



Compliance Training for Medicare Programs

Version 1.0

2/22/2013



The Compliance Program

Setting standards for working with integrity



Compliance Program Elements

AmeriHealth is committed to compliance with all applicable federal, state and local laws, regulatory requirements, and contractual obligations for the government programs in which we participate, including but not limited to, the Medicare Advantage (Part C) and Prescription Drug (Part D) Programs.

The AmeriHealth Compliance Program is made up of seven elements that ensure we achieve compliance and meet our contractual obligations.

As you learn about the elements, pay close attention to the part that **YOU** are expected to play in each one.



Code of Conduct and Policies

The **Code of Conduct and Policies** are a key component of the Compliance Program. They communicate the rules for conducting company business in accordance with all applicable laws and regulations and with the highest ethical standards.

Upon hire and annually thereafter, you and your employees are required to read a Code of Conduct and indicate that they understand what they've read and that they will comply with it. If your organization has your own Code of Conduct, it must meet the Centers for Medicare & Medicaid Services (CMS) requirements.

Your Code and Corporate Policies Must Achieve the Following

1. Articulate commitment to comply with all applicable federal and state standards.
2. Describe compliance expectations.
3. Implement the operation of the compliance program.
4. Provide guidance to employees and others on dealing with suspected, detected, or reported compliance issues.
5. Identify how to communicate compliance issues to appropriate compliance personnel.
6. Describe how suspected, detected, or reported compliance issues are investigated and resolved.
7. Include a policy of non-intimidation and non-retaliation for good faith participation in the compliance program, including, but not limited to, reporting potential issues, investigating issues, conducting self-evaluations, audits and remedial actions, and reporting to appropriate officials.

Laws and Regulations to Consider in Standards of Conduct and/or Training

- Title XVIII of the Social Security Act
- Medicare regulations governing Parts C and D found at 42 C.F.R. §§ 422 and 423 respectively
- Patient Protection and Affordable Care Act (Pub. L. No. 111-148, 124 Stat. 119)
- Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191)
- False Claims Acts (31 U.S.C. §§ 3729-3733)
- Federal Criminal False Claims Statutes (18 U.S.C. §§ 287,1001)
- Anti-Kickback Statute (42 U.S.C. § 1320a-7b(b))
- The Beneficiary Inducement Statute (42 U.S.C. § 1320a-7a(a)(5))
- Civil monetary penalties of the Social Security Act (42 U.S.C. § 1395w-27 (g))
- Physician Self-Referral (“Stark”) Statute (42 U.S.C. § 1395nn)
- Fraud and Abuse, Privacy and Security Provisions of the Health Insurance Portability and Accountability Act, as modified by HITECH Act
- Prohibitions against employing or contracting with persons or entities that have been excluded from doing business with the Federal Government (42 U.S.C. §1395w-27(g)(1)(G))
- Fraud Enforcement and Recovery Act of 2009
- All sub-regulatory guidance produced by CMS and HHS (manuals, training materials, HPMS memos, and guides)
- Prescription Drug Benefit Manual Chapter 9 – Compliance Program Guidelines (*Rev. 15, 07-27-12*)
- Medicare Managed Care Manual Chapter 21 – Compliance Program Guidelines (*Rev. 109, 07-27-12*)

Effective Lines of Communication

Any time you become aware of or suspect any illegal, unethical, or fraudulent activity related to AmeriHealth, you have an obligation to report it.

You may want to first discuss this with your organization's Compliance Department, Compliance Officer, or the Legal Department.

To report compliance or suspected illegal, unethical, and fraudulent activity, you may also contact the Fraud and Compliance Hotline at AmeriHealth by calling **1-866-282-2707**.

Reports can be made anonymously through this line. Retaliation, intimidation, or any other form of reprisal against anyone who makes a good-faith report of a violation of law is strictly prohibited.



Education & Training

CMS requires your employees to complete periodic training to ensure that they stay informed about CMS and AmeriHealth standards, applicable laws, and regulatory requirements, including, but not limited to, those related to Medicare. All new hires, within 90 days of hire and annually thereafter, must complete a series of training modules that introduce them to:

- Compliance
- Fraud, Waste, and Abuse
- HIPAA Privacy and Security
- Other job-specific training required to complete their job

Response to Non-Compliance

Reports of suspected non-compliance with the law are thoroughly reviewed and investigated.

Investigations are performed in a uniform and timely manner, and all findings are documented. If you or your staff is asked to participate in an investigation, you are expected to cooperate and must maintain confidentiality throughout. You should never discuss investigations with coworkers, friends, or family.

In the event that an investigation identifies misconduct, violation of applicable laws or regulations, or non-compliance, AmeriHealth will ensure that prompt and appropriate action is taken.



Enforcement of Standards

You and your staff are expected to comply with your company's code of conduct, contractual requirements, applicable laws, and regulatory requirements (including, but not limited to, CMS Medicare program requirements) at all times.

AmeriHealth outlines the disciplinary measures that can be undertaken to correct, among other things, violations of contractual, and/or regulatory or legal requirements:

- Contractual penalties
- Formal counseling/written action plan
- Written warning
- Up to and including termination from participation with the AmeriHealth network
- Referral to law enforcement

Auditing and Monitoring

AmeriHealth maintains an internal auditing system to ensure compliance with the laws and regulations that apply to our business, including, but not limited to, CMS regulations. The system involves:

- Appropriate controls
- Oversight of contractual requirements
- Audits
- Ongoing monitoring
- Program effectiveness reviews

You are required to cooperate with external government investigations and audits. When asked, you are expected to play your part in any activities that support audits/monitoring and inquiries.



Exclusion List Monitoring

CMS requires that you review the Office of Inspector General (OIG) and General Services Administration (GSA) exclusions lists to ensure that employees or contractors are not excluded from federal programs.

Reviews against sanctions lists must occur upon initial hire, annually thereafter, and when monthly updates are released. If an excluded individual or entity is identified, you must immediately remove the individual or entity from any work related directly or indirectly to any federal health care program and report the issue to AmeriHealth to ensure appropriate corrective actions have been taken.

Conflicts of Interest

Any activity, practice, or act, including outside activities or personal interests that could influence — or even appear to influence — your ability to make objective business decisions, that distracts or hinders you from the performance of your job is considered a **conflict of interest**.

You should avoid any actions or activities that may present a conflict of interest or promptly disclose those actions or activities and seek guidance and resolution from your management.



Privacy and Security

Keeping confidential information secure



HIPAA

The **Health Information Portability and Accountability Act of 1996 (HIPAA)** is a federal law that, among other things, protects the privacy and security of health information.

HIPAA contains a Privacy Rule and a Security Rule, and compliance with these rules is mandatory for all entities that use health information (referred to as “covered entities”), including health plans like AmeriHealth.

HIPAA Privacy and Security Rules

PRIVACY refers to WHAT information is protected and WHO is permitted to use, disclose, or access it.

The **HIPAA Privacy Rule** establishes regulations for the use and disclosure of protected health information (PHI).

SECURITY refers to HOW information is safeguarded. Information security efforts control access to information and protect it from destruction, loss, or inappropriate disclosure.

The **HIPAA Security Rule** establishes the safeguards necessary to protect PHI in electronic form (known as EPHI).



Protected Health Information

Protected health information (PHI) is individually identifiable health information transmitted or maintained in any form or medium (including written, spoken, or electronic) related to:

HEALTH CARE

The provision of health care to an individual

or

HEALTH CONDITIONS

The past, present, or future physical or mental health or condition of an individual

or

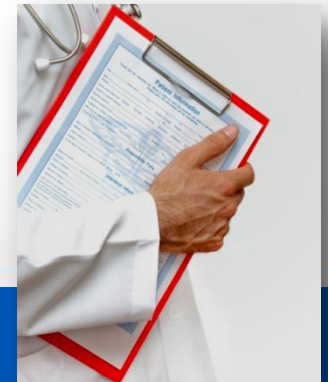
PAYMENT FOR CARE

The payment for the provision of health care to an individual

and

IDENTITY

The information identifies the individual or there is a reasonable basis to believe it can be used to identify the individual



Elements of PHI

PHI may consist of any unique identifying number, characteristic, or code.

The elements that make up PHI fall into some general categories:

- Names
- Locators
- Dates and ages
- Numbers
- Prints
- Images

Personally Identifiable Information

In addition to HIPAA, several state and federal laws have been enacted to safeguard what is generally known as **personally identifiable information (PII)**, which links a person with his/her identifying or transactional information. If information can be used to trace an individual's identity, it must be treated confidentially.

PERSON

First name
(or first initial)
and last name

and

IDENTITY INFORMATION

Examples include Social Security number, fingerprint, date of birth

or

TRANSACTIONAL INFORMATION

Examples include credit card number, digitized signature



Elements of PII

The identifying and transactional information that are elements of PII fall into some general categories:

- Social Security number
- Date of birth
- Financial account information
- Biometric data
- Electronic identification numbers
- Parent's legal surname prior to marriage
- Digitized/electronic signature
- Employee ID number
- Driver's license/state ID
- Federal ID number

Member Rights

What are Member Rights?

Members have certain rights regarding the use and/or disclosure of their PHI.

AmeriHealth maintains forms that members must use to exercise their privacy rights. These forms are available by contacting AmeriHealth.

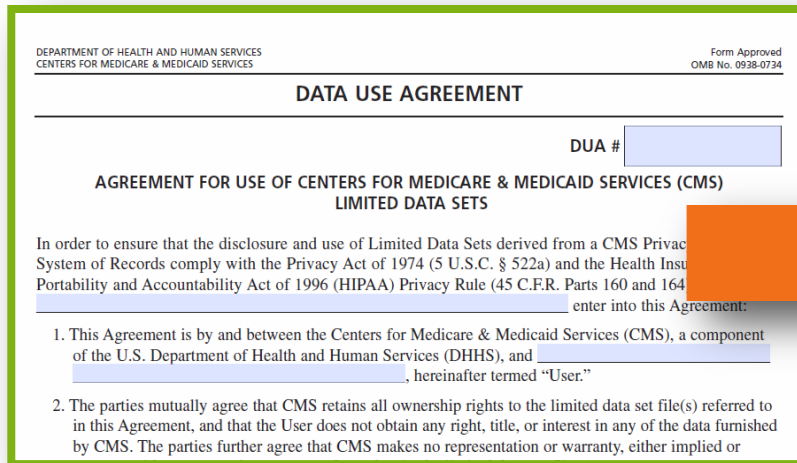


Member Rights Continued (Forms & Requests)

- **Notice of Privacy Practices** – (available on amerihealth.com) Covered entities must provide individuals with a written notice of their privacy practices, which includes how individuals can review their PHI.
- **Access to PHI** – Individuals have the right of access to (inspect and obtain) a copy of their PHI.
- **Amendment to PHI** – A covered entity must allow individuals the opportunity to request changes to their PHI, for as long as that information is maintained by the covered entity. A covered entity may deny this request if the covered entity did not create the PHI. Most health care information originates in a provider's office.
- **Accounting of Disclosures** – A covered entity must allow individuals the opportunity to request a report of certain disclosures of their protected health information that are made without their authorization.
- **Restriction** – A covered entity must allow individuals the opportunity to request restrictions on their PHI. The covered entity does not have to agree to every requested restriction. If the covered entity accepts the restriction, however, it must follow through and honor the individual's request.
- **Confidential Communication** – An individual has the right to ask a provider or health plan for confidential communications. A confidential communication request enables an individual to receive his or her information in an alternative form – for example, written, electronic, or to receive it at a different location.
- **Authorization** – An individual's permission to use or disclose PHI (unless the HIPAA Privacy Rule permits or requires a use or disclosure without the individual's permission).
- **Personal Representative** – A person that, as permitted, authorized, or qualified under applicable state or other law, has the authority to act on behalf of an individual.

CMS Data Use Agreement

The **CMS Data Use Agreement (DUA)** defines the confidentiality requirements for our limited data set* release policies and procedures. Covered entities like AmeriHealth must agree to abide by those requirements.



DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

Form Approved
OMB No. 0938-0734

DATA USE AGREEMENT

DUA #

**AGREEMENT FOR USE OF CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
LIMITED DATA SETS**

In order to ensure that the disclosure and use of Limited Data Sets derived from a CMS Privacy System of Records comply with the Privacy Act of 1974 (5 U.S.C. § 522a) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (45 C.F.R. Parts 160 and 164), _____ enter into this Agreement:

1. This Agreement is by and between the Centers for Medicare & Medicaid Services (CMS), a component of the U.S. Department of Health and Human Services (DHHS), and _____, hereinafter termed "User."
2. The parties mutually agree that CMS retains all ownership rights to the limited data set file(s) referred to in this Agreement, and that the User does not obtain any right, title, or interest in any of the data furnished by CMS. The parties further agree that CMS makes no representation or warranty, either implied or

- Specifies permitted uses of a limited data set
- Identifies who is permitted to receive/use a limited data set
- States that the recipient will not use the data for anything other than its intended use
- Ensures recipients will use appropriate safeguards to protect the data
- Holds any agent of the recipient to the standards, restrictions, and conditions stated in the agreement

*A **limited data set** consists of PHI that excludes certain direct identifiers of an individual.

Consequences of Privacy/Security Violations

The Office for Civil Rights is the federal agency charged with enforcing privacy and security regulations.

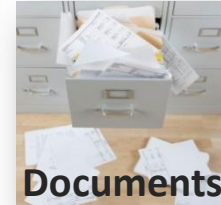
Ramifications for violating these regulations can include financial and reputational harm.

Criminal penalties for violating HIPAA privacy and security laws apply to covered entities. Penalties can range from \$50,000 and one year in prison to up to \$250,000 and ten years in prison.



Safeguarding Information

We are all responsible for maintaining appropriate administrative, technical, and physical safeguards to reasonably protect the privacy of PHI from any intentional or unintentional use or disclosure that is in violation of the HIPAA Privacy Rule.



Safeguarding Information



Addressing Privacy Concerns

You may have a Privacy Office within your organization that can provide guidance and oversight on compliance and privacy regulations. Contact your **Privacy Office** immediately when you suspect or know that:

- A privacy policy or procedure has been violated;
- Documents containing an individual's PHI (e.g., Explanation of Benefits, member ID card, precertification letters, provider/group rosters) are received by the wrong person or are lost or stolen;
- Someone has accessed or viewed member PHI for reasons other than company business;
- Containers for secure disposal of PHI are not locking properly or when PHI is otherwise disposed of in an unsecure way.



Important Compliance Contact Information at AmeriHealth

Fraud and Compliance Hotline: 1-866-282-2707

Members, providers, and contractors can anonymously report suspected illegal, unethical, or fraudulent activity.

Privacy Hotline: 215-241-4735

For reporting HIPAA violations (mishandling of PHI)

Compliance Department

Attn: AmeriHealth Compliance Officer

1901 Market Street

Philadelphia, PA 19103

Additional Information for Business Associates

For more information regarding the AmeriHealth HIPAA Privacy and Security Best Practices, visit www.amerihealth.com/privacy.