Subcommittee: HIE Operations, Compliance, and Efficiency

Chairs: Ms. Gayle Hurt

Date: April 27, 2023

Status: Draft

District of Columbia Health Information Exchange Policy Board

Recommendation on Best Practices for the Secure Access, Use, and Disclosure of Health Information

I. SUMMARY

HIE Policy Board Operations, Compliance, and Efficiency subcommittee proposes the publication of best practices for the secure access, use, and disclosure of health information. This listing is in response to § 8711.8 of the HIE final rule and span five (5) overarching categories, including:

1. Privacy & Security
2. Identity & Access Management
3. Data Use & Exchange
4. Audits
5. Organizational & Governance Considerations

The best practices aim to encourage the use of national and industry-recognized standards for HIE tools and initiatives. These best practices were adapted from existing criteria from industry-recognized accreditation and frameworks and were developed in conjunction with registered and designated entities.

II. PROBLEM STATEMENT

The HIE Final Rule identifies in §8700.3 that "*DHCF shall provide ongoing monitoring to ensure compliance with criteria for registration and designation of HIE entities.*" Similarly, § 8711.8 of the HIE final rule outlines that "*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*." In support of this, the Operations, Compliance, and Efficiency (OCE) subcommittee initially considered two simultaneous activities – (1) Developing monitoring and compliance plans for registered and designated entities, and (2) Creating a list of best practices that align with national standards and other industry trends. In this process, the subcommittee chose to first conduct research to establish best practices, which would then inform the development of Monitoring and Compliance plans for DC HIE entities. The subcommittee also researched several industry standard accreditations and certifications. However, many members indicated that while organizations are encouraged to voluntarily pursue accreditation, requiring HIE entities to obtain an accreditation may impose undue burden.

Subcommittee: HIE Operations, Compliance, and Efficiency

Chairs: Ms. Gayle Hurt

Date: April 27, 2023

Status: Draft

III. SUBCOMMITTEE GOAL AND ACTIVITY

This activity can be added under Goal #2 under the subcommittee's workplan – *Review and Recommend updates to baseline operational and benchmark performance standards.* This activity falls within the specific subcommittee activity of *Analyzing best practices in HIE operational standards and compliance*.

IV. DISCUSSION

The HIE Operations, Compliance, and Efficiency (OCE) subcommittee lists out five (5) overarching categories of best practices that promote the secure access, use, exchange, and disclosure of health information –

1. Privacy & Security
2. Identity & Access Management
3. Data Use & Exchange
4. Audits
5. Organizational & Governance Considerations

Each category has relevant subcategories of information aimed at encouraging the use of national and industry-recognized standards, exclusive of standards and practices included in legal and regulatory requirements. All categories were developed in conjunction with registered and designated entity representatives. As requiring an HIE entity to obtain an accreditation may be burdensome, the subcommittee chose to highlight select criteria from existing accreditation modules and other resources that may bolster HIE entity actions to support the secure use, access, and disclosure of health information. These best practices are located in Appendix 1. To ensure that these best practices remain updated, the subcommittee will periodically review these best practices to ensure alignment with the latest industry/national standards. Upon approval by the Policy Board, the finalized set of best practices will be posted on the DHCF HIE website. *Please note – the Stakeholder Engagement subcommittee is working on best practices related to HIE Education and Engagement. These best practices will be presented to the HIE Policy Board at a future meeting*.

V. RECOMMENDATION(S) FOR BOARD ACTION:

The Operations, Compliance, and Efficiency (OCE) subcommittee proposes that the DC HIE Policy Board approve the best practices in Appendix 1 for publication on the DHCF website.

***

***Committee Members*:** Ms. Gayle Hurt, Dr. Sonya Burroughs, Dr. Jessica Herstek, Ms. Lucinda Wade, Ms. Stephanie Brown, Mr. Ronald Emeni, Ms. Donna Ramos-Johnson, Mr. Jim Costello, Mx. Deniz Soyer, Ms. Adaeze Okonkwo, Mr. Robert Kaplan, Mr. Nathaniel Curry, Ms. Maava Khan and Ms. Asfiya Mariam

Subcommittee: HIE Operations, Compliance, and Efficiency

Chairs: Ms. Gayle Hurt

Date: April 27, 2023

Status: Draft

Appendix 1: Best Practices

Best Practices for the Secure Access, Use, and Disclosure of Health Information

The HIE final rule also outlines in §8711.8 guidance regarding nationally recognized standards for the secure access, use, and disclosure of health information. In response, the HIE Operations, Compliance, and Efficiency (OCE) subcommittee recommends the following best practices across several categories – these best practices may be utilized by registered and designated HIE entities in the District.

Please note: The best practices listed within these categories are intended as recommendations only.

Table of Contents

Subcommittee: HIE Operations, Compliance, and Efficiency

Chairs: Ms. Gayle Hurt

Date: April 27, 2023

Status: Draft

Category 1 – Privacy & Security

1.1 – General

- Organizations are encouraged to apply for and obtain certifications or accreditations that demonstrate compliance with industry standards for privacy and security by undergoing a third-party review. Some recommended accreditations are listed below.
  Please note that this list is not inclusive of all certifications or accreditations.
  - EHNAC Privacy & Security
  - EHNAC Health Information Exchange Accreditation Program
  - HITRUST r2 Validated Assessment

- When applicable, organizations are encouraged to include measures that adhere to the **latest** versions of established guidelines and standards related to health information access, privacy, and security. Current versions of these guidelines are listed below:
  - NIST Special Publication 800-171 (Rev. 2)
  - NIST Cybersecurity Framework (1.1)
  - NIST Special Publication 800-63-3
  - HHS Health Industry Cybersecurity Practices (HICP)

- Organizations are encouraged to develop and maintain a plan that ensures adherence to all relevant federal and state regulatory requirements. These include, but are not limited to:
  - Maintain notification procedures related to privacy, security, and breaches in compliance with HIPAA. *EHNAC HIEAP II.E.1*
  - Develop an implementation plan, including a timetable, for any applicable District and/or federal laws and regulations governing the use, access, maintenance, and disclosure of health information. *45 CFR 162*
  - Identify and maintain a staff person(s) responsible for privacy and security items as outlined in HIPAA, for example a Privacy Officer, Chief Technology Officer (CTO), and/ or Chief Information Security Officer (CISO). *45 CFR 164.308(a)(2)*
    - Note: If the organization is a registered HIE entity as part of the DC HIE, the registered HIE entity must follow additional requirements as listed within the DC HIE final rule.

- Organizations are encouraged to outline their processes and procedures regarding information collected from any direct entry tools. These may include (but are not limited to): *EHNAC HIEAP III - PHW Data*
  - Develop and maintain a process for the collection, storage, use, disclosure, and transmission of data entered using direct entry tools.

  - Establish formal policies to handle consumer requests to obtain data entered using direct entry tools, including providing a copy of the data, a process for amending/correcting information, and any requests to delete these data.
  - Provide technical assistance and guidance, where appropriate, to any third-party organizations that may utilize, or view data entered by or received by direct entry tools.

1.2 – Responses to Security Vulnerabilities

- Organizations are encouraged to establish a resiliency plan to deliver critical services for all operating states (such as, during an incident, recovery, and normal operations) *NIST CSF ID.BE-5*

- Organizations are encouraged to develop an incident classification grid that outlines the scope of the incident, types of information involved, and examples of events within each class. Utilize the incident grid to inform organizational response plan in the event of an incident. *NIST CSF ID.RA*

- Organizations are encouraged to develop an incident response plan to identify, respond, and document privacy, security, and cybersecurity incidents, including any measures that are taken to address these gaps. Recommended plan items may include: *45 CFR § 164.308(a)(6)*
  - Implementing measures to scan for vulnerabilities in systems and applications, as well as controls to remediate any gaps and correct any deficiencies. This may include: *EHNAC HIEAP VII. F and NIST CSF DE*
    - Establishing a baseline of data flows and operations for each authorized system/ user and a threshold for incident alerts *NIST CSF DE.AE-1 and NIST CSF DE.AE-5*
    - Implementing a continuous monitoring plan that works to identify network, physical environment, and personnel-related security threats and analyzes the effectiveness of existing incident prevention methods *NIST CSF DE.CM*
    - Maintaining and regularly updating a listing of system administrators or other relevant points of contact at participating organizations
  - Developing and maintaining workflows to ensure security updates to any deployed software, both internally at the organization and for any external parties (if appropriate). *EHNAC HIEAP VI.I.2*
  - Assigning roles and responsibilities for internal staff and related external stakeholders that clearly outline their roles and responsibilities in the event of a security incident. *EHNAC HIEAP VII. F and NIST CSF DE.DP-5, RS.IM, RC.IM*
  - Establishing an incident resolution plan to document, analyze, and contain any incidents or vulnerabilities as detected by internal systems, personnel, or external stakeholders. This may include: *NIST CSF RS.AN-5*

        - Conducting forensic analysis and root-cause investigations for effective response and recovery *NIST CSF RS.AN*
        - Initiating appropriate containment activities to prevent expansion *NIST CSF RS.MI-1*
        - Addressing any vulnerabilities that may have been exploited during the incident by either mitigating them or establishing them as accepted risks. *NIST CSF RS.MI-1*
    - Developing an incident recovery plan that includes any necessary remediation or recovery actions to restore affected systems *NIST CSF RC.RP-1*
    - Ensuring thorough documentation of incidents and related recovery activities and communicating these activities to internal and external stakeholders. *NIST CSF RC.CO-3*

- Organizations are encouraged to enhance incident response by continuously improving their processes and procedures related to incident detection, response, and recovery. *EHNAC HIEAP VII. F and NIST CSF DE.DP-5, RS.IM, RC.IM*

- Organizations are encouraged to implement a process to inform internal stakeholders, system administrators/ points of contact at participating organizations, DHCF Privacy and Security Officers of any exploitable security vulnerabilities, and external authorities as appropriate. *EHNAC HIEAP VII. F.2 and NIST CSF ID.RA-2*

1.3 – Reducing Cyber Risk, Technology Errors, and Omissions

- Organizations are encouraged to conduct quarterly threat and vulnerability assessments. Results from the assessment may be used to develop an improvement process. *EHNAC HIEAP VII.K. 3*

- Organizations are encouraged to, whenever appropriate, offer guidance and/or technical assistance to system administrators of participating organizations. *NIST CSF PR.AT*

- Organizations are encouraged to develop controls that ensure that internal networks are physically and logically separate from system components that are publicly accessible *EHNAC HIEAP VII.K. 3*

- When appropriate, organizations are encouraged to implement controls to maintain physical security of systems, equipment, and operating environments. Some recommended items include: *EHNAC HIEAP VII.J*
    - Controlling and managing physical access devices
    - Inventorying physical devices and systems and classifying them based on criticality, and business value *NIST CSF ID.AM-1 and ID.AM-5*
    - Maintaining audit logs of physical access
    - Safeguarding access to PHI in alternative/remote work sites

- Organizations are encouraged to have the ability to maintain a backup archive for all data stored for a minimum of seven (7) years. *EHNAC HIEAP II.E.1*

1.4– Considerations for Technology Providers

- Organizations that outsource any technology to third-party organizations are encouraged to take appropriate measures to ensure the safety of PHI. These measures may include:
  - Requiring third-party organizations to implement and maintain appropriate security controls for the protection of PHI *45 CFR § 164.308(b)(2)*
  - Providing guidance and resources to delegated third-party organizations regarding the protection of PHI *Common Agreement 12.1.5*
  - Developing a reasonable notice policy if the third-party organization ceases operations *HIE Final Rule*

- Organizations are encouraged to document how data is handled and stored by each third- party organization, including any backups, snapshots, maintenance, etc. *EHNAC HIEAP VII.L.7*

Subcommittee: HIE Operations, Compliance, and Efficiency

Chairs: Ms. Gayle Hurt

Date: April 27, 2023

Status: Draft

Category 2 – Identity & Access Management

2.1 – Mapping Authorized Users of the HIE

- HIE entities are encouraged to educate participating organizations on how their users can access the HIE. This may include developing policies, when appropriate, to identity proof any users as they directly access the HIE, such as the use of third-party authentication systems. *EHNAC HIEAP IX and HIE Final Rule*

- Organizations are encouraged to develop and maintain an access grid that maps user types and outlines recommended levels of access. Access permissions may be managed by categorizing individuals by using the principles of least privilege and separation of duties*. *MD Rule - 10.25.18.05 §D and NIST CSF PR.AC-1 4*

- Organizations are encouraged to ensure that user access policies are appropriately tailored to address all user types that access the HIE (such as participating organizations, non-HIPAA covered entities, and health care consumers), including any data trading partners. *EHNAC HIEAP IX*

- Organizations are encouraged to ensure that issuance, verifications and/or revocation of credentials for authorized users are appropriately managed and regularly audited to limit any unauthorized access*. *NIST CSF PR.AC-1*

  **Note – This practice may differ based on how users access the HIE. For organizations that utilize Single Sign On (SSO) features to access the DC HIE, a user may be onboarded to the practice's EHR, and would thereby obtain access to the DC HIE. The practice may also have policies specific to issuance, verification, and revocation of credential. In these instances, HIE entities are encouraged to provide technical assistance and guidance to these participating organizations.*

2.2 – Identity Proofing and Authentication

- Organizations are encouraged to adopt and implement an authentication process to include: *MD Rule - 10.25.18.05 §D, EHNAC HIEAP VIIA*
  - Authentication of a ***human user*** at log in, to comply with **Level 2** of the latest requirements in NIST Special Publication 800-63
  - Ensuring that all ***automated systems*** that access PHI have a human sponsor, and that electronic authentication of the automated system complies with **Level 3** of the latest requirements in NIST Special Publication 800-63
  - Encouraging multi-factor authentication at log in, which includes a username, password, and/ or device registration.

  - Assigning a unique name and/or number for identifying and tracking user identity.
  - Recording authentication actions of each unique user and ensuring the encryption of stored authentication data to the latest industry standards (including active and non-active user IDs and passwords)
  - Recording authorized user attestation regarding the purpose of accessing PHI.

- Organizations are encouraged to develop and maintain policies regarding identity proofing for health care consumers when they access PHI (when allowed). This may include: *ONC Identity Management Guide and EHNAC HIEAP VII*
  - Processes for issuing and managing digital credentials for consumers.
  - Identification and management of consumer relationships to family members and caregivers
  - Policies regarding PHI access for minors

2.3 – Patient Matching

- Organizations are encouraged to follow the latest version of the ONC Interoperability Standards Advisory (ISA) criteria on patient record matching. Some recommended standards and implementation specifications are listed below. *2023 ISA Standards*
  - Patient Demographic Record Matching standards from HL7 2.5.1 (or later), IHE specifications for patient demographic queries
  - ONC Project US@ Technical Specifications for Patient Addresses – *Version 1.0,*
    January 2022
  - AHIMA Recommended Data Elements for Capture in the Master Patient Index –
    January 2022
  - FHIR at Scale Taskforce (FAST) Initiative Identity Tiger Team recommendations and proposed solutions

Subcommittee: HIE Operations, Compliance, and Efficiency

Chairs: Ms. Gayle Hurt

Date: April 27, 2023

Status: Draft

Category 3 – Data Use & Exchange

3.1 – Aligning to Industry Standards for Clinical Data and Data Sharing

- Organizations are encouraged to implement policies and procedures to maintain compliance with the Information Blocking section of the 21st Century Cures Act. *Section VIII.B*

- Organizations are encouraged to document data provenance whenever possible by adhering to industry standards and implementation specifications, with the goal of ensuring data authenticity, reliability, and trustworthiness of data received from participating organizations and/or HIE users that utilize direct entry tools. *2023 ISA Standards*

- Organizations are encouraged to augment their interoperability efforts by:
  - Educating third-party application developers regarding the CARIN Code of Conduct
  - Utilizing the HL7 FHIR Implementation Safety Checklist and ONC's Inferno Framework to analyze the impact of FHIR on system design and for FHIR conformance testing.

3.2 – General Practices regarding Data Sharing

- Organizations are encouraged to work with connected provider organizations (such as hospitals) to transmit data elements necessary to support timely and effective transitions of care. These may include:
  - Enhancing outreach and engagement efforts with organizations that have recently upgraded legacy EHR systems to enhance data sharing.
  - Evaluating differences in nomenclature (CCD vs FHIR) to inform standardization efforts.
  - Encouraging expedited transmission of data elements that may be more time- sensitive or may have an impact on care decisions (such as ADT notifications, Z- codes, etc.)

- Organizations are encouraged to collaborate with District partners and connected provider organizations to establish appropriate expectations around information sharing. These may include:
  - Identifying facility-specific examples or stories to describe ideal timelines for information sharing.
  - Cataloguing facility-specific examples to illustrate any differences in timelines.

Subcommittee: HIE Operations, Compliance, and Efficiency

Chairs: Ms. Gayle Hurt

Date: April 27, 2023

Status: Draft

Category 4 – Audits

4.1 – General

- Organizations are encouraged to adhere to the current version of the audit standards as established in 45 CFR 170.210. *45 CFR 170.210(e)*

- Organizations are encouraged to maintain a clear, accurate, and accessible audit trail for all data transactions, user access logs, and physical access logs for a minimum of seven years. *EHNAC HIEAP, NIST CSF PR.PT-1, and HIE final rule 8704.1(g)*

- Organizations are encouraged to implement mechanisms that: *EHNAC HIEAP*
    - Monitor usage patterns to determine suspicious activity by users.
    - Provide alerts to the entity in the event of an audit logging process failure.
    - Match internal system times to an authoritative source to generate audit record time stamps.
    - Protect audit information and logging tools from unauthorized access and deletion. These may include limiting access to a subset of users.

- Organizations are encouraged to have policies requiring audits to monitor compliance with existing HIE policies, federal and District privacy laws, and to check for third-party organization compliance to privacy requirements. *EHNAC HIEAP*

- Organizations are encouraged to conduct an annual independent audit of their financial statements to demonstrate consistency with generally accepted accounting principles and requirements. *EHNAC HIEAP*

4.2 – Audits of Information from Direct Entry Tools

- Organizations are encouraged to have policies and procedures regarding the audit of information entered using direct-entry tools on the HIE, or where the HIE is the originator of patient data. This may include:
    - User access logs
    - Patient requests for copies of data
    - Change logs to monitor amendments or deletion to the data by the patient or by a member of their care team.

- Organizations are encouraged to implement policies and procedures regarding patient- generated data. *EHNAC HIEAP*

Subcommittee: HIE Operations, Compliance, and Efficiency

Chairs: Ms. Gayle Hurt

Date: April 27, 2023

Status: Draft

Category 5 – Organizational & Governance Considerations

5.1 – General

- Organizations are encouraged to implement an organizational framework that includes a formal structure (such as a governing board) that provides oversight for the exchange of health information and ensures accountability to the organization's goal. This governing body may: *HIEAP Criteria VI.P and TEFCA QHIN Onboarding SOP*
    - Have an established structure that outlines key personnel and how they work with the governing body to support electronic exchange of health information.
    - Be representative of participating organizations.
    - Have established meeting procedures (such as meeting cadence and officer roles)
    - Have an established dispute resolution mechanism that ensures that any issues are resolved collaboratively.

- Organizations are encouraged to implement processes that support organizational efficiency. These include:
    - Regular maintenance of organizational documents (such as bylaws, organization mission, articles of incorporation, participation agreements etc.), along with any related amendments.
    - Workflows to ensure that the HIE is only used for purposes that are established within §§ 8703.2 and 8703.3 of the HIE final rule.
    - Maintenance and tracking of any certifications or accreditations it may hold, along with any related documentation.
    - A financial model that outlines the organization's approach to financial sustainability, including pricing models/ user fees (if any) and any plans that address how the organization will manage increasing participation.