Privacy & Security of Beneficiary Data

Effective Date: 7/28/2014 Draft/Review Date: 8/18/2014

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 Participants, Providers/Suppliers 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 Participants, Providers/Suppliers, 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 Medicare Shared Savings Program, Health Insurance Portability and Accountability Act (HIPAA), and 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.

    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. Upon assignment to the ACO, Beneficiaries will be given the opportunity to decline the sharing of their data including historical and ongoing claims information and individual PHI.
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 request data from CMS for the purposes of improving Beneficiary health, reducing growth in healthcare costs, improving care coordination and process improvement initiatives.
4. Requests from the ACO for aggregate data may be made at the beginning of the agreement year, on a quarterly basis throughout the year, and at the beginning of each performance year following specific protocols.

G. **Patient Identifiable Data**

1. The ACO must certify that:
    a. Claims data requested is for the Beneficiaries and reflects the minimum data needed for the ACO to conduct the healthcare operations; or,
    b. Claims data requested is for the Beneficiaries and reflects the minimum data needed for the Participants and Providers/Suppliers to conduct healthcare operations.
2. 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.
3. Data will not be used to reduce, limit or restrict appropriate care for individual Beneficiaries.
4. The ACO may only request claims data about a Beneficiary if the following occurs:
    a. The Beneficiary name is on the preliminary prospective assignment list either initially or quarterly from CMS; **OR,**

b. The Beneficiary has received primary care services from a Participant during the agreement period; **AND,**

c. The Beneficiaries did not decline having his/her unique claims data shared with the ACO.

H. **Evaluate Performance of Participants and Providers/Suppliers**

1. The ACO must certify the following when requesting data:

a. The request is for the minimum data necessary to conduct ACO healthcare operations according to paragraphs 1 and 2 of 45 CFR § 164.502.

b. ACO business associates are HIPAA covered entities and will comply with those same requirements in 45 CFR § 164.502.

2. 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.

3. The Compliance & Ethics Subcommittee will be notified of any Participant or Provider/Supplier 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 Participants and Providers/Suppliers 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 and at least annually thereafter.

Reporting

A. N/A

Related Documentation

A. 42 CFR Medicare Shared Savings Program Subpart H – Data Sharing with ACOs

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

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)