mc21

people caring for people

Medicare Part D Regulatory Pharmacy Training

urac

ACCREDITED
PHARMACY BENEFIT
MANAGEMENT

Training Agenda

Introduction

- Training Purpose
- Training Requirements
- Acronyms

Medicare Part D General Compliance

- Objectives
- Lesson: Compliance Program

Combating Medicare Part D Fraud, Waste & Abuse

- Objectives
- Lesson 1: Your role in the fight against FWA
- Lesson 2: FWA Program

Privacy

- Objectives
- Lesson: HIPAA

Lesson Review

- Lesson Summary Review
- Knowledge Check

mc21

people caring for people

Training Purpose

Where do I fit in?

As an entity who provides health or administrative services for Medicare enrollees, your every action potentially affects Medicare enrollees, and the Medicare Program.

The Part D Plan Sponsor is a CMS Contractor. Part D Plan Sponsors may enter into contracts with FDRs. This stakeholder relationship shows examples of functions that relate to the Sponsor's Medicare Part D contracts.

First Tier entities (examples: Call Centers and Pharmacy Benefit Management) and **related entities** (examples: Entity with common ownership or control of a Sponsor) of the Part D Plan Sponsor may contract with **downstream entities** (examples: pharmacies and doctors' offices) to fulfill their contractual obligations to the Sponsor.

MC-21 Corporation is a First-tier entity where we provide a Pharmacy Network, considered by CMS as downstream entities.

Completing this training module satisfies the Medicare Part D plan Sponsors annual training requirements in the regulations and sub-regulatory guidance at:

- 42 Code of Federal Regulations (CFR) Sections:
  - 401.713
  - 422.503(b)(4)(vi)
  - 422.503(b)(4)(vi)(C)
  - 423.504(b)(4)(vi)
  - 423.504(b)(4)(vi)(C)
- Section 50.3 and 50.3.2 of the Compliance Program Guidelines:
  - Chapter 9 of the "Medicare Prescription Drug Benefit Manual"
  - Chapter 21 of the "Medicare Managed Care Manual"
- Section 164.530 of the HIPAA privacy rule
- June 17, 2015, Health Plan Management System (HPMS) memo: Update – Reducing the Burden of the Compliance Program Training Requirements
- 42 Code of Federal Regulations (CFR) Section CMS-4159-F, Medicare Program Contract Year 2015 Policy and Technical Changes in the Medicare Advantage and the Medicare Prescription Drug Benefit Programs

Training Requirements

Why Do I Need Training?

Plan Employees, Governing Body Members, and First-Tier, Downstream, or Related Entity (FDR) Employees require certain trainings due to the involvement in Medicare Part D services.

All employees of Medicare Advantage Organizations (MAOs) and Prescription Drug Plans (PDPs) must receive training for compliance and preventing, detecting, and correcting FWA.

Compliance and FWA training must occur within 90 days of initial hire and at least annually thereafter.

This course was prepared originally by CMS, as a service to the public and is not intended to grant rights or impose obligations.

The information provided is only intended to be a general summary; it is not intended to take the place of either the written law or regulations.

Learn more about Medicare Part D

Medicare Part D, the Prescription Drug Benefit, provides prescription drug coverage to all beneficiaries enrolled in Part A and/or Part B who elect to enroll in a Medicare Prescription Drug Plan (PDP) or an MA Prescription Drug (MA-PD) plan. Insurance companies or other companies approved by Medicare provide prescription drug coverage to individuals who live in a plan's service area.

Acronyms

ACRONYM	TITLE TEXT
MA	*Medicare Advantage*
CFR	*Code of Federal Regulations*
WBT	*Web-Based Training*
FWA	*Fraud, Waste, and Abuse*
FDR	*First-Tier, Downstream, or Related Entity*
CFR	*Code of Federal Regulations*
FCA	*False Claims Act*
OIG	*Office of Inspector General*
EPLS	*Excluded Parties List System*
LEIE	*List of Excluded Individuals and Entities*
CMS	*Centers for Medicare & Medicaid Services*
MLN	*Medicare Learning Network®*
HIPAA	*Health Insurance Portability and Accountability Act*

The Medicare Parts C and D General Compliance Training course is brought to you by the Medicare Learning Network®, a registered trademark of the U.S. Department of Health & Human Services (HHS)

urac
ACCREDITED
PHARMACY BENEFIT
MANAGEMENT

mc21
people caring for people

Objectives

Objectives
This training section outlines effective compliance programs:

- Recognize how a compliance program operates; and
- Recognize how compliance program violations should be reported.

Compliance Program Requirement
An effective compliance program should:

- Articulate and demonstrate an organization's commitment to legal and ethical conduct;
- Provide guidance on how to handle compliance questions and concerns; and
- Provide guidance on how to identify and report compliance violations.

Lesson: An Effective Compliance Program

What Is an Effective Compliance Program?

An effective compliance program fosters a culture of compliance within an organization and, at a minimum:

- Prevents, detects, and corrects non-compliance;
- Is fully implemented and is tailored to an organization's unique operations and circumstances;
- Has adequate resources;
- Promotes the organization's Standards of Conduct; and
- Establishes clear lines of communication for reporting non- compliance.

An effective compliance program is essential to prevent, detect, and correct Medicare non-compliance as well as Fraud, Waste, and Abuse (FWA).

It must, at a minimum, include the seven core compliance program requirements.

For more information, refer to:

- 42 Code of Federal Regulations (CFR) Section 422.503(b)(4)(vi)
- 42 CFR Section 423.504(b)(4)(vi)
- "Medicare Managed Care Manual," Chapter 21
- "Medicare Prescription Drug Benefit Manual," Chapter 9

Lesson: Seven Core Compliance Elements

CMS requires that an effective compliance program must include seven core requirements:

1. **Written Policies, Procedures, and Standards of Conduct**
   These articulate the Sponsor's commitment to comply with all applicable Federal and State standards and describe compliance expectations according to the Standards of Conduct.

2. **Compliance Officer, Compliance Committee, and High-Level Oversight**
   The Sponsor must designate a compliance officer and a compliance committee that will be accountable and responsible for the activities and status of the compliance program, including issues identified, investigated, and resolved by the compliance program.

3. **Effective Training and Education**
   This covers the elements of the compliance plan as well as prevention, detection, and reporting of FWA. This training and education should be tailored to the different responsibilities and job functions of employees.

4. **Effective Lines of Communication**
   Effective lines of communication must be accessible to all, ensure confidentiality, and provide methods for anonymous and good- faith reporting of compliance issues at Sponsor and First-Tier, Downstream, or Related Entity (FDR) levels.

5. **Well-Publicized Disciplinary Standards**
   Sponsor must enforce standards through well-publicized disciplinary guidelines.

6. **Effective System for Routine Monitoring, Auditing, and Identifying Compliance Risks**
   Conduct routine monitoring and auditing of Sponsor's and FDR's operations to evaluate compliance with CMS requirements as well as the overall effectiveness of the compliance program.

7. **Procedures and System for Prompt Response to Compliance Issues**
   The Sponsor must use effective measures to respond promptly to non-compliance and undertake appropriate corrective action.

Lesson: Your Role in Compliance

Compliance Training–Sponsors and their FDRs

CMS expects that all Sponsors will apply their training requirements and "effective lines of communication" to their FDRs. Having "effective lines of communication" means that employees of the Sponsor and the Sponsor's FDRs have several avenues to report compliance concerns.

Ethics–Do the Right Thing!

It's about doing the right thing!

- Comply with all applicable laws, regulations, and CMS requirements; and
- Report suspected violations.

How Do You Know What Is Expected of You?

Beyond following the general ethical guidelines on the previous page, how do you know what is expected of you in a specific situation? Standards of Conduct (or Code of Conduct) state compliance expectations and the principles and values by which an organization operates. Contents will vary as Standards of Conduct should be tailored to each individual organization's culture and business operations. If you are not aware of your organization's standards of conduct, ask your management where they can be located.

Lesson: Code of Conduct

Code of Conduct

MC-21 expects their contracted FDRs' to adhere by their Standards of Conduct as required under CMS regulation. You can obtain a copy of our Standards of Conduct through our website at: http://mc-21.com/wp-content/uploads/2016/07/rev-cl-Legal-005-CODE-OF-CONDUCT-AND-ETHICS-.pdf .

MC-21s' Commitment

It is MC-21's organizational commitment to require all contracted downstream entities providing services to Medicare Part D beneficiaries conduct their business in an ethical and legal manner.

- Act fairly and honestly;
- Adhere to high ethical standards in all you do.

Conflict of Interest

As downstream entities, it is your responsibility to ensure all employees, representatives, contractors, delegated or related entities, including agents which provide services to Medicare Part D beneficiaries sign a conflict of interest statement at the moment of hire, in which they confirm that they are free from any personal or business related conflicts of interest for the administration or services provided to Medicare Part D beneficiaries.

Everyone has a responsibility to report violations of Standards of Conduct and suspected non-compliance.

An organization's Standards of Conduct and Policies and Procedures should identify this obligation and tell you how to report suspected non-compliance.

Lesson: Non-Compliance

What Is Non-Compliance?

Non-compliance is conduct that does not conform to the law, Federal health care program requirements, or an organization's ethical and business policies. CMS has identified the following Medicare Parts C and D high risk areas:

- Ethics;
- FDR oversight and monitoring;
- Health Insurance Portability and Accountability Act (HIPAA);
- Marketing and enrollment;
- Pharmacy, formulary, and benefit administration;
- Agent/broker misrepresentation;
- Quality of care.
- Appeals and grievance review;
- Beneficiary notices;
- Conflicts of interest;
- Claims processing;
- Credentialing and provider networks;
- Documentation
- Timeliness requirements.

Know the Consequences of Non-Compliance

Failure to follow Medicare Program requirements and CMS guidance can lead to serious consequences including:

- Contract termination;
- Criminal penalties;
- Exclusion from participation in all Federal health care programs; or
- Civil monetary penalties.

Additionally, your organization must have disciplinary standards for non-compliant behavior such as:

- Mandatory training or re-training;
- Disciplinary action; or
- Termination.

Lesson: Reporting Non-Compliance

Non – Compliance Affects EVERYBODY

Without programs to prevent, detect, and correct non-compliance, we all risk:

Harm to beneficiaries, such as:

- Delayed services
- Denial of benefits
- Difficulty in using providers of choice
- Other hurdles to care

Less money for everyone, due to:

- High insurance copayments
- Higher premiums
- Lower benefits for individuals and employers
- Lower Star ratings
- Lower profits

How to Report Potential Non-Compliance

Employees of a Sponsor

- Call the Medicare Compliance Officer;
- Make a report through your organization's website; or
- Call the Compliance Hotline.

First-Tier, Downstream, or Related Entity (FDR) Employees

- Talk to a Manager or Supervisor;
- Call your Ethics/Compliance Help Line; or
- Report to the Sponsor.

Beneficiaries

- Call the Sponsor's Compliance Hotline or Customer Service;
- Make a report through the Sponsor's website; or
- Call 1-800-Medicare.

Don't Hesitate to Report Non-Compliance

There can be no retaliation against you for reporting suspected non-compliance in good faith. Each Sponsor must offer reporting methods that are:

- Anonymous;
- Confidential; and
- Non-retaliatory.

Lesson: Investigation & Corrective Actions

What Happens After Non-Compliance Is Detected?

After non-compliance is detected, it must be investigated immediately and promptly corrected. However, internal monitoring should continue to ensure:

- There is no recurrence of the same non-compliance;
- Ongoing compliance with CMS requirements;
- Efficient and effective internal controls; and
- Enrollees are protected.

What Are Internal Monitoring and Audits?

- Internal monitoring activities are regular reviews that confirm ongoing compliance and ensure that corrective actions are undertaken and effective.
- Internal auditing is a formal review of compliance with a particular set of standards (for example, policies and procedures, laws, and regulations) used as base measures.

Organizations must create and maintain compliance programs that, at a minimum, meet the seven core requirements. An effective compliance program fosters a culture of compliance. To help ensure compliance, behave ethically and follow your organization's Standards of Conduct. Watch for common instances of non-compliance, and report suspected non-compliance.

Know the consequences of non-compliance, and help correct any non-compliance with a corrective action plan that includes ongoing monitoring and auditing.

Prevent: Operate within your organization's ethical expectations to prevent non-compliance!

Detect & Report: If you detect potential non- compliance, report it!

Correct: Correct non-compliance to protect beneficiaries and save money!

The Combating Medicare Parts C and D Fraud, Waste, and Abuse Web-Based Training course is brought to you by the Medicare Learning Network®, a registered trademark of the U.S. Department of Health & Human Services (HHS)

Objectives

Objectives

This training section outlines FWA:

- What Is FWA?
- FWA Examples and Differences
- Civil False Claims Act
- Health Care Fraud Statute
- Anti-Kickback Statute
- Stark Statute
- Civil Monetary Penalties
- OIG Exclusion
- Criminal Fraud
- Your Responsibilities
- Identify how to report FWA
- Recognize how to correct FWA
- FWA Key Indicators

Lesson: What is FWA?

Fraud is knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program, or to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program.

In other words, fraud is intentionally submitting false information to the Government or a Government contractor to get money or a benefit.

The Health Care Fraud Statute makes it a criminal offense to knowingly and willfully execute a scheme to defraud a health care benefit program. Health care fraud is punishable by imprisonment for up to 10 years.

It is also subject to criminal fines of up to $250,000.

Waste includes overusing services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare Program. Waste is generally not considered to be caused by criminally negligent actions but rather by the misuse of resources.

Abuse includes actions that may, directly or indirectly, result in unnecessary costs to the Medicare Program. Abuse involves payment for items or services when there is not legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment.

For the definitions of fraud, waste, and abuse, refer to Chapter 21, Section 20 of the "Medicare Managed Care Manual" and Chapter 9 of the "Prescription Drug Benefit Manual" on the Centers for Medicare & Medicaid Services (CMS) website.

Lesson: FWA Examples & Differences

Examples of FWA

Examples of actions that may constitute Medicare **fraud** include:

- Knowingly billing for services not furnished or supplies not provided, including billing Medicare for appointments that the patient failed to keep;
- Billing for non-existent prescriptions; and
- Knowingly altering claim forms, medical records, or receipts to receive a higher payment.

Examples of actions that may constitute Medicare **waste** include:

- Conducting excessive office visits or writing excessive prescriptions;
- Prescribing more medications than necessary for the treatment of a specific condition; and
- Ordering excessive laboratory tests.

Examples of actions that may constitute Medicare **abuse** include:

- Billing for unnecessary medical services;
- Billing for brand name drugs when generics are dispensed;
- Charging excessively for services or supplies; and
- Misusing codes on a claim, such as upcoding or unbundling codes.

Differences Among Fraud, Waste, and Abuse

There are differences among fraud, waste, and abuse. One of the primary differences is intent and knowledge. Fraud requires intent to obtain payment and the knowledge that the actions are wrong. Waste and abuse may involve obtaining an improper payment or creating an unnecessary cost to the Medicare Program, but does not require the same intent and knowledge.

Understanding FWA

To detect FWA, you need to know the law.

The following screens provide high-level information about the following laws:

- Civil False Claims Act, Health Care Fraud Statute, and Criminal Fraud;
- Anti-Kickback Statute;
- Stark Statute (Physician Self-Referral Law);
- Exclusion; and
- Health Insurance Portability and Accountability Act (HIPAA).

Civil False Claims Act

Civil False Claims Act (FCA)

The civil provisions of the FCA make a person liable to pay damages to the Government if he or she knowingly:

- Conspires to violate the FCA;
- Carries out other acts to obtain property from the Government by misrepresentation;
- Knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay the Government;
- Makes or uses a false record or statement supporting a false claim;
- Presents a false claim for payment or approval.

Whistleblowers: A whistleblower is a person who exposes information or activity that is deemed illegal, dishonest, or violates professional or clinical standards.

Protected: Persons who report false claims or bring legal actions to recover money paid on false claims are protected from retaliation.

Rewarded: Persons who bring a successful whistleblower lawsuit receive at least 15 percent but not more than 30 percent of the money collected.

Damages and Penalties: Any person who knowingly submits false claims to the Government is liable for three times the Government's damages caused by the violator plus a penalty. The Civil Monetary Penalty (CMP) may range from $5,500 to $11,000 for each false claim. For more information, refer to 31 United States Code (U.S.C.) Sections 3729-3733 on the Internet.

EXAMPLE: A Medicare Part C plan in Florida:

- Hired an outside company to review medical records to find additional diagnosis codes that could be submitted to increase risk capitation payments from the Centers for Medicare & Medicaid Services (CMS);
- Was informed by the outside company that certain diagnosis codes previously submitted to Medicare were undocumented or unsupported;
- Failed to report the unsupported diagnosis codes to Medicare; and
- Agreed to pay $22.6 million to settle FCA allegations.

Law	Available At
Civil False Claims Act 31 U.S.C. Sections 3729–3733	http://www.gpo.gov/fdsys/pkg/USCODE-2013-_title31/pdf/USCODE-2013-title31-subtitleIII-chap37-_subchapIII.pdf

Health Care Fraud Statute

Health Care Fraud Statute

The Health Care Fraud Statute states that "Whoever knowingly and willfully executes, or attempts to execute, a scheme to … defraud any health care benefit program … shall be fined … or imprisoned not more than 10 years, or both."

Conviction under the statute does not require proof that the violator had knowledge of the law or specific intent to violate the law. For more information, refer to 18 U.S.C. Section 1346 on the Internet.

EXAMPLES

A Pennsylvania pharmacist:

- Submitted claims to a Medicare Part D plan for non-existent prescriptions and for drugs not dispensed;
- Pleaded guilty to health care fraud; and
- Received a 15-month prison sentence and was ordered to pay more than $166,000 in restitution to the plan.

The owners of two Florida Durable Medical Equipment (DME) companies:

- Submitted false claims of approximately $4 million to Medicare for products that were not authorized and not provided;
- Were convicted of making false claims, conspiracy, health care fraud, and wire fraud;
- Were sentenced to 54 months in prison; and
- Were ordered to pay more than $1.9 million in restitution.

Law	Available At
Health Care Fraud Statute 18 U.S.C. Section 1347	http://www.gpo.gov/fdsys/pkg/USCODE-2013-title18/pdf/USCODE-2013-title18-partI-chap63-sec1347.pdf

Anti-Kickback Statute

Anti-Kickback Statute

The Anti-Kickback Statute prohibits knowingly and willfully soliciting, receiving, offering, or paying remuneration (including any kickback, bribe, or rebate) for referrals for services that are paid, in whole or in part, under a Federal health care program (including the Medicare Program).

For more information, refer to 42 U.S.C. Section 1320A-7b(b) on the Internet.

Damages and Penalties

Violations are punishable by:

- A fine of up to $25,000;
- Imprisonment for up to 5 years; or
- Both.

EXAMPLE: A radiologist who owned and served as medical director of a diagnostic testing center in New Jersey:

- Obtained nearly $2 million in payments from Medicare and Medicaid for MRIs, CAT scans, ultrasounds, and other resulting tests;
- Paid doctors for referring patients;
- Pleaded guilty to violating the Anti-Kickback Statute; and
- Was sentenced to 46 months in prison.

The radiologist was among 17 people, including 15 physicians, who have been convicted in connection with this scheme.

Law	Available At
Anti-Kickback Statute 42 U.S.C. Section 1320A-7b(b)	http://www.gpo.gov/fdsys/pkg/USCODE-2013-title42/pdf/USCODE-2013-title42-chap7-subchapXI-partA-sec1320a-7b.pdf

Stark Statute

Stark Statute (Physician Self-Referral Law)

The Stark Statute prohibits a physician from making referrals for certain designated health services to an entity when the physician (or a member of his or her family) has:

- An ownership/investment interest; or
- A compensation arrangement (exceptions apply).

For more information, refer to 42 U.S.C. Section 1395nn on the Internet.

Damages and Penalties

Medicare claims tainted by an arrangement that does not comply with the Stark Statute are not payable. A penalty of up to **$15,000** may be imposed for each service provided. There may also be up to a **$100,000** fine for entering into an unlawful arrangement or scheme.

EXAMPLE

A physician paid the Government $203,000 to settle allegations that he violated the physician self-referral prohibition in the Stark Statute for routinely referring Medicare patients to an oxygen supply company he owned.

For more information, visit https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral on the CMS website and refer to the Act, Section 1877 on the Internet.

Law	Available At
Physician Self-Referral Law 42 U.S.C. Section 1395nn	http://www.gpo.gov/fdsys/pkg/USCODE-2013-title42/pdf/USCODE-2013-title42-chap7-subchapXVIII-partE-sec1395nn.pdf

Civil Monetary Penalties

Civil Monetary Penalties Law

The Office of Inspector General (OIG) may impose Civil penalties for a number of reasons, including:

- Arranging for services or items from an excluded individual or entity;
- Providing services or items while excluded;
- Failing to grant OIG timely access to records;
- Knowing of an overpayment and failing to report and return it;
- Making false claims; or
- Paying to influence referrals.

Damages and Penalties

The penalties range from $10,000 to $50,000 depending on the specific violation. Violators are also subject to three times the amount:

- Claimed for each service or item; or
- Of remuneration offered, paid, solicited, or received.

For more information, refer to the Act, Section 1128A(a) on the Internet.

EXAMPLE

A California pharmacy and its owner agreed to pay over $1.3 million to settle allegations they submitted claims to Medicare Part D for brand name prescription drugs that the pharmacy could not have dispensed based on inventory records.

Law	Available At
Civil Monetary Penalties Law 42 U.S.C. Section 1320a-7a	http://www.gpo.gov/fdsys/pkg/USCODE-2013-title42/pdf/USCODE-2013-title42-chap7-subchapXI-partA-sec1320a-7a.pdf

OIG Exclusion

Exclusion Verification

No Federal health care program payment may be made for any item or service furnished, ordered, or prescribed by an individual or entity excluded by the OIG. The OIG has authority to exclude individuals and entities from federally funded health care programs and maintains the List of Excluded Individuals and Entities (LEIE). You can access the LEIE at https://exclusions.oig.hhs.gov.

The United States General Services Administration (GSA) administers the Excluded Parties List System (EPLS), which contains debarment actions taken by various Federal agencies, including the OIG. You may access the EPLS at https://www.sam.gov on the Internet.

If looking for excluded individuals or entities, make sure to check both the LEIE and the EPLS since the lists are not the same.

Pharmacy Responsibility

The Pharmacy must have policies and procedures in place to verify and validate the exclusion lists published by the Office of the Inspector General (OIG) and the General Administration Services (GSA) prior to hiring new employees, representatives and/or contractors to ensure no employee, representative or contractor has been excluded from federal health care programs (for example Medicare and Medicaid).

In addition and on a monthly basis thereafter, these exclusion lists must be verified to ensure no employee, representative, managerial personnel or contractor who has direct or indirect responsible for administering or delivering Medicare Part D benefits (i.e. prescriptions), has been excluded from participation of Federal healthcare programs.

Additionally, if any employee or contractor is identified through the exclusion lists, said employee or contractor must be immediately removed from performing any direct or indirectly Federal healthcare program related duties (for example Prescription administration, dispatch or delivery).

EXAMPLE: A pharmaceutical company pleaded guilty to two felony counts of criminal fraud related to failure to file required reports with the Food and Drug Administration concerning oversized morphine sulfate tablets. The executive of the pharmaceutical firm was excluded based on the company's guilty plea. At the time the executive was excluded, he had not been convicted himself, but there was evidence he was involved in misconduct leading to the company's conviction.

Law	Available At
Exclusion: 42 U.S.C. Section 1320a-7	http://www.gpo.gov/fdsys/pkg/USCODE-2013- title42/pdf/USCODE-2013-title42-chap7-subchapXI-partA- sec1320a-7.pdf

Criminal Fraud

Criminal Fraud

Persons who knowingly make a false claim may be subject to:

- Criminal fines up to $250,000;
- Imprisonment for up to 20 years; or
- Both.

If the violations resulted in death, the individual may be imprisoned for any term of years or for life. For more information, refer to 18 U.S.C. Section 1347 on the Internet.

Law	Available At
Health Care Fraud Statute 18 U.S.C. Section 1347	http://www.gpo.gov/fdsys/pkg/USCODE-2013- title18/pdf/USCODE-2013-title18-partI-chap63-sec1347.pdf

Lesson: Your Responsibilities

What Are Your Responsibilities?

You play a vital part in preventing, detecting, and reporting potential FWA, as well as Medicare non-compliance.

- **FIRST**, you must comply with all applicable statutory, regulatory, and other Medicare Part C or Part D requirements, including adopting and using an effective compliance program.
- **SECOND**, you have a duty to the Medicare Program to report any compliance concerns, and suspected or actual violations that you may be aware of.
- **THIRD**, you have a duty to follow your organization's Code of Conduct that articulates your and your organization's commitment to standards of conduct and ethical rules of behavior.

How Do You Prevent FWA?

- Look for suspicious activity;
- Conduct yourself in an ethical manner;
- Ensure accurate and timely data/billing;
- Ensure you coordinate with other payers;
- Keep up to date with FWA policies and procedures, standards of conduct, laws, regulations, and the Centers for Medicare & Medicaid Services (CMS) guidance; and
- Verify all information provided to you.

Stay Informed About Policies and Procedures

Familiarize yourself with your entity's policies and procedures. Every Sponsor and First-Tier, Downstream, or Related Entity (FDR) must have policies and procedures that address FWA. These procedures should help you detect, prevent, report, and correct FWA.

Standards of Conduct communicate to employees and FDRs that compliance is everyone's responsibility, from the top of the organization to the bottom. Standards of Conduct should describe the Sponsor's expectations that:

- All employees conduct themselves in an ethical manner;
- Appropriate mechanisms are in place for anyone to report non-compliance and potential FWA; and
- Reported issues will be addressed and corrected.

Lesson: Reporting FWA

Report FWA

Everyone must report suspected instances of FWA. Your Sponsor's Code of Conduct should clearly state this obligation. Sponsors may not retaliate against you for making a good faith effort in reporting.

Do not be concerned about whether it is fraud, waste, or abuse. Just report any concerns to your compliance department or your Sponsor's compliance department. Your Sponsor's compliance department area will investigate and make the proper determination. Often, Sponsors have a Special Investigations Unit (SIU) dedicated to investigating FWA. They may also maintain an FWA Hotline.

Reporting FWA Outside Your Organization

If warranted, Sponsors and FDRs must report potentially fraudulent conduct to Government authorities, such as the Office of Inspector General, the Department of Justice, or CMS.

Individuals or entities who wish to voluntarily disclose self-discovered potential fraud to OIG may do so under the Self-Disclosure Protocol (SDP).

Self-disclosure gives providers the opportunity to avoid the costs and disruptions associated with a Government- directed investigation and civil or administrative litigation.

Details to Include When Reporting FWA

When reporting suspected FWA, you should include:

- Contact information;
- Details of the alleged FWA;
- Identification of the specific Medicare rules allegedly violated;
- The suspect's history of compliance, education and training.

WHERE TO REPORT FWA

Every Sponsor must have a mechanism for reporting potential FWA by employees and FDRs. Each Sponsor must accept anonymous reports and cannot retaliate against you for reporting. When in doubt, call your Compliance Department or FWA Hotline.

HHS Office of Inspector General:

- Phone: 1-800-HHS-TIPS (1-800-447-8477) or TTY 1-800-377-4950
  Fax: 1-800-223-8164
- Email: HHSTips@oig.hhs.gov Online: https://forms.oig.hhs.gov/hotlineoperations

For Medicare Parts C and D:

- National Benefit Integrity Medicare Drug Integrity Contractor (NBI MEDIC) at 1-877-7SafeRx (1-877-772-3379)

For all other Federal health care programs:

- CMS Hotline at 1-800-MEDICARE (1-800-633-4227) or TTY 1-877-486-2048

HHS and U.S. Department of Justice (DOJ): https://www.stopmedicarefraud.gov

Lesson: Corrective Action Plan

Correction

Once fraud, waste, or abuse has been detected, it must be promptly corrected. Correcting the problem saves the Government money and ensures you are in compliance with CMS requirements.

Develop a plan to correct the issue. Consult your organization's compliance officer to find out the process for the corrective action plan development. The actual plan is going to vary, depending on the specific circumstances. In general:

- Design the corrective action to correct the underlying problem that results in FWA program violations and to prevent future non-compliance;
- Tailor the corrective action to address the particular FWA, problem, or deficiency identified. Include timeframes for specific actions;
- Document corrective actions addressing non-compliance or FWA committed by a Sponsor's employee or FDR's employee and include consequences for failure to satisfactorily complete the corrective action; and
- Once started, continuously monitor corrective actions to ensure they are effective.

Corrective Action Examples

Corrective actions may include:

- Adopting new prepayment edits or document review requirements;
- Conducting mandated training;
- Providing educational materials;
- Revising policies or procedures;
- Sending warning letters;
- Taking disciplinary action, such as suspension of marketing, enrollment, or payment; or
- Terminating an employee or provider.

Lesson: FWA Key Indicators

Key Indicators: Potential Beneficiary Issues

- Does the prescription, medical record, or laboratory test look altered or possibly forged?
- Does the beneficiary's medical history support the services requested?
- Have you filled numerous identical prescriptions for this beneficiary, possibly from different doctors?
- Is the person receiving the medical service the actual beneficiary (identity theft)?
- Is the prescription appropriate based on the beneficiary's other prescriptions?

Key Indicators: Potential Provider Issues

- Are the provider's prescriptions appropriate for the member's health condition (medically necessary)?
- Does the provider write prescriptions for diverse drugs or primarily for controlled substances?
- Is the provider performing medically unnecessary services for the member?
- Is the provider prescribing a higher quantity than medically necessary for the condition?

Key Indicators: Potential Pharmacy Issues

- Are drugs being diverted (drugs meant for nursing homes, hospice, and other entities being sent elsewhere)?
- Are the dispensed drugs expired, fake, diluted, or illegal?
- Are generic drugs provided when the prescription requires that brand drugs be dispensed?
- Are PBMs being billed for prescriptions that are not filled or picked up?
- Are proper provisions made if the entire prescription cannot be filled (no additional dispensing fees for split prescriptions)?
- Do you see prescriptions being altered (changing quantities or Dispense As Written)?

The General Privacy and Security Training course complies with HIPAA training requirements.

urac
ACCREDITED
PHARMACY BENEFIT
MANAGEMENT

mc21
people caring for people

Objectives

Objectives

This training section outlines HIPAA Privacy guidelines:

- HIPAA, Privacy Rule
- Uses and disclosures of PHI
- Protected healthcare identifiers (PHIs)
- Minimum necessary rule
- Your role in protecting confidential information
- Reporting privacy incidents
- HIPAA, Security Rule
- Enforcement and penalties for non-compliance

Lesson: What is HIPAA?

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA created greater access to health care insurance, protection of privacy of health care data, and promoted standardization and efficiency in the health care industry. HIPAA safeguards help prevent unauthorized access to protected health care information.

Damages and Penalties

Violations may result in Civil Monetary Penalties. In some cases, criminal penalties may apply.

HIPAA Administrative Simplification

Three sets of regulations issued by DHHS:

- Privacy Rule – April 14, 2003
- Security Rule – April 20, 2005 for most covered entities
- Transaction Standards – October 16, 2002, unless a request for extension has been filed, then the deadline was October 16, 2003.

What Types of Information Does HIPAA Protect?

The Privacy Rule protects most individually identifiable health information held or transmitted, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information" or "PHI." Individually identifiable health information is information, including demographic information, that relates to:

- The individual's past, present, or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual.

Lesson: Where Does MC-21 Fit In?

Covered Entity

The HIPAA Rules apply to covered entities and business associates. Individuals, organizations, and agencies must comply with the requirements to protect the privacy and security of health information by maintaining reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Business Associates

If a covered entity engages a business associate to help it carry out its health care activities and functions, the covered entity must have a written business associate contract that establishes specifically what services have been engaged to do and requires the business associate to comply with appropriate requirements to protect the privacy and security of protected health information (PHI).

First-tier Entity

Sponsors may enter into contracts with their PBM's. Pharmacy Benefit Managers are known as First-tier entities where administrative services are provided on behalf of the Sponsor.

Downstream Entity

MC-21, as a First-tier Entity, contracts pharmacies that provide health services to Medicare part D enrollees. Pharmacies included in our network are considered downstream entities.

Lesson: What is Privacy?

Privacy Rule

The Privacy Rule establishes national standards for the protection of certain health information. It applies to all forms of individuals' protected health information, whether electronic, written, or oral. The goal of the Privacy Rule is to make sure an individuals' health information is properly protected while allowing the flow of health information needed to provide high quality health care and to strike a balance that permits important uses of information.

The disclosure of Protected Health Information (PHI) in any form except as required or permitted by law is prohibited. The HIPAA Privacy rule mandates how PHI may be used and disclosed. The Privacy Rule protects PHI in any form including but not limited to:

- E-mail
- Fax
- Information on the computer
- Voice
- Paper

Protected Health Information (PHI)

PHI is health information collected from an individual, created or received by a covered entity that:

- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;
- That identifies the individual; With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- Maintained by an electronic or any other form, except educational records and employment records

Your Role Under HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) Rules provide federal protections for health information held by Covered Entities (CEs) and Business Associates (BAs). The Breach Notification Rule Covered Entities (CEs) and Business Associates (BAs) to provide notification following a breach of unsecured Protected Health Information (PHI).

Lesson: PHI Identifiers & Examples

Protected Healthcare Identifiers (PHI)

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form of media, whether electronic, paper, or oral. HIPAA protects information that alone or combined may identify a patient, the patient's relatives, employer or household members. Health information that contains even one identifier is protected under HIPAA. Examples include:

1. Name; Address; Birthdate; Social Security number; Telephone, Fax number; E-mail address
2. Medical record number and Health plan beneficiary number
3. Other characteristics which may identify the individual's past, present, or future physical/mental health/condition

Personal Information:

Name; Date of Birth; Social Security Number; Address.

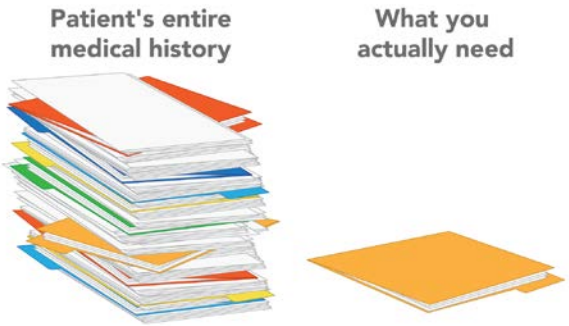
Clinical Information:

Medical Condition; Prescribed Medication demonstrating medical diagnosis; Health plan contract number.

Financial Information:

Bank Account Number; Pay Statements.

Lesson: Minimum Necessary



The Minimum Necessary Rule requires, when using, disclosing, or requesting Protected Health Information (PHI), you must make reasonable efforts to limit PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request.

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today.

The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information.

It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.

The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

Lesson: Confidentiality

Confidentiality Statement

It is the responsibility of all employees, committee members, and board members to preserve the confidentiality of individually-identifiable health information. Any employee who handles PHI must take appropriate measures to secure and protect it from unauthorized or improper access or viewing.

E-mail Confidentiality Statement

ATTENTION: "This message is a PRIVILEGED AND CONFIDENTIAL communication. This message and all attachments are a private communication and it is confidential and/or protected by privilege. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of the information contained in or attached to this message is strictly prohibited. Please notify the sender of the delivery error by replying to this message, and then delete it from your system. Thank you."

Fax Confidentiality Statement

ATTENTION: "This faxed information is intended only for use of the individual or entity to which it is addressed and contains information that is confidential. Furthermore, this information may be protected by Federal Law relating to confidential (42 CFR Part 2) prohibiting any further disclosure. If the reader of this message is not the intended recipient of the employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any review, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and return the original message to us at the above address via mail. Thank you."

Lesson: Your Role In Protecting PHI

Protecting Confidential Information is part of your daily tasks.

You must ask yourself: “What do I need to do to protect PHI in my job?”

- Safeguard confidential information.
- Access and read related privacy policies and procedures.
- Ask your supervisor or your compliance contact if you feel you need additional expertise.
- Access only the minimum necessary health information as appropriate.
- Place papers with PHI in a secured area.
- Don't leave PHI exposed where other can see the content.
- Discuss particular cases in private.
- Use passwords to keep other people from accessing your computer files.
- Make sure your computer is locked when you leave your desk.
- Minimize PHI in e-mails. Include as little as possible.
- Protect fax machines that will be receiving PHI.

Lesson: Reporting Privacy Concerns

What to Do If You Have a Breach?

A **breach** is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI.

An impermissible use or disclosure of unsecured PHI is presumed to be a breach unless it can be demonstrated that there is a low probability the PHI has been compromised.

The Rules require you to notify affected individuals and the Secretary of HHS of the loss, theft, or certain other impermissible uses or disclosures of unsecured PHI.

In particular, you must promptly notify the Secretary of HHS if there is any breach of unsecured PHI that affects **500 or more** individuals.

Reports of breaches affecting **fewer than 500** individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

Secured PHI	Unsecured PHI
An unauthorized person cannot use, read, or decipher any PHI obtained because your company: • Encrypts the information; • Clears, purges, or destroys media that stored or recorded PHI; • Shreds or otherwise destroys paper PHI.	An unauthorized person may use, read, and decipher PHI obtained because your company: • Does not encrypt or destroy the PHI; • Encrypts PHI, but the decryption key has also been breached.

Lesson: Security Overview

The HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule establishes a national set of minimum security standards for protecting all ePHI that a Covered Entity (CE) and Business Associate (BA) create, receive, maintain, or transmit. The Security Rule has several types of safeguards and requirements:

1. **Administrative Safeguards** – Administrative safeguards are administrative actions, policies, and procedures to prevent, detect, contain, and correct security violations. Administrative safeguards involve the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of workforce members in relation to the protection of that information.

2. **Physical Safeguards** – These safeguards are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. These safeguards implement appropriate use of ePHI and access.

3. **Organizational Standards** – These standards require a Covered Entities to have contracts with Business Associates that will have access to the covered entities' ePHI.

4. **Policies and Procedures** – These standards require a Covered Entity to adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. While maintaining written documents and related records of required actions, activities, or assessments until six years after the date of their creation or last effective date (whichever is later). These policies and procedures must be periodically reviewed and updated.

Lesson: Sanctions & Monetary Penalties

HIPAA Enforcement, and Other Laws and Requirements

Covered Entities (CEs) and Business Associates (BAs) that fail to comply with HIPAA Rules can receive civil and criminal penalties.

1. Civil Penalties - The Office for Civil Rights (OCR) is able to impose substantial civil penalties for organizations that fail to comply with the HIPAA Rules.

2. Criminal Penalties - The U.S. Department of Justice investigates and prosecutes criminal violations of HIPAA, and can impose criminal penalties for:
    - Knowing misuse of unique health identifiers;
    - Knowing and unpermitted acquisition or disclosure of Protected Health Information (PHI).

Penalties for Violations

Intent	Minimum Per Incident	Annual Cap
Did Not Know or Could Not Have Known	$100 – $50,000	$1.5 million
Reasonable Cause and Not Willful Neglect	$1,000 – $50,000	$1.5 million
Willful Neglect, but Corrected Within 30 Days	$10,000 – $50,000	$1.5 million
Willful Neglect and Not Corrected Within 30 Days	$50,000	$1.5 million

NOW THAT YOU HAVE A GENERAL INSIGHT ON TOPICS SUCH AS COMPLIANCE, FRAUD, WASTE & ABUSE AND HIPAA, YOU CAN TEST YOUR KNOWLEDGE BY TAKING THE FOLLOWING LESSON REVIEW.

Lesson Review

1. **What is the major goal of the Privacy Rule (HIPAA)?**
   a. Protect the provider
   b. Protect and individuals' information by defining the uses and disclosure of such information
   c. Keep documents sealed

2. **A person comes to your pharmacy to drop off a prescription for a beneficiary who is a "regular" customer. The prescription is for a controlled substance with a quantity of 160. This beneficiary normally receives a quantity of 60, not 160. You review the prescription and have concerns about possible forgery. What is your next step?**
   a. Fill the prescription for 160
   b. Fill the prescription for 60
   c. Call the prescriber to verify the quantity

3. **Your job is to submit a risk diagnosis to the Centers for Medicare & Medicaid Services (CMS) for the purpose of payment. As part of this job you verify, through a certain process, that the data is accurate. Your immediate supervisor tells you to ignore the Sponsor's process and to adjust/add risk diagnosis codes for certain individuals. What should you do?**
   a. Do what your immediate supervisor asked you to do and adjust/add risk diagnosis codes
   b. Report the incident to the compliance department (via compliance hotline or other mechanism)
   c. Discuss your concerns with your immediate supervisor

4. **Which of the following requires intent to obtain payment and the knowledge that the actions are wrong?**
   a. Fraud
   b. Abuse
   c. Waste

5. **You are in charge of payment of claims submitted by providers. You notice a certain diagnostic provider ("Doe Diagnostics") requested a substantial payment for a large number of members. Many of these claims are for a certain procedure. You review the same type of procedure for other diagnostic providers and realize that Doe Diagnostics' claims far exceed any other provider that you reviewed. What should you do?**
   a. Call Doe Diagnostics and request additional information for the claims
   b. Consult with your immediate supervisor for next steps or contact the compliance department (via compliance hotline, or other mechanism)
   c. Reject the claims

CONGRATULATIONS!

YOU HAVE COMPLETED THIS TRAINING!

Knowledge Check

Please select the correct answer and mark it in the boxes before each question.

1. **Compliance is the responsibility of the Compliance Officer only**.
   a. True
   b. False

2. **Which are examples of ways to report compliance issues?**
   a. Telephone hotlines
   b. Report on the Sponsor's website
   c. In-person reporting to the supervisor
   d. All of the above

3. **These are examples of issues that can be reported to a Compliance Department: Suspected Fraud, Waste, and Abuse; and Unethical behavior/employee misconduct**.
   a. True
   b. False

4. **Bribes or kickbacks of any kind for services that are paid under a Federal health care program constitute fraud by the person making as well as the person receiving them.**
   a. True
   b. False

5. **Waste includes any misuse of resources such as the overuse of services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare Program.**
   a. True
   b. False

6. **Abuse involves payment for items or services when there is no legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment.**
   a. True
   b. False

7. **Some of the laws governing Medicare Part D Fraud, Waste, and Abuse include the Health Insurance Portability and Accountability Act (HIPAA); the False Claims Act; the Anti-Kickback Statute; the List of Excluded Individuals and Entities (LEIE); and the Health Care Fraud Statute.**
   a. True
   b. False

8. **What do you need to do to protect PHI in your job?**
   a. Safeguard confidential information
   b. Leave your reports on your desk
   c. Discuss confidential cases in public
   d. None of the above

9. **Civil penalties are imposed by the Office of Civil Rights.**
   a. True
   b. False

Resources

Resource	Website
OIG's Provider Self-Disclosure Protocol	https://oig.hhs.gov/compliance/self-disclosure-info/files/Provider-Self-Disclosure-Protocol.pdf
Physician Self-Referral	https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral
Medicare Managed Care Manual, Chapter 21	https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/mc86c21.pdf
Medicare Prescription Drug Benefit Manual, Chapter 9	https://www.cms.gov/Medicare/Prescription-Drug-Coverage/PrescriptionDrugCovContra/Downloads/Chapter9.pdf
Avoiding Medicare Fraud and Abuse	https://oig.hhs.gov/compliance/physician-education
Safe Harbor Regulations	https://oig.hhs.gov/compliance/safe-harbor-regulations
Compliance Education Materials: Compliance 101	https://oig.hhs.gov/compliance/101
Health Care Fraud Prevention and Enforcement	https://oig.hhs.gov/compliance/provider-compliance-training
Part C and Part D Compliance and Audits - Overview	https://www.cms.gov/medicare/compliance-and-audits/part-c-and-part-d-compliance-and-audits
Information Shield Requirements	http://www.informationshield.com/security-awareness-requirements.html
Security Final Rule 164.308(a)(5)(i)(R)	https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
The Centers for Medicare & Medicaid Services Glossary	https://www.cms.gov/apps/glossary
CMS Compliance Program Policy and Guidance	https://www.cms.gov/Medicare/Compliance-and-Audits/Part-C-and-Part-D-Compliance-and-Audits/CompliancePrograMPolicyandGuidance.html

Reference Hyperlinks

HYPERLINK URL	TITLE TEXT
https://www.gpo.gov/fdsys/pkg/CFR-2014-title42-vol3/pdf/CFR-2014-title42-vol3-sec422-503.pdf	42 CFR Section 422.503(b)(4)(vi)
https://www.gpo.gov/fdsys/pkg/CFR-2014-title42-vol3/pdf/CFR-2014-title42-vol3-sec423-504.pdf	42 CFR Section 423.504(b)(4)(vi)
http://www.gpo.gov/fdsys/pkg/USCODE-2013-title31/pdf/USCODE-2013-title31-subtitleIII-chap37-subchapIII.pdf	31 U.S.C. Sections 3729-3733
http://www.gpo.gov/fdsys/pkg/USCODE-2013-title18/pdf/USCODE-2013-title18-partI-chap63-sec1346.pdf	18 U.S.C. Section 1346
http://www.gpo.gov/fdsys/pkg/USCODE-2013-title42/pdf/USCODE-2013-title42-chap7-subchapXI-partA-sec1320a-7b.pdf	42 U.S.C. Section 1320A-7b(b)
https://www.ssa.gov/OP_Home/ssact/title11/1128B.htm	Social Security Act Section 1128B(b)
http://www.gpo.gov/fdsys/pkg/CFR-2014-title42-vol5/pdf/CFR-2014-title42-vol5-sec1001-1901.pdf	42 CFR Section 1001.1901
https://exclusions.oig.hhs.gov	OIG Exclusions
http://www.gpo.gov/fdsys/pkg/USCODE-2013-title42/pdf/USCODE-2013-title42-chap7-subchapXVIII-partE-sec1395nn.pdf	42 U.S.C. Section 1395nn
http://www.gpo.gov/fdsys/pkg/USCODE-2013-title42/pdf/USCODE-2013-title42-chap7-subchapXI-partA-sec1320a-7.pdf	42 U.S.C. Section 1320a-7
http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap63-sec1347.pdf	18 U.S.C. Section 1347
https://www.ssa.gov/OP_Home/ssact/title18/1877.htm	Social Security Act, Section 1877
http://www.ssa.gov/OP_Home/ssact/title11/1128A.htm	Social Security Act, Section 1128A(a)
https://www.gpo.gov/fdsys/pkg/CFR-2014-title42-vol3/pdf/CFR-2014-title42-vol3-sec422-503.pdf	42 CFR Section 422.503(b)(4)(vi)
https://www.gpo.gov/fdsys/pkg/CFR-2014-title42-vol3/pdf/CFR-2014-title42-vol3-sec423-504.pdf	42 CFR Section 423.504(b)(4)(vi)