GOVERNMENT OF THE DISTRICT OF COLUMBIA
Department of Health Care Finance

Office of the Interim Senior Deputy Director and Medicaid Director **Transmittal 23-56**

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 19, 2023**

SUBJECT: **Policy Guidance on Identifying Authorized Users for Access, Use, and Disclosure of Protected Health Information through the DC Health Information Exchange (HIE)**

Purpose
The purpose of this guidance is to provide additional information on §§ 8703 and 8708 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:

- Meeting minimum technical requirements to ensure that only an authorized user accesses, uses, or discloses protected health information (PHI) from the HIE entity; and
- Developing a methodology to document user types and modes of accessing PHI at participating organizations.

The Department of Health Care Finance (DHCF) is committed to supporting Registered HIE entities' ability to comply with the guidance on identifying authorized users for access, use, and disclosure of PHI.

Details

Minimum Technical Requirements
As outlined in § 8703.5(a), Registered HIE entities must use and ensure that their participating organizations are using minimum requirements set forth in the latest edition of NIST Special Publication (SP) 800-63, *Digital Identity Guidelines*. This SP offers details and technical specifications regarding identity proofing and authentication for users. This NIST SP is also referenced in the HIE rule at § 8703.5. To do this, Registered HIE entities must:

- For human users, comply with Level 2 requirements set by Special Publication 800-63.

- For automated systems, comply with Level 3 requirements set by Special Publication 800-63 and include a human sponsor.
- Record and maintain a listing of each unique user identifier that tracks user identity.
- Require multi-factor authentication (MFA) for authorized users, which includes, but is not limited to, unique user identifiers, device registration, and other authentication methods.

Additionally, as outlined in § 8703.6(c), Registered HIE entities must ensure that any third-party system used by a participating organization to authenticate users follows NIST Special Publication 800-63 guidelines. To do so, HIE entities must:

- Ensure the third-party system can monitor and audit user activities. This is applicable if the HIE entity utilizes Single Sign-On (SSO) functionality within Electronic Health Record (EHR) systems at a participating organization.
- Ensure that system administrators at participating organizations carry out all actions listed within § 8703.7. This is applicable if a participating organization includes users that access the HIE via a web portal.

Where applicable, HIE entities must adhere to Recognized Security Practices as outlined in Public Law 116-321.

System Administrator Requirements
As per §§ 8703.6(a) and 8703.7, Registered HIE entities must require system administrators to carry out several actions to ensure appropriate access to the HIE. Given that the HIE can be accessible via a web portal or via SSO, HIE entities must fulfill the requirements listed in §§ 8703.6(a) and 8703.7 by working with system administrators to:

- Ensure that each authorized user's access to PHI is matched to their respective activities;
- Develop and maintain a methodology matrix that maps each authorized user type at the organization;
- Ensure compliance with any organizational policies regarding access to PHI; and
- Conduct a periodic review of the methodology matrix.

In addition, as outlined § 8708.5(g), Designated HIE entities must offer technical assistance and guidance to system administrators at participating organizations in identifying and managing authorized users.

Definitions: The following definitions are applicable:
- Human Sponsor: An individual responsible for the manual oversight of an automated system that controls identity proofing and authentication for users.

- Methodology Matrix: A system that documents user types at a participating organization and their respective access levels. The matrix must also indicate how the organization's users access the HIE (such as via a web portal or via SSO).

- Multi Factor Authentication (MFA): Multi-factor authentication is a layered approach to securing data and applications where a system requires a user to present a combination of two (2) or more credentials to verify a user's identity for login.

- Single Sign-On (SSO): The functionality that allows a user to sign on to multiple related, yet independent software systems with a single user identification and password.

- Unique User Identifiers: Elements that allow HIE entities to identify individual users that directly access the HIE, or the information contained within the HIE. These elements allow entities to track user identity. These include, but are not limited to, username, password, or user ID number.

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)