

**Department of Behavioral Health
TRANSMITTAL LETTER**

SUBJECT Electronic Health Records		
POLICY NUMBER DBH Policy 115.6	DATE NOV 21 2016	TL# 305

Purpose. To establish policies and procedures on electronic health records (EHR)..


Applicability. Applies to DBH, DBH-certified or licensed providers with a Human Care Agreement and contractors.


Policy Clearance. Reviewed by affected responsible staff and cleared through appropriate Behavioral Health Authority (BHA) offices and providers (see applicability above).

Effective Date. This policy is effective immediately.

Superseded Policy. None.

Distribution. This policy will be posted on the DBH web site at www.dbh.dc.gov under Policies and Rules. Applicable entities are required to ensure that affected staff is familiar with the contents of this policy.


Tanya A. Royster, MD **Date** 11/21/2016
Director, DBH

GOVERNMENT OF THE DISTRICT OF COLUMBIA  DEPARTMENT OF BEHAVIORAL HEALTH	Policy No. 115.6	Date NOV 21 2016	Page 1
	Supersedes: None		
Subject: Electronic Health Records			

1. **Purpose.** To establish policies and procedures on electronic health records (EHR).
2. **Applicability.** Applies to DBH, DBH-certified or licensed providers with a Human Care Agreement and contractors.
3. **Authority.** Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub. L. 104–191, enacted August 21, 1996); The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009; The DBH Policy 1000.3 Privacy Manual, dated January 13, 2014.

4. **Definitions.**

Business Associate. A person or organization who, on the organization’s behalf, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, and practice management or provides legal, actuarial, accounting, consulting, data aggregation, accreditation, or financial services.

Business record. A document (hard copy or digital) kept in the normal course of business that records business dealings.

Designated record set. Any item, grouping, or collection of information that includes protected health information (defined in 45 C.F.R. § 160.103) and is maintained, collected, used, or disseminated by or for a covered entity.

Electronic Health Record (EHR). An electronic record of patient health information from one or more encounters in any care delivery setting. The EHR automates and streamlines the clinician’s workflow. The EHR generates a complete record of clinical encounters, as well as supporting other care-related activities directly or indirectly via interface, such as evidence-based decision support, quality management and outcomes reporting.

Electronic Protected Health Information (EPHI). Protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in electronic

form.

Individuals or persons. DBH consumers of mental health (MH) services, clients participating in substance use disorder (SUD) treatment services or individuals in care who are treated at Saint Elizabeths Hospital.

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.

Providers. Both DBH direct services staff and DBH provider agencies with a Human Care Agreement and contractors who provide mental health or substance use disorder treatment services.

5. **Policy.** The DBH Network shall maintain a behavioral health record that accurately documents care and services provided to individuals receiving services from DBH or a DBH provider. Behavioral health records must be maintained in a manner that complies with applicable HIPAA regulations, accreditation standards, professional practice standards, and legal standards. The Department currently utilizes the Integrated Care Applications Management Systems (iCAMS) Electronic Health Record (EHR) system for documentation activity related to mental health services and the DATA WITS system for substance abuse services. The iCAMS EHR is an integrated system with the capacity to share protected health information between the Contractor, the Department, and other network providers when authorized by the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”) and associated regulations promulgated at 45 CFR Parts 160, 162 and 164 as amended, and the D.C. Mental Health Information Act (“MHIA”), D.C. Official Code § 7-1201.01 et seq. DBH and its Network providers that utilize iCAMS or DATA WITS have joint legal responsibilities to protect the data in each system in accordance with the HIPAA Privacy and Security Rule, the MHIA and 42 CFR Part 2, as applicable. Therefore, each organization must identify the content required for its own legal health record as well as the standards for maintaining the integrity of that content.

6. **Responsibilities and Procedures.** DBH providers shall:

6a. Designate a staff member who will function as the health information privacy officer. The health information privacy officer shall be the custodian of the provider’s legal health record (LHR)¹ and partner with the information technology (IT) personnel² to ensure compliance with the HIPAA privacy and security rule.

6b. Use and maintain an EHR system that is able to collect uniform information that meets the following criteria: (1) represents the person’s health history (e.g., a record of health status and

¹ Custodian of LHR addresses the maintenance and security of all written and electronic health records within a facility and shall serve as the point of contact for LHR.

² Information technology personnel manage the technical infrastructure of the EHR.

the services provided, over time); (2) provides a method for clinical communication and treatment planning among providers and practitioners serving the person; (3) serves as the legal document describing the healthcare services provided; and (4) serves as a source of data for clinical, health services, and outcomes for mental health and substance use services. The EHR shall have the standardized field requirements:

- (1) Demographics and Eligibility Verification
 - a. Name
 - b. Date of birth
 - c. Identification Number (assigned number for EHR)
 - d. Address
 - e. Living situation³
 - f. Residency Status
 - g. Gender
 - h. Contact information
 - i. Legal status (e.g., guardianship information, as applicable)
 - j. Emergency contact
 - k. Family members
 - l. Advocate, as applicable
 - m. Primary health care contacts
 - n. School or employment status
 - o. Other relevant information (as determined by clinician)

- (2) Consents and Declarations
 - a. Signed privacy Forms
 - b. Consent to participate in service/care
 - c. Other signed and dated consents for treatments including psychotropic medications
 - d. Other releases, as appropriate
 - e. Advance directives
 - f. Signed review of consumer's rights and responsibilities and grievance procedures.

- (3) Assessments.

- (4) Encounter notes.

- (5) Treatment Plan.

- (6) Other Documentation. Documents as required by regulation or as determined to be necessary by clinician:
 - a. Advance directives discussion
 - b. Referrals/Consults and Transfer of Responsibility

³ Best description of person's residential circumstance (e.g., house, apartment, living with family or friend, homeless).

c. Discharge Summary/planning

6c. Create user access protocols as follows:

(1) Appropriate controls for systems (e.g., workstations, interfaces, applications, processes, or other computer-based mechanisms) for accessing electronic protected health information (EPHI) based on authorized personnel's role including the following:

- a. Unique identification/authentication mechanism with appropriate formats.
- b. Password protections that enforce the use of passwords as part of the identification/authentication mechanism.
- 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. Background checks, where appropriate, before any individual is granted access to EHR.
- b. Limiting authorized individual's access to EHR only to the extent necessary for that individual's job responsibilities.
- c. Terminating access to EHR when the employment of an individual ends or the job responsibilities no longer warrant access to EHR.
- d. Periodically reviewing the EHR accounts to ensure that only currently authorized individuals have access.

6d. Establish administrative safeguards that shall include 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. Chart created, viewed, updated, or deleted
- c. System security administration
- 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)

l. System administration

(3) 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 EHR or in locations where it might be accessed.

(5) Develop procedures that determine staff access, if any, to EHR.

(6) Implement procedures for terminating access to 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. Such suspected or known incidents are subject to the DBH Policy on Major Unusual Incidents and Unusual Incidents.

(8) Ensure access protections to EHR with business associates are contractually delineated.

6e. Establish physical safeguards that address the following:

(1) Access. Providers shall have procedures that grant access to EHR by establishing, documenting, reviewing, and modifying a user's right of access to workstation, software application, transaction, or process.

(2) Business continuity. Providers shall have exact data backups that are maintained and retrievable. Such procedures shall enable continuation of critical DBH business processes for the security of EPHI while operating in an emergency.

(3) Physical Access. Providers shall implement procedures to limit physical access to EPHI at the facility/facilities in which they are housed, yet ensure properly authorized access is allowed.

(4) Media movement. Providers shall establish protocols that govern the receipt and removal of hardware and electronic media that contain EPHI into the facility, out of the facility, and the movement of these items within the facility.

(5) Media final disposition. 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.

6f. Institute technical safeguards that shall include:

(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 insure 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.

6g. Ensure system integrity:

(1) Conduct staff training on HIPAA privacy and security requirements.


(2) Ensure the EHR identifies changes to the original entry such as addendums, corrections, deletions and amendments.

(3) Ensure audit trails include the name of the user, the application triggering the audit, workstation, specific document, and 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 health record and provide auditors a starting point for compliance audits [also, see sec. 6d (2)].

(4) Any authorization for release of information must comply with the DBH Privacy Manual.⁴

7. **Compliance.** All providers and contractors shall ensure that contributors to the EHR within their organization follow this policy, and internal procedures and protocols related to this policy.

Approved by:


Tanya A. Royster, MD (Date) 11/21/2016
Director, DBH

⁴ DBH Privacy Manual, 1000.3, January 13, 2014.