 CFR § 170.210(g) as a system clock that has been synchronized following (RFC 5905) **Network Time Protocol Version 4**: Protocol and Algorithms Specification, June 2010.

Wherever applicable, HIE entities must ensure that technical audits adhere to Recognized Security Practices as outlined in Public Law 116-321.

HIE entities must also ensure that audit trails and logs are immutable or support non-repudiation (i.e., information in logs cannot be altered by anyone regardless of access privilege). As per § 8704.1(g) of the HIE Rule, HIE entities must maintain an audit trail of user access logs in a retrievable storage medium.

Where applicable, HIE entities must report the results of any periodic and ad hoc audits to DHCF Privacy and Security officers at DHCFPrivacy@dc.gov.

User and Application Audits
As outlined in § 8704.1(d), HIE entities must investigate any unusual findings identified in access log audits to determine instances of improper access, use and disclosure of protected health information (PHI). To do this, HIE entities must conduct user and application audits, which include, at a minimum:

- Conduct regular review of user access logs to discover unauthorized access or unauthorized lookups; and
- Document and monitor unauthorized lookups or queries for patient data, except in the case of emergency.

Technical Audits
Technical audits ensure that the entity's system is appropriately protected against security threats. As per § 8703.9 of the HIE final rule, HIE entities must undergo annual assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI. To do so:

- HIE entities may choose to outline these items as part of their annual third-party privacy and security audit.
- HIE entities that have voluntarily obtained certifications or accreditations that demonstrate compliance with industry standards for privacy and security may provide DHCF a copy of their approved accreditation or certification.

Reporting Unusual Findings
As per § 8704.1(f), HIE entities must report unusual findings to participating organizations. Unusual findings are defined in § 8799 of the HIE Rule. To do so, HIE entities must develop and implement protocols, methodologies, and a monitoring approach designed to discover any unusual findings. HIE entities may also choose to use analytics and/or privacy monitoring software to conduct regular monitoring.

As per § 8704.1(f), upon discovery of a potential incident, HIE entities must notify participating organizations. To do so, HIE entities must notify participating organizations in a reasonable timeframe. At a minimum, the notification must include the following elements:

- Date of incident;
- Date of discovery of incident;
- Nature of the incident; and
- Identification of each individual whose PHI was or was reasonably believed to be unsecure.

If the HIE entity identifies additional information relevant to the incident that was not included in the initial notice, the HIE entity must provide this information as soon as possible after the initial notice.

If the HIE entity has reason to believe that a HIPAA breach has occurred, it must follow notification and investigation procedures outlined in the HIE Rule at § 8705.3.

Conducting Investigations
As per § 8705.3, HIE entities shall conduct an investigation if there is reason to believe that a HIPAA breach or non-HIPAA violation has occurred. In this process, the HIE entity may coordinate with privacy and security officers, system administrators, site administrators, and/or other relevant points of contact at the participating organization(s) to conduct investigations regarding any unusual findings.

As per § § 8705.1 and 8705.2, HIE entities shall immediately suspend an authorized user's access if it determines there is harm to the privacy of persons, security of health information, or ongoing risk of improper use, access, maintenance, or disclosure of PHI. Hence, in the event that the participating organization does not provide a timely response during investigations, the HIE entity must suspend user access until an investigation can be completed.

Remedial Actions and Associated Timeframes
As per § 8705.4(a)(2), HIE entities must require that remedial actions be completed within a reasonable timeframe. HIE entities must require that any remedial actions be completed within ten (10) business days of receipt of the results of the investigation. Remedial actions may include:

- Implementation of new controls to mitigate risks;

- Required completion of user training regarding the use of the HIE for the user or participating organization;
- Temporary restriction of the authorized user's or participating organization's access to the HIE; or
- Termination of access to the HIE.

HIE entities may choose to coordinate with privacy and security officers, system administrators, site administrators, and/or other relevant points of contact at the participating organization(s) in the development of remedial actions.

Contact
If you have questions, please contact Asfiya Mariam, Policy Analyst, Division of Digital Health at asfiya.mariam@dc.gov or (202) 442-4622.

Cc: District Registered Entity – CRISP DC
District Registered Entity – DC Primary Care Association (CPC-HIE)