



# Building a Successful Compliance Program for Health Plans

HCCA's Managed Care  
Compliance Conference  
February 21, 2010



## Objectives

- Gateway Background
- Ethical Principles
- ***Compliance Program Components***
- Compliance Considerations
- Monitoring and Auditing Activities
- Education and Training
- Comprehensive Compliance Plan





## Gateway Background



## Background

- Gateway Health Plan<sup>®</sup> offers two products in Pennsylvania:
  - Medicaid HMO Plan
  - *Medicare Assured<sup>®</sup> HMO*
- Unlike many health insurance companies, Gateway Health Plan<sup>®</sup> focuses entirely on serving the needs of the most vulnerable citizens - the poor, elderly and disabled





## Gateway's History

- Gateway was established In 1992 as an alternative to Pennsylvania's Department of Public Welfare's Medical Assistance Program.
- For more than 15 years, members have benefited from services such as disease management, health and wellness programs and preventive care.
- Today, Gateway Health Plan® is a top-ranked managed care organization that provides service to more than 260,000 members eligible for medical assistance.
- Gateway Health Plan *Medicare Assured*® HMO, a Special Needs Plan for more than 24,000 members, who are eligible for both Medicare and Medicaid, is one of the nation's largest Medicare programs for the dual-eligible population.



## Background

- Gateway's goal is to help improve the health and well-being of its members.
- Gateway developed Prospective Care Management (PCM®), a proactive holistic approach to healthcare.
  - By identifying the Behavioral, Environmental, Economic, Medical, Social, and Spiritual (BEEMSS<sup>SM</sup>) issues a member faces, Gateway can design a plan to ensure that the member receives the care he or she needs.





## Ethical Principles



## Managed Care Organization (MCO) Goals

- Prevent disease
- Promote health
- Provide equitable access
- Provide affordable access
  
- **REDUCE COSTS....while providing access, quality, care, and service.**





## MCO Goals

- Three players in achieving MCO goals
  - **Member**
  - Plan
  - Provider



## Underlying Ethical Principles

- Autonomy
- Non-maleficence
- Beneficence
- Justice





## Autonomy

- MCOs and their participating providers have a duty to respect the right of **members** to **make decisions** about the course of their lives



## Non-maleficence

- MCOs and their participating providers are obligated **not to harm** their members





## Beneficence

- Each member should be treated in a manner that ***respects her/his own goals and values***; plans must also promote the good of the members as a group.



## Justice

- MCOs and their providers should allocate resources in a way that ***fairly distributes*** benefits and burdens among members





## Basic Ethical Guidelines for Allocation

- Guidelines
  1. Group needs balanced with individual needs
  2. Appropriate limitation on resources
  3. Equitable access
  4. Non-discrimination



## Guideline #1

- The basic ethical criterion for the planned allocation of resources in a MCO setting at the policy level is:
  - *The well-being of the **entire group** for whom the decisions are being made*
  - ***Balanced** by the requirement to respect **individual** healthcare need*





## Guideline #2

- The MCO is ***not obligated*** to provide unlimited resources to any individual member except for medically necessary treatment covered by the plan



## Guideline #3

- Each member covered by the same contract should have ***equal access*** to the same benefits.





## Guideline #4

- ***No member should be denied*** medically appropriate healthcare because of race, color, religion, sex, age, national origin, ethnicity, sexual preference, lifestyle choices, disability or geographic location



## Ethical MCO Composition

- ***Respects*** and honors member ***rights***
- ***Assesses*** healthcare ***needs*** of membership and provides care to meet needs
- Provides ***accurate information*** to members, providers about benefits and outcome data
- Takes ***corrective action*** if inappropriate treatment is discovered
- Provides ***adequate resources***, such as information and professional development for providers
- ***Includes providers*** in development of clinical guidelines and standards of care





## ***Compliance Program Components***



## **Compliance Program Components**

1. Security and Privacy
2. Documentation
3. Fraud, Waste, and Abuse
4. Employee Conduct
5. Financial Statements
6. Federal and State Oversight





# Compliance Program Components

## 1. Security and Privacy



# Security and Privacy

- HIPAA
- ARRA





## HIPAA

- The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to:
  - Establish national standards for electronic health care transactions
  - Establish national identifiers for providers, health plans, and employers.
  - **Security and privacy of health data.**



## HIPAA

- The **Security Rule** sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information.
- The **Privacy Rule** sets national standards for the protection of individually identifiable health information by three types of covered entities:
  - Health plans
  - Health care clearinghouses
  - Health care providers





## Security Program

- Risk and threat assessment
  - HIPAA Security Assessment
- Business continuation
  - Corporate Plan
  - Testing
  - Updates
  - Vendor Review
- Incident response
  - Internal
  - Business Associate Agreements
- Security compliance and auditing
- Security awareness and training
- Information risk management



## HIPAA Security Assessment

- CMS noted the following common deficiencies:
  - Completing HIPAA security risk assessments
  - Ensuring current policies and procedures
  - Training employees on security compliance
  - Conducting clearance checks on employees
  - Ensuring adequate workstation security
  - Ensuring encryption is properly employed
- National Institute of Standards and Technology (NIST) Special Publication 800-66

*CMS HIPAA Compliance Review Analysis and Summary of Results 2008 HIPAA Compliance Reviews*





## Business Continuation

- **Corporate plan**
  - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
  - Train those with defined plan responsibility
- **Testing**
  - Test the contingency plan on a predefined cycle (stated in the policy developed under Key Activity), if reasonable and appropriate.
- **Updates**
  - Implement procedures for periodic testing and revision of contingency plans
- **Vendor review**
  - If possible, involve external entities (vendors, alternative site/service providers) in testing exercises.

*National Institute of Standards and Technology (NIST) Special Publication 800-66 –  
Administrative Safeguards - 4.7. Contingency Plan (§164.308(a)(7))*



## Incident Response

- **Internal**
  - System monitoring and tracking
  - Response and documentation
  - Remediation efforts
- **Business Associate Agreements**
  - Notification timeframes
  - Penalties
  - Reimbursement of notification fees





## Privacy Program

- Uses and disclosures
- Minimum necessary
- Recipient access



## Uses and Disclosures

- Plan operations
- Required by law
- Judicial or administrative proceedings
- Law enforcement purposes
- Victims of abuse, neglect or domestic violence
- Business associates
- Person involved in member care and notification
- Other types of requestors





## Minimum Necessary

- "**Minimum Necessary**" means using the least amount of information necessary to accomplish a task. This includes use of the following:
  - Medical and billing records
  - Enrollment, payment, claims adjudication
  - Case and medical management records
  - Any database that contains PHI



## Recipient Access

- Telephonic request
- Written request





## ARRA

- American Recovery and Reinvestment Act of 2009
  - Regulations requiring health care providers, health plans and other entities covered under HIPAA to notify individuals when their health information is breached.
    - More than 500 individuals
    - Less than 500 individuals



## More than 500 Individuals

- Regulations require HIPAA covered entities to ***promptly notify*** the following:
  - Affected individuals of a breach
  - HHS Secretary
  - Media
- Tracking and notification
  - Breach classification form
  - General breach notification letter must be sent to each impacted person as timely as possible, but no later than 60 days of identification of the breach.
  - Tracking form for high volume breach cases





## Less than 500 Individuals

- Breaches affecting less than 500 individuals will be reported to the HHS secretary on an **annual basis**.
- Tracking and notification
  - Breach classification form
  - General breach notification letter must be sent to each impacted person as timely as possible, but no later than 60 days of identification of the breach.
  - Tracking form for low volume breach cases



<u>Conditions of HIPAA Violation</u>	<u>Minimum Civil Penalty</u>	<u>Maximum Civil Penalty</u>
• Individual did not know that he/she violated HIPAA and would not have known by exercising reasonable diligence	• \$100 per violation, with an annual maximum of \$25,000 for repeat violations	• \$50,000 per violation, \$1.5 million annual maximum Note: Maximum that can be imposed can be set by State Attorneys General regardless of type of violation
• Violation is due to reasonable cause and not due to willful neglect on the part of the individual, CE or BA	• \$1,000 per violation, with an annual maximum of \$100,000 for repeat violations	• \$50,000 per violation, \$1.5 million annual maximum
• Violation due to willful neglect but is corrected within a prescribed required time period	• \$10,000 per violation, with an annual maximum of \$250,000 for repeat violations	• \$50,000 per violation, \$1.5 million annual maximum
• The violation is due to willful neglect and is not corrected within the timeframe mandated by authorities	• \$50,000 per violation, with an annual maximum of \$1.5 million	• \$50,000 per violation, \$1.5 million annual maximum

# Compliance Program Components

## 2. Documentation



# CMS Guidance

- CMS asserted that having written standards with a strong commitment by Management can ***mitigate risks***.
- CMS advised ***policies should be reviewed and revised periodically*** (annually) to evolve according to the following:
  - Risks
  - Applicable laws, regulation, and other requirements





## Documentation

- **Evidence** that processes are completed:
  - Effectively
  - Accurately
  - Timely



## Policy for the Policies

1. **Developing a new policy**
  - Statement of format
  - Naming convention
2. **Completion**
  - Statement of required information
  - Management signature
3. **Review and Comment Period**
  - Related departments
  - Revisions
4. **Signature**
  - Director / Manager – all standards have been achieved
  - Vice President – review and signature



*Continued on next slide*



## Policy for the Policies

### 5. Maintenance

- Table of Contents
- Current / inactive
- Storage / location

### 6. Revision Schedule

- Annual review
- Changes during the year (government, regulatory, or accreditation standards)

### 7. Changing responsible departments

- New department's Vice President approval
- Update Table of Contents

*Continued on next slide*



## Policy for the Policies

### 8. Template for policy format

- Identification and ownership
- Statement
- Definitions
- Attachments
- Procedures





# Compliance Program Components

## 3. Fraud, Waste, and Abuse



# Fraud, Waste, and Abuse

- Definitions
- Fraud and abuse laws
- Types of investigations
- Law enforcement





## Definitions

- **Fraud**
  - An intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to himself or some other person. It includes any act that constitutes fraud under applicable Federal or State law. (42 CFR 42 §455.2)



## Definitions

- **Waste**
  - Over-utilization of services, or other practices that result in unnecessary costs. Waste is generally not considered to be caused by criminally negligent actions but rather the is use of resources.





## Definitions

- **Abuse**

- Provider practices that are inconsistent with sound fiscal, business, or medical practices, and result in an unnecessary cost to the Medicaid, Medicare Advantage or Medicare Part D program, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for healthcare. It also includes recipient practices that result in unnecessary cost to the Medicaid, *Medicare Assured*<sup>®</sup>, or Medicare Part D program. (42 CFR § 455.2)



## Fraud and Abuse Laws

- **Anti-Kickback Statute**

- Prohibits the offer or receipt of certain remunerations in return for referrals for or recommending purchase of supplies and services reimbursable under government health care programs. Anyone found to be violating this statute shall be guilty of a felony and upon conviction shall be fined not more than \$25,000 or imprisoned for not more than 5 years or both.





## Fraud and Abuse Laws

- **Stark Law**
  - Prohibits physicians' referrals for the furnishing of any "designated health services" for which payment may be made under the Medicare Part B program ( and to some extent, Medicaid) to any entity with which the referring physician (or an immediate family member) has a "financial relationship"



## Fraud and Abuse Laws

- **Deficit Reduction Act of 2005**
  - Title VI Medicaid and SCHIP
    - Chapter 3 Eliminating Fraud, Waste and Abuse in Medicaid
    - Requires entities receiving annual Medicaid payments of at least \$5 million to establish written policies with respect to the False Claims Act
    - Established the Medicaid Integrity Program
    - Provided increased funding for Medicaid fraud and abuse control activities of the OIG.
    - Goal of Deficit Reduction Act was to reduce total Medicaid spending by \$4.3 billion over the next five years.





## Fraud and Abuse Laws

- **False Claims Act**

- The False Claims Act imposes civil liability on any person or entity who submits a false or fraudulent claim for payment to the United States Government.
  - A person who violates the act must repay three times the amount of damages suffered plus a mandatory civil penalty of at least \$5,500 and no more than \$11,000 per claim.
  - The stiff penalties have made this act one of the government's favorite tools to combat fraud and abuse in government funded programs.



## Fraud and Abuse Laws

- **Fraud Enforcement and Recovery Act of 2009 (FERA)**

- FERA makes it clear that the FCA imposes liability for knowing and improper retention of a Medicare overpayment. Consequently, a health care provider may now violate the FCA if it conceals, improperly avoids or decreases an "obligation" to pay money to the government.





## Types of Investigations

- Member
- Physician
- Hospital
- Pharmacies
- Other ancillary providers
- Vendor



## Law Enforcement

- Attorney General
- Office of Inspector General
- Medics
- Pennsylvania Bureau of Program Integrity
- U.S. Attorney
- Local law enforcement
- FBI





## Compliance Program Components

### 4. Employee Conduct



## Employee Conduct

- Employee conduct is maintained through a comprehensive ***Code of Conduct*** that states the company's expectations for employee behavior.





## Employee Conduct

- CMS *Medicare Prescription Drug Manual* designed and provided Code of Conduct standards to Medicare companies.
- CMS stated that an effective compliance program will have a ***Code of Conduct*** that articulates an organization's commitment to ethical behavior.



## Employee Conduct

- CMS provided the following requirements for the ***Code of Conduct***:
  1. Clearly ***articulate the Company's commitment*** to comply with statutory, regulatory, and other program requirements
  2. Delineate the ***Company's expectations*** of employees and vendors to act in an ethical and compliant manner
  3. Include ***ramifications*** for failure to comply





## Employee Conduct

- **Code of Conduct** should include the following policies and procedures:
  - Conflict of Interest
  - HIPAA
  - Applicable criminal state and federal laws
  - Reporting misconduct
    - Confidentiality, anonymity, and non-retaliation
  - Employee disciplinary guidelines



## Employee Conduct

- CMS requires employees and encourages vendors to distribute the Code of Conduct in the event of the following:
  - Time of hire
  - Code of Conduct revisions
  - Annual
- CMS requires employees to certify that they have **read, received and will comply** with the Code of Conduct.



## Compliance Program Components

### 5. Financial Statements



## National Association of Insurance Commissioners (NAIC)

- A state regulator's primary responsibility is to protect the interests of insurance consumers, and the NAIC helps regulators fulfill that obligation.
  - The NAIC and the regulators' shared objectives are financial and market conduct regulation.

*Continued on next slide*





## National Association of Insurance Commissioners (NAIC)

- The first major step in that process was ***the development of uniform financial reporting by insurance companies*** with the considerations of the following multidimensional concepts:
  - New legislation
  - New levels of expertise in data collection and delivery
  - New technological capability



## NAIC Mission

- Protect the public interest
- Promote competitive markets
- Facilitate the fair and equitable treatment of insurance consumers
- Promote the reliability, solvency and financial solidity of insurance institutions
- Support and improve state regulation of insurance





## NAIC – New Regulation

- Model Audit Rule
  - ***Implementation Guide for the Annual Financial Reporting Model Regulation***
    - New requirements for 2010 related to financial reporting:
      - Auditor (external) independence
      - Corporate governance
      - Internal controls



## Model Audit Rule: Auditor Independence

- Independent Certified Public Accountant
- Lead Audit Partner Rotation Requirements
  - The lead audit partner (having primary responsibility for the audit) may not act in that capacity for more than five (5) consecutive years; and
  - The person shall be disqualified from acting in that or a similar capacity for the same company or its insurance subsidiaries or affiliates for a period of five (5) consecutive years.





## Model Audit Rule: Auditor Independence

- Requirements for Audit Committees:
  - **Independence**
    - A policyholder
    - A person who serves on the Board of Directors of a contracting entity
    - An otherwise non-independent member of the Board of Directors is considered independent if state law requires participation on the Board as long as the member is not an officer or employee of the insurer or one of its affiliates.



## Model Audit Rule: Internal Controls

- Management's **Report of Internal Controls** over Financial Reporting
  - Management must **annually** provide their domiciliary insurance department with a **report on internal controls** over the statutory financial statement process.





## Model Audit Rule: Internal Controls

- Management must make an assertion regarding the effectiveness of the insurer's internal controls over financial reporting to the best of its knowledge and belief after ***diligent inquiry***.
  - ***Diligent inquiry*** – Conducting a search and thorough review of relevant documents which are reasonably likely to contain significant information with regards to Internal control over financial reporting and making reasonable inquiries of current employees and agents whose duties include responsibility for Internal control over financial reporting.



## Model Audit Rule: Internal Controls

- The report must disclose any ***unremediated material weaknesses*** with internal controls over financial reporting that exist as of the balance sheet date.
  - Not permitted to conclude that its Internal control over financial reporting is effective; and
  - Must include a description of the nature of any unremediated material weakness in the report.





## Model Audit Rule: Internal Controls

- **Significant Deficiency:**
  - A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.
- **Material Weakness:**
  - A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.



## Model Audit Rule: Internal Controls

- Internal controls over financial reporting has the following ***inherent limitations:***
  - Human misjudgments
  - Compliance breakdowns
  - Collusion
  - Improper management
- Therefore, it is possible to design into the process safeguards to reduce, though not eliminate, this risk.





## Model Audit Rule: Internal Controls

- **Control Environment**
  - (Entity-Level Controls) may include:
    - Code of Conduct
    - Policy Requirements
    - Compliance Programs



## Model Audit Rule: Internal Controls

- **Risk Assessments** of the following:
  - Investments (including capital expenditures)
  - Policy and claim reserves
  - Benefit payments
  - Premiums / agent's balances
  - Reinsurance
  - Related party (affiliate) transactions
  - Operating expenses/taxes





## Model Audit Rule: Internal Controls

- **Control Activities** may include:
  - Daily or monthly controls
  - System and manual controls
  - SAS 70 reporting controls



## Model Audit Rule: Internal Controls

- In monitoring and testing processes, insurers may want to consider describing the following:
  - Internal audit department purpose and function
  - Other self audit and analysis activities
- In the information and communication processes, insurers may want to consider describing the following:
  - Frequency of reporting and monitoring activities
  - Communication of internal control responsibilities





## NAIC – Model Audit Rule

- New requirements for 2010 related to financial reporting:
  - Auditor independence
  - Corporate governance
  - Internal controls



## Securities and Exchange Commission (SEC)

- The SEC oversees the following elements of the Security Exchange Act:
  - Companies publicly offering securities for investment dollars must tell the public the truth about their businesses, the securities they are selling, and the risks involved in investing.
  - People who sell and trade securities – brokers, dealers, and exchanges – must treat investors fairly and honestly, putting investors' interests first.
- Sarbanes-Oxley Act (SOX)
  - Enacted on July 31, 2002





## Sarbanes-Oxley Act (SOX): Section 404

- The SEC stated the following:
  - **Section 404** of the Sarbanes-Oxley Act requires public companies' annual reports to include the company's own assessment of internal control over financial reporting, and an auditor's attestation.



## SOX 404

- Compliance with the Model Audit Rule - Internal Controls utilizing the following SOX Principles:
  1. Identify risks and controls
  2. Assess effectiveness of controls
  3. Report deficient controls

*(SEC – Sarbanes-Oxley Section 404: A Guide for Small Businesses)*





## Beginning Your Evaluation

- Evaluation of effectiveness of internal control begins with consider the following two questions:
  1. Do my employees understand what they need to do to properly prepare external financial reports?
  2. What information do I need to make sure they have done those things?



## Step #1 - Identification

- Identifying Financial Reporting Risks
  - **RISKS:**  
("What could go wrong?")
    - ***Inherent*** risks
      - Both internal and external
    - Risk in the way you ***authorize, process, and record transactions*** that are reflected in your financial statement.
    - Your company's vulnerability to ***fraud***





## Step #1 - Identification

- Identifying Financial Reporting Controls
  - **CONTROLS:**  
("Which controls address the risks?")
    - ***Entity-level controls***
    - ***Multiple controls*** that addresses the same financial statement risks
    - ***Automated / manual controls***
    - ***Key controls*** - only those that address financial reporting risks

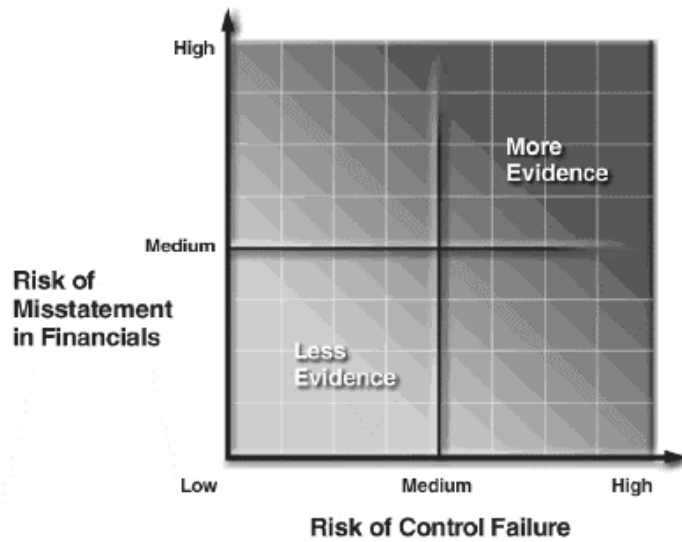


## Step #2 - Assessment

- ***Do your controls work in practice?***
  - Effectiveness of controls are based on the following assessments:
    1. The risk of a material misstatement in the financial reports
    2. The risk that the control will fail to operate as designed



## How Much Evidence Do You Need to Establish That Internal Controls Are Effective?



## Step #2 - Assessment

- As internal control risk increases, however, you may need to consider:
  - Using personnel who are more objective
  - More extensively validating the controls
  - Testing over longer periods





## Step #2 - Assessment

- Once the evidence is gathered, you then determine whether the control is operating effectively. In making your assessment, you should consider:
  - Whether the control operates as designed
  - How it is applied
  - Whether it operates consistently
  - Whether the personnel responsible for the control have the authority, and the competence, to do the job



## Step #3 - Reporting

- The SEC's new guidance highlights the factors that you should consider in deciding whether a control deficiency is a material weakness. For example:
  - How susceptible is the related financial reporting element to loss or fraud?
  - How significant are the financial statement amounts or the transaction totals that are exposed to the deficiency?





## Step #3 - Reporting

- If you identify any material weaknesses, you must describe them in your assessment of the internal controls that appears in your annual report. You should also consider including the following in your assessment:
  - A analysis of how the material weakness affects the company's financial reporting and internal controls
  - Your current plans (or the actions you've already taken) to address the material weakness



## Step #3 - Reporting

- Finally, you should describe these **material weaknesses** to the audit committee and your external auditor, along with any control deficiencies you've found that didn't rise to the level of a **material weakness**, but which you think are important enough to merit their attention. Control deficiencies of this kind are defined as "**significant deficiencies**" in the SEC's rules.





## Compliance Program Component

### 6. Federal and State Oversight



## Federal and State Oversight

- Centers for Medicaid and Medicare Services (CMS)
- State Medicaid agencies
- Department of Health (DOH)
- Department of Insurance (DOI)





## Centers for Medicaid & Medicare Sciences (CMS)

- CMS Audit Guides
- OIG Work Plan
- Medicare Part C and Part D
- Benefit Integrity
- Compliance plan
- Fraud, waste and abuse



## State Medicaid Agencies

- Encounters
- Performance measures
- Required reporting
- Overpayments
- Fraud, waste and abuse





## Department of Health

- Promote health lifestyles
- Prevent injury or disease
- Assure the safe delivery of healthcare



## Department of Insurance

- Monitor the financial solvency of insurance companies;
- License insurance companies and producers/agents;
- Review and approve insurance policy language and rates;
- Coordinate the rehabilitation and liquidation of insolvent insurance companies; and
- Administer health insurance programs for eligible adults and children.





## Compliance Considerations



## Compliance Considerations

- Roles and Responsibilities
- Reporting Structure
- Centralized Vs. Decentralized





## Roles and Responsibilities

- Internal Audit
- Corporate Compliance
- Special Investigations



## Reporting Structure

- Board of Directors
- Audit Committee
- Compliance Committee
- Audit workgroups
- Compliance workgroups
- Multi-disciplinary workgroups



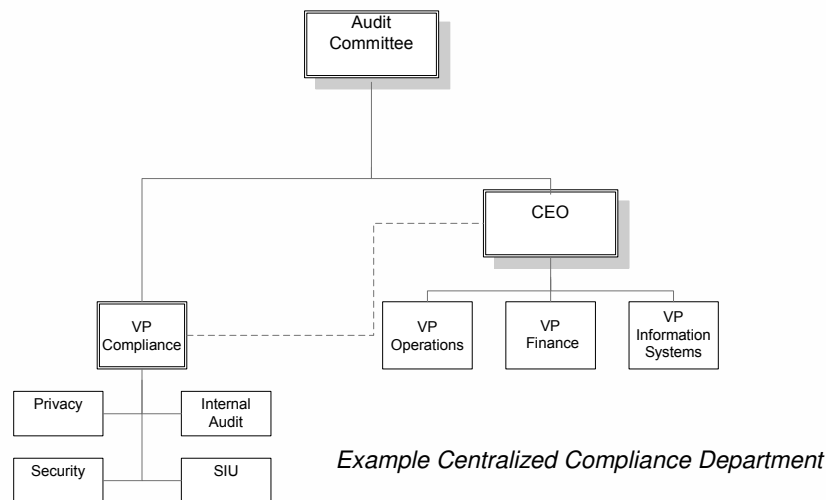


# Centralized Vs. Decentralized

- **Centralized:**
  - Places the responsibility for decision-making at higher levels, concentrating both authority and power at the top of management



# Centralized Vs. Decentralized



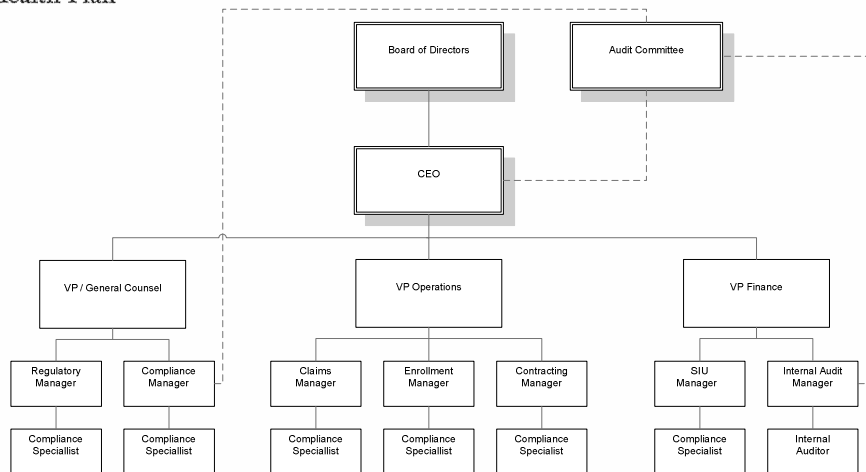


# Centralized Vs. Decentralized

- **Decentralized:**
  - Places decision authority in the hands of the individuals and teams who are closest to a problem or who manage a process



# Centralized Vs. Decentralized



*Example Decentralized Compliance Department*





## Monitoring and Auditing



## Monitoring and Auditing

- **Monitoring:**
  - A planned, systematic, and ongoing process to gather and organize data, and aggregate results in order to evaluate performance.





## Monitoring and Auditing

- **Monitoring:**
  - Monitoring procedures
  - Reporting and tracking of incidents
  - Special audits



## Monitoring and Auditing

- **Auditing:**
  - Focused evaluation of processes that often includes sampling of records or documents to determine compliance.





## Monitoring and Auditing

- Auditing:
  - Scope
    - Purpose
  - Methodology
    - Sample Size Standards
    - Time period
  - Communication
  - Corrective Action Plan Recommendations
  - Remediation and implementation
  - Follow-up testing



## Education and Training





## Education and Training

- **Employee**
  - Annual compliance training
  - Compliance reminders
  - Intranet / Internet
- **Vendor / Provider**
  - Annual compliance training
  - Compliance reminders
  - Internet



## Education and Training

- **Employee Education and Training**
  - Annual Compliance Training
    - Security and Privacy
    - Documentation
    - Fraud, waste, and abuse
    - Employee conduct
    - Duty to report
    - Violations





## Education and Training

- Employee Education and Training
  - Compliance Reminders
    - Current compliance issues posted in public areas, such as:
      - Bulletin boards
      - Displayed posters
    - Newsletters



## Education and Training

- Employee Education and Training
  - Intranet / Internet
    - Compliance program description
    - Code of conduct
    - Policies and procedures
    - Compliance and HIPAA terms
    - Fraud and compliance contact list





## Education and Training

- Vendor / Provider Education and Training
  - Annual Compliance Training
    - Code of Conduct
    - Conflict of interest
    - Security and privacy
    - Fraud, waste, and abuse



## Education and Training

- Vendor / Provider Education and Training
  - Compliance Reminders
    - Newsletters
    - Email alerts





## Education and Training

- Vendor / Provider Education and Training
  - Internet
    - Fraud, waste, and abuse training and certification
    - Fraud, waste, and abuse policy



## Compliance Plan





## Compliance Plan

1. **Written policies, procedures, and standards of conduct articulating Gateway's commitment to comply with all applicable Federal and State standards.**
  - **Written Policies and Procedures**
    - Existing policies are reviewed & edited at least annually
    - New policies are created as needed or required
    - Policy changes and new policies are presented to Compliance Committee
  - **Compliance Program**
    - A complete annual review & update of the Compliance Program is conducted.
    - Revised Compliance Program is presented for Board approval, as needed.



## Compliance Plan

2. **The designation of a compliance officer and compliance committee accountable to senior management.**
  - The organizational and reporting structure of a successful compliance plan includes the following:
    - Executive Committee & Board of Directors
    - President & Chief Executive Officer (CEO)
    - Vice President Strategic Planning & Medicare
    - Vice President Regulatory, Compliance & Legal
    - Chief Financial Officer
    - Corporate Compliance Officer
    - Medicare Compliance Officer
    - Manager, Special Investigation Unit & Internal Audit
    - Audit Committee
    - Compliance Committee





## Compliance Plan

3. Effective training and education between:
  - Compliance officer
  - Employees
  - Managers and directors
  - First tier, downstream, and related entities.



## Compliance Plan

4. Effective lines of communication between:
  - Compliance officer
  - Compliance and Audit Committees,
  - Employees
  - Managers and directors
  - First tier, downstream, and related entities.





## Compliance Plan

5. Enforcement of standards through well-publicized disciplinary guidelines.
  - Annual evaluations and job descriptions
  - Criminal background checks / drug screening
  - Disciplinary actions



## Compliance Plan

6. Procedures for effective internal monitoring and auditing.





## Compliance Plan

### 7. Procedures for ensuring:

- Prompt responses to suspected or detected offenses
- Development of corrective action initiatives relating to plan sponsors



## To Be Successful

- Executive support
- Management commitment
- Employee participation
- ***Compliance Environment***





## Questions?



## Contact Information

- **Tom Figurski**  
Manager, Special Investigations\Internal Audit  
(412) 255-4655  
[tfigurski@gatewayhealthplan.com](mailto:tfigurski@gatewayhealthplan.com)
- **Melissa Hooks**  
Internal Auditor  
(412) 918-8429  
[mhooks@gatewayhealthplan.com](mailto:mhooks@gatewayhealthplan.com)

