2022 Pharmacy Training

MC-Rx
Powered by ProCare Rx

Training Agenda

General Compliance

- Objectives
- Compliance Program Overview

Combating Fraud, Waste & Abuse

- Objectives
- Your role in the fight against FWA
- FWA Program Overview

Privacy

- Objectives
- HIPAA Overview

Lesson Review

- Lesson Summary Review
- Knowledge Check

General Compliance Training

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.

Seven Core Compliance Elements

An effective compliance program must include seven core requirements:

1. **Written Policies, Procedures, and Standards of Conduct**
   These articulate 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**
   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.

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 operations to evaluate compliance as well as the overall effectiveness of the compliance program.

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

Your Role in Compliance

Compliance Training

- You must apply training requirements and "effective lines of communication" to employees. Having "effective lines of communication" means that employees 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 regulatory 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.

Code of Conduct

Code of Conduct

- MC-Rx expects their contracted pharmacies to adhere by their Standards of Conduct. You can obtain a copy of our Standards of Conduct through our website.

- Our organization's Standards of Conduct and Policies and Procedures identify the obligation to report suspected non-compliance.

MC-Rx's Commitment

- It is MC-Rx's organizational commitment to require all contracted pharmacies providing services to 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

- It is your responsibility to ensure all employees, representatives, contractors, delegated or related entities, including agents which provide services to 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 beneficiaries.

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

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.

- High risk areas include: Ethics; HIPAA; Marketing and Enrollment; Pharmacy and Benefit Administration; Appeals and Grievances; Conflicts of Interest; Among others.

Know the Consequences of Non-Compliance

Failure to follow these requirements 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.

Reporting Non-Compliance

Non – Compliance Affects EVERYBODY

- Risks:
- Harm to beneficiaries, such as:
  - Delayed services
  - Denial of benefits
- Less money for everyone, due to:
  - High insurance copayments
  - Higher premiums
  - Lower profits

How to Report Potential Non-Compliance

- **Employees**
  - Call the Compliance Officer (787) 286-6032 ext. 3123;
  - Call the Compliance Hotline: (787) 286-6032 ext. 3800;
  - Call the Compliance Direct Hotline: (787) 773-1328;
  - Send a Confidential email: cumplimiento@mc-rx.com ;

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;
- 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.

Cultural Competency

Definition: Cultural competence is the ability of health organizations to recognize the cultural beliefs, values, attitudes, traditions, language preferences, and health practices of diverse populations, and to apply that knowledge to produce a positive health outcome.

Cultural Variables: Ethnicity, Race, Gender, Religion/Spirituality, History of the culture, Sexual Orientation, Language/Dialect.

Cultural Sensitivity: Achieve to make people of different ethnicities, gender, age, etc. comfortable; Build rapport and trust; Explain why you must ask personal or sensitive questions ; may require an expression of sympathy for doing so; Watch for patient's verbal and non-verbal cues; allow patient to ask questions at frequent intervals.

Federal Mandates and Regulations: Title VI of the Civil Rights Act of 1964 considers the denial or delay of medical care due to language barriers to be discrimination.

Section 1557 – Patient Protection and Affordable Care Act: Section 1557 is the nondiscrimination provision of the Affordable Care Act (ACA). The law prohibits discrimination on the basis of race, color, national origin, sex, age, or disability in certain health programs or activities

Health Literacy: Health literacy is the degree to which individuals have the capacity to obtain, process, and understand basic health information and services needed to make appropriate health decisions.

Cultural and Linguistic Competency: Competency includes communicating in a manner that is linguistically and culturally appropriate. For many individuals with limited English proficiency (LEP), the inability to communicate in English is the primary barrier to accessing health information and services. Health information for people with LEP needs to be communicated plainly in their primary language, using words and examples that make the information understandable.

Combating FWA

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; Criminal Fraud
- OIG Exclusion
- Your Responsibilities
- Identify how to report FWA
- Recognize how to correct FWA
- FWA Key Indicators

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.

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.

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.

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 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.

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.

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.

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.

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

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.

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.

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 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).

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.

Your Responsibilities

What Are Your Responsibilities?

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

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
- Verify all information provided to you.

Stay Informed About Policies and Procedures

Familiarize yourself with your entity's policies and procedures. You 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 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.

Reporting FWA

Report FWA

Everyone must report suspected instances of FWA. Your 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. Your compliance department area will investigate and make the proper determination.

How to Report Potential FWA to MC-Rx

- Call the Compliance Officer (787) 286-6032 ext. 3123;
- Call the Compliance Hotline: (787) 286-6032 ext. 3800;
- Call the Compliance Direct Hotline: (787) 773-1328;
- Send a Confidential email: cumplimiento@mc-rx.com ;

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

You must have a mechanism for reporting potential FWA by employees. You 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

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 regulatory 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 employees 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;
- Conducting mandated training; Providing educational materials;
- Revising policies or procedures;
- Taking disciplinary action, such as suspension of marketing, enrollment, or payment; or
- Terminating an employee or provider.

Privacy Training

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

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.

Where Does MC-Rx 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. MC-Rx is a covered entity under HIPAA.

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).

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 or 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).

PHI Identifiers & Examples

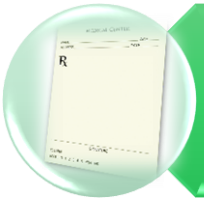
Protected Healthcare Identifiers (PHI)

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.

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.

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.”

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.

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.

How to Report Potential Privacy Concerns to MC-Rx

- Call the Compliance Officer (787) 286-6032 ext. 3123;
- Call the Compliance Hotline: (787) 286-6032 ext. 3800;
- Call the Compliance Direct Hotline: (787) 773-1328;
- Send a Confidential email: cumplimiento@mc-rx.com ;
- Send an email: lreyes@mc-rx.com

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.

CMS 10147 Notice to Members

Pharmacy responsibility to distribute and educate NOTICE to members:

All contracted pharmacies are required to distribute the CMS 10147 notice to Part D enrollees when a prescription cannot be covered ("filled") under the Medicare Part D benefit at the point of sale (POS).

The notice must be provided to the enrollee if the pharmacy receives a transaction response (rejected or paid) indicating the claim is not covered by Part D. The notice instructs enrollees about their right to contact their Part D plan to request a coverage determination, including an exception. This notice fulfills the requirements at 42 CFR § 423.562(a)(3) and § 423.128(b)(7)(iii).

Where can you locate the CMS 10147 Notice?

Visit our webpage www.mc-rx.com for valuable information and materials:

- ✓ CMS Notice 10147 Medicare Prescription Drug Coverage and your Rights

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

YOU HAVE GAINED KNOWLEDGE OF COMPLIANCE, FWA, HIPAA, AND MORE…

PLEASE PROCEED TO THE NEXT SLIDES FOR A KNOWLEDGE CHECK AND A QUICK EXAM TO PUT YOUR KNOWLEDGE TO THE TEST...

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 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

Lesson Review

Correct Answers: 1. B; 2. C; 3. B; 4. B; 5. A

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

Knowledge Check

CONGRATULATIONS!

YOU HAVE COMPLETED THIS TRAINING!

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)