HEALTHCARE REGULATORY LAWS AFFECTING PHYSICIAN PRACTICES

Jennifer C. Monroe, Esq.
Langdale Vallotton, LLP
1007 North Patterson Street
Valdosta, Georgia 31602
229-244-5400
jmonroe@langdalelaw.com

LANGDALE VALLOTTON, LLP
ATTORNEYS AT LAW

- Impact of 2016 U.S. Presidential Election:
  - During the campaign, candidate Trump vowed repeatedly to "repeal and replace" President Obama's Patient Protection and Affordable Care Act (ACA)
  - Following the election, President-Elect Trump has indicated that he may keep certain parts of the ACA, including the pre-existing condition requirement and provisions allowing parents to cover children under their plans until their mid-20s. See Donald Trump Says he May Keep Parts of Obama Health Care Act, *The New York Times*, November 11, 2016.
  - Last week, President-Elect Trump announced Republican Representative Tom Price, as his choice as the Secretary of Health and Human Services. Mr. Price is an orthopedic surgeon, turned politician, who has been a staunch critic of the ACA. See Tom Price, Obamacare Critic, is Trump's Choice for Health Secretary, *The New York Times, November 28*, 2016.

- Which, if any, portions of the ACA will remain under President-Elect Trump's Administration?
- Which portions of the ACA will be eliminated?
- Will the ACA's payment and delivery system reforms which impact physician practices be maintained, modified or eliminated?
- The future is unclear. So, until more is known, the best practice for physician practices is to stay the course.

Fraud and Abuse Laws

- According to the U.S. Department of Justice, it recovered approximately $1.9 billion dollars from companies and individuals in the health care industry for allegedly providing unnecessary or inadequate care, paying kickbacks to health care providers to induce the use of certain goods and services, or overcharging for goods and services paid for by Medicare, Medicaid, and other federal health care programs.
- This $1.9 billion represents federal losses only. In many cases, the DOJ was instrumental in recovering additional millions of dollars for consumers and state Medicaid programs.
- Justice Department Recovers Over $3.5 Billion From False Claims Act Cases in Fiscal Year 2015, December 3, 2015, www.justice.gov

- Due to the significant sums at stake, recovery of improper healthcare payments to providers is a priority for the State and Federal Government
- Regulators operate through numerous agencies and under numerous laws/regulations in their recovery efforts

- According to the Department of Health & Human Services Office of the Inspector General, the five most important Federal fraud and abuse laws that apply to physicians are:
  1. The False Claims Act (FCA)
  2. The Anti-Kickback Statute (AKS)
  3. The Physician Self-Referral Law (Stark law)
  4. The Exclusion Authorities
  5. The Civil Monetary Penalties Law (CMPL)

- The Government agencies charged with enforcing these fraud and abuse laws include:
  1. The Department of Justice (DOJ)
  2. The Department of Health and Human Services Office of Inspector General (OIG)
  3. Centers for Medicare and Medicaid Services (CMS)

- Federal False Claims Act (FCA)
  - Protects the Federal government from being overcharged or sold substandard goods or services
  - Passed in 1863 – intended to combat defense contractor fraud against federal government
  - Now, significant portion of FCA claims involve the healthcare industry
  - FCA authorizes private citizens ("relators") to file whistleblower actions, entitling them to a percentage of the government's recovery

- Civil FCA
  - Prohibits knowingly submitting or causing to be submitted a false claim for payment to the government or using a false record to get a claim approved
  - Violations occur through submission of a false claim, submission of a false record to get a claim paid, or conspiring to get a false claim paid.
  - "Knowingly" includes "actual knowledge," "deliberate ignorance," or "reckless disregard."
  - Therefore, no proof of specific intent to defraud is required to violate the Civil FCA.
  - Up to 10 year statute of limitations

- Criminal FCA
  - Knowingly "and willfully" makes or causes to be made any false statement or representation of material fact to obtain benefit from the program

- Civil Penalties for Violating the FCA:
  - May include fines of up to three times the amount of damages sustained by the Government as a result of the false claims plus up to $21,563 per false claim filed (for violations occurring after November 2, 2015)
    - This recent change represents a significant increase in the penalties assessed under the FCA, which had previously been set at a minimum of $5,000 and a maximum of $10,000 per false claim
  - May also include exclusion from federal healthcare programs
- Criminal Penalties for Violating the FCA:
  - Fines and/or imprisonment

- The government uses the FCA to pursue:
  - Stark / Anti-Kickback Statute violations (physician relationships and vendor relationships)
  - Other violations including services not rendered, upcoding, cost reporting, and quality of care
- Example of FCA violation:
  - A physician knowingly submits claims to Medicare for a higher level of medical services than actually provided or higher level than the medical record documents.

- Anti-Kickback Statute (AKS):
  - The AKS prohibits the knowing and willful payment of "remuneration" to induce or reward patient referrals or the generation of business involving any item or service payable by the Federal health care programs, including drugs, supplies, or healthcare services for Medicare or Medicaid patients.
  - "Remuneration" is broadly defined, and includes *any* benefit, whether it be direct or indirect, overt or covert, in cash or in kind.
  - Examples:
    - A provider receives cash or below fair market value for rent for medical office space in exchange for referrals
    - Excessive compensation for medical directorships or consultancies

- According to the OIG "in some industries, it is acceptable to reward those who refer business to you. However, in the Federal health care programs, paying for referrals is a crime."
- AKS applies to everyone and to just about every aspect of the relationships between providers, their referral sources, vendors and patients
  - AKS covers the payers of the kickbacks (those who offer or pay remuneration); and
  - The recipients of the kickbacks (those who solicit or receive remuneration)
- The parties' intent is an element of the AKS

- AKS Penalties
  - Civil monetary penalty of $73,588 per kickback plus *three times* the amount of the remuneration (kickback)
  - Criminal penalties of fines, imprisonment or both
  - Exclusion from participation in federal healthcare programs
- AKS violation = Liability under the False Claims Act
- Remember: Physician can violate AKS even if physician actually rendered the service and the service was medically necessary
- NOTE: There are numerous Statutory Exceptions and Regulatory Safe Harbors under the AKS – if certain types of arrangements satisfy these exceptions/safe harbors, they may not violate the AKS

- Physician Self Referral Law (Stark Law)
  - Prohibits a physician from making a referral for certain designated health services payable by Medicare or Medicaid to an entity in which the physician (or an immediate family member) has an ownership/investment interest or with which he or she has a compensation arrangement, unless an exception applies.

- Designated Health Services are:
  - Clinical laboratory services;
  - Physical therapy, occupational therapy, and outpatient speech-language pathology services;
  - Radiology and certain other imaging services;
  - Radiation therapy services and supplies;
  - DME and supplies;
  - Parenteral and enteral nutrients, equipment, and supplies;
  - Prosthetics, orthotics, and prosthetic devices and supplies;
  - Home health services;
  - Outpatient prescription drugs; and
  - Inpatient and outpatient hospital services
- Stark law is strict liability, which means proof of specific intent to violate the law is not required.
- Prohibits the submission, or causing the submission, of claims in violation of the law's restrictions.

- Example:
  - A provider refers a beneficiary for a designated health service to a business in which the provider has an investment interest.
- Penalties:
  - May include fines, civil monetary penalties of up to $23,863 for each service, repayment of claims, and potential exclusion from all Federal health care programs.
- NOTE: The Stark law has numerous exceptions which may be applicable to an arrangement

- Exclusion Statute
  - Under the Exclusion Statute, the OIG must exclude from participation in all federal health care programs any providers and suppliers convicted of any of the following:
    - Medicare fraud, as well as any other offenses related to the delivery of items or services under Medicare
    - Patient abuse or neglect
    - Felony convictions for other health care-related fraud, theft, or other financial misconduct
    - Felony convictions for unlawful manufacture, distribution, prescription or dispensing of controlled substances

- OIG also has discretion to impose permissive exclusions on other grounds, including:
  - Misdemeanor convictions related to health care fraud other than Medicare or Medicaid fraud, or misdemeanor convictions with the unlawful manufacture, distribution, prescription, or dispensing of controlled substances
  - Suspension, revocation, or surrender of a license to provide health care for reasons bearing on professional competence, professional performance, or financial integrity
  - Provision of unnecessary or substandard services, submission of a false or fraudulent claims to a Federal health care program
  - Engaging in unlawful kickback arrangements
  - Defaulting on a health education loan or scholarship obligation
  - Excluded providers may not participate in Federal health care programs for a designated period.
  - An excluded provider may not bill Federal health care programs (including, but not limited to Medicare, Medicaid, and State Children's Health Insurance Program) for services he or she orders or performs
  - An employer or group practice may not bill for an excluded provider's services
  - The OIG maintains a List of Excluded Individuals/Entities, which can be found on their website

- Civil Monetary Penalties Law
  - Authorizes the imposition of CMPs for a variety of health care fraud violations.
  - Different amounts of penalties and assessments may be authorized based on the type of violation.
  - Penalties range from $21,563 to $73,568 per violation.
  - CMPs may also include an assessment of up to three times the amount claimed for each item or service, or up to three times the amount of remuneration offered, paid, solicited, or received.

- Violations that may justify CMPs include:
  - Presenting a claim you know, or should know, is for an item or service not provided as claimed or that is false and fraudulent
  - Presenting a claim you know, or should know, is for an item or service for which Medicare will not pay
  - Violating the AKS

- CMS Contractors. To support its efforts to prevent, detect and investigate potential Medicare fraud and abuse, CMS also contracts with the contractors listed below:
  - Comprehensive Error Rate Testing (CERT) Contractors. Help calculate the Medicare Fee For Service (FFS) improper payment rate by reviewing claims to determine if they were paid properly
  - Medicare Administrative Contractors (MACs). Process claims and enroll providers and suppliers.
  - Medicare Drug Integrity Contractors (MEDICs). Monitor fraud, waste, and abuse in the Medicare Parts C and D Programs.

- Recovery Audit Program/Recovery Auditors (RACs). Reduce improper payments by detecting and collecting overpayments and identifying underpayments.
- Zone Program Integrity Contractors (ZPICs). Investigate potential fraud, waste and abuse for Medicare Parts A and B; Durable Medical Equipment, Prosthetics, Orthotics, and Supplies; and Home Health and Hospice.
- Unified Program Integrity Contractor (UPIC). Will operate under restructured/consolidated Medicare and Medicaid Program Integrity audit and investigation work (not yet implemented)

- State of Georgia False Claims Act – liability for any person who:
  - Knowingly presents or causes to be presented to the Georgia Medicaid program a false or fraudulent claim for payment or approval;
  - Knowingly makes, uses or causes to be made or used a false record or statement material to a false or fraudulent claim;
  - Has possession, custody, or control of property or money used or to be used by the Georgia Medicaid program and, intending to defraud the Georgia Medicaid program, makes or delivers the receipt without completely knowing that the information on the receipt is true;
  - knowingly makes, uses or causes to be made or used a false record or statement material to an obligation to pay or transmit property or money to the Georgia Medicaid program, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit property to money to the Georgia Medicaid program;
  - Conspires to commit a violation of any of the above.

- "Knowing" and "Knowingly" require no specific intent to defraud and mean that a person, with respect to information:
  - Has actual knowledge of the information;
  - Acts in deliberate ignorance of the truth or falsity of the information; or
  - Acts in reckless disregard of the truth or falsity of the information

- Georgia False Claims Act – Penalties
  - $5,500 - $11,000 for each false or fraudulent claim
  - Three times the amount of damages which the Georgia Medicaid program sustains because of the act of such person; and
  - All costs of any civil action brought to recover the damages and penalties provided for under the Georgia False Claims Act

- State Entities Responsible for Enforcing Medicaid Fraud
  - Medicaid Fraud Control Unit (MCFU) – Division of Georgia Department of Law
  - Georgia Department of Community Health (DCH), Medicaid Program Integrity Unit
  - DCH's Recovery Audit Contractor (RAC) – Meyers and Stauffer

HIPAA

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Includes Privacy and Security standards which are designed to protect the confidentiality, integrity and availability of an individual's health care information
  - HIPAA applies to Covered Entities, which are defined as a health plan, a health care clearinghouse or healthcare provider, which transmits any health information in electronic form in connection with a transaction covered by HIPAA

- HIPAA Privacy Rule
  - The permitted, authorized and restricted uses and disclosures of protected health information (PHI)
  - A Covered Entity's Administrative Requirements
  - An individual's rights of access to, and control over the use and disclosure of his or her PHI

- HIPAA Privacy Rule –
  - Administrative Requirements require Covered Entities to develop and implement written privacy policies and procedures
    - Conduct risk analysis audit
    - Once risk analysis audit is complete, covered entity should perform a "gap" analysis to identify where PHI may not be properly protected
    - Upon completion of risk analysis and gap audit, practice should draft appropriate privacy policies and procedures
    - Train Employees on Privacy Policies

- HIPAA Privacy Rule – Business Associate Agreements
  - Business Associates are persons or entities who perform services or functions for a Covered Entity and, as part of that job, necessarily must have access to PHI
  - Covered Entities must obtain assurances from their Business Associates, in writing, that the Business Associates will appropriately safeguard PHI they receive or create on behalf of the Covered Entity
  - See HHS, Office of Civil Rights website for sample Business Associate Agreement language

- HIPAA Security Rule
  - Requires Covered Entities to establish policies and procedures to:
    - Assess current security, risks and gaps;
    - Develop security policies and procedures;
    - Implement security measures and solutions;
    - Document its analysis, decisions and rationale for its decisions; and
    - Periodically review and update security measures and documentation.

- HIPAA Enforcement
  - Civil Penalties enforced by both CMS and the HHS Office of Civil Rights (OCR)
  - Criminal Penalties enforced by Department of Justice
- HIPAA Civil Monetary Penalties:
  - Where a person "did not know" at least $100, but no more than $50,000 for each violation
  - Where there was "reasonable cause" but no willful neglect, at least $1,000, but no more than $50,000 for each such violation; or
  - If there was willful neglect, at least $10,000, but no more than $50,000 for each such violation

- HIPAA Criminal Penalties
  - Penalties for one who knowingly, and in violation of the Privacy Rule, discloses PHI to another individual, vary, depending on the circumstances:
    - Lowest tier of penalties includes a fine of not more than $50,000 and imprisonment of not more than one year, or both.
    - If the violation is committed under false pretenses, the violator may be fined not more than $100,000 and imprisoned for not more than five years, or both.
    - If the violation is committed with the intent to sell, transfer or use PHI for commercial advantage, personal gain, or malicious harm, the person may be fined not more than $250,000 and imprisoned for not more than 10 years, or both.

- OCR is Focused on Physician Practices:
  - In 2012, OCR settled a HIPAA investigation for $100,000 with Phoenix Cardiac Surgery of Phoenix and Prescott, Arizona.
  - Phoenix Cardiac Surgery was a five physician practice.
  - OCR initiated its investigation based on a complaint that the practice was posting clinical and surgical appointments for its patients on an internet-based calendar that was publically accessible. The investigation also revealed that the practice:
    - failed to implement adequate policies and procedures to appropriately safeguard patient information;
    - Failed to document that it trained any employees on its policies and procedures on the Privacy and Security Rules; failed to identify a Security Official to conduct a risk analysis; and
    - Failed to obtain Business Associate Agreements with internet-based email and calendar services where the provision of the service included storage of and access to its ePHI
- OCR's statement in its press release is significant:
  - "*We hope that health care providers pay careful attention to this resolution agreement and understand that the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity*."

Identifying Risk Areas and Compliance Best Practices

- A good way to identify government audit/investigative focus and priorities, is to review the DHHS OIG's Work Plan
- In the Autumn of each year, OIG publishes its Work Plan for the following federal fiscal year ("FFY")
- OIG's Work Plan for FFY 2017 was recently published
- The following slides contain some of the topics/areas included in the 2017 Work Plan which may be applicable to a physician practice.

- Medicare Payments for Transitional Care Management ("TCM")
  - TCM includes services provided to a patient whose medical and/or psychosocial problems require moderate or high-complexity medical decision-making during transitions in care from an inpatient hospital setting, partial hospital, observation status in a hospital, or skilled nursing facility, to the patient's community setting.
  - Medicare-covered services, including chronic care management, end-stage renal disease, and prolonged services without direct patient contact, cannot be billed during the same service period as TCM.
  - OIG will determine whether payments for TCM services were in accordance with Medicare requirements.

- Medicare Payments for Chronic Care Management ("CCM")
  - CCM is defined as the non-face-to-face services provided to Medicare beneficiaries who have multiple significant chronic conditions that place the patient at significant risk of death, acute exacerbation/ decompensation, or functional decline, and are expected to last at least 12 months
  - CCM cannot be billed during the same health service period as TCM, home health care supervision/hospice care, or certain end-stage renal disease services.
  - OIG will determine whether payments for CCM services were in accordance with Medicare requirements.

- Medicare payments for service dates after individuals' dates of death

- Physician Financial Interests under Open Payment Program
  - The Physicians Payment Sunshine Act requires that manufactures disclose to CMS payments made to physicians, as well as ownership and investment interests held by physicians.
  - OIG will analyze 2015 data from the Open Payments website to determine the number and nature of financial interests.
  - OIG will determine how much Medicare paid for drugs and DMEPOS (durable medical equipment, prosthetics, orthotics, and supplies) ordered by physicians who had financial relationships with manufactures and group purchasing organizations
  - OIG will determine the volume and total dollar amount associated with drugs and DMEPOS ordered by these physicians in Medicare Parts B and D for 2015.

- Prolonged Services – Reasonableness of Services
  - Prolonged services are for additional care provided to a beneficiary after an evaluation and management (E/M) service has been performed.
  - OIG/CMS considers the necessity of prolonged services to be rare and unusual.
  - The Medicare Claims Processing Manual includes requirements that must be met in order to bill for a prolonged E/M service code.
  - OIG will determine whether Medicare payments to physicians for prolonged E/M services were reasonable and made in accordance with Medicare requirements.

- Electronic Health Records / Meaningful Use
  - As an incentive for using EHRs, the Federal Government has made payments to providers that attest to the "meaningful use" of EHRs.
  - According to CMS, more than $30 billion in incentives have been paid through the Medicare and Medicaid EHR incentive programs.
  - The General Accountability Office (GAO) has identified improper payments as the primary risk to the EHR incentive programs, noting that these programs may be at greater risk of improper payments because of their *complex requirements*.

- OIG has indicated that it will focus on the following two aspects of Meaningful Use:
  1. Medicare Incentive Payments for Adopting Electronic Health Records
     - OIG will review Medicare incentive payments to eligible health care professionals for adopting EHRs and CMS safeguards to prevent erroneous incentive payments.
     - OIG will review Medicare incentive payment data to identify payments to providers that should not have received incentive payments (e.g., those not meeting selected meaningful-use criteria).
     - OIG will assess CMS' plan to oversee incentive payments for the duration of the program and corrective actions taken regarding erroneous incentive payments.

2. Security of Certified EHR Technology Under Meaningful Use

- A core meaningful-use objective for eligible providers is to protect electronic health information created or maintained by certified EHR technology by implementing appropriate technical capabilities.
- To meet and measure this objective, providers must conduct a security risk analysis of certified EHR technology.
- OIG will perform audits of various covered entities receiving EHR incentive payments from CMS to determine whether they adequately protect electronic health information created or maintained by certified EHR technology.

Compliance for the Physician Practice

- In 2000, the OIG issued its Compliance Guidance for Individual and Small Group Physician Practices
- OIG stated that the Guidance contains seven components that provide a solid basis upon which a physician practice can create a *voluntary* compliance program.
- "Voluntary" aspect of physician compliance programs effectively eliminated by the Affordable Care Act
  - Providers must establish compliance programs as a condition of enrollment in Medicare, Medicaid and CHIP programs
  - CMS indicates that required compliance programs will incorporate the core elements of Chapter 8 of the U.S. Federal Sentencing Guidelines Manual

- According to CMS' Affordable Care Act Provider Compliance Programs Getting Started Webinar, the ACA compliance program mandate:
  - Is intended to induce all health care professionals to implement a compliance program;
  - Is not a guarantee that the risk of fraud, waste, abuse or inefficiency will not occur; and
  - Will aid providers in better protecting themselves from risk of improper conduct.

- CMS states that a well-composed compliance program can:
  - Increase the potential of proper submission and payment of claims;
  - Reduce billing mistakes;
  - Improve the results of reviews conducted on Medicare claims by the Medical Review Department, Comprehensive Error Rate Contractor (CERT), Recovery Auditor and the Zone Program Integrity Contractor (ZPIC);
  - Avoid the potential for fraud, waste and abuse; and
  - Promote patient safety and ensure delivery of high quality patient care

- CMS' Seven Core Elements of an Effective Compliance Program:
  1. Written Policies, Procedures and Standards of Conduct
  2. Compliance Program Oversight
  3. Training and Education
  4. Opening the Lines of Communication
  5. Auditing and Monitoring
  6. Consistent Discipline
  7. Corrective Action

Element #1: Written Policies, Procedures and Standards of Conduct

- Clearly written and describe expectations in detail
- Readily available to all employees
  - Require employee certification that have read and agree to comply
- Reviewed by employees within 90 days of hire, and annually thereafter
- Regularly reviewed and updated
- Detailed code of conduct and reporting mechanisms
- Describe compliance staff roles and responsibilities

Element #2: Compliance Program Oversight

- Establish who will oversee the compliance program as the organization's Compliance Officer and/or Compliance Committee
- Compliance Officer/Committee should be qualified and be responsible for reasonable oversight of the compliance program
- Not "One Size Fits All"
- Compliance Officer/Committee should be instrumental in developing, implementing, overseeing compliance plan and have broad authority to audit, collect data, interview employees, enforce compliance and recommend policy, procedure and process improvements

Element #3: Training and Education

- Training is essential to ensure staff is aware of expectations and standards
- Training should, when appropriate, use actual compliance scenarios and/or investigations of non-compliance as examples of risks that employees and managers may encounter
- Make the training as interactive as possible to increase the takeaway value to employees
- Conduct training upon hire, annually, and as needed to instruct on compliance program changes or new developments

Element #4: Opening the Lines of Communication

- Requirements for all employees to be proactive and report issues timely
- A formal process for managers to communicate compliance issues and results to staff
- A process to allow anonymous reporting without fear of retaliation (again – not "one size fits all")

- Remember the What, Who, How and When of Communication:
  - Communicate *all known or perceived instances* of compliance issues, or fraudulent or illegal behavior
  - Report to immediate supervisor or Compliance Officer/Committee
  - Make several methods available as to how employees communicate reporting issues (in person, electronically, anonymously (drop box/hotline)
  - Compliance issues should be reported immediately or as soon as they are identified
- Emphasize open door policy for reporting

Core Element #5: Auditing and Monitoring:

- Monitoring – includes day-to-day regular reviews which are performed by practice staff as part of the practice's normal operations
- Auditing – more comprehensive and involves
  - Ensuring compliance with a range of statutory and CMS requirements in critical operations areas
  - Conducting regular, periodic evaluations of the compliance program to determine the program's overall effectiveness
  - Conducting auditing at least annually, or more frequently as appropriate
  - Written reports of audit findings, recommendations and proposed corrective actions

- Consistency in response to issues. When issues are identified, the practice should be consistent in its application of the written policies and procedures to the offense, and the policies should cover:
  - A plan of how internal investigations should be conducted
  - A time limit for closing an investigation
  - Options for corrective action
  - When to have an investigation performed by an outside, independent contractor; and
  - How and when to refer an act of non-compliance to CMS or law enforcement authorities

- Conduct Risk Assessments, which should
  - Include areas of concern identified by CMS, beneficiaries and providers; and
  - Identify risk levels (high, medium or low)
- Include Risk Assessment results in monitoring and auditing work plans.
  - High risk areas should be audited regularly

- Identify Specific Risk Areas – Examples:
  - Billing, Coding and Documentation
    - E/M Services
    - "Incident to" rules/requirements
    - Standards for refunding credit balances
    - Supervision requirements
  - Medically Necessary Services
  - Improper Financial Relationships (Anti-Referral Laws)

- When issues are identified, corrective must be taken and must:
  - Ensure problem or violation does not reoccur (or minimize possibility that it could recur);
  - Be based on root cause analysis of the problem; and
  - Contemplate reviews of the effectiveness of the corrective action going forward

- Summary: Monitoring and Auditing Work Plans should:
  - Outline monitoring/auditing specifics;
  - Be based on results of risk assessment;
  - Include a process for responding to results; and
  - Include corrective actions.

Core Element #6: Consistent Discipline

- Written policies should include sanctions for:
  - Non-compliance with written standards of conduct;
  - Failure to detect non-compliance when routine observation or due diligence should have provided adequate clues; and
  - Failure to report actual or suspected non-compliance.

- Discipline must be imposed timely and enforced consistently.
- Disciplinary policies must:
  - Be clearly written and widely publicized;
  - Describe expectations as well as consequences for non-compliant, unethical, and illegal behaviors; and
  - Be reviewed with staff regularly (at least annually)

Core Element #7: Corrective Action

- When vulnerabilities or non-conformances are identified and/or reported, corrective action must be conducted in response to potential violations
- Corrective action examples include:
  - Repayment of overpayments; and
  - Disciplinary action against responsible employees.

Compliance Plan Best Practices

- Review the OIG's Guide for Physician Practice Groups (October 5, 2000), http://oig.hhs.gov/authorities/docs/physician.pdf
- Keep the plan simple
  - Concise and to the point – otherwise, risk that it will never be read
  - Include specific, relevant examples
- Set a date to review the plan every year – put the date on your calendar

- Positive and frequent visibility
  - Emails, internal memos, updates, etc.
- Have a real person behind the Compliance Plan
  - Staff need to know the fact of the Compliance Plan and that they are accessible
- Compliance Plan (and Compliance Officer) needs to be clear and fair where everyone understands the rules and consequences

Questions?

Jennifer C. Monroe, Esq.
Langdale Vallotton, LLP
1007 North Patterson Street
Valdosta, Georgia
229-244-5400
jmonroe@langdalelaw.com

The views expressed by the presenter do not necessarily represent the views, positions, or opinions of the presenter's organization. These materials, and the oral presentation accompanying them, are for educational purposes only and do not constitute legal advice or create an attorney-client relationship.

LANGDALE VALLOTTON, LLP
ATTORNEYS AT LAW