

# Health Network Solutions

## Compliance Training

for Contracted Health Care Professionals



Revised 07/12/16

# Introduction



HNS has developed a compliance program to establish a culture within the HNS network that promotes prevention, detection, and resolution of conduct that does not conform to federal and state law, federal, state, and private payor health care program requirements, and/or HNS' ethical and business policies.

The HNS Compliance Program requires HNS to provide compliance training to contracted health care professionals. Compliance training helps increase awareness of our legal environment and helps us detect and prevent violations of laws applicable to our industry.

CMS requires that the compliance training provided by organizations like HNS include certain specific information published by CMS. Accordingly, those slides are included in this training module at the end of HNS' Compliance Training. These slides are easily identified by the slide colors of blue and yellow.

# Commitment to Compliance



Compliance is everyone's responsibility.

HNS is committed to conducting our business in accordance with the highest ethical standards and in accordance with federal and state laws and regulations that govern our industry.

***HNS expects that same commitment from our contracted health care professionals.***



# Limitations on HNS' Compliance Training



This training module provides general information regarding compliance, fraud, waste and abuse laws, HIPAA/HITECH laws, security awareness, and HNS' compliance policies.

Neither the content of this training module nor the information in this section of this web site are offered as, or constitute, legal advice. No one should rely on this training module, information included on the HNS website, or information obtained from HNS representatives, without first seeking appropriate professional legal advice.

HNS makes no claim, promise, or guarantee of any kind about the accuracy, completeness, or adequacy of the content of the presentation and expressly disclaims liability for errors and omissions in such content.

# Goals of Compliance Training



The goals of HNS' compliance training are to:

- ❧ Promote ethical conduct and business practices;
- ❧ Help ensure your familiarity and compliance with HIPAA and HITECH laws and regulations;
- ❧ Help ensure your familiarity and compliance with fraud, waste and abuse (FWA) laws;
- ❧ Assist you in the prevention and detection of accidental and intentional non-compliance with those laws;
- ❧ Ensure you understand your responsibilities for preventing, detecting, and reporting violations, and of HNS' disciplinary actions for non-compliance.

# Who Must Complete this Compliance Training?



- ❧ **HNS contracted health care professionals.**
- ❧ **All employees** of contracted health care professionals.
- ❧ **Vendors/contracted individuals or entities.**  
If your organization has contracted with individuals or entities to provide health and/or administrative services on behalf of Federal health plan members, you must also provide this training to those subcontractors. (An example of an entity to which you should provide this training is a billing company you contract with for billing/collection services.)



# Written Standards & Policies



Pursuant to compliance guidance issued by the Office of the Inspector General (OIG), HNS has developed written compliance standards (the **HNS Compliance Policies**) which establish HNS' expectations for contracted health care professionals.

Additionally, HNS maintains written business policies and procedures (P&Ps) for contracted health care professionals developed to improve quality of care, treatment outcomes, and to provide guidance for routine and required operational processes. These policies are posted in the HNS website.

HNS reserves the right to periodically review and revise its policies and will provide timely notification to contracted health care professionals of any material changes.

HNS' P&Ps will comply with all applicable federal and state laws, regulations, and requirements related to Medicare, Medicaid, and private health care programs.

# Compliance Responsibilities



Based on recommendations by the OIG for organizations like HNS, which contract with health care professionals, HNS has enumerated those compliance functions that are shared responsibilities of HNS and our contracted health care professionals, those which are the sole responsibility of HNS, and those which are the sole responsibility of the contracted health care professional.



# Shared Responsibilities of HNS & Contracted Health Care Professionals



The following **Compliance Policies**  
represent the responsibilities of  
**both**  
HNS and contracted health care professionals.

# Shared Responsibilities of HNS & Contracted Health Care Professionals



**Both HNS and our contracted health care professionals are responsible for:**

- ☞ Complying with all applicable federal and state laws and regulations;
- ☞ Adhering to the HNS Standards of Conduct, Code of Ethics, and generally recognized medical and professional ethical standards;
- ☞ Cooperating with all compliance investigations;
- ☞ Developing and maintaining a written compliance plan that seeks to detect, prevent, and correct instances of non-compliance;
- ☞ Maintaining all records relating to compliance programs for a period of 10 years;

# Shared Responsibilities of HNS and HNS Contracted Health Care Professionals



**Both HNS and our contracted health care professionals are responsible for:**

- Investigating and correcting instances of non-compliance;
- Reporting all suspected or actual instances of non-compliance and immediately escalating any incidents of suspected fraud, waste and abuse;
- Ensuring employees and contractors are eligible for participation in Federal health care plans (both at initial hire and monthly thereafter) by querying the OIG's List of Excluded Individuals & Entities (LEIE);
- Retaining documentation which substantiates that the organization conducted the initial and monthly reviews of the List of Excluded Individuals & Entities. This information must be available upon request by HNS, contracted health care plans, and CMS. These records must be maintained for 10 years;

# Shared Responsibilities of HNS and HNS Contracted Health Care Professionals



**Both HNS and contracted health care professionals are responsible for:**

- ✧ Removing any employee (or contractor) who has *pending* criminal charges relating to health care, or *proposed exclusion* from participation in any federally or state funded health care program from direct responsibility or involvement in any federally or state funded health care programs;
- ✧ Ensuring we do not act in a manner that prohibits competition. We shall not communicate formally or informally with competitors to fix or control prices, allocate markets, boycott customers or suppliers, or limit the sale of our products/services;

# Shared Responsibilities of HNS and HNS Contracted Health Care Professionals



**Both HNS and our contracted health care professionals are responsible for:**

- ❧ Ensuring that we develop, implement, enforce, and audit policies and procedures to ensure the privacy and security of protected health information (PHI) and the confidentiality of personal and other information protected by statute;
- ❧ Ensuring appropriate safeguards are in place to maintain the integrity of our information and billing systems and to prevent the unauthorized access of computer systems, including but not limited to, anti-virus protection and appropriate internal safeguards; and
- ❧ Maintaining back-up systems that ensure our ability to retrieve data in the event of an emergency or disaster.

# Responsibilities of HNS



The following **Compliance Policies** represent the responsibilities of HNS.

# Responsibilities of HNS



## **Integrity of HNS Employees**

Prior to, or within the first 30 days of employment with HNS, HNS shall conduct reasonable and prudent background investigations of each employee which shall include criminal background checks.

HNS shall prohibit employment of individuals who have been recently convicted of a criminal offense related to health care or who are listed as debarred, excluded, or otherwise ineligible for participation in federal health care programs.

# Responsibilities of HNS



## **Education and Training**

HNS shall be responsible for making compliance training available to our employees, officers, directors (herein after referred to as HNS personnel), and to all contracted health care professionals, both for their own training and for training their staff members.

## **Open Communication**

HNS shall be responsible for ensuring open and effective lines of communication between HNS and HNS personnel, and between HNS and our contracted health care professionals.

HNS shall maintain toll-free telephone and facsimile lines to promote open and frequent communication. HNS shall communicate those numbers to HNS personnel, to members, and to HNS contracted health care professionals by posting those numbers on the HNS website.



# Responsibilities of HNS



## **Quality of Health Care Data**

HNS shall be responsible for ensuring we do not alter or modify the health care data on claims received from contracted health care professionals.

HNS shall be responsible for ensuring the accuracy of claims data manually input into HNS computer systems by HNS personnel.

Except as indicated here, HNS shall not be responsible for the accuracy, validity, or quality of claims data submitted to HNS by contracted health care professionals.

# Responsibilities of HNS



## **Suspicious Claims**

HNS shall prevent the submission of all claims when HNS suspects fraud or deceit until such time as HNS can determine if a violation has occurred. HNS shall notify the contracted health care professional, in writing, of this determination within 30 days of the date of the determination. The notification shall include all claim specific information and the rationale for such a determination.

## **Duplicate Billing**

HNS shall implement internal controls designed to prevent the submission of duplicate claims. (*HNSConnect* shall include an edit designed to identify duplicate claims (as defined by HNS parameters) and prevent the submission of those claims.)

# Responsibilities of HNS



## **Notification**

HNS shall be responsible for the timely notification to HNS personnel and contracted health care professionals of suspected violations of applicable laws, HNS' policies, and the policies of contracted health care plans, as well as the investigation of such violations.

## **Sanctions for Non-Compliance**

HNS shall be responsible for developing and enforcing disciplinary guidelines and sanctions for non-compliance and shall ensure HNS' Sanction Policies are well publicized by posting these policies in a prominent location at HNS offices and on the Compliance section of the HNS web site.

# Responsibilities of Contracted Health Care Professionals



The following **Compliance Policies** represent those responsibilities which are the **sole** responsibility of HNS contracted health care professionals.

These policies are applicable to ALL services provided to members whose health care plan contracts with HNS and to services provided to beneficiaries of federally funded health care plans.

A complete list of the responsibilities of contracted health care professionals (*HNS Compliance Policies*) is included in the Compliance Section of the HNS website. HNS recommends contracted health care professionals print these policies and review them frequently.

# Responsibilities of Contracted Health Care Professionals



## Compliance Training Requirements for Contracted Health Care Professionals (Only for Physicians)

- ☞ **Initial Training:** contracted health care professionals shall complete this training module within 15 days of the effective date of their participation in the HNS Network.
- ☞ **Annual Compliance:** contracted health care professionals shall complete this training annually, by the end of July of each year.
- ☞ **Compliance Training Certification.** All contracted healthcare professionals must complete the Compliance Training Certification form which is included at the end of this training module and *a signed and dated copy of this certificate must be provided to HNS by the due dates indicated above.* The certificate may be emailed or faxed to HNS.

HNS Fax Number: (877) 329-2620

# Responsibilities of Contracted Health Care Professionals



## **Compliance Training (cont.)**

### ***Employee Training Required***

Contracted health care professionals shall ensure all their employees complete this training module **annually**. While copies of certificates of completion of the training must be maintained by the contracted healthcare professional, *those are not required to be submitted to HNS.*

### ***Vendor Training Required***

Contracted health care professionals shall ensure that applicable vendors/contractors receive this training **annually**. While copies of certificates of completion of the training must be maintained by the contracted healthcare professional, *those are not required to be submitted to HNS.*

# Responsibilities of Contracted Health Care Professionals



## Retention of Compliance Records

Contracted health care professionals shall maintain ALL records associated with their own compliance training; the training of their employees and contractors and vendors (as applicable) for **10 years**. At a minimum, records which must be maintained include:

- ☞ The name of the individual or entity that completed the training;
- ☞ The date of the training;
- ☞ The training material used (i.e. a copy of this training module); and
- ☞ Copies of the HNS Compliance Training Certification.

These records shall be available if requested by HNS, contracted health care plans, and/or CMS.

# Responsibilities of Contracted Health Care Professionals



## **Failure to Comply with Training Requirements**

Failure to comply with all HNS Compliance Training requirements, as outlined herein, may result in the temporary suspension of contracted health care professional's access to *HNSConnect*, to the submission of claims to HNS via *Office Ally*, and/or termination from the network.



# Responsibilities of Contracted Health Care Professionals



## **Compliance with Policies**

Contracted health care professionals shall comply with all HNS policies and the Corporate Medical Policies of contracted health care plans.

# Responsibilities of Contracted Health Care Professionals



## **Quality of Health Care Data**

Contracted health care professionals shall ensure the validity, reliability, accuracy, and quality of health care data submitted to HNS and to any federal or private health care plan.

The validity, reliability, accuracy, and quality of health care data submitted to HNS by contracted health care professionals shall be the **sole responsibility** of the contracted health care professional who provided the services (and/or under whose supervision the services were provided), and whose name is on the claim form as the rendering provider.

# Responsibilities of Contracted Health Care Professionals



## **HNS Clinical Records Quality Standards**

Contracted health care professionals shall ensure that care provided to members of HNS contracted health care plans is provided and documented pursuant to the ***HNS' Clinical Records Quality Standards***. These standards are posted on the HNS website.

# Responsibilities of Contracted Health Care Professionals



## **Documentation**

Contracted health care professionals shall ensure that claims are only submitted for payment when the documentation in the health care record supports the services or items on the claim, and only when such documentation is legible, maintained, appropriately organized, and is available for audit and review.

## **Coding**

Contracted health care professionals shall ensure that services billed through HNS are properly coded with the most appropriate and most current ICD, CPT, and/or HCPCS codes, and, as applicable, are appended by appropriate modifiers, and that those codes are supported by documentation in the health care record.

# Responsibilities of Contracted Health Care Professionals



## **Submission of Claims to HNS**

Contracted health care professionals shall submit claims to HNS for all covered services provided to members whose health care plans contract with HNS. This includes claims for secondary coverage if the secondary payor contracts with HNS.

**Exception:** If a patient specifically requests that a contracted health care professional not file claims to their health care plan, the contracted health care professional shall comply with the request, **but may do so ONLY if the request is properly documented in the patient's health care record.**

# Responsibilities of Contracted Health Care Professionals



## **Unbundling**

Contracted health care professionals shall not unbundle codes (use separate codes for services that have an aggregate code which should be used).

## **Duplicate Billing**

Contracted health care professionals shall not submit duplicate billings in an attempt to gain duplicate payment.

# Responsibilities of Contracted Health Care Professionals



## **Balance Billing**

Contracted health care professionals shall not balance bill for covered contracted services. Balance billing refers to billing members the difference between the contracted health care professional's charge and the contracted allowable. For **covered** services provided, contracted health care professionals shall only collect from members the applicable co-payment, co-insurance, and/or deductible amount.

## **Posting Payments**

Contracted health care professionals shall ensure that all payments, including zero dollar payments, are posted to patient accounts within 15 days of receipt.

# Responsibilities of Contracted Health Care Professionals



## **Refunds/Overpayments**

Contracted health care professionals shall not retain payments to which they are not entitled.

If a contracted health care professional receives payment for services he/she did not provide, or *to which they are not entitled*, they shall **immediately notify HNS** (if the payment was issued by HNS) or the issuing entity, if not HNS, to arrange to refund those monies.

Overpayments received from HNS or an HNS contracted health care plan shall be resolved pursuant to **HNS Refund/Overpayment Policies**.



# Responsibilities of Contracted Health Care Professionals



## **Accuracy of Name/Number of Rendering Provider**

Contracted health care professionals shall not knowingly misuse provider name and/or identification numbers. The name and the Type I NPI number of *the health care professional who actually rendered the service(s)* shall be included on health care claims. The health care professional's name on the claim form is an attestation that he/she performed the services reported on the claim.

**Exception:** If services are provided by a locum tenens (“fill-in”) health care provider and all locum tenens requirements have been met, services provided by the locum tenens provider may be submitted under the name/NPI number of the health care professional who contracted with the locum tenens provider. For additional clarification on locum tenens, please review the HNS ***Locum Tenens Policy***.

# Responsibilities of Contracted Health Care Professionals



## **Compensation to Billing Personnel (includes staff, billing companies and/or consultants)**

HNS contracted health care professionals shall not compensate billing staff, billing companies, and/or consultants in a manner that provides financial incentive(s) to improperly code claims.

## **Cooperating with Investigations**

HNS contracted health care professionals shall cooperate with all compliance investigations initiated by HNS, contracted health plans, government entities, or as otherwise required by law.

# Responsibilities of Contracted Health Care Professionals



## **Ethical and Professional Standards**

Contracted health care professionals shall adhere to generally recognized standards of medical and professional ethics, the ethical and professional standards set forth by their respective licensing board, and the **HNS Code and Standards of Conduct**.

# Ethical Standards



# HNS' Code of Conduct



The HNS Code of Conduct is a guide that helps us carry out our day-to-day professional responsibilities in accordance with the highest possible standards of ethical behavior and in compliance with laws that regulate our business.

Everyone in the HNS Network shall:

- ❧ Conduct themselves in a manner consistent with generally accepted ethical principles and the HNS Standards of Conduct;
- ❧ Treat each other and all those we serve with kindness, respect, and the highest degree of professionalism;
- ❧ Conduct themselves in a professional manner, in accordance with all state and federal laws and regulations, HNS policies, and the policies of contracted health care plans; and
- ❧ Perform their professional responsibilities diligently, in good faith, and to the best of their ability.

# Standards of Conduct

## *Compliance to Laws & Regulations*



Our first and most fundamental obligation is to **obey both the letter and spirit of the law.**

Each of us must comply with all federal and state laws and regulations.

# Standard of Conduct Integrity



Each of us is expected to act with the highest degree of integrity.

All contracted health care professionals shall at all times conduct their business with fairness, honesty, and integrity, which means that each individual's behavior is characterized by truthfulness, the absence of deception or fraud, and respect for the laws applicable to the health care industry.

# Do the Right Thing, in the Right Way



Even in cases where interpretation of the law could be ambiguous, permissive, or lenient, HNS expects its contracted health care professionals to **always do the right thing, in the right way,** and choose the course of honesty and integrity.



# Legal Standards (Relevant Laws)



While the scope of this Compliance Training may be expanded in the future to cover additional areas of regulatory compliance applicable to the health care industry, this section of the training focuses on the following laws:

- ❧ Fraud, Waste and Abuse (**FWA**) Laws
- ❧ Personal Information Privacy and Security Laws (**HIPAA**)



# Fraud, Waste and Abuse (FWA)



# FWA is Everyone's Problem



Health care fraud and abuse is a national problem that, either directly or indirectly, affects all of us.

National estimates project that billions of dollars are lost to health care fraud and abuse on an annual basis.

These losses lead to increased health care costs and potential increased costs for health care coverage.

**FWA laws apply to all HNS contracted health care professionals.**

# What is Fraud, Waste & Abuse?



**Fraud** is knowingly and willfully executing, or attempting to execute, a scheme to:

- ☞ -Defraud any health care program
- ☞ -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, a health care program.

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

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

# Differences Between Fraud, Waste & Abuse



**The real difference between fraud and waste and abuse is the person's intent.**

**Fraud** is an *intentional* deception or misrepresentation that someone makes, knowing it is false, that could result in unauthorized benefit/payment. It is important to note that attempt itself is fraud, regardless of whether it is successful.

**Waste and abuse** involves actions that are inconsistent with accepted, sound medical, business, or fiscal practices. Waste and abuse result in unnecessary costs to CMS and America's health care delivery system through improper payments.

# Examples of FWA



*Examples of **fraud** include:*

- ❧ Intentionally billing for services not furnished;
- ❧ Upcoding; and
- ❧ Altering medical records to justify payments

*Examples of **waste and/or abuse**:*

- ❧ Billing for services that are not medically necessary;
- ❧ Performing unnecessary tests on a beneficiary to establish medical necessity;
- ❧ When the diagnosis for the member is not supported in the medical record; and
- ❧ Retaining reimbursement for services not owed to the health care professional.



# FWA Regulatory Agencies



The primary regulatory agencies for FWA laws are:

❧ **The Department of Health & Human Services (DHHS) Office of the Inspector General (OIG).**

❧ **Centers for Medicare and Medicaid Services (CMS).**

CMS is a federal entity within the U.S. Department of Health and Human Services. CMS is responsible for oversight of the Medicare and Medicaid programs.



# Relevant FWA Laws



Some of the most important federal Fraud, Waste and Abuse laws applicable to our contracted health care professionals are:

- ❧ The Federal False Claims Act (FCA);
- ❧ The Fraud Enforcement and Recovery Act (FERA);
- ❧ The Deficit Reduction Act (DRA);
- ❧ The Anti-Kickback Statute (AKS); and
- ❧ The Physician Self-Referral Law (Stark Law).



# Federal False Claim Act (FCA)



The Federal False Claims Act, sometimes referred to as the FCA or Lincoln Law, is a law that creates liability for the intentional submission of false claims to the government. This law is a powerful tool used by the government to combat fraud.



# Qui Tam (Whistleblower Provision)



An important provision of the **False Claims Act** is known as “qui tam,” which allows any person or entity to bring actions to enforce the False Claims Act. Under qui tam, any person with evidence of fraud against federal programs or contracts may file a qui tam lawsuit on behalf of the U.S. Government. The government has the right to intervene and join the action.

Those who file qui tam lawsuits are informally known as “**whistleblowers.**”

**Incentive:** As compensation for the risk and effort of filing a qui tam case, the whistleblower may be awarded a portion of the funds recovered.

**Protection:** Any person who is discharged, demoted, suspended, threatened, harassed, or discriminated against because of filing a qui tam case is entitled to seek double the amount of back-pay, reinstatement, and other damages and fees.

# Examples of Violations of the False Claims Act



**Examples** of false or fraudulent claims include, but are not limited to:

- Double billing;
- Upcoding; and
- Submitting claims for items or services not provided and/or not medically necessary (unless covered under the benefit plan), and/or billing for non-covered services.



# Violations/Penalties of the False Claim Act



Violators of the False Claims Act are required to pay the federal government **three (3) times the amount of damages sustained** by the government and civil penalties between **\$5500 and \$11,000 for each false or fraudulent claim. Effective August 1, 2016, penalties will increase to \$10,781 - \$21,562 per claim.**

Note: The Federal False Claims Act covers the entire nation, however, some states, including North Carolina, have state-specific False Claims Act laws.

# Fraud Enforcement & Recovery Act (FERA)



The Fraud Enforcement and Recovery Act increases the government's power to investigate and prosecute any financial fraud against the government and expands liability under the False Claims Act.

This law makes it easier for the government to pursue violators of the False Claims Act.

This law expanded liability under the False Claims Act, most notably by:

- ✧ Expanding the definition of a claim;
- ✧ Reducing the intent required to establish liability; and
- ✧ Expanding the protection of whistleblowers.

# Deficit Reduction Act (DRA)



A primary purpose of this law is to provide guidelines and incentives for states to create their own state-specific False Claims Act legislation.

The primary incentive is an increase to the state's share of the amount recovered under such laws by 10%. This means that the state will receive a larger portion of the recovered amount from fraud cases.

# Anti-Kickback Statute (AKS)



The first Anti-Kickback provision in the Social Security Act Amendments was designed to prevent fraud and outlaw conduct that was already considered unethical.

This statute imposes penalties on any person that knowingly and willfully solicits, receives, offers, or pays any remuneration (including any kick-back, bribe, or rebate) for referrals for services that are paid in whole or in part by a federal health care program, which includes Medicare and Medicaid.

In other words, it is a crime for individuals or entities to knowingly or willfully offer, pay, solicit, or receive something of value in exchange for rewarding referrals of business under federal health care programs.

# Anti-Kickback Statute (Cont.)



The primary function of the Anti-Kickback Statute is to ensure that financial motives do not undermine the integrity of the medical judgment that must be maintained by health care professionals.

This statute promotes referrals based on medical need rather than referrals based on financial or other types of incentives.



# Penalties of AKS



The Federal Anti-Kickback Statute is a **criminal statute** and the penalties for violations can be severe.

Penalties can include up to **\$25,000** per violation, felony conviction punishable by imprisonment of up to **5 years**, **or BOTH**, as well as possible exclusion from participation in federal health care programs.

# Physician Self-Referral Law (Stark Law)



Commonly called the “Stark Law” after U.S. Congressman Pete Stark, who initially sponsored the bill, this law addresses the practice of a physician referring a patient to a medical facility in which the physician has a financial interest, be it ownership, investment, or a structured compensation arrangement.

This law prohibits a physician from referring Medicare or Medicaid patients for certain **designated health services** to an entity in which the physician, or an immediate family member, has a financial interest.

Similar to the Anti-Kickback Statute, the primary function of this statute is to ensure that financial motives do not undermine the integrity of the medical judgment of health care providers.

# “Designated Health Services” under Stark



## ☞ Designated health services include:

- ✓ Radiology & Imaging services;
- ✓ Physical & occupational therapies;
- ✓ DME and supplies (example: TENS units);
- ✓ Clinical Laboratory services;
- ✓ Prosthetics, orthotics, & prosthetic devices & supplies;
- ✓ Outpatient speech/language pathology services;
- ✓ Radiation therapy services & supplies;
- ✓ Parenteral and enteral nutrients, equipment & supplies;
- ✓ Home health services;
- ✓ Outpatient prescription drugs; and
- ✓ Inpatient & outpatient hospital services.



# Penalties – Stark Law



Penalties for violating the Stark Law include:

- ❧ Denial of payment from Medicare/Medicaid for those services that violated the Stark Law;
- ❧ Exclusion from the Medicare and Medicaid programs;
- ❧ Any payment received from a prohibited referral must be refunded;
- ❧ Up to **\$15,000 fine** for EACH service provided that a person “knows or should know” was provided in violation of this statute; and
- ❧ Up to **\$100,000 fine** for entering into an arrangement or scheme that violates this law.

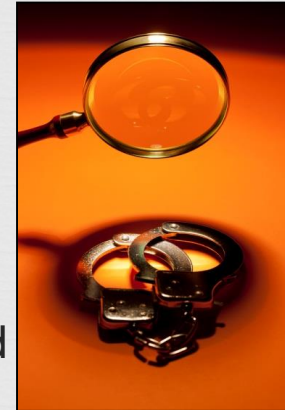
**Proof of specific intent to violate the law is not required.**

# Consequences of Committing Fraud, Waste or Abuse



The following are potential consequences for committing Fraud, Waste or Abuse. The actual consequence depends on the violation, but may include:

- ❧ Civil Money Penalties;
- ❧ Criminal Conviction/Fines;
- ❧ Imprisonment;
- ❧ Loss of Physician License;
- ❧ Exclusion from Federal health care programs; and
- ❧ Termination of participation in the HNS network.



# Best Practices to Assure Compliance to FWA laws...



- ☞ Be committed to ensuring compliance with FWA laws.
- ☞ Develop and document policies and procedures to ensure compliance and provide annual FWA training to employees.
- ☞ Always be on the lookout for suspicious activity and report it.
- ☞ Always verify insurance information provided by members with the applicable health care plan.
- ☞ Ensure the information in the health care record is accurate.
- ☞ Ensure the information reported on claims is accurate and consistent with the information in the health care record.

# Best Practices to Assure Compliance to FWA laws...



- ☞ Conduct ongoing monitoring of health care records and claims data to assure accuracy of information. If you determine an inadvertent error, promptly file a corrected claim to correct the error.
- ☞ If you receive payment for services you did not provide or *to which you are not entitled*, immediately notify HNS (or the entity that issued the payment) to arrange to refund those monies.
- ☞ Stay up-to-date with laws, regulations, and policies, including all HNS Policies and the medical policies of contracted payors.

# HIPAA





# HIPAA



The **Health Insurance Portability and Accountability Act (HIPAA)** is a federal law passed in 1996 due to the rapid growth of health information systems and the need to ***safeguard individuals' health information***.

HIPAA contains provisions and rules to protect privacy and help control fraud, waste, and abuse within the health care system.

The primary regulatory agency for HIPAA laws is the Department of Health & Human Services, Office of Civil Rights (OCR).

# HIPAA



HIPAA is comprised of many components. The focus of this HIPAA training is:

- ❧ The Federal Beneficiary Inducement Statute;
- ❧ The HIPAA Privacy Rule; and
- ❧ The HIPAA Security Rules.

# Who Must Comply with HIPAA?



**HIPAA applies to Covered Entities and Business Associates.**

**Covered Entities (CE)** are individuals or entities who **transmit any health information in electronic form in connection with a transaction.**

**Business Associates** are those to whom the Covered Entity discloses protected health information (PHI) to carry out, assist with performance of, or perform on the behalf of, a function or activity for the Covered Entity.

# Covered Entities



CEs include health plans, health care professionals, health care clearinghouses, and employer sponsored health plans.

**Health Plans** - Individual and group plans that provide or pay the cost of medical care are **Covered Entities**.

**Health Care Providers** - Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a **Covered Entity**. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which the Department of Health and Human Services (HHS) has established standards.

Note: Using electronic technology, such as email, does not mean a health care provider is a Covered Entity; the transmission must be in connection with a standard transaction.

# Covered Entities



## **Health Care Clearinghouses**

*Health care clearinghouses* are entities that process nonstandard information they receive from another entity into standard (i.e., standard format or data content), or vice versa and are **Covered Entities** under HIPAA.

**(HNS falls under the category of a health care clearinghouse.)**

# Business Associates



In general, a Business Associate (BA) is a person or organization, other than a member of a Covered Entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a Covered Entity that involve the use or disclosure of individually identifiable health information.

Business Associate functions or activities on behalf of a Covered Entity include claims processing, data analysis, quality and utilization review, and billing. However, persons or organizations are not considered Business Associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.

**A Covered Entity can be the Business Associate of another Covered Entity.**

(HNS is a Covered Entity as defined by HIPAA but acts as a *Business Associate of* each contracted health care professional.)

# Business Associate Agreements (BAA)



When a Covered Entity uses a contractor or other non-workforce member to perform “*Business Associate*” services or activities, the Privacy Rule requires that the Covered Entity include certain protections for the information in a *Business Associate Agreement (BAA)*. In the Business Associate Agreement, a Covered Entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its Business Associates. Moreover, a Covered Entity may not contractually authorize its Business Associate to make any use or disclosure of protected health information that would violate the HIPAA Regulations.

(HNS maintains BAAs with each contracted health care professional.)

# Protected Health Information



Protected Health Information (PHI) is individually identifiable health information that is transmitted or maintained **in any form or medium (e.g., electronic, paper, or oral)**.

To be considered PHI, the information must have two (2) components:

- ☞ **Medical Information** – Information about an individual's past, present, or future physical or mental health care; and
- ☞ **Personally Identifiable Information** – Data elements that can identify or reasonably lead to the identification of an individual.



# Examples of Personally Identifiable Information



Personally identifiable Information includes any unique identifying number, characteristic or code.

Examples include:

- ☞ Names;
- ☞ Addresses;
- ☞ Dates, including birth date, date of service, date of death, etc.;
- ☞ Telephone or fax number;
- ☞ E-Mail address;
- ☞ Subscriber ID number;



# More Examples of Personally Identifiable Information



- ❧ Social Security numbers;
- ❧ NPI numbers;
- ❧ URL, IP Addresses;
- ❧ Full-Face Photos and Comparable Images;
- ❧ License numbers, account numbers, medical record number;
- ❧ Vehicle Identifier and serial numbers (License plates); and
- ❧ Device identifiers & serial numbers.

# HIPAA Regulations



# HIPAA Regulations - Federal Beneficiary Inducement Statute



This law is part of **HIPAA**, and makes it **illegal** to offer a remuneration that a person knows, or should know, is likely to influence a patient to select a particular provider or supplier.

The statute defines “remuneration” to include, without limitation,

- **waivers of co-payments and deductible amounts** (or any part thereof) and
- **transfers of items or services for free or for other than fair market value.**

# Penalties - Federal Beneficiary Inducement Statute



Violations of the Federal Beneficiary Inducement Statute  
may result in civil money penalties (CMPs) of up to  
**\$10,000 for each wrongful act.**

# HIPAA Regulations - HIPAA Privacy Rule



The Privacy Rule is a core component of HIPAA. The Privacy Rule is a set of standards for the **protection of certain health information.**

These standards address the **use and disclosure** of individually protected health information.

The standards also **grant specific rights to members.**

# HIPAA Privacy Rule



The Privacy Rule protects  
**ALL** "individually identifiable health information",  
also called Protected Health Information (*PHI*) held or transmitted by a  
Covered Entity or its Business Associate  
**in any form or media, whether electronic, paper, or oral.**

# HIPAA Regulations

## HIPAA Security Rules



**The HIPAA Security Regulations** outline specific protections and safeguards for ***electronic*** Protected Health Information.





# HIPAA Security Rules



While the HIPAA Privacy Rule protects the privacy of all PHI, the **Security Rule** protects a subset of information covered by the Privacy Rule.

The subset of information protected by the Security Rule is all ***individually identifiable health information a Covered Entity creates, receives, maintains, or transmits in electronic form.***

The Security Rule calls this information “electronic protected health information” (**e-PHI**).

The Security Rule does NOT apply to PHI transmitted orally or in writing.

# Examples of PHI subject to the Security Rules



- ✧ Emails that include PHI.
- ✧ Claims that are received or transmitted electronically.
- ✧ Remittance information (EOB) that is received or transmitted electronically.

# HITECH



The Health Information Technology for Economic and Clinical Health Act (HITECH) was enacted in 2009, as part of the American Recovery and Reinvestment Act (ARRA) **to encourage the adoption and “meaningful use” of electronic health records (EHR)**, as the use of EHR has been shown to improve quality, safety, and coordination of health care.

# HIPAA Omnibus Rule



The Omnibus Rule is a set of regulations modifying HIPAA's Privacy, Security, and Enforcement Rules to implement various provisions of the HITECH Act.

Highlights of the Omnibus Rule include:

- ☞ Makes Covered Entities and their Business Associates directly liable for compliance with certain requirements;
- ☞ Strengthens the limitations on the use and disclosure of PHI; and
- ☞ Expands an individual's rights to receive and restrict his/her electronic health information for which the member has paid out-of-pocket in full.

# PHI - Use & Disclosure



The HIPAA Privacy Rule defines and limits the circumstances in which an individual's PHI may be used and disclosed.

## **Use**

To use means to share, utilize, examine, or analyze PHI within your organization.

## **Disclose**

To disclose means to release, transfer, or share PHI to an individual or entity outside of your organization.

Covered Entities shall not use or disclose an individual's PHI *except as permitted by law*.

# Use and Disclosure- Minimum Necessary



The Privacy Rule includes a **Minimum Necessary Rule**. This rule restricts the use and disclosure of PHI to ONLY the amount necessary to perform a specific task. To comply with this rule:

- ☞ Use the least amount of PHI required to complete the task;
- ☞ Look at PHI only if the task requires it;
- ☞ Talk to others about PHI only if it is necessary to perform the task; and
- ☞ Give PHI to others only when it is necessary for them to perform their tasks.

# PHI - Use & Disclosure



HIPAA allows the use and disclosure  
of PHI (without the member's consent)  
if it relates to  
**Treatment, Payment, or Operations,**  
which is referred to as **TPO.**

# PHI - Use & Disclosure



Besides TPO, there are very specific situations when a Covered Entity can Disclose PHI *without a member's consent*. These allowed disclosures can include, but are not limited to:

- ☞ If required by law or law enforcement;
- ☞ For public health reasons;
- ☞ To report abuse; and
- ☞ To avert a serious threat.



# Required Disclosures of PHI



You are required to disclose PHI:

- ☞ To an individual member seeking to access their PHI in your possession;
- ☞ To the Secretary of Health and Human Services (HHS) to investigate or determine compliance with regulations; and
- ☞ As otherwise required by law.

# Permitted Use & Disclosures of PHI



You are **permitted** to use/disclose PHI:

- ☞ To carry out health care operations;
- ☞ To the individual patient, or authorized representative with a valid authorization from the patient; and
- ☞ To those with whom you do business, such as HNS, health care or managed care plans with which you contract, certain vendors (ex: your billing company), and BAs, **provided you have first obtained satisfactory assurances that the information will be adequately safeguarded.**

# Breach



## A “breach”

is an unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA.

## The **Breach Notification Rule**

requires HIPAA Covered Entities and their Business Associates to provide notification following a breach of unsecured PHI.

# Breach Notification Rule



The Breach Notification Rule has specific requirements regarding who must be notified in the event of a breach:

- ☞ **Individuals** who are affected by a breach must be notified within 60 days from the time of discovery;
- ☞ The Covered Entity must maintain an annual log of all breaches. Logs of breaches involving **less than 500 individuals** must be submitted to the Secretary of the Department of Health and Human Services annually, no more than 60 days after the end of the calendar year;
- ☞ The media must be notified of any breaches that involve 500 or more individuals no later than 60 days from discovery; and
- ☞ If a breach involves 500 or more individuals, the Secretary of the **U.S. Department of Health and Human Services** (HHS) must be notified without unreasonable delay and *in no case later than 60 days following the discovery of the breach.*

# Breach Notification Rule



Per the Rule, **it is NOT a breach when:**

- ☞ The information is accessed unintentionally by a workforce member or someone working under the authority of a CE or BA, if it was done in good faith and within the scope of authority, etc.;
- ☞ It is an inadvertent disclosure by a person authorized to access PHI to another person authorized to access PHI at the SAME Covered Entity, BA, or organized health care arrangement in which the Covered Entity participates; or
- ☞ Where the Covered Entity or BA has a good faith belief that the unauthorized person would not reasonably have been able to retain the PHI.

# Breach Notification Rule



Per the Rule, **it is presumed to be a breach unless** the Covered Entity or BA demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- ❧ The nature and extent of the PHI involved, including identifiers;
- ❧ The unauthorized person who used the PHI or to whom it was disclosed;
- ❧ Whether the PHI was actually acquired or viewed; and
- ❧ The extent to which the risk was mitigated.

# NC & SC Breach Reporting Requirements



In addition to reporting to Federal agencies and media:

**North Carolina** law requires that in the event of a breach of *personal* information we:

- ❧ Immediately notify the individual; and
- ❧ Report the breach to the NC Consumer Protection Division of the Attorney General's Office.
- ❧ Below is the web address which can be used to report:
- ❧ <http://www.ncdoj.gov/Protect-Yourself/2-4-3-Protect-Your-Identity/Protect-Your-Business/Report-a-Security-Breach.aspx>

**South Carolina** law requires that in the event of a breach of *personal* information we:

- ❧ Immediately notify the individual;
- ❧ If more than 1000 people at one time, report the breach to the SC Office of Consumer Affairs and all national consumer reporting agencies. Below is information on how to report:
- ❧ Phone:1-800-922-1594
- ❧ [scdca@scconsumer.gov](mailto:scdca@scconsumer.gov)
- ❧ SC Office of Consumer Affairs  
PO Box 5757  
Columbia SC 29250-5246

# HIPAA

## Penalties/Violations



The improper acquisition, access, use, or disclosure of PHI is a violation of HIPAA. HIPAA penalties can be severe.

**Civil monetary penalties** for non-compliance depend on the nature of the violation and can range from **\$100-\$50,000 per violation**, with a maximum penalty of **\$1.5 million per year** for violations of an identical provision.

**Criminal Penalties** can range from **\$50,000-\$250,000** and between **1 and 10 years imprisonment**.



# Patient Rights Under HIPAA



Under HIPAA, each individual has rights regarding their PHI. These rights include:

- ✧ The right to receive a copy of the health care professional's "Notice of Privacy Practices," which details how individually identifiable health information may be used or disclosed by the organization;
- ✧ The right to review or obtain a copy of medical records about that member or, as applicable, the member's minor children;
- ✧ The right to request restrictions on the use or disclosure of the member's medical records;

# Patient Rights Under HIPAA



- ✧ The right to receive individually identifiable health information at an alternate address or through alternate delivery means, such as by fax or courier;
- ✧ The right to request amendments to medical records, with certain limitations;
- ✧ The right to an accounting of certain disclosures of individually identifiable health information; and
- ✧ The right to file a privacy complaint directly with the contracted health care professional, HNS, or with the federal government.

# Best Practices to Assure Compliance to HIPAA laws...



Be committed to complying with HIPAA rules.

Develop and document privacy policies and procedures and provide annual HIPAA training to employees.

Report and track improper disclosures of PHI.

Conduct, at a minimum, an annual Risk Assessment and whenever there is a change in business operations that would necessitate a new risk assessment.



# Best Practices to Assure Compliance to HIPAA laws...



- ☞ Speak quietly and *only to those necessary* when discussing PHI with ANYONE.
- ☞ Never discuss member information or conditions in common areas.
- ☞ Verify that you have the correct email address before emailing PHI.
- ☞ Send all e-mails that contain PHI via a secure email system.
- ☞ Verify that you have the correct fax number before faxing PHI.
- ☞ Always include an appropriate disclaimer when faxing or emailing PHI.
- ☞ Do not leave documents containing PHI in any common areas, other than as required to fulfill duties and responsibilities.
- ☞ Disclose only the minimum amount of PHI necessary to accomplish the task.
- ☞ Ensure Business Associate Agreements are in place with applicable individuals and/or organizations.

# Best Practices to Assure Compliance to HIPAA laws...



- ❧ Never give out confidential information unless you are certain the recipient has a right to the information.
- ❧ Never share your computer password with anyone.
- ❧ Change computer passwords every 45 days.
- ❧ Never open links included in emails unless you are confident the email is from a trusted source.
- ❧ Never open attachments to emails unless you know the email is from a trusted source.
- ❧ Never access PHI using a public Wi-Fi system.
- ❧ Ensure the proper disposal of PHI.
- ❧ Ensure your computer will lock automatically after 15 minutes of inactivity.
- ❧ Ensure all computers and servers have up-to-date anti-virus and malware protection.

# Best Practices to Assure Compliance to HIPAA laws...



- ❧ Develop and enforce social media policies.
- ❧ Keep personal social media accounts separate from practice accounts.
- ❧ Never post or share photographs, or any form of PHI, on social media without written consent from the patient or his/her legal guardian.
- ❧ Understand that even if a patient posts every last detail about his or her health and treatments, no health care professional or staff should repost or retweet this information.
- ❧ Never comment on a patient's Facebook page about their health condition or treatment; that information goes to all the patient's friends!

# Non-Compliance



# Non-Compliance



Non-compliance is conduct that does not conform to the law, federal health care program requirements, or to an organization's ethical, business, and compliance policies.



# Investigating Non-Compliance



HNS will investigate all bona fide complaints of known or suspected violations by contracted health care professionals.



Contracted health care professionals must cooperate fully with any compliance investigation undertaken by HNS' Compliance department, any contracted health care plan, and/or governmental agency.

# Duty to Report Violations

## (FWA, HIPAA & Standards of Conduct)



You have a **duty to report** and immediately escalate any incidents of potential non-compliance or suspected fraud, waste and abuse.

Contracted health care professionals who fail to report suspected or known non-compliant conduct will be subject to HNS' Disciplinary Actions and Sanction Policies.

# How to Report Violations



Report known or suspected violations to HNS.

Via email: [HNSCompliance@healthnetworksolutions.net](mailto:HNSCompliance@healthnetworksolutions.net)

OR

Contact the HNS Compliance Officer  
at (877) 426-2411, ext. 130

# How to Report Violations



You may also report violations to one or more of the following appropriate federal and state authorities:

**US Office of Inspector General (OIG)**

(FWA violations)

Compliance Hotline: 1-800-447-8477  
Office of Inspector General

**Centers for Medicare and Medicaid (CMS)**

(FWA violations)

Compliance Hotline: 1-800-MEDICARE  
1-800-633-4227 or 1-877-486-2048

**Secretary, Department of Health and Human Services**

Office of Civil Rights (OCR)

(HIPAA violations)

<http://www.hhs.gov/ocr/privacy/hipaa/complaints>

# Confidentiality / No Retaliation



## ***Confidentiality of Identity of Reporting Individual***

When reporting suspected or known violations you may remain anonymous if you choose. Anyone reporting non-compliance is assured that such reports will be treated with appropriate confidentiality.

## **Whistle Blower Protection**

Federal and state laws contain **protections** for “whistleblowers” who alert the appropriate governmental authority of a violation of laws. Under these laws, any person with actual knowledge of an allegedly false claim, including employees, may, under certain conditions, notify the appropriate state or federal governmental authorities about potential violations, without fear of retaliation. Whistleblowers may also be entitled to relief, including employment reinstatement, back pay, and other compensation arising from retaliatory conduct against him or her.

# Correcting Non-Compliance



Correcting non-compliance helps to avoid the recurrence of the same non-compliant behavior/conduct, and promotes efficiency and effective internal controls.

# Penalties for Non-Compliance



HNS takes our compliance responsibilities seriously and failure to comply with HNS Compliance Policies and the policies of contracted health care plans will subject contracted health care professionals to disciplinary action by HNS, up to and including termination of their Practitioner's Participation Agreement.

Additionally, health care professionals who violate laws and regulations risk individual criminal prosecution and penalties, civil actions for damages and penalties, and exclusion from federal and private health care programs.

# Enforcement of Standards and Policies



By enforcing compliance to HNS' policies, HNS seeks to prevent accidental and intentional non-compliance with applicable laws, to detect such non-compliance if it occurs, to discipline those involved in non-compliant behavior, to remedy the effects of non-compliance, and to prevent repeat non-compliance.

If a material violation of applicable law, regulations, and/or compliance plan requirements occurs, HNS is committed to taking appropriate steps to correct the problem, including appropriate disciplinary actions.

HNS reserves the right to modify its sanction policies at any time and will provide timely notification to contracted health care professionals of any material changes.



# Application of Sanctions



The review of misconduct and the imposition of sanctions for contracted health care professionals shall be the responsibility of HNS' Compliance Officer and CEO.

Written notifications of sanctions/disciplinary actions will be communicated to the individual engaged in the misconduct and will include the misconduct, and as applicable, may include a summary of the results of the investigation.

# Disciplinary Action



If HNS concludes that an individual has violated laws, regulations, or HNS Policies, the individual will be subject to appropriate disciplinary action.

Disciplinary measures will be taken on a case-by-case basis. HNS reserves the right to apply sanctions at its discretion, based on the seriousness of the misconduct, but all disciplinary action will be applied on an equitable basis.

Enforcement and discipline may include discipline of individuals *who fail to report suspected or known non-compliant conduct* and/or who fail to fully cooperate with compliance investigations.

Any combination of the following sanctions may be applied for misconduct relating to non-compliance.

# Disciplinary Action



## Sanctions for Negligent Action - First or Second Offense

- ✧ Issuing verbal or written warning;
- ✧ Requiring additional compliance training or other educational requirements;
- ✧ Requiring the completion and submission of a corrective action plan (CAP);
- ✧ Temporarily suspending the health care professional's access to *HNSConnect* or his/her ability to submit claims to HNS via Office Ally;
- ✧ Auditing of patient health care and financial records; and/or
- ✧ Placing the health care professional on probationary status with HNS.

# Disciplinary Action



## Sanctions for Negligent Action - Third Offense

- ⌘ Requiring additional compliance training or other educational requirements;
- ⌘ Requiring the completion and submission of a corrective action plan (CAP);
- ⌘ Temporarily suspending the health care professional's access to *HNSConnect* or his/her ability to submit claims to HNS via Office Ally;
- ⌘ Auditing of patient health care and financial records;
- ⌘ Terminating the health care professional from the network; and/or
- ⌘ Reporting the misconduct to the appropriate federal and state authorities, including, but not limited to, state licensing boards and the National Practitioner's Data Bank (NPDB).

# Disciplinary Action



## Sanctions for Intentional Action - First Offense

- ❧ Requiring additional compliance training;
- ❧ Requiring the completion and submission of a corrective action plan (CAP);
- ❧ Temporarily suspending the health care professional's access to *HNSConnect* or his/her ability to submit claims to HNS via Office Ally;
- ❧ Auditing of patient health care and financial records;
- ❧ Placing the health care professional on probationary status with HNS;
- ❧ Terminating the health care professional from the network;
- ❧ Reporting the misconduct to the appropriate federal and state authorities, including but not limited to, state licensing boards and the National Practitioner's Data Bank (NPDB); and/or
- ❧ Prosecuting the individual.

# Disciplinary Action



## Sanctions for Intentional Action - Second Offense

- ❧ Terminating the health care professional from the network;
- ❧ Reporting the misconduct to the appropriate federal and state authorities, including but not limited to, state licensing boards and the National Practitioner's Data Bank (NPDB); and/or
- ❧ Prosecuting the individual.

# Questions about Non-Compliance



Despite best efforts by each of us to comply with applicable laws, inevitably there will be questions about the appropriateness of a behavior, action, or practice by ourselves, our employees, and/or our colleagues.

## **HNS is here to help!**

If you have questions regarding the information presented in this training module, or whether certain conduct should be reported, please contact the HNS Compliance Officer.

**[HNSCompliance@HealthNetworkSolutions.net](mailto:HNSCompliance@HealthNetworkSolutions.net)**

(877) 426-2411, ext. 130

# Summary



All of us must conduct business in accordance with the highest ethical standards and in accordance with federal and state laws and regulations that govern our industry.

Compliance training helps us meet this objective by increasing awareness of our legal environment and by helping us detect and prevent violations of laws applicable to our industry.

*Remember.*

**Prevent, Detect, Report, and Correct  
Non-Compliance!**



# Putting It All Together...



This concludes the portion of this training developed by HNS.

The following slides are from CMS' Compliance Training module and are required to be included in the HNS Compliance Training.





# Part 2: Medicare Parts C & D Compliance Training



*Developed by the  
Centers for Medicare  
& Medicaid Services*

# IMPORTANT NOTICE

This training module will assist Medicare Parts C and D plan Sponsors in satisfying the Compliance training requirements of the Compliance Program regulations at 42 C.F.R. §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi) and in Section 50.3 of the Compliance Program Guidelines found in Chapter 9 of the Medicare Prescription Drug Benefit Manual and Chapter 21 of the Medicare Managed Care Manual.

While Sponsors may choose to use this module to satisfy compliance training requirements, completion of this training in and of itself does not ensure that a Sponsor has an “effective Compliance Program.” Sponsors are responsible for ensuring the establishment and implementation of an effective Compliance Program in accordance with CMS regulations and program guidelines.

# Why Do *I* Need Training?

Compliance is EVERYONE'S responsibility!

As an individual who provides health or administrative services for Medicare enrollees, every action you take potentially affects Medicare enrollees, the Medicare program, or the Medicare trust fund.

# Training Objectives



To understand the organization's commitment to ethical business behavior



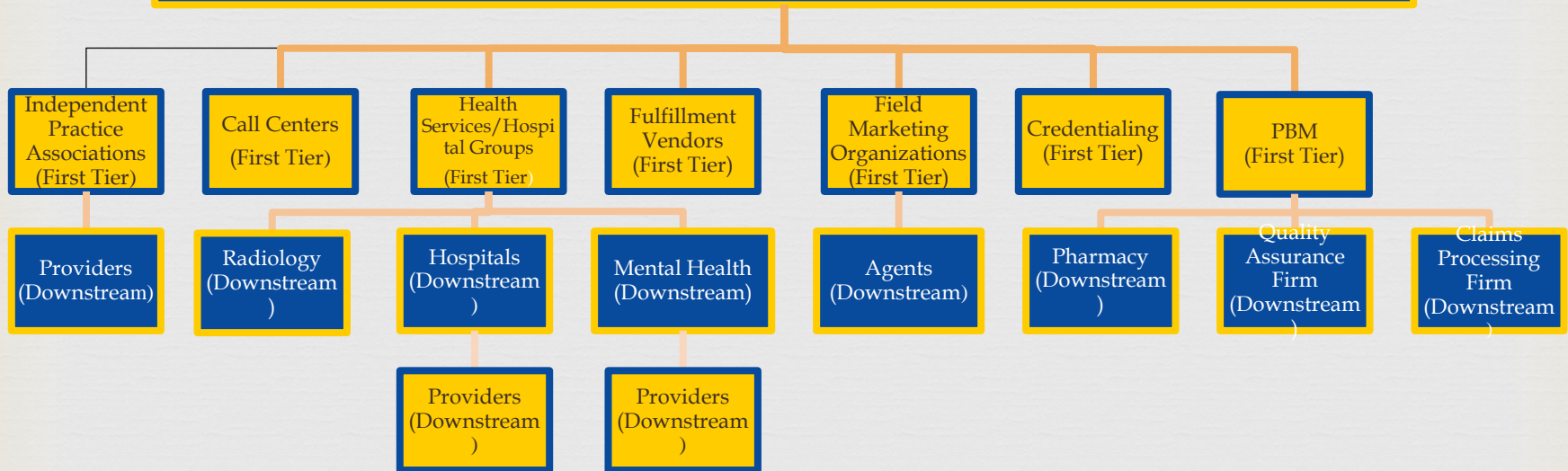
To understand how a compliance program operates



To gain awareness of how compliance violations should be reported

# Where Do I Fit in the Medicare Program?

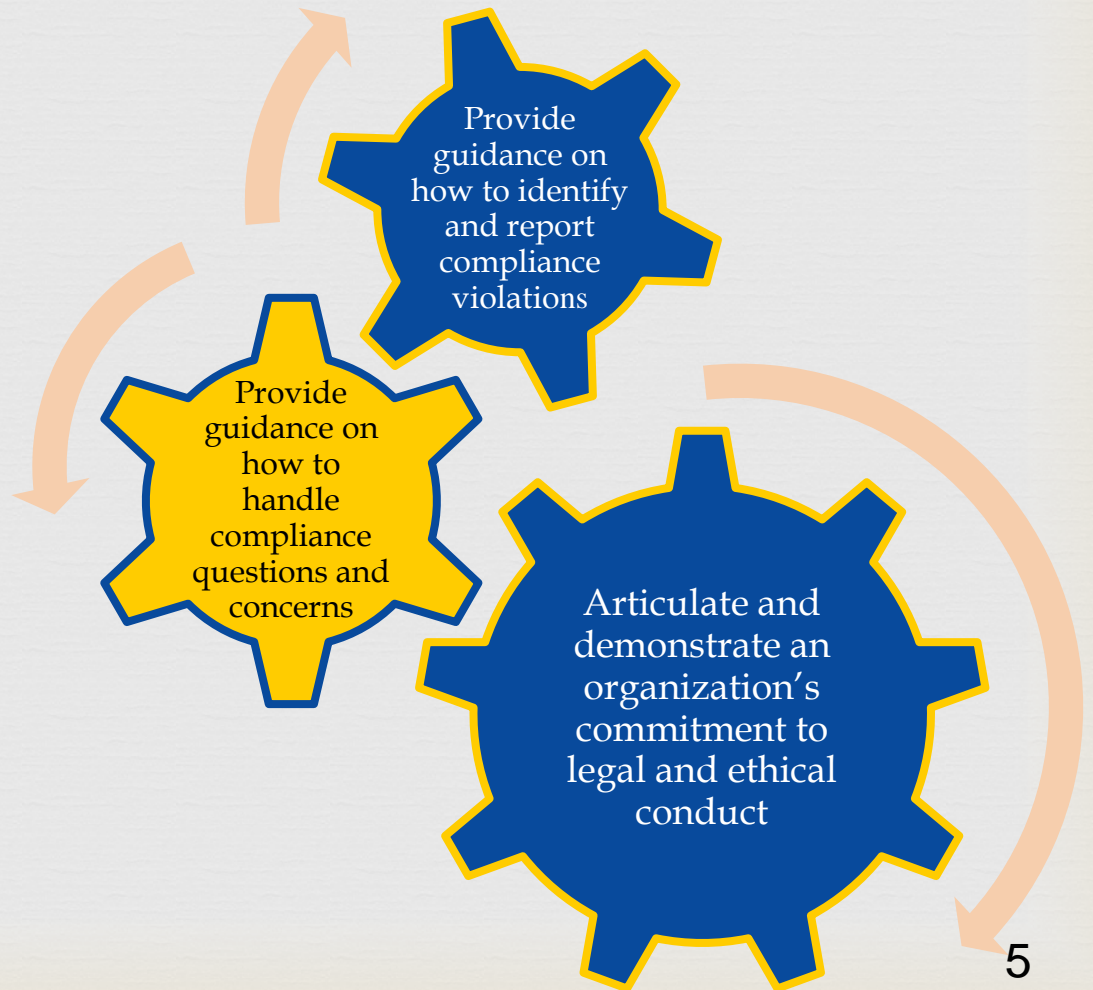
## Medicare Advantage Organization, Prescription Drug Plan, and Medicare Advantage-Prescription Drug Plan



# Background

☞ CMS requires Medicare Advantage, Medicare Advantage-Prescription Drug, and Prescription Drug Plan Sponsors (“Sponsors”) to implement an effective compliance program.

☞ An effective compliance program should:



# Compliance

A culture of compliance within an organization:

Prevents  
noncompliance

Detects  
noncompliance

Corrects  
noncompliance



# Compliance Program Requirements

At a minimum, a compliance program must include the 7 core requirements:

1. Written Policies, Procedures and Standards of Conduct;
2. Compliance Officer, Compliance Committee and High Level Oversight;
3. Effective Training and Education;
4. Effective Lines of Communication;
5. Well Publicized Disciplinary Standards;
6. Effective System for Routine Monitoring and Identification of Compliance Risks; and
7. Procedures and System for Prompt Response to Compliance Issues

42 C.F.R. §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi); Internet-Only Manual (“IOM”), Pub. 100-16, Medicare Managed Care Manual Chapter 21; IOM, Pub. 100-18, Medicare Prescription Drug Benefit Manual Chapter 9

# Compliance Training

- ✧ CMS expects that all Sponsors will apply their training requirements and “effective lines of communication” to the entities with which they partner.
- ✧ Having “effective lines of communication” means that employees of the organization and the partnering entities have several avenues through which to report compliance concerns.

# Ethics – Do the Right Thing!

Act Fairly and Honestly

Comply with the letter and spirit  
of the law

As a part of the Medicare program,  
it is important that you conduct  
yourself in an ethical and legal  
manner.

It's about doing the right thing!

Adhere to high ethical standards  
in all that you do

Report suspected violations

# How Do I Know What is Expected of Me?

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.

# How Do I Know What is Expected of Me (cont.)?

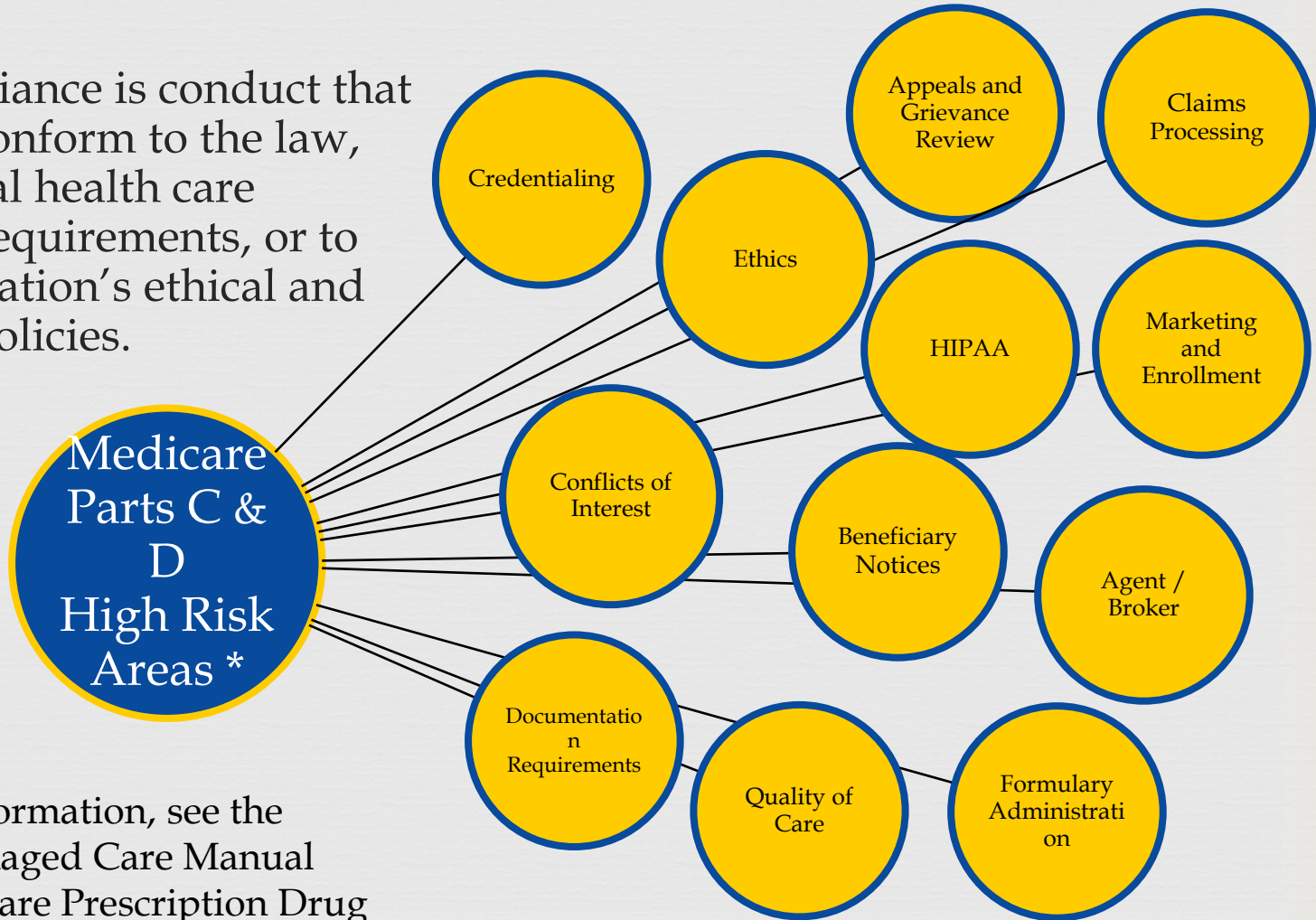
---

*Everyone* is required to report violations of Standards of Conduct and suspected noncompliance.

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

# What Is Noncompliance?

Noncompliance is conduct that does not conform to the law, and Federal health care program requirements, or to an organization's ethical and business policies.



\* For more information, see the Medicare Managed Care Manual and the Medicare Prescription Drug Benefit Manual on

<http://www.cms.gov>

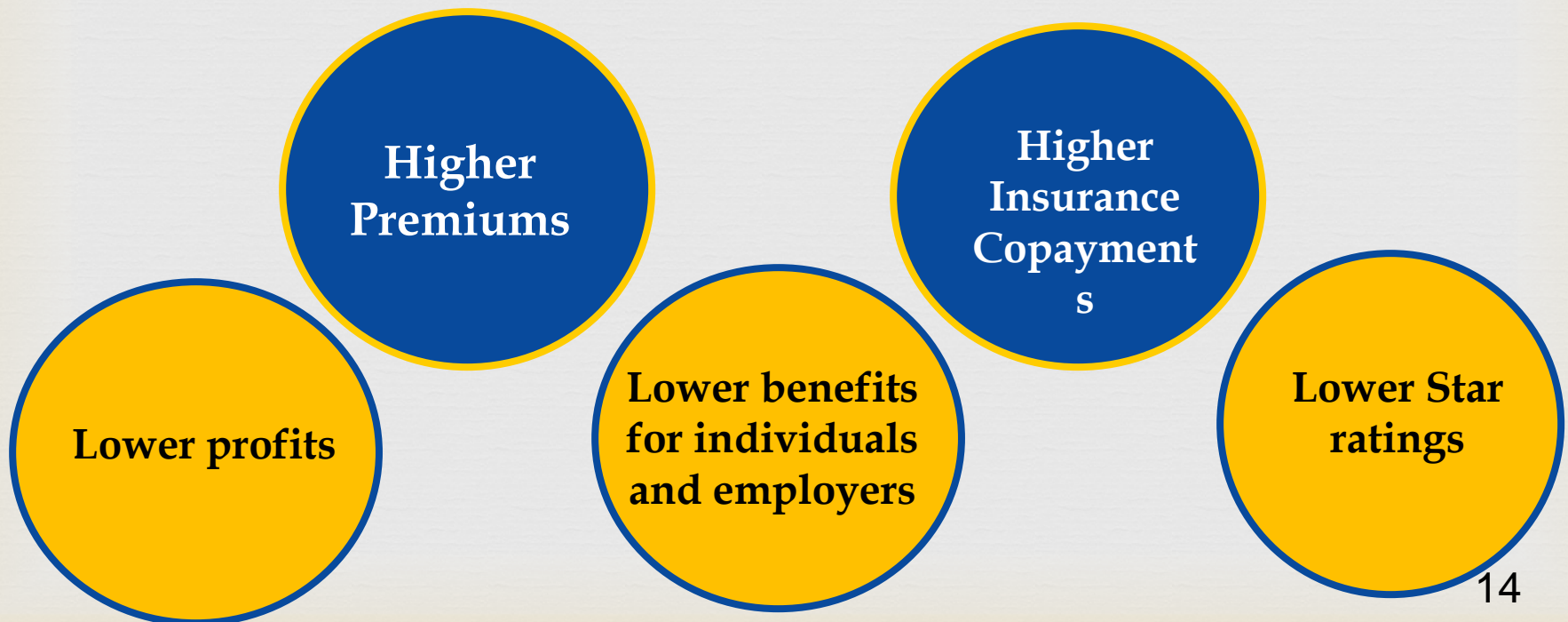
# Noncompliance Harms Enrollees



# Noncompliance Costs Money

Non Compliance affects EVERYBODY!

Without programs to prevent, detect, and correct noncompliance you risk:

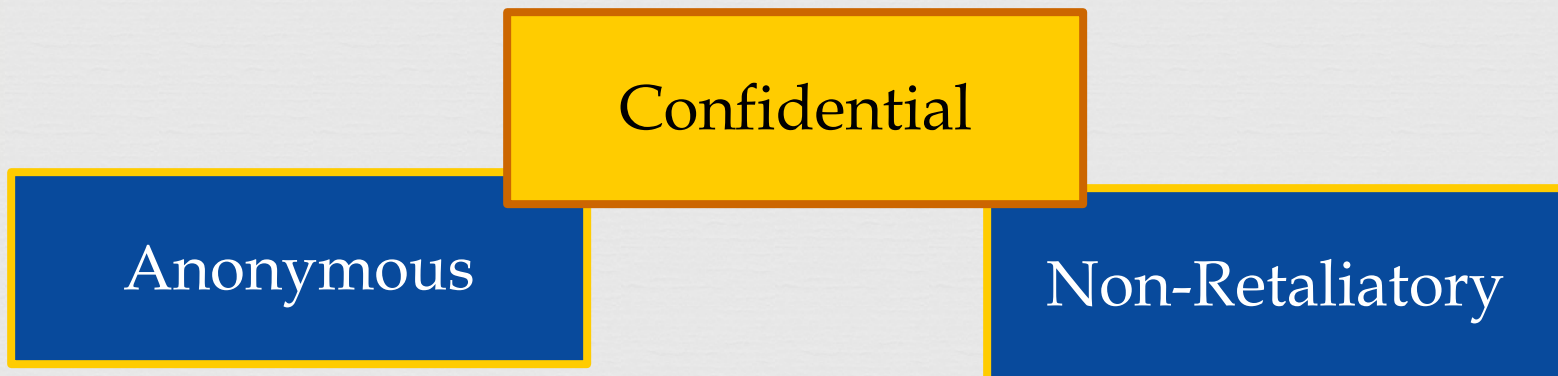




# I'm Afraid to Report Noncompliance

There can be NO retaliation against you for reporting suspected noncompliance in good faith.

Each Sponsor must offer reporting methods that are:



# How Can I Report Potential Noncompliance?

## **Employees of an MA, MA-PD, or PDP Sponsor**

- Call the Medicare Compliance Officer
- Make a report through the Website
- Call the Compliance Hotline

## **FDR Employees**

- Talk to a Manager or Supervisor
- Call Your Ethics/Compliance Help Line
- Report through the Sponsor

## **Beneficiaries**

- Call the Sponsor's compliance hotline
- Make a report through Sponsor's website
- Call 1-800-Medicare

# What Happens Next?

After noncompliance has been detected...

It must be investigated *immediately*...

And then *promptly* correct any noncompliance

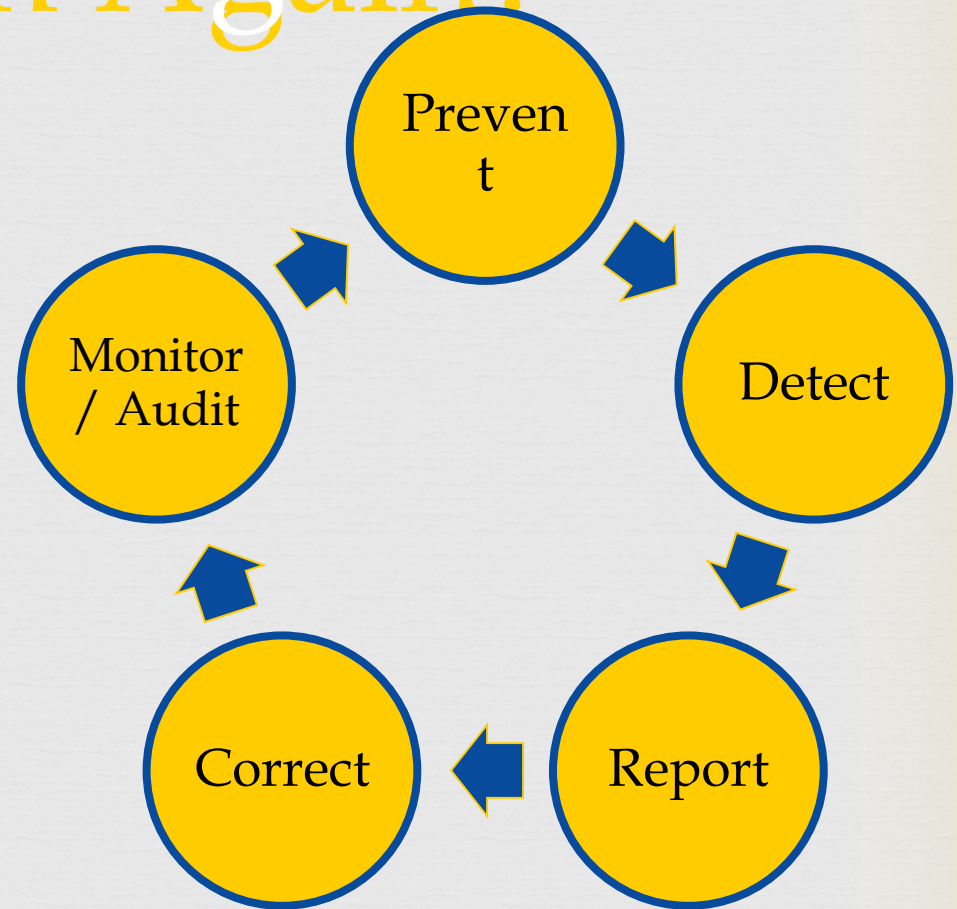
## Correcting Noncompliance

- ☞ Avoids the recurrence of the same noncompliance
- ☞ Promotes efficiency and effective internal controls
- ☞ Protects enrollees
  - Ensures ongoing compliance with CMS requirements

# How Do I Know the Noncompliance Won't

## Happen Again?

- Once noncompliance is detected and corrected, an ongoing evaluation process is critical to ensure the noncompliance does not recur.
- Monitoring activities are regular reviews which confirm ongoing compliance and ensure that corrective actions are undertaken and effective.
- Auditing is a formal review of compliance with a particular set of standards (e.g., policies and procedures, laws and regulations) used as base measures



# Know the Consequences of Noncompliance

Your organization is required to have disciplinary standards in place for non-compliant behavior. Those who engage in non-compliant behavior may be subject to any of the following:



# Compliance is EVERYONE'S Responsibility!!

## PREVENT

- Operate within your organization's ethical expectations to PREVENT noncompliance!

## DETECT & REPORT

- If you DETECT potential noncompliance, REPORT it!

## CORRECT

- CORRECT noncompliance to protect beneficiaries and to save money!

# Scenario 1

---

You have discovered an unattended email address or fax machine in your office which receives beneficiary appeals requests. You suspect that no one is processing the appeals. What should you do?

# Scenario 1

- A) Contact Law Enforcement
- B) Nothing
- C) Contact your Compliance Department
- D) Wait to confirm someone is processing the appeals before taking further action
- E) Contact your supervisor



# Scenario 1

**The correct answer is: C – Contact your Compliance Department.**

Suspected or actual noncompliance should be reported immediately upon discovery. It is best to report anything that is suspected rather than wait and let the situation play out.

Your Sponsor's compliance department will have properly trained individuals who can investigate the situation and then, as needed, take steps to correct the situation according to the Sponsor's Standards of Conduct and Policies and Procedures.

# Scenario 2

A sales agent, employed by the Sponsor's first-tier or downstream entity, has submitted an application for processing and has requested two things:

- i) the enrollment date be back-dated by one month
- ii) all monthly premiums for the beneficiary be waived

What should you do?

# Scenario 2

- A) Refuse to change the date or waive the premiums, but decide not to mention the request to a supervisor or the compliance department
- B) Make the requested changes because the sales agent is responsible for determining the beneficiary's start date and monthly premiums
- C) Tell the sales agent you will take care of it, but then process the application properly (without the requested revisions). You will not file a report because you don't want the sales agent to retaliate against you
- D) Process the application properly (without the requested revisions). Inform your supervisor and the compliance officer about the sales agent's request.
- E) Contact law enforcement and CMS to report the sales agent's behavior.

# Scenario 2

**The correct answer is: D - Process the application properly (without the requested revisions). Inform your supervisor and the compliance officer about the sales agent's request.**

The enrollment application should be processed in compliance with CMS regulations and guidance. If you are unclear about the appropriate procedure, then you can ask your supervisor or the compliance department for additional, job-specific training.

Your supervisor and the compliance department should be made aware of the sales agent's request so that proper retraining and any necessary disciplinary action can be taken to ensure that this behavior does not continue. *No one*, including the sales agent, your supervisor, or the Compliance Department, can retaliate against you for a report of noncompliance made in good faith.

# Scenario 3

You work for an MA-PD Sponsor. Last month, while reviewing a monthly report from CMS, you identified multiple enrollees for which the Sponsor is being paid, who are not enrolled in the plan.

You spoke to your supervisor, Tom, who said not to worry about it. This month, you have identified the same enrollees on the report again.

What do you do?

# Scenario 3

- A) Decide not to worry about it as your supervisor, Tom, had instructed. You notified him last month and now it's his responsibility.
- B) Although you have seen notices about the Sponsor's non-retaliation policy, you are still nervous about reporting. To be safe, you submit a report through your Compliance Department's anonymous tip line so that you cannot be identified.
- C) Wait until next month to see if the same enrollees are on the report again, figuring it may take a few months for CMS to reconcile its records. If they are, then you will say something to Tom again.
- D) Contact law enforcement and CMS to report the discrepancy.
- E) Ask Tom about the discrepancies again.

# Scenario 3

**The correct answer is: B - Although you have seen notices about the Sponsor's non-retaliation policy, you are still nervous about reporting. To be safe, you submit a report through your Compliance Department's anonymous tip line so that you cannot be identified.**

There can be no retaliation for reports of noncompliance made in good faith. To help promote reporting, Sponsors should have easy-to-use, confidential reporting mechanisms available to its employees 24 hours a day, 7 days a week.

It is best to report any suspected noncompliance to the Compliance Department promptly to ensure that the Sponsor remains in compliance with CMS requirements. Do the right thing! Compliance is everyone's responsibility.

# What Governs Compliance?

- **Social Security Act:**
  - Title 18
- **Code of Federal Regulations\*:**
  - 42 CFR Parts 422 (Part C) and 423 (Part D)
- **CMS Guidance:**
  - Manuals
  - HPMS Memos
- **CMS Contracts:**
  - Private entities apply and contracts are renewed/non-renewed each year
- **Other Sources:**
  - OIG/DOJ (fraud, waste and abuse (FWA))
  - HHS (HIPAA privacy)
- **State Laws:**
  - Licensure
  - Financial Solvency
  - Sales Agents

\* 42 C.F.R. §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)



# Additional Resources

- ☞ For more information on laws governing the Medicare program and Medicare noncompliance, or for additional healthcare compliance resources please see:
- Title XVIII of the Social Security Act
  - Medicare Regulations governing Parts C and D (42 C.F.R. §§ 422 and 423)
  - Civil False Claims Act (31 U.S.C. §§ 3729-3733)
  - Criminal False Claims Statute (18 U.S.C. §§ 287,1001)
  - Anti-Kickback Statute (42 U.S.C. § 1320a-7b(b))
  - Stark Statute (Physician Self-Referral Law) (42 U.S.C. § 1395nn)
  - Exclusion entities instruction (42 U.S.C. § 1395w-27(g)(1)(G))
  - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191) (45 CFR Part 160 and Part 164, Subparts A and E)
  - OIG Compliance Program Guidance for the Healthcare Industry:  
<http://oig.hhs.gov/compliance/compliance-guidance/index.asp>

Congratulations!  
You have successfully completed HNS' and CMS (Part C & D)  
FWA/Compliance Training.

**Please sign, date the Compliance Training Certificate  
(the next slide) and fax or email the certificate to HNS.**



As a final reminder, be sure to **save a copy of this training module and your signed certificate**, as you are required to produce these if requested by HNS, CMS or other regulatory bodies.

# HNS Compliance Training Certification



I hereby certify that I have completed the HNS and CMS (Part C & D) Compliance Training Module. I understand my responsibility to comply with the requirements addressed in this training module.

Further, I understand my responsibility to save this certificate, as well as a copy of this training module, for a period of no less than **10 years** from the date shown below.

\_\_\_\_\_  
Name (please print)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date of Training

**You must sign, date and fax or email this to HNS.  
You must also retain this form AND a copy of this training module  
for 10 years.**