# Program Integrity

## FWA, Compliance and HIPAA Training
## Providers

Prevent, Detect and Report


ia health link | AmeriHealth Caritas Iowa

Presented by: Program Integrity, Compliance Department

# Agenda

- Fraud, waste and abuse defined.
- Overview of Iowa and federal laws used to fight fraud and abuse.
- Your role.
- Examples of Medicaid fraud and abuse.
- Special Investigations Unit process overview.
- Prevent, detect and report.
- Compliance Program overview.
- Privacy and Health Insurance Portability and Accountability Act and overview.

# What are fraud, waste and abuse (FWA)?

- **Fraud** is an intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to him or herself or some other person. It includes any act that constitutes fraud under applicable federal or state law.
- **Waste** includes incurring unnecessary costs as a result of deficient management, practices or controls.
- **Abuse** means provider practices that are inconsistent with sound fiscal, business or medical practices that result in an unnecessary cost to the Medicaid program or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. It also includes beneficiary practices that result in unnecessary cost to the Medicaid program.

# Federal and Iowa rules

- The Federal False Claims Act (FCA) and Iowa False Claims Act.
- The Fraud Enforcement and Recovery Act (FERA) and Deficit Reduction Act (DRA).
- The Anti-Kickback Statute.
- The Physician Self-Referral Law (Stark Law).
- The Health Insurance Portability and Accountability Act (HIPAA).

# I am a long-term supports and services (LTSS) provider — what is my role?

**As an LTSS provider, you can prevent, detect and report in the following ways:**

- If you suspect or detect fraud, report it immediately.
- Ensure you are billing only for the services you provide.
- Understand roles and responsibilities as a participating provider.
- Know licensure responsibilities and restrictions.
- Monitor medical records to ensure documentation supports the services rendered.
- Take swift action if you identify an internal problem.
- Establish effective lines of communication.
- Practice self-disclosure.
- Stay educated on fraud, waste and abuse.

# Examples of fraud and abuse

- Billing for services not provided.
- Misrepresenting dates.
- Taking kickbacks for patient referrals.
- Billing for unnecessary or unreasonable services.
- Coding a service at a higher level than what was rendered (i.e., upcoding).
- Writing false prescriptions for durable medical equipment.
- Not providing the level of supervision included in the service plan.
- Being on the lookout for changing start and end times of services to be able to bill more units, or, for CDAC providers, billing the same number of units every month regardless of how many days in the month or if the member was away on vacation.
- One person billing supported community living for two or more members simultaneously.
- Pre-signing time sheets.

# Examples of fraud and abuse

**In the news:**

- Medicaid fraud probe targets DeWitt care center where the Iowa Department of Human Services found a credible allegation of fraud. The center terminated services of the chief executive officer, chief operating officer and chief financial officer, as well as two others in management.
    - http://qctimes.com/news/local/medicaid-fraud-probe-targets-dewitt-care-center/article_e64a3f74-7148-5316-830e-191a24883e5f.html
- Iowa home health provider to pay $5.6 million to settle false claims allegations for billing Medicare and Medicaid.
    - http://www.thegazette.com/subject/news/iowa-home-health-provider-to-pay-56-million-to-settle-false-claims-allegations-xa0xa0-20150211

# Role of the Special Investigations Unit (SIU)

## Our process

| Intake | Investigation | Referrals |
|---|---|---|
| • Compliance Hotline.<br>• SIU Fraud Tip Email.<br>• Member service verification letters.<br>• External Referrals. | • Preliminary screening.<br>• Data collection.<br>• Data analysis.<br>• Clinical Review.<br>  – Post-Pay Review.<br>  – Pre-Pay Review.<br>• Findings.<br>• Overpayments.<br>• Provider education. | • State.<br>  – Medicaid Fraud Control Unit.<br>  – Office of Inspector General.<br>• Law Enforcement. |

# Role of the Special Investigations Unit (SIU)

## Document's you may see from the SIU:

**Initial Request Notification Letter (30 Days)**

- List of members' records requested
- Date records are due
- Investigator's name and address for mailing

**2nd Request Letter for Records (If Necessary, 15 Days)**

- 1st request letter included
- Date extension for record receipt
- Consequences for non-compliance

**Findings Letter**

- Date for receipt of overpayment payment
- Detailed spreadsheet with overpayment issues outlined
- Corrective Action Plan and due date
- Provider Education to be done by Provider Relations

**If Applicable - Payment Arrangement Letter**

- Arrangements for provider payment
- Signature required

**If Applicable - Prepayment Notification Letter**

- Pending of claims for record review prior to payment

# Prevent and detect

1. Monitor your claims for accuracy and ensure coding reflects the services you provided.
2. Monitor medical records to ensure documentation supports the services rendered.
3. Perform regular internal audits.
4. Establish effective lines of communication.
5. Take action if you identify a problem.

# Report fraud, waste and abuse

**Program Integrity:**

- **Contact:** Jane Shulman Brown, Program Integrity Manager, or Stephanie Jones, Investigator.
- **Email:** FraudTip@amerihealthcaritas.com.
- **iNSIGHT Online:** Report Fraud box (red button).
- **Fraud Tip hotline: 1-866-833-9718.**
- **Mail:**
  - Special Investigations Unit
    200 Stevens Drive
    Mail Stop 13A
    Philadelphia, PA 19113
- **Iowa Medicaid Fraud: 1-515-281-5717 (DIA).**

# The Seven Elements of an Effective Compliance Program

# What is compliance?

Act fairly and honestly.

Comply with the letter and spirit of the law.

As a part of the community that serves Medicare beneficiaries and Medicaid enrollees, it is important that you conduct yourself in an ethical and legal manner.

It's about doing the right thing in the right way!

Adhere to high ethical standards in all that you do.

Report suspected violations.

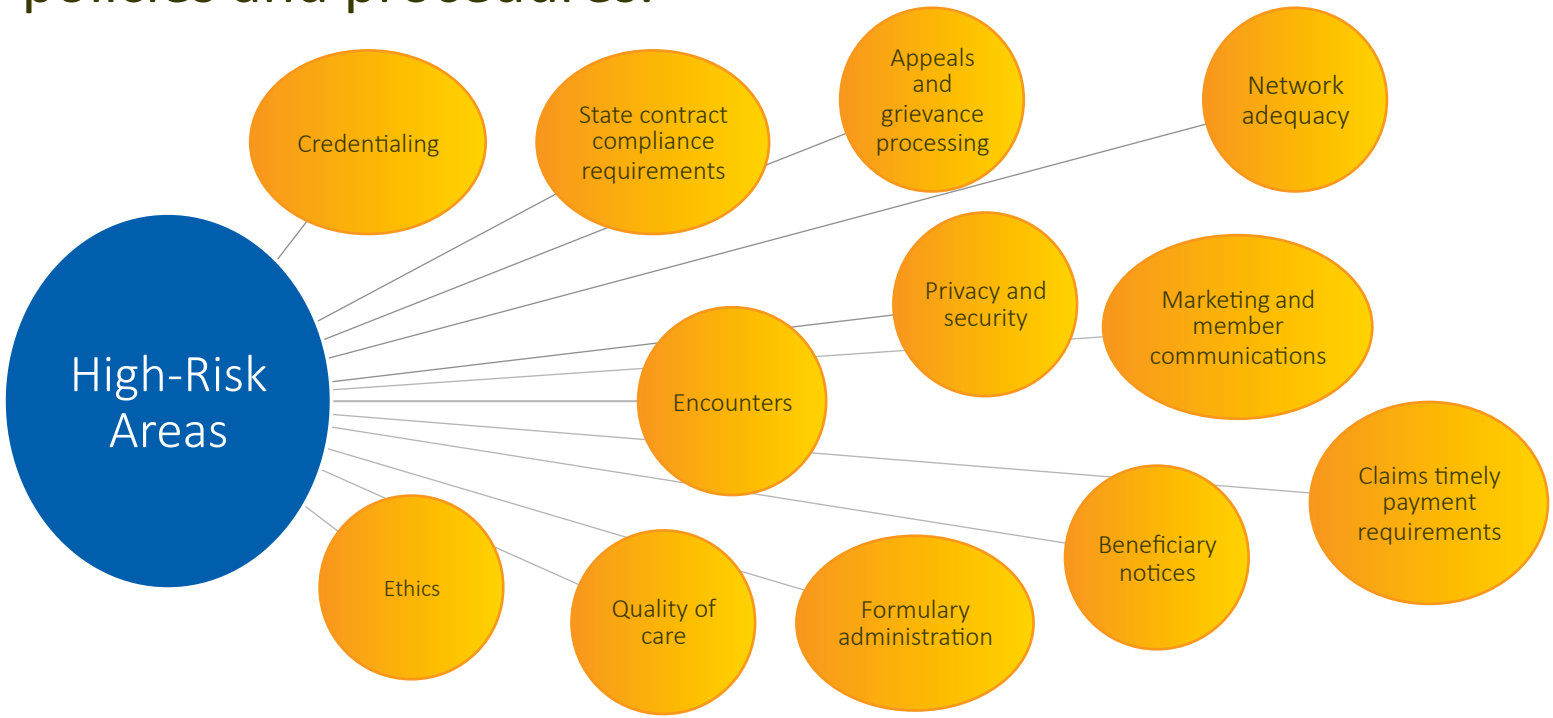
# Compliance program requirements

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

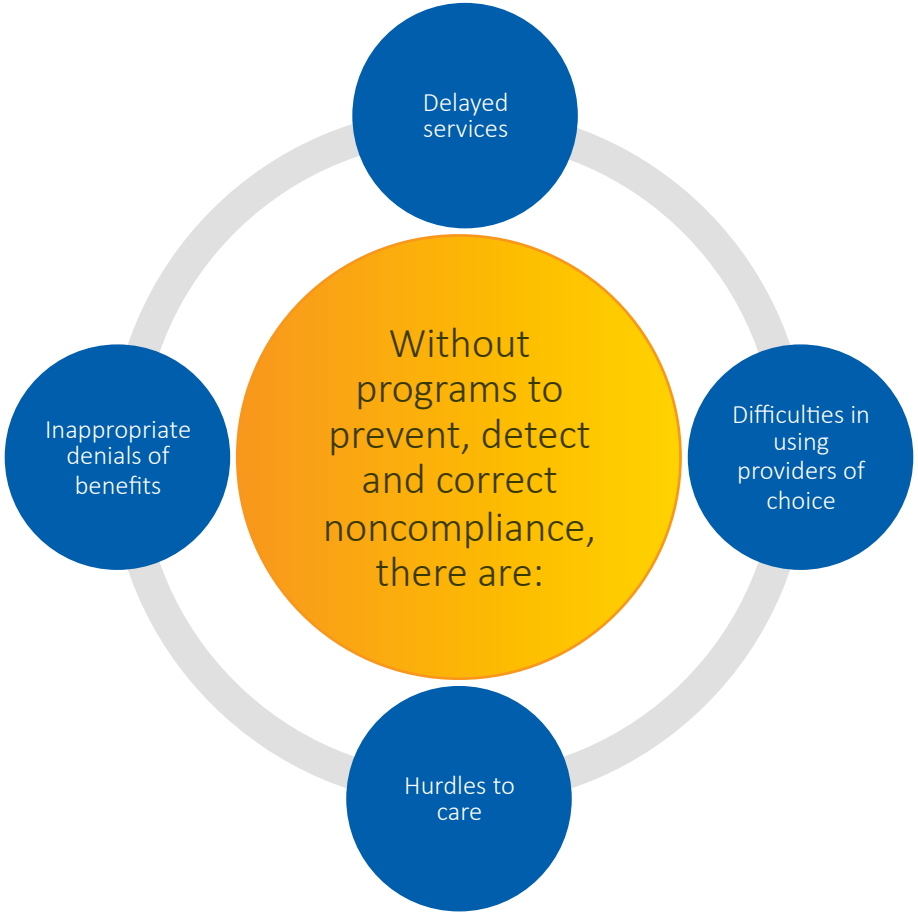
1. Written policies, procedures and standards of conduct.
2. Compliance officer, compliance committee and high-level oversight.
3. Effective training and education.
4. Effective lines of communication.
5. Well-publicized disciplinary standards.
6. Effective system for routine monitoring and identification of compliance risks.
7. Procedures and system for prompt response to compliance issues.

# What is noncompliance?

Noncompliance is conduct that does not conform to the rules and regulations applicable to state and federal health care program requirements, or to the organization's standards of conduct or policies and procedures.



# Noncompliance harms enrollees



# Reporting issues of noncompliance

**Effective lines of communication**

Any provider may bring his or her concerns directly to the Corporate Compliance Officer or the respective plan or line-of-business Compliance Officer in the following ways:

**Corporate Compliance**
**In person or in writing to:**

**Corporate Compliance**
200 Stevens Drive, Bldg. 100, Third Floor, Philadelphia, PA 19113

**Toll-free anonymous hotline:** 1-800-575-0417

**Email: CorpCompliance@amerihealthcaritas.com**

**Additional questions can be directed to:**

- **Lauren Hansen, Director, Compliance/Regulatory Affairs, Iowa Implementation**
  - **1-515-330-3795 or lhansen@amerihealthcaritas.com**

Please remember all reporting will remain confidential. Reporting by use of the toll-free hotline will allow the individual to remain anonymous. However, there may be instances that require further involvement or information from the reporting individual during the investigation.

# HIPAA and Privacy


# HIPAA and HITECH background information

- 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.
- The Health Information Technology for Economic and Clinical Health Act, commonly referred to as the HITECH Act, was enacted as part of the American Recovery and Reinvestment Act of 2009 to encourage the adoption and "meaningful use" of electronic health records.
- The HIPAA Omnibus Rule, enacted in 2013, is a set of regulations that modified HIPAA's Privacy, Security, and Enforcement Rules to implement various provisions of the HITECH Act.

# The Privacy Rule

- The Privacy Rule is a set of national standards for the protection of certain health information.
- The HIPAA Privacy Rules apply to all covered entities and their business associates.
  - **Covered entity** — A health care provider, health plan or health care clearinghouse that electronically transmits and receives protected health information (PHI).
  - **Business associate** — An entity or person who performs services or functions for a covered entity. The Privacy Rule allows a covered entity to share PHI with its business associates. However, a covered entity must have a contract that prohibits these business associates from using or disclosing PHI in any way that would violate the Privacy Rule.

# PHI

- The HIPAA Privacy Rule protects the privacy and confidentiality of information known as protected health information, commonly referred to as PHI.
- PHI is individually identifiable health information that is:
  - Transmitted by electronic media.
  - Maintained in electronic media.
  - Transmitted or maintained in any other form or medium.
- To be considered PHI, the information must have two components:
  - **Medical information** — Information about an individual's past, present or future physical or mental health care received, or health care payment information.
  - **Personally identifiable information (PII)** — Data elements that can identify or can reasonably lead to the identification of an individual.

# Breach notification rule

- A breach is an unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA.
- The Breach Notification Rule requires covered entities to notify affected individuals, the U.S. Department of Health and Human Services and, in some cases, the media, of a breach of unsecured PHI.
  - The U.S. Department of Health and Human Services requires health care companies to submit a log of all breaches involving fewer than 500 individuals once a year, no later than 60 days after the end of the calendar year.
  - For a breach that involves 500 or more individuals, health care companies must notify the U.S. Department of Health and Human Services no later than 60 days from the time of discovery.

# Member PHI use and disclosure

- The Privacy Rule defines and limits the circumstances in which an individual's PHI may be used and disclosed.
- In order for covered entities to perform their functions, the HIPAA Privacy regulations allow covered entities to use or disclose PHI without a member's permission in the following situations (TPO):
    - For treatment of members.
    - For payment of a provider.
    - For health care operations.
- Besides TPO, there are very specific occasions 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 purposes.
    - To report abuse.
    - To avert a serious threat.
- **Minimum necessary rule** — Restricts the use and disclosure of PHI to only the amount necessary to perform a specific task.

# HIPAA civil and criminal fines and penalties

- HIPAA violations can be severe!
- Civil penalties:
  - Range from $100 to $50,000 per violation, with a maximum penalty of $1.5 million per year for violations of an identical provision.
- Criminal penalties:
  - Covered entities and specified individuals who knowingly obtain or disclose PHI in violation of HIPAA may be fined up to $50,000 and one year of imprisonment.
  - Offenses committed under false pretenses may be fined up to $100,000 and up to five years of imprisonment.
  - Offenses committed with the intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm may be fined up to $250,000 and up to 10 years of imprisonment.

# Questions?


More than

# 30 YEARS

of making

**care** the **heart**

of our **work.**