Policy

DEPARTMENT: Compliance	
TITLE: Distribution of Protected Health Information and Sensitive Information	**VERSION:** 1.0
APPROVED BY: Sandra Ferguson	**DATE:** 09/28/2021
DEPENDENCIES: *HIPAA Privacy and Security Plan; Disciplinary Standards Policy*	

Contents

Purpose **2**

Definitions, Abbreviations, and Acronyms **2**

Scope **3**

Policy **3**

Change Log ..... Error! Bookmark not defined.

Purpose

Perennial Advantage is committed in complying with all the standards, requirements, and guidelines associated with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The purpose of this document is to provide clarification and additional information as it pertains to the distribution, transmission, and dissemination of Protected Health Information (PHI) and sensitive information as defined in *HIPAA Privacy and Security Plan*.

Definitions, Abbreviations, and Acronyms

Term/Acronym	Meaning
Breach	Protected health information (PHI) is defined as the acquisition, access, use, or disclosure of unsecured PHI, in a manner not permitted by HIPAA, which poses a significant risk of financial, reputational, or other harm to the affected individual.
Business Associate	A person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.
Employee	Means any full time, part time, or temporary employee of the Plan who works directly or indirectly on the Medicare Advantage and/or Prescription Drug (Part D) plans. Additionally, for the purposes of this Program, the term employee includes the Plan volunteers who work directly or indirectly on the Medicare Advantage and/or Prescription Drug (Part D) plans.
ePHI	All protected health information that is created, received, used or maintained in electronic form.
FDR	First Tier, Downstream, or Related Entity
First Tier Entity	Any party that enters into a written arrangement, acceptable to CMS, with a MAO or Part D plan sponsor or applicant to provide administrative services or health care services to a Medicare eligible individual under the MA program or Part D program. *(See 42 C.F.R. § 423.501).*
Health Plans	Individual and group plans that provide or pay the cost of medical care are covered entities.
HIPAA	Health Insurance Portability and Accountability Act of 1996
Minimum Necessary	When using or disclosing PHI or when requesting PHI for another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
PBM	Pharmacy Benefit Manager
PHI	Protected Health Information Information that is created or received by [the Plan] and relates to the past, present, or future physical or mental health condition of a Patient/Client ("Member"); the provision of health care to a Member; or the past, present, or

Term/Acronym	Meaning
	future payment for the provision of health care to a Member; and that identifies the Member or for which there is a reasonable basis to believe the information can be used to identify the Member. PHI includes information of persons living or deceased.
UAD	Unauthorized Disclosure Unauthorized acquisition, access, use, or disclosure of PHI.

Scope

This policy applies to all employees working within or on behalf of Perennial Advantage, designated as such for purposes of complying with the privacy and security provisions of the HIPAA. This policy establishes encrypted electronic transmission of PHI via e-mail as the preferred method for distribution and details the safeguards PA employees will employ to protect the security and privacy of both PHI and ePHI.

Note: Within this document, the term "employee" refers to all permanent, temporary, full-time, part-time and volunteer employees who: 1) have primary job duties related to PA's Part C and Part D operations and/or sales; and/or 2) are members of the PA Board of Directors. The terms "employee" or "staff member" includes all these types of workers.

Policy

PHI means information that is created or received by Perennial Advantage and relates to the past, present, or future physical or mental health condition of a Patient/Client ("Member"); the provision of health care to a Member; or the past, present, or future payment for the provision of health care to a Member; and that identifies the Member or for which there is a reasonable basis to believe the information can be used to identify the Member. PHI includes information of persons living or deceased.

Some examples of PHI include the following:

- Member's medical record number.
- Member's demographic information (e.g., address, telephone number.
- Information doctors, nurses, and other health care providers put in a Member's medical record.
- Images of the Member.
- Conversations a provider has about a Member's care or treatment with nurses and others;
- Information about a Member in a provider's computer system or a health insurer's computer system.
- Billing information about a Member at a clinic.

- Any health information that can lead to the identity of an individual or the contents of the information can be used to make a reasonable assumption as to the identity of the individual.

It is Perennial Advantage's policy to comply fully with HIPAA regulations. To that end, all Plan employees who have access to member PHI must comply with the *HIPAA Privacy and Security Plan.*

Any use, disclosure or distribution of PHI must be permitted or required by law, or pursuant to a valid authorization executed by the member. The recipient must have a need to have the information, and be an employee, or a delegated entity (e.g., Navitus). PHI must be limited to the minimum information necessary for the permitted or required purpose.

When transmitting, sending, and disseminating PHI and sensitive information, the first, best, and preferred method of delivery is encrypted e-mail. The following actions must be taken to ensure the safe transmission of data to the intended recipient, limiting the likelihood of an unauthorized disclosure (UAD) or Breach:

- The recipient(s) and e-mail address(es) are verified,
- The e-mail is encrypted (**Note: E-mails are encrypted if the words "Secure," "Secured," Encrypt," or "Encrypted" are included in the subject line.**).

When delivery by an encrypted e-mail is not practical, PHI and sensitive data may be transmitted via USPS certified mail or courier delivery service (FEDEX/UPS) with the following precautions:

- The recipient(s) and address(es) must be verified.
- The information must be sent with a tracking option (if USPS certified mail, if FedEx or UPS, a tracking number must be supplied).
    - Within 24 hours of the expected receipt date, the sender must confirm receipt with the recipient of the package.
    - If the recipient has not received the package within a reasonable period of time, notify the Compliance Officer and provide the date sent, date receipt expected, the address sent to, and the tracking number. The Compliance Officer will initiate an investigation concerning the missing package.

Failure to comply with PHI security protocols may result in disciplinary action, up to and including termination, based on the frequency and severity of the occurrence(s) per the *Disciplinary Standards* policy.

If there is any doubt about whether PHI should be sent, the method to send it, or who it should be sent to, consult the PA Compliance team, or Compliance Officer.

Change Log

Document Version	Major or Minor Revision?	Date	Name	Comments
1.0	New	7/23/2021	Sandra Ferguson	Initial creation
				Compliance Officer Approval Sandra Ferguson
				Compliance Committee Approval: 06/17/2021
				Board Approval: 09/28/2021