Sunshine
Senior Services

Policy Title:	Health Plan Document and Data Retention	Effective Date:	1.1.2023
Functional Unit:	Compliance		
Policy Owner (Title):	Corporate Compliance Officer	Page Number:	1 of 4

I. POLICY STATEMENT and PURPOSE

It is the policy of the Company to comply at all times with applicable federal, state and local laws, including adherence to the rules and regulations established by the Centers for Medicare & Medicaid Services (CMS), in managing the operations of Medicare Advantage Organizations (MAOs). The Company requires the appropriate retention of certain documents and data for the purposes of conducting its business, maintaining a history of business activities, and compliance with all legal and regulatory duties and requirements. This Policy defines 'business documentation' and provides guidelines for the systematic review and retention of documents and data received or created by the Company in connection with its Health Plan business transactions.

II. DEFINITIONS

Business Documentation (or Documents) – Recorded communications of the Company, regardless of format. Documents include both hard-copy paper form as well as any type of electronically stored information.

Document Files – Any type of containers that hold documents, such as file folders (paper or electronic), file boxes, electronic devices (CDs, DVDs, portable drives), networks, or any other type of paper or electronic data storage.

Downstream Entity – Any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the Medicare Advantage (MA) benefit or Part D benefit, below the level of the arrangement between an MAO or applicant or a Part D plan sponsor or applicant and a first tier entity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services.

First Tier Entity – Any party that enters into a written arrangement, acceptable to CMS, with an MAO or Part D plan sponsor or applicant to provide administrative or health care services to a Medicare-eligible individual under the MA program or Part D program.

Protected Health Information (PHI) – Any information that is transmitted or maintained in any format, including electronic media,

- that is created or received by a Covered Entity; and
- relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and
- includes demographic information collected from an individual that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

NOTE: For purposes of this Policy and other Company policies relating to the use and disclosure of PHI, the definition of PHI does not include information records covered by the Family Educational Right and Privacy Act. It also does not include PHI contained in employment records maintained by the Company in its role as employer.

Related Entity – Any party that is related to an MAO or Part D sponsor by common ownership or control and performs some of the MAO or Part D plan sponsor's management functions under contract or delegation; furnishes services to Medicare enrollees under an oral or written agreement; or leases real property or sells materials to the MAO or Part D plan sponsor at a cost of more than $2,500 during a contract period.

Workforce – For purposes of this policy, the full and part-time employees, contingent workers (consultants and contractors), trainees, and governing body of the Company, and other persons whose conduct in the performance of work for the Company is under the direct control of the Company, whether or not they are paid by the Company.

III. OWNERSHIP & TRAINING

The Corporate Compliance Officer (CCO) is responsible for administration, oversight, and training with regard to performance under this policy and procedure.

IV. PROTOCOLS

a. To adequately manage the business needs of Health Plan operations, comply with all regulatory requirements, ensure data integrity, and practice efficiency in the use of facility storage space, the Company has identified in this Policy certain types of business documentation and data that are required to be retained for a specified time period and destroyed after that time period has expired (unless otherwise directed as described herein).

b. All users of systems and data who create, receive, use, or disclose Health Plan information for any purpose, including protected health information, are required to adhere to the document storage and retention standards outlined in this Policy.

c. All documents listed below shall be retained by the Company and its FDRs for a minimum period of ten (10) years.

    i. All records and documentation required by federal or state law and the program requirements of federal health plans. Such requirements include but are not limited to the following: all records that demonstrate the decision-making process for claims payment; organization determinations; appeals; grievances; enrollment and disenrollment of beneficiaries; contracting and credentialing providers; and customer service inquiries.

ii. All records necessary to protect the integrity of the Company's Compliance Program and confirm the effectiveness of the Program, including (but not limited to):

1. Evidence of adequate employee training, including (at a minimum) the training topic, date, attendance, certificates of completion (if applicable), and test scores (if applicable);
2. Reports of compliance violations, capturing the date the violation was reported and a description of the violation;
3. Results of any investigation conducted as a consequence of a report of a compliance violation, including the date of investigation, summary of findings, disciplinary action taken, and the date action was taken;
4. Modifications to the Compliance Program;
5. All written notifications to FDRs regarding compliance activities;
6. Results of auditing and monitoring efforts.

iii. Files regarding in-network and out-of-network providers that have been the subject of complaints, investigations, violations, and prosecutions;

iv. All records as required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

v. All records as required for accounting, financial reporting, and income tax purposes.

vi. Personnel records.

vii. Any other documentation relative to Health Plan business transactions.

d. Documents that are not specifically identified in this Policy will be retained for the same length of time as a substantially similar document that is specified in this Policy. If in doubt as to the retention guideline for a document or type of data, contact the Compliance Department.

e. Business documents and data should be stored in a manner that accurately identifies the information, provides adequate confidentiality and protection from theft or damage, and allows for easy retrieval by authorized parties. All stored documents or document files must be clearly and accurately labeled with a description of the contents and the date (or time period) of the materials. Any type of documents or data containing regulated or protected information must be stored in a manner consistent with the governing regulatory requirements (i.e. secured files, limited access, etc.)

f. Department management is responsible for the business documentation within their area of oversight, and must authorize the destruction of any business documents or data identified in this Policy. *Prior to* destroying any Health Plan business documents or data, the Department Manager (or designee) should notify the Compliance and/or Legal Department of the document(s)/data that are due for destruction and await Compliance/Legal approval before disposing of the materials.

g. Electronic business documents (including, but not limited to, e-mail, e-mail attachments, voice mail, video, word processing, spreadsheets and other commonly-used applications, databases, files stored in ancillary storage devices, files stored on networks, desktop, and laptop computers, CDs, disks, cellular phones, etc.) produced using Company equipment and/or stored on Company property or devices, whether in-office or remotely, are business documents. All such documents are the property and proprietary interest of the Company, and are subject to the guidelines defined in this Policy.

h. In the event of a potential or actual lawsuit or government investigation, the Company will preserve and retain all original documents and data relevant to that lawsuit or investigation, regardless of the timeframe outlined in this Policy.

    i. Legal Hold. As soon as the Company becomes aware of the reasonable probability of a lawsuit or investigation, the Legal Department will distribute any necessary communications regarding the placement of a legal hold on specific types of documents or data, including electronically stored information and back-up systems. In the event of a legal hold, all workforce members will adhere to the requirements and directives of the legal hold until official notification is received that the legal hold is no longer required.

i. The Company has a duty and obligation to retain certain business documents and data. Workforce members who knowingly and/or willfully destroy or alter business documents or data, or violate a legal hold directive, may be subject to disciplinary action in accordance with applicable policies and procedures.

V. REGULATORY REFERENCES / CITATIONS

Health Insurance Portability and Accountability Act (HIPAA) 5 CFR 164
CMS Medicare Managed Care Manual, Chapter 21

VI. RELATED POLICIES / PROCEDURES

None

VII. ATTACHMENTS

None

Owner Sunshine Senior Services: L. Jarod Frost, Jerry Frost, Robert L. Anderson