Department: Health Services Department	**Number:** HS-041
Title: Records and Document Management	
Original Effective Date: 1/1/2021	**Latest Revision Date:** 6/3/2025

PURPOSE:

To outline standardized procedures for records and document management within the Sonder Health Plans ("SHP") Health Services Department ("HSD") to support effective care coordination, data integrity, and regulatory compliance. This policy applies to all employees, contractors, and consultants within the HSD of SHP as well as all activities within the HSD, including electronic and paper-based records, and ensures adherence to HIPAA, HITECH, and Georgia state-specific regulations.

POLICY STATEMENT:

The HSD of SHP is committed to maintaining accurate and complete records and documentation in accordance with federal, state, and CMS regulations. This policy establishes procedures for the creation, storage, retention, and disposal of records and documents to ensure compliance, confidentiality and accessibility in compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH), and applicable Georgia healthcare privacy laws.

DEFINITIONS:

- **Record:** Any documented information created, received, and maintained as evidence and information by the U.S. Department of Health and Health Services (HHS) or other regulatory body, including medical records, authorizations, case notes, and communication logs.
- **Document Management:** The process of handling documents in a way that allows for storage, retrieval, security and eventual disposal.
- **Confidential Information:** Any personal, health, or sensitive information that is protected by privacy laws and regulations, such as HIPAA and Georgia healthcare privacy laws.
- **Georgia Healthcare Privacy Laws**: State-specific regulations governing the protection, use, and disclosure of healthcare information, including O.C.G.A. § 31-33-2 (Access to Medical Records)
- **HIPAA** (The Health Insurance Portability and Accountability Act of 1996) - Federal law that protects the privacy and security of health information.
- **HITECH Act** – Federal law that promotes the adoption and meaningful use of health information technology, enhancing privacy and security protections for health data.
- **Protected Health Information** ("PHI") – individually identifiable health information, held or maintained by a covered entity or its business associates acting for the covered entity, that is transmitted or maintained in any form or medium (including the individually identifiable health information of non-U.S. citizens). This includes identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse. For purposes of the Privacy Rule, genetic information is considered to be health information.

PROCEDURES:

I. Record Creation and Documentation Standards:

A. **Documentation Requirements:**
   i. All HSD staff will document interactions, clinical decisions, and care coordination activities accurately and timely in the member's health record. Documentation should include:
      a. Member Identification (name, SHP ID number, date of birth).
      b. Date, time, and type of interaction (e.g. telephonic, email).
      c. Details of clinical decisions, authorizations, and care coordination.
      d. Follow-up actions and next steps.

B. **Use of Electronic Health Records (EHR) and SHP Systems:**
   i. All HSD Staff will utilize approved electronic systems for all documentation to ensure consistency, accessibility, and data integrity in compliance with HITECH Act requirements.
   ii. All HSD Staff will ensure all entries are accurate, legible, and appropriately dated and signed.
   iii. SHP has implemented measures to track and log access to electronic records.

II. <u>Record Storage and Security:</u>

A. **Electronic Record Storage:**
   i. All HSD Staff will store all electronic records in the designated EHR or SHP system with appropriate security measures.
   ii. This includes ensuring systems are password-protected, encrypted, and accessible only to authorized personnel to comply with HITECH Act provisions for secure electronic health information and Georgia laws on electronic data protection.

B. **Physical Record Storage:**
   i. All HSD Staff will ensure physical records are stored in secure, locked cabinets within the HSD or other designated secure storage space.
   ii. Access to physical records is limited to authorized SHP personnel only.
   iii. Physical records should be converted to Electronic Records and stored electronically whenever possible.

C. **Remote Access Protocols:**
   i. Remote access will be through secure channels (e.g., VPN) and adhere to SHP's cybersecurity policies. Protocols comply with HITECH Act requirements for secure electronic access to PHI. When working remotely, staff will follow SHP's PHI policies and protocols.

III. <u>Record Retention and Disposal:</u>

A. **Record Retention Period:**
   i. All HSD Staff will retain records for the duration of time required by federal, state, and CMS regulations, including the HITECH Act and Georgia healthcare privacy laws.
   ii. Standard:
      a. Generally, follow the retention schedule in SHP's Records Retention Policy (CO-017).
      b. Medical Records retention: Minimum of 10 years from the last date of service.
      c. Authorizations and care plans: Minimum of 10 years or as required by applicable laws.

B. **Disposal of Records:**
   i. All HSD Staff will dispose of records that have met their retention period in a secure and compliant manner and will use the approved methods for disposal as described in SHP's Records Retention Policy (CO-017).

IV. <u>Access and Confidentiality:</u>

A. **Access to Records:**
   i. HSD Staff will grant access to records only to authorized personnel who need it to perform their job duties, the member, and others as outlined in HIPAA's permitted uses and disclosures.
   ii. Access will be role-based, as established by SHP, and follow the principle of least

privilege to ensure compliance with applicable state and federal requirements.

B. **Confidentiality of Records:**
   i. HSD Staff will ensure all records containing confidential information are handled in accordance with SHP's protocols as well as applicable regulatory guidance, including the use of encryption and other security measures.
   ii. Confidential information should not be shared or disclosed without appropriate authorization.

C. **Member Rights to Access Records:**
   i. Unless otherwise prevented by law as outlined in 45 CFR 164.524(a)(2), HSD Staff will provide members with access to their records upon request, utilizing SHP's internal procedures for release of member information, as noted in ii, below.
   ii. HSD Staff will coordinate these efforts with SHP's Compliance Officer or other SHP designee to ensure that medical information is released only in accordance with applicable Federal or state law or pursuant to court orders or subpoenas.
   iii. HSD Staff or SHP's records request designee will respond to member requests within 30 days and provide records in the preferred format when feasible. Electronic copies will be provided securely in accordance with HITECH Act provisions.

D. **Permissible Charges for Copies of Medical Records:**
   i. HSD Staff or SHP's records request designee will ensure that fees for providing copies of medical records to an individual are in alignment with HIPAA requirements. Specifically, HIPAA allows SHP to use either a flat fee of $6.50 or calculate the average or actual cost of copying medical records.
      a. The HIPAA Privacy Rule permits a "reasonable, cost-based fee" that may include only the cost of: (1) labor for copying the PHI requested by the individual, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media (e.g. CD or USB drive) if requested; (3) postage if the request is to have the records mailed; (4) preparation of an explanation or summary of the PHI, if agreed to by the individual.

V. <u>Examples of SHP documentation covered under this policy and procedure (this is not an exhaustive list):</u>

A. Member Identification; Requestor's Information; Rendering Provider Information
B. Request Dates
C. Services Requested (approved and standardized codes/descriptions)
D. Date(s) of Service (DOS); Place of Service (POS)Diagnosis
E. Visits/Units/Measurements
F. Priority Requested/Changes
G. Determination Dates/Times, as applicable
H. Indicator/Evidence of Clinical Reviews
I. Verbal Notifications Date/Time, as applicable
J. Written Notifications Date/Time, as applicable
K. Re-openings
L. Supporting medical records (labs, H&P, diagnostic studies etc.)

<u>ATTACHMENT(S):</u>

<u>N/A</u>

<u>STATUTORY REFERENCE(S):</u>

- **Federal**
  - 42 CFR §422.118: Confidentiality and Accuracy of Enrollee Records
  - 42 CFR § 422.119: Access to and Exchange of Health Data and Plan Information
  - 42 CFR 422.504(d) and (e)): Maintenance of Records; Access to Facilities and Records
  - 45 CFR § 164.524(c)(4): Access of Individuals to Protected Health Information
  - HITECH Act: Title XIII of the American Recovery and Reinvestment Act of 2009

- CMS Medicare Managed Care Manual: Chapter 4, Benefits and Beneficiary Protections
- **State**
  - Georgia Healthcare Privacy Laws: O.C.G.A. § 31-33-2 (Access to Medical Records)

CONTRACT REFERENCE(S):

- Medicare Advantage D-SNP Health Plan Agreement Between Georgia Department of Community Health and Sonder Health Plans, Inc.

ELEMENT REFERENCE(S):

N/A

RELATED POLICY(S):

- CO-017 – SHP Records Retention Policy