


<p style="text-align: center;">GOVERNMENT OF THE DISTRICT OF COLUMBIA</p>  <p style="text-align: center;">DEPARTMENT OF BEHAVIORAL HEALTH</p>	<p>Policy No. 115.6A</p>	<p>Date 1/23/23</p>	<p>Page 1</p>
	<p>Supersedes DBH Policy 115.6, DBH Electronic Health Records, dated November 21, 2016</p>		
<p>Subject: DBH Electronic Health Records</p>			

1. **Purpose.** To establish a policy that clarifies requirements governing the use and maintenance of electronic health records (EHR) for Department of Behavioral Health (DBH or the Department) certified providers. The intent of this policy is to outline the requirements and procedures for providers to: 1) ensure that their EHR system is certified with the Office of the National Coordinator for Health Information Technology (ONC); 2) transition from a Fully Integrated Provider (FIP) to a Partially Integrated Provider (PIP); and 3) submit Behavioral Health Supplemental Data (BHSD) from the provider's EHR system to DBH.
2. **Applicability.** All DBH-certified providers with a Human Care Agreement (HCA).
3. **Authority.** Mental Health Information Act (MHIA), D.C. Official Code §§ 7-1201.01 *et seq.* and DBH Policy 1000.3 Privacy Manual, dated January 13, 2014.
4. **Superseded Policy.** This policy replaces Policy 115.6 DBH Electronic Health Records, dated November 21, 2016.
5. **Background.** EHR assist providers in supporting patient care by storing electronic Protected Health Information (ePHI). All providers within the DBH network must maintain an EHR system for mental health and Substance Use Disorder (SUD) services. The Department currently utilizes the Integrated Care Applications Management Systems (iCAMS) EHR system to document mental health services and supports, and the DATA WITS system for SUD services and supports. Providers may opt to use the full iCAMS or DATA WITS system as a FIP or partially use the iCAMS or DATA WITS system as a PIP in accordance with applicable regulations and legal standards. As providers transition from FIPs to PIPs, they must coordinate their EHRs using the process outlined in this policy.
6. **Definitions.**

Behavioral Health Supplemental Data. Client-level information about consumers/clients and the services they receive from a DBH-Certified mental health and SUD treatment providers.

Business Associate. A person or organization who performs work or activities on behalf of a covered entity that may involve the use or disclosure of Protected Health Information (PHI).

Consumers/clients. People who are eligible to receive behavioral health services and/or supports from DBH or its certified providers.

DBH Network. For purposes of this policy, all DBH-certified providers with an HCA who render or coordinate care to consumers and/or clients.

Electronic Health Record (EHR). An electronic record of patient health information from one or more encounters in any care delivery setting. The EHR generates a complete record of clinical encounters and supports other care-related activities.

Electronic Protected Health Information (ePHI). PHI that is produced, saved, transferred or received in electronic form.

Fully Integrated Provider (FIP). Providers that opt to use the full iCAMS or DATA WITS system without using any other EHR systems.

Legal Health Record (LHR). Documentation generated at or for a healthcare organization, identified by that organization as its business record, which would be released upon request. The legal health record is a subset of records from the designated record set.

Network Providers. Both DBH direct services staff and DBH provider agencies with an HCA that provide mental health or SUD treatment services and supports.

Partially Integrated Provider (PIP). Providers that opt to partially use iCAMS or DATA WITS while also using other real-time interfacing systems.

7. Policy.

7a. DBH has historically provided access to the iCAMS and DATA WITS EHR systems to network providers. DBH will no longer provide EHR service to network providers beginning on October 1, 2023. Consequently, by October 1, 2023, each network provider must take all necessary steps to procure an EHR system that complies with the MHIA, Health Insurance Portability and Accountability Act (HIPAA) and 42 Code of Federal Regulations (C.F.R.) Part 2; meets the standards established by ONC for Health Information Technology Certification Program; and has the ability to accurately document the services and supports provided to consumers/clients. All network providers' EHR systems must meet the criteria for meaningful use as defined 42 C.F.R. § 495.24.

7b. The iCAMS EHR is an integrated system with the capacity to share ePHI between the Department and other network providers when authorized by HIPAA, MHIA or 42 C.F.R. Part 2. DBH and network providers that utilize iCAMS or DATA WITS shall have joint legal responsibilities to protect the data in each system in accordance with HIPAA, the MHIA and 42 C.F.R. Part 2. Each organization must identify the content required for its own LHR as well as the standards for maintaining the integrity of that content.

8. Procedures.

8a. Network Provider Responsibilities

(1) Each network provider shall designate staff members who will function as the privacy officer and the custodian of record. The privacy officer may be the custodian of the network provider's LHR and partner with IT personnel to ensure compliance with HIPAA, the MHIA and/or 42 C.F.R. Part 2.

(a) The Custodian of LHR shall ensure that the network provider's EHR is properly and securely maintained and shall serve as the point of contact for LHR.

- (b) IT personnel shall manage the EHR's technical infrastructure.
- (2) Network providers shall use and maintain an EHR system that collects uniform information that meets the following criteria:
 - (a) Represents the person's health history (*e.g.*, a record of health status and the services provided over time);
 - (b) Provides a method for clinical communication and treatment planning among providers and practitioners serving the person;
 - (c) Serves as the legal document describing the healthcare services provided; and
 - (d) Serves as a source of data for the behavioral health services and outcomes that that the network provider renders.
- (3) The Integrated Technology Engine (ITE) Provider Extract Companion Guide outlines the instructions for network providers to submit Behavioral Health Supplemental Data (BHSD) transactions through their own EHR system. The ITE Guide is available at <https://dbh.dc.gov/>. Providers must submit BHSD monthly within ten (10) calendar days from the last day of the reporting period as defined in the ITE Provider Extract Companion Guide. Providers must submit BHSD for all consumers/clients served regardless of payor.
 - (a) By October 1, 2023, all providers shall migrate their records from DATA WITS and iCAMS to their own EHRs.
 - (b) Providers must submit a successful test BHSD file transfer to DBH before October 1, 2023.
 - (c) DBH providers with their own EHR shall begin to submit BHSD following successful submission testing.

8b. Network providers shall create written user access protocols as follows:

- (1) Appropriate controls for systems (*e.g.*, workstations, interfaces, applications, processes, or other computer-based mechanisms) for accessing ePHI based on authorized personnel's role including the following:
 - (a) Unique identification/authentication mechanism with appropriate user ID/password specification requirements;
 - (b) Password protections that enforce the use of passwords as part of the identification/authentication mechanism (*e.g.* restrictions on login attempts); and
 - (c) Controlled privileged user accounts (*e.g.* system administrators who typically require higher levels of access to ePHI).
- (2) Procedures that require managerial approval before any person is granted access to systems managing EHR, to include the following:

- (a) Limiting authorized individual's access to the EHR only to the extent necessary for that individual's job responsibilities;
- (b) Immediate termination of access to the EHR when the employment of an individual ends or the job responsibilities no longer warrant access to the EHR; and
- (c) Periodically reviewing the EHR accounts to ensure that only currently authorized individuals have access.

8c. Network providers shall establish administrative safeguards including the following:

- (1) Sanctions against staff who fail to comply with the security procedures in their organization per personnel policies and procedures.
- (2) Procedures to regularly review records of information systems activity, such as audit logs, access reports, and security incident tracking report. Audit logs shall generate records when auditable events happen, including but not limited to the following:
 - (a) User login/logouts;
 - (b) Each occurrence that the chart created, viewed, updated, or deleted;
 - (c) System security administration (e.g. system account setup, backend management of application);
 - (d) System starts and stops;
 - (e) Scheduling;
 - (f) Query;
 - (g) Order;
 - (h) Node-authentication failure;
 - (i) Signature created or validated;
 - (j) Download and/or exports;
 - (k) PHI import (e.g., from external information source); and
 - (l) Develop access rights procedures which assign unique names or numbers for identifying and tracking user identity. Such procedures shall ensure appropriate access during an emergency. Electronic sessions shall terminate automatically after a predetermined time. EPHI shall be encrypted and decrypted when necessary for electronic transmission.
- (4) Establish procedures for the authorization and/or supervision of staff who work with the EHR or in locations where it might be accessed.
- (5) Develop procedures that determine staff access, if any, to the EHR.
- (6) Implement procedures for terminating access to the EHR when employment ends or need for access no longer exists.

- (7) Employ procedures for responding to, documenting, reporting and mitigating suspected or known security incidents, including reporting the incident pursuant to DBH Policy 480.1B, Reporting a Major Unusual and an Unusual Incident.
- (8) Ensure access protections to the EHR with business associates are contractually delineated and enforced.

8d. Network providers shall establish physical safeguards that address the following:

- (1) Access: Network providers shall adopt procedures that grant access to the EHR by establishing, documenting, reviewing and modifying a user's right of access to workstation software application, transaction, or process.
- (2) Business continuity: Network providers shall adopt procedures that ensure that exact data backups are maintained and retrievable to enable continuation of critical business processes and ensure the security of ePHI in an emergency.
- (3) Physical access: Network providers shall implement procedures to limit physical access to ePHI at the facility/facilities in which they are housed to only those staff who are properly authorized to access it.
- (4) Media movement: Network providers shall establish protocols that govern the receipt and removal of hardware and electronic media that contain ePHI in, out and within the facility.
- (5) Media final disposition: Network providers shall institute procedures that address the final disposition of ePHI, including the hardware or electronic media on which it is stored. Procedures shall include removal process of ePHI from electronic media before it is made available for other's use or before discarding.
- (6) Data exchange: Network providers shall ensure the secure exchange of data that is received and transmitted between entities in accordance with HIPAA, the MHIA and/or 42 C.F.R. Part 2.

8e. Network providers shall institute technical safeguards including:

- (1) Data Integrity: Procedures that protect ePHI from improper alteration or destruction, which shall include a mechanism to authenticate ePHI and corroborate that it has not been altered or destroyed in an unauthorized manner.
- (2) Authentication: Procedures or mechanisms to verify the identity of the person or entity seeking access to ePHI.
- (3) Data Transmissions: Technical safeguards to ensure ePHI transmitted over an electronic communications network is not accessed by unauthorized persons or groups, and that such information is not improperly modified without detection.

8f. Network providers shall ensure system integrity by:

- (1) Conducting staff training on HIPAA, the MHIA and 42 C.F.R. Part 2.
- (2) Ensuring the EHR identifies changes to the original entry such as addendums, corrections, deletions and amendments.

(3) Ensuring audit trails include the name of the user, the application triggering the audit, workstation, specific document, a description of the event being audited (*e.g.*, amendment, correction, or deletion with the date and time). The audit trail must capture the triggering event (including deletions) within the EHR and provide auditors a starting point for compliance audits.

(4) Complying with the DBH Policy 1000.3A, DBH Privacy Manual.

9. Fully Integrated to Partially Integrated Processes.

9a. Network providers transitioning from a FIP to a PIP must coordinate with their Provider Relations Specialist in advance of the transition and complete the following at least ninety (90) calendar days in advance of the transition from FIP to PIP. In order to meet the October 1, 2023 deadline for providers to establish their own EHR system, all FIPs must initiate the transition process no later than July 1, 2023:

(1) Provide written notification of the transition to their Provider Relations Specialist.

(a) After a network provider notifies the Department in writing of its transition, the network provider may only create new user accounts as a PIP for a minimum of two (2) and maximum of twenty (20) new users.

(b) If the PIP provider utilizes iCAMS for a program in which FIP status is required (*e.g.* Health Homes), 9a(1)(a) does not apply. In this instance, the provider must follow the same guidelines set for FIPs.

(c) Provide written confirmation to the Provider Relations Specialist that the partially-integrated EHR vendor's system complies with the requirements outlined in this policy.

(2) Coordinate with the new EHR vendor to determine the required format for the import of data, *e.g.*, authorizations, visit/service data, or eligibility information.

(3) Submit a test claims batch of local claims to the Claims and Billing Division of DBH using the new EHR vendor format. DBH Claims staff will confirm the format of the new EHR and work with the network provider to resolve any formatting issues.

9b. Thirty (30) calendar days before the system transition, the network provider shall update DBH with the import data format. DBH IT staff will process the network provider's request for import data using the successfully tested format within ten (10) business days of receipt.

9c. Following the system transition from FIP to PIP:

(1) Within thirty (30) calendar days the network provider shall finalize any outstanding documentation of clinical services by clinicians, front desk staff, and Core Service Agency Administrators.

(2) Within ninety (90) calendar days:

(a) The network provider shall complete billing and reconcile all local dollar claims in iCAMS.

- (a) DBH IT staff will deactivate all non-administrative iCAMS accounts and put provider administrative accounts on limited access. Limited access will include access to the Administrative Program, which grants the provider the ability to submit requests, *e.g.*, specialty service, supplemental units, and discharge/disenrollment.
- 10. **Compliance**. All network providers shall ensure that contributors to the EHR within their organization adhere to this policy.
- 11. **Contact**. Questions regarding the transition from FIP to PIP are to be directed to the Provider Relations Specialist.

Approved By:
Barbara J. Bazron, Ph.D.
Director, DBH

Barbara J. Bazron 01/23/2023
(Signature) (Date)