

Privacy & Security of Beneficiary Data

Effective Date: 01/01/2018

Policy

- A. It is the policy of the ACO to provide guidelines for the secure sharing of Beneficiary identifiable data among CMS, the ACO, its Next Generation Participants, Preferred Providers, Next Generation Professionals and other individuals or entities performing functions or services related to the ACO's activities. The Beneficiary's identifiable data is shared by CMS on the condition that all ACO care coordination activities, and those involved in such activities, observe the relevant statutory and regulatory provisions of use, including confidentiality and privacy, and comply with the data use agreement.

Applicability

This policy and procedure applies to all Next Generation Participants, Preferred Providers, Next Generation Professionals and other individuals or entities performing functions or services related to the ACO's activities.

Procedure

- A. The ACO will take reasonable steps to limit the use or disclosure of, and requests for, protected health information (PHI) to the minimum necessary to accomplish a permitted use of the data.
- B. The ACO will preserve Beneficiary confidentiality, including protecting the confidentiality of Beneficiaries' health and medical records. The ACO will enforce strict adherence to this policy to protect the confidentiality of PHI from improper or illegal use or disclosure.
- C. Compliance is responsible for ensuring that periodic risk assessments occur no less than every three years to identify risks associated with potential noncompliance with the privacy and security mandates of federal regulations, including but not limited to the Next Generation ACO Model Participation Agreement, the Data Use Agreement between CMS and the ACO, the Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health (HITECH) Act.
 1. The Compliance Officer, or his/her designee, will compile the individually identified risks into a master document to serve as the risk analysis and develop actionable steps and timelines surrounding the steps for creation of a work plan to effectuate the risk analysis.
 2. Work plans will be prioritized, implemented and evaluated on an ongoing basis.
- D. Any documentation that contains PHI must be sent using secure means:
 1. Mailings must be sent via a trackable method and include return service postage, sealed envelopes and only the minimum necessary addressee information shown on any outer envelopes.

Privacy & Security of Beneficiary Data

Effective Date: 01/01/2018

2. All emails containing confidential information will be sent via secure email.
 3. Documents sent by fax to external sources include a cover sheet identifying the confidentiality of the information, and are sent to a single, verified fax number.
- E. Ensuring data privacy and security**
1. Claims data is provided by CMS for the purpose of:
 - a. Evaluating performance of Participants and Providers/Suppliers;
 - b. Conducting quality assessment and improvement activities; and,
 - c. Improving the health and quality of care for the Beneficiaries.
 2. The ACO shall provide Beneficiaries who inquire about and wish to modify their data sharing preferences information about how to modify their data sharing preferences via 1-800-MEDICARE.
 - a. CMS will maintain the data sharing preferences of Beneficiaries who elect to decline data sharing.
 3. All records, documents and any other information containing PHI will be kept in a secure location according to applicable regulations.
 4. Electronic medical records will follow HITECH standards for PHI protection.
- F. Aggregate Reports**
1. CMS will initially aggregate metrics on the ACO-assigned Beneficiary population based on historical claims data.
 2. CMS will utilize the historical claims data to calculate a benchmark.
 3. The ACO may receive data from CMS for the purposes of improving Beneficiary health, reducing growth in healthcare costs, improving care coordination and process improvement initiatives.
- G. Patient Identifiable Data**
1. Under the Next Generation ACO Model Participation Agreement, CMS may provide certain data and reports to the ACO upon request by the ACO.
 2. The ACO represents and warrants that the use of data received from CMS will be only to develop and implement activities related to coordinating care and improving the quality and efficiency of care for the Beneficiaries.
 3. The ACO processes for Data Sharing must ensure that unique Beneficiary identifiers and claims data is limited to only necessary data and that management, efficiency and quality of care improvement activities will be applied uniformly to all Beneficiaries.
 4. Data will not be used to reduce, limit or restrict appropriate care for individual Beneficiaries.

Privacy & Security of Beneficiary Data

Effective Date: 01/01/2018

H. Evaluate Performance of Participants and Providers/Suppliers

1. Historical claims data will enable the ACO to develop outcomes-based benchmarks from which performance patterns for utilization and spending for the assigned ACO population can be measured against specific improvement goals.
 2. The Governing Body will be notified of any Next Generation Participant, Preferred Provider, Next Generation Professional, or other individual or entity providing functions or services related to ACO activities, who fails to abide by privacy and data security policies, to investigate and take remedial action as appropriate which may result in termination from the ACO.
- I. The ACO will train Next Generation Participants, Preferred Providers, Next Generation Professionals and other individual or entities providing functions or services related to ACO activities, to meet all privacy and security standards and regulations in their facilities and with use of any electronic devices where PHI might reside.
- J. Training will be provided upon hire or contracting and at least annually thereafter.

Reporting

- A. N/A

Related Documentation

- A. Next Generation ACO Model Participation Agreement Section V.I, VI and XVII
- B. 42 CFR § 164.502
- C. 42 CFR § 425.706
- D. ACO Terms & Definitions Policy
- E. Beneficiary Rosters
- F. CMS Data Use Agreement Form – Example:
<http://www.cms.gov/cmsforms/downloads/cms-r-0235.pdf>
- G. Health Information Technology and Clinical Health (HITECH) Act:
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>
- H. Health Insurance Portability and Accountability Act (HIPAA):
https://www.cms.gov/HIPAAgenInfo/02_TheHIPAALawandRelated%20Information.asp
- I. Medicare Rights & Protections:
www.medicare.gov/Publications/Pubs/pdf/11534.pdf
- J. Medical Records Policy

Privacy & Security of Beneficiary Data

Effective Date: 01/01/2018

K. NCQA Standards and Guidelines for the Accreditation of ACOs:

1. AA 1, Elements B-H
2. PC 1, Element E: Care Management
3. CM 1, Elements A-H

L. Privacy Rule Summary:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>

M. Provider Access & Availability Policy

N. Record Retention Requirements Policy

O. Security Rule Summary:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html>

P. Social Security Act Sec. 1899(b)(3)(B)