Status **Active** PolicyStat ID **16193250**

Origination	01/2024
Last Approved	08/2024
Effective	08/2024
Last Revised	08/2024
Next Review	08/2025

Owner	Stephanie Clark: Director, Compliance & ACO Compliance Officer
Area	Compliance
Applicability	Privia Health and All Markets

ACO Compliance with HIPAA and DUA Requirements

Purpose:

The purpose of the Privacy and Security (PVS) Policies and Procedures is to outline the ACOs policies for ensuring compliance with all privacy requirements.

Scope:

This policy applies to all Privia Quality Networks, all PQN's, CMG ACO and all ACO Related Individuals as defined in this policy.

Definitions:

- **ACO Participant**- An entity identified by a Medicare-enrolled billing TIN through which one or more ACO providers/suppliers bill Medicare, that alone or together with one or more other ACO participants compose an ACO, and that is included on the list of ACO participants that is required under 42 C.F.R. § 425.118.
- **ACO Related Individual**: ACO officers, directors, employees, ACO Participant, ACO Provider/ Supplier, or any other individual or entity providing functions or services related to ACO Activities.
- **Beneficiary** - Medicare Fee-For-Service beneficiary attributed to the ACO by CMS.
- **Data Use Agreement (DUA)** - An agreement between CMS and the ACO that addresses the conditions under which CMS will disclose and the user will obtain, use, reuse and disclose CMS data file(s) that contain direct individual identifiers or elements that can be used in concert with other information to identify individuals.
- **DUA Custodian** - The individual responsible for the observance of all conditions of data use

and for establishment and maintenance of security arrangements, as specified in the DUA, to prevent unauthorized use or disclosure. The custodian is the individual who accesses the requested data files and oversees others within the organization who have access to it.

- **DUA Requestor** - Serves as the person authorized to legally bind the ACO to the terms of the DUA.
- **HIPAA** - Health Insurance Portability and Accountability Act of 1996.
- **HIPAA Definitions** - For additional HIPAA definitions, please refer to the following document: PMG.HPA.000.01 HIPAA Policy Definitions
- **Medicare Shared Savings Program (MSSP)** - Medicare Shared Savings Program, established under section 1899 of the Social Security Act.
- **Personally Identifiable Information (PII)** - Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- **Protected Health Information (PHI)** - Means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Policy:

It is the policy of the ACO to maintain the privacy and security of all ACO related information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, the Date Use Agreement (DUA) signed between the ACO and the Centers for Medicare and Medicaid Services (CMS), all relevant HIPAA Privacy and Security guidance applicable to the use and disclosure of protected health information, as well as applicable state laws and regulations.

Procedure:

The ACO requires that all ACO related activities comply with all elements of applicable federal and state laws, regulations, and standards governing privacy of health care information. In accordance with the HIPAA and the Privacy Rules; the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act (ARRA) of 2009, Gramm-Leach-Bliley Act (GLBA), and the Data Use Agreement signed with the CMS.

A. Any data shared by the ACO will be done only in accordance with the Business Associate Agreement signed by each ACO Participant.

B. The ACO Compliance Officer and Privacy Officer and/or their designees are responsible for ensuring compliance with this privacy policy, and utilizes the ACO's Monitoring & Oversight program to ensure that the ACO is compliant with all applicable privacy regulations and standards.

C. The ACO requires all Relevant Individuals to use the best practices listed below in an effort to protect Beneficiaries, personally identifiable information (PII), protected health information (PHI), and other sensitive data:

    1. Avoid sharing PII, PHI or sensitive data by email. If data must be emailed, it is sent as an encrypted file and the password is sent to the recipient by phone or fax.

2. Passwords for encrypted files are not sent via email.
3. Passwords are not shared.
4. Work information is not sent to or from personal email accounts.

D. Privacy concerns are reported to the Privacy Office at privacy.priviahealth.com or via email at privacy@priviahealth.com and are investigated according to Privacy Office policies. The report, investigation and any follow-up activities are documented according to Privacy Office policies.

E. The Privacy Office is responsible for reporting violations to law enforcement as required by the regulations.

1. Any breach of personally identifiable information (PII) from the CMS data file(s), loss of these data or disclosure to any unauthorized persons must be reported to the CMS Action Desk by telephone at (410) 786-2580 or by e-mail notification at cms_it_service_desk@cms.hhs.gov within one hour and to cooperate fully in the federal security incident process.
2. The ACO shall take reasonable steps to mitigate, to the extent practicable, any harmful effect (that is known to the ACO) of a use or disclosure of PHI by the ACO in violation of an agreement with an ACO Participant, or the ACO's Data Use Agreement with the ACO.

F. As part of its participation in the Medicare Shared Savings Program, the ACO has signed a Data Use Agreement (DUA) with the Centers for Medicare and Medicaid Services (CMS). The ACO will only share data in accordance with the terms of that agreement.

1. Data is not physically moved, transmitted, or disclosed in any way from or by the site indicated in the DUA without written approval from CMS unless such movement, transmission or disclosure is required by a law.
2. If the ACO needs to send information covered by the DUA outside of the ACO, the ACO will ensure that the receiving entity agrees to abide by the terms of the DUA through the use of a Data Use Acknowledgement Form prior to sharing any data files received from CMS as part of the Shared Savings Program. This form will capture, at a minimum, the following data elements to ensure the ability of the ACO to respond to CMS in the event of an audit:
    a. The legal name and full address of the entity;
    b. The individual within the entity ultimately responsible for ensuring compliance with the requirements of the DUA;
    c. The date the ACO began sharing data with the entity;
    d. The date the ACO stopped sharing data with the entity; and
    e. Upon termination of the arrangement, a certification by the individual identified in paragraph two above, that all data has been destroyed or returned to the ACO.

G. The ACO has designated a Custodian of the CMS data files who is responsible for the observance of all conditions of use and for the establishment and maintenance of security arrangements as specified in the DUA to prevent unauthorized use. The ACO shall notify CMS within 15 days of any change of custodianship.

1. All individuals identified as an ACO Contact in ACO-MS are deemed by CMS to be ACO Custodians, and are thus responsible for ensuring the ACO's Compliance with all requirements of the Data Use Agreement signed by the ACO.

H. Availability of PHI for Amendment: Within fifteen (15) business days of receipt of a written request from an ACO Participant for the amendment of an Individual's PHI maintained by the ACO, the ACO shall provide such information for amendment and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526. If the ACO receives a request for amendment to PHI directly from an Individual, the ACO shall forward such request to the ACO Participant or Provider/Supplier within ten (10) business days.

I. Accounting of Disclosures: Within thirty (30) business days of written notice by an ACO Participant or Provider/Supplier that it has received a request for an accounting of disclosures of PHI (other than disclosures to which an exception to the accounting requirement applies), the ACO shall make available such information as is in the ACO's possession and is required for the ACO Participant to make the accounting required by 45 C.F.R. §164.528.

J. Each ACO Related Individual is required to complete Compliance Training, including HIPAA and Privacy training, upon hire or contracting and at least annually thereafter. The Compliance Office is responsible for ensuring the appropriate documentation of training completions and retention of training records. The Compliance and Privacy and Security Office is also responsible for ensuring that this training is reviewed and updated as needed, but no less than annually.

K. Requests to add vendors or contractors to the Data Use Agreement with CMS are submitted to the DUA Custodian and/or Requestor. Once approval is received from CMS, the DUA Custodian and/or Requestor provides notification to the appropriate individual within the ACO to allow for the sharing of data as necessary.

L. All data requests, uses and disclosures are limited to the minimum necessary to achieve the purposes of the ACO and the MSSP.

M. DUA Attachment A: Information derived from the files specified in Section 5 of the Data Use Agreement may be shared and used within the legal confines of the ACO and its ACO Participants in a manner consistent with Section A-2 to enable the ACO to improve care integration and be a patient-centered organization.

N. Users may reuse original or derivative data without prior written authorization from CMS for clinical treatment, care management and coordination, quality improvement activities, and provider incentive design and implementation, but shall not disseminate original or derived information from the files specified in Section 5 of the Data Use Agreement, with or without direct identifiers, to anyone who is not an ACO Participant or an ACO provider/supplier in an ACO that has entered into a signed agreement with CMS. Users may disseminate and link information derived from the files specified in Section 5 of the Data Use Agreement to other sources of individually-identifiable (patient-specific) health information, such as medical records, available to the ACO and its ACO Participants unless expressly prohibited by theMedicare beneficiary. When using or disclosing protected health information (PHI) or personally identifiable information (PII), obtained under the Data Use Agreement, Users must make "reasonable efforts to limit" the information to the "minimum necessary" to accomplish the intended purpose of the use, disclosure or request. Users shall limit disclosure of information to the established Privacy Act "routine uses," which are categories established by

the Privacy Act which dictate the types of uses under which data can be disclosed.

Reporting

The Privacy Officer or their designee reports on any privacy issues to the Governing Body or appropriate Sub-Committee at least quarterly.

Approval Signatures

Step Description	Approver	Date
Chief Audit & Compliance Officer Approval	Dana Fields: Chief Audit & Compliance Officer	08/2024
ACO Compliance Leadership Approval #1	Stephanie Clark: Director, Compliance & ACO Compliance Officer	07/2024
	Stephanie Clark: Director, Compliance & ACO Compliance Officer	07/2024