REGULATIONS YOUR PRACTICE MUST COMPLY WITH:

Patient Protection and Affordable Care Act

- States that providers "shall, as a condition of enrollment" in Medicare and Medicaid programs, have a compliance program.
- Allows the Secretary of HHS to suspend payment for Medicaid and Medicare services based on a credible allegation of fraud.
    - Suspension can be instituted without prior notice.
    - Initial suspension period is 180 days.
    - Can be extended an additional 180 days.
    - Provider/supplier knowledge of fraudulent conduct unnecessary.
- A credible allegation of fraud is an allegation from any source can trigger a Medicaid or Medicare payment hold, including but not limited to:
    - Fraud hotline complaints
    - Claims data mining
    - Patterns identified through:
    - Provider audits
    - Civil false claims cases
    - Law enforcement investigations
- Allegations are considered credible when they have indicia of reliability
- Many state enforcement agencies have adopted similar laws.
- Grants authority to the Secretary of HHS to revoke a provider's billing number if several grounds exist including:
    - Non-compliance with enrollment requirements;
    - Provider or supplier conduct, such as instances where a provider employs an excluded individual;
    - Felonies – the provider, supplier, or any owner of the provider/supplier who had been convicted of a felony within the last 10 years;

    - Providing false information on an application to enroll or participate in a Federal health care program; and
    - Billing for deceased individuals or others who could not possibly have received the service (e.g., the provider was out of state but billed for services).
- Revocations, unlike payment suspensions:
    - Stay in effect for at least a year and
    - Could last for up to 3 years based on the severity of the situation.

Anti-Kickback Statute

- Criminal statute that prohibits the exchange (or offer to exchange), of anything of value, in an effort to induce (or reward) the referral of federal health care program business.
- Establishes penalties for individuals and entities on both sides of the prohibited transaction.
- An intent-based statute that requires the party to "knowingly and willfully" engage in the prohibited conduct.
- Under the Anti-Kickback Statute, the government:
    - Must prove that a defendant intended to violate the law.
    - Does not have to prove the defendant intended to violate the Anti-Kickback Statute itself.
- Any submitted claim that violates the Anti-Kickback Statute automatically constitutes a false or fraudulent claim under the False Claims Act.
- Penalties include:
    - Up to five years in prison.
    - Criminal fines up to $25,000.
    - Administrative civil penalties in the form of treble damages plus $50,000 for each violation.
    - Exclusion from participating in federal health care programs

Federal False Claims Act

- The federal Civil and Criminal False Claims Act ("FCA") imposes liability on any person who:
    - Knowingly bills for services not rendered
    - Knowingly includes improper entries on cost reports.

- Knowingly assigns incorrect codes to secure higher reimbursement for services rendered.
- Knowingly characterizes unallowable services or costs in a way that secures reimbursement.
- Does not seek payment from beneficiaries who may have other primary payment sources.
- Knowingly falsifies, forges, alters, or destroys documents to secure payment.
- Knowingly conceals, avoids or decreases an obligation to pay money to the government.

- The False Claims Act defines "knowingly" as instances where a person:
  - 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.
- The False Claims Act does not require proof of specific intent to defraud.
- Penalties:
  - A person found to have violated the False Claims Act is liable for a civil penalty for each claim of not less than $5,500 and not more than $11,000, plus
  - Three times the amount of damages sustained by the federal government (treble damages).

<u>Meaningful Use Requirements</u>

- Federal government program that encourages health care providers to implement or upgrade electronic health records (EHR) technology and standardize the exchange of patient clinical data between healthcare providers, between healthcare providers and insurers, and between healthcare providers and patients.
- Provided incentives for adopting EHR technology and satisfying the Meaningful Use requirements.
  - For eligible professionals (which includes physicians, nurse practitioners, dentists and certain physician assistants at federally qualified health centers or rural health clinics, as well as optometrists in certain states) up to $44,000
  - For eligible hospitals, base payments of $2 million.
- Eligible professionals (EP) and eligible hospitals must meet and attest to all of the EHR program requirements for at least a 90-day period within the 2011 or 2012 federal fiscal year and for the entire year thereafter in order to qualify for payments.

- In order to qualify for the incentives, an eligible provider or eligible hospital must:

    - Use a computerized Use computerized provider order entry (CPOE) for medication orders directly entered by a licensed healthcare professional who can enter orders into the medical record per state, local and professional guidelines. More than 30 percent of all unique patients with at least one medication in their medication list seen by the EP have at least one medication order entered using CPOE.

    - Enable the drug-drug and drug-allergy interaction functionality for the entire EHR reporting period. The EP has enabled this functionality for the entire EHR reporting period.

    - Maintain an up-to-date problem list of current and active diagnoses. More than 80 percent of all unique patients seen by the EP have at least one entry or an indication that no problems are known for the patient recorded as structured data.

    - Generate and transmit permissible prescriptions electronically (eRx). More than 40 percent of all permissible prescriptions written by the EP are transmitted electronically using certified EHR technology.

    - Maintain active medication list. More than 80 percent of all unique patients seen by the EP have at least one entry (or an indication that the patient is not currently prescribed any medication) recorded as structured data

    - Maintain active medication allergy list. More than 80 percent of all unique patients seen by the EP have at least one entry (or an indication that the patient has no known medication allergies) recorded as structured data.

    - Record all of the following demographics: preferred language, gender, race, ethnicity, and date of birth. More than 50 percent of all unique patients seen by the EP have demographics recorded as structured data.

    - Record and chart changes in vital signs: height, weight, blood pressure, calculate and display body mass index (BMI), plot and display growth charts for children 2-20, including BMI. More than 50 percent of all unique patients age 2 and over seen by the EP, height, weight, and blood pressure are recorded as structured data.

    - Record smoking status for patients 13 years old or older. More than 50 percent of all unique patients 13 years old or older seen by the EP have smoking status recorded as structured data.

    - Implement one clinical decision support rule relevant to specialty or high clinical priority along with the ability to track compliance with that rule. Implement one clinical decision support rule relevant to specialty or high clinical priority along with the ability to track compliance to that rule.

        - Provide patients with an electronic copy of their health information (including diagnostics test results, problem list, medication lists, medication allergies) upon request. Provide more than 50 percent of all patients who request an electronic copy of their health information within three business days.

        - Provide clinical summaries for patients for each office visit. Provide clinical summaries to patients for more than 50 percent of all office visits within three business days.

        - Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities. Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

    - Penalties for meaningful use fraud (falsely attesting that the practice has completed the meaningful use requirements) include repayment of all meaningful use incentive payments and the return of all Medicaid or Medicare payments made during the period of the violation.

Stark self-referral statute (sometimes called physician self-referral law or the "Stark Law")

- Prohibits a physician from making referrals for certain designated health services (DHS) payable by Medicare to an entity with which he or she (or an immediate family member) has a financial relationship (ownership, investment, or compensation), unless an exception applies. Many states have a similar law for Medicaid.

- Stark defines "physician" as a doctor of medicine or osteopathy, a doctor of dental surgery or dental medicine, a doctor of podiatric medicine, a doctor of optometry, or a chiropractor.

- Prohibits the entity from presenting or causing to be presented claims to Medicare (or billing another individual, entity, or third party payer) for those referred services.

- Establishes a number of specific exceptions and grants authority to the Secretary to create exceptions when financial relationships pose no risk of program or patient abuse.

Stark defines DHS as the following:

1. Clinical laboratory services.

2. Physical therapy services.

3. Occupational therapy services.

4. Outpatient speech-language pathology services.

5. Radiology and certain other imaging services.

6. Radiation therapy services and supplies.

7. Durable medical equipment and supplies.

8. Parenteral and enteral nutrients, equipment, and supplies.

9. Prosthetics, orthotics, and prosthetic devices and supplies.

10. Home health services.

11. Outpatient prescription drugs.

12. Inpatient and outpatient hospital services

The Stark law and regulations have nine general exceptions to the ownership and compensation prohibitions:

1. Physician services

    - Services personally by another physician in the same group practice as the referring physician or

    - Under the personal supervision of another physician in the same group practice as the referring physician.

2. In-office ancillary services, i.e., DHS services ordered by physicians in the context of their own practices.

    - DHS

    - Certain durable medical equipment (DME)

    - Infusion pumps that are DME (including external ambulatory infusion pumps)

    The in-office ancillary services exception must satisfy three tests to qualify for the exception:

    - The practitioner test (who may furnish the services)

    - The location test (the "same building" where the referring physicians provide their regular medical services or in a "centralized building" (where the group practice is located))

    - The billing test. The DHS service must be billed by one of the following:

- The performing or supervising physician
- The performing or supervising physician's group practice, under the group practice's billing number
- The referring or supervising physician or the referring or supervising physician's group practice wholly owned entity
- A third-party billing agent acting as an agent of the physician, group practice, or the wholly owned entity

3. Prepaid plans
4. Intra-family rural referrals
5. Academic medical centers
6. Implants furnished by an Ambulatory Surgery Center
7. Erythropoietin, (also known as EPO, a hormone that controls red blood cell production) and other dialysis-related drugs furnished or ordered by an ESRD facility
8. Preventive screening tests, immunizations and vaccines
9. Eyeglasses and contact lenses following cataract surgery

Stark is a strict liability (intent irrelevant) law that prohibits certain referrals by physicians to entities with which the physician has a financial arrangement.

Compliance with a Stark exception does not immunize an arrangement under the Anti-Kickback statute.

Stark penalties for violations are:

- Denial of payment
- Refund
- $15,000 for each bill/claim
- 3X the amount claimed
- $100,000 for each arrangement
- Exclusion for federal health plans.

Occupational Safety and Health Administration (OSHA)

OSHA requires the practice to:

- Provide a workplace free from recognized hazards and comply with OSHA standards.
- Provide training required by OSHA standards
- Keep records of injuries and illnesses.
- Provide medical exams when required by OSHA standards and provide workers access to their exposure and medical records
- Not discriminate against workers who exercise their rights under OSHA.
- Post OSHA citations and hazard correction notices.
- Provide and pay for most personal protective equipment (PPE).
- Have a written, complete hazard communication program that includes information on:
    - Container labeling,
    - Safety Data Sheets (SDSs), and
    - Worker training.
- The practice must:
    - Report each worker death to OSHA.
    - Report each work-related hospitalization, amputation, or loss of an eye.
    - Maintain injury & illness records.
    - Inform workers how to report an injury or illness to the employer.
    - Make records available to workers.
    - Allow OSHA access to records.
    - Post annual summary of injuries & illnesses.
- The practice's employees have the right to:
    - A safe and healthful workplace.
    - Know about hazardous chemicals.
    - Report injury to employer.

- Complain or request hazard correction from employer.
- Training.
- Hazard exposure and medical records.
- File a complaint with OSHA.
- Participate in an OSHA inspection.
- Be free from retaliation for exercising safety and health rights.

- Penalties under OSHA:

Up to $70,000 for each willful violation, with a minimum penalty of $5,000 for each violation.	For willful violations where the practice intentionally and knowingly commits or a violation with plain indifference to the law.
Up to $7,000 for serious violations.	For serious violations where there is substantial probability that death or serious physical harm that the employer knew, or should have known, of the hazard.
Up to $7,000 for each other-than-serious violation	For other than serious, where violations have a direct relationship to safety and health, but probably would not cause death or serious physical harm.
Up to $70,000 for each repeated violation	For repeated violations, that are the same or similar to a previous violation.

Qui Tam Actions

- An action where persons (typically past or current employees) and entities with evidence of fraud against federal programs or contracts may sue the wrongdoer on behalf of the United States Government.
- The government has the right to intervene and join the qui tam action.
- If the government declines, the private plaintiff may proceed on his or her own. Some states have passed similar laws concerning fraud in state government contracts.
- In a qui tam action, the person bringing the suit is entitled to a percentage of the penalty recovered as a reward for exposing the wrong-doing and recovering funds for the government.

Whistleblowers

- A whistleblower is an employee who:
    - Believes or has reason to believe his or her employer has violated some law, rule or regulation.
    - Testifies or commences a legal proceeding on the legally protected matter.
    - Refuses to violate the law.
- Most whistleblowers are internal whistleblowers, who report misconduct to a fellow employee or superior within their company.
- External whistleblowers, however, report misconduct to outside persons or entities.
- In these cases, whistleblowers may report the misconduct to lawyers, the media, law enforcement or watchdog agencies, or other local, state, or federal agencies.
- Employers can't legally retaliate against whistleblowers in any way.
    - For example, employers can't legally discharge, demote, suspend or harass employees for exercising their rights under laws that have whistleblower protection provisions.
- Encourages employees to halt, report or testify about employer acts that are illegal or unhealthy, without fear of employer retaliation.
- If employers retaliate, whistleblower protection provisions provide avenues of relief for victims.
- Many state and federal laws have whistleblower protection provisions.
- Whistleblower laws make it illegal for employers to retaliate against employees who:
    - Report employers' violations of whistleblower laws to the proper authorities.
    - Refuse to engage in activities made unlawful by whistleblower laws.
    - Participate in legal proceedings under whistleblower laws.
- Retaliation provisions typically include protection from discharge and harassment, and allow victims to file lawsuits for damages.
- An employee turned whistleblower is entitled to:
    - Employment reinstatement at the same level of seniority;
    - Two times the amount of back pay;

- Interest on the back pay; and,
- Compensation for special damages incurred as a result of the employer's inappropriate actions.

Health Insurance Portability and Accountability Act (HIPAA)

- HIPAA Privacy Rule: (http://www.hhs.gov/ocr/privacy/hipaa/understanding/)
  - Requires covered entities (health care providers, health plans and clearinghouses) and their business associates to provide a minimal level of protections for protected health information in their possession.
  - Gives patients an array of rights with respect to their protected health information held by covered entities and business associations.
  - Establishes processes for disclosing health information needed for patient care and other important purposes.
  - Under HIPAA, the practice patient has the right to:
    - Request access to health info.
    - Request to amend their health info.
    - Request restrictions to information sharing
    - Request accountability of disclosures
  - The practice's Notice of Privacy Practices, which outlines how protected health information about an individual will be used and disclosed and how a patient can get access to their information.
  - The practice is required to keep patient records for seven years.
  - The practice must have appropriate safeguards for its patients' protected health information.
  - The practice must enter into Business Associate Agreements with business associates who maintain, transmit, receive, process and store protected health information for the practice to obtain reasonable assurances that the business associate has appropriate protections.
  - HIPAA Security Rule - a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

- Under HIPAA's administrative safeguards, the practice must have various policies and procedures, including the following:

    - Security management process – a framework for developing and implementing policies and procedures to prevent, detect, contain, and correct security violations.

    - Risk analysis - an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the practice's electronic protected health information. Components of a risk assessment include:

        - Develop an inventory of information systems that maintain, transmit, receive, process and store protected health information for the practice

        - Develop a list of the practice's business associates, their contact information and services provided to the practice

        - Determine whether your practice has policies and procedures that satisfy the administrative, physical and technical safeguards.

        - Determine the threat/vulnerability level for each safeguard.

        - Describe your practice's current activities to satisfy the administrative, physical and technical safeguards.

        - If your practice does not comply with the administrative, physical and technical safeguards, provide a reason for noncompliance, such as cost, practice size, complexity or alternative solution.

        - Determine your practice's level of compliance against the HIPAA Privacy Rule and Breach Notification requirements.

        - Conduct a vulnerability test, which scans the practice's information systems for a variety of vulnerabilities across information systems that may be:

            - Vendor related, such as software bugs, missing operating system patches, vulnerable services, insecure default configurations, and web application vulnerabilities.

            - System administration activities, such as incorrect or unauthorized system configuration changes, lack of password protection policies, etc.

            - General day-to-day user activities, such as sharing directories to unauthorized parties, failure to run virus

scanning software, software updates and patches, and malicious activities, such as deliberately introducing system backdoors.

- Remediate vulnerabilities identified through scanning along with the development of a durable vulnerability testing program.

- Conduct a penetration test on the practice's information systems, which evaluates the IT infrastructure security by safely attempting to exploit system vulnerabilities, including operating systems, service and application flaws, improper configurations, and even risky end-user behavior.

    - Remediate weaknesses identified through the penetration scanning along with the development of a durable penetration testing program.

- Create a written risk assessment report which outlines and rates the practice's compliance against HIPAA and provides remediation suggestions for those findings that are less than fully compliant.

- Create a written management action plan to remediate prioritized findings.

- Appropriate sanctions against workforce members who fail to comply with the practice's privacy and security policies and procedures.

- Information system activity review – procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

- Security awareness and training – a security awareness and training program for all members of the practice's workforce.

- Workforce security – policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information.

- Information access management – policies and procedures for authorizing access to electronic protected health information

- Access establishment and modification – policies and procedures that, based upon the practice's access authorization policies, establish, document, review, and modify a user's right.

- Protection from malicious software – procedures for guarding against, detecting, and reporting malicious software.

- Log-in monitoring – procedures for monitoring log-in attempts and reporting discrepancies.

- Password management – procedures for creating, changing, and safeguarding passwords.

- Data backup plan – procedures to create and maintain retrievable exact copies of electronic protected health information.

- Disaster recovery plan – procedures to restore any loss of data.

- Emergency mode operation plan – procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

- Testing and revision procedures – procedures for periodic testing and revision of contingency plans.

- Under HIPAA's physical safeguards, a practice must have physical safeguards, which consist of physical measures, policies, and procedures to protect the practice's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. Under HIPAA's physical safeguards, the practice must have various policies and procedures, including the following:

    - Facility access controls – policies and procedures to limit physical access to its electronic information systems and the practice in which they are housed, while ensuring that properly authorized access is allowed.

    - Device and media controls – policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of the practice, and the movement of these items within the practice.

    - Disposal – policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

- Under HIPAA's technical safeguards, a practice must utilize technology, policies and procedures to protect electronic protected health information and control access to it. Technical controls require the practice to have:

    - Access Control – technical policies and procedures that allow authorized persons to access the electronic protected health information.

    - Audit controls – hardware, software, and/or procedural mechanisms that record and examine access and other activity in information system.

- Integrity Controls – policies and procedures that ensure electronic protected health information is not improperly altered or destroyed. Electronic measures must be in place to confirm that electronic protected health information has not been improperly altered or destroyed.

- Transmission Security – technical security measures that guard against unauthorized access to electronic protected health information that is being transmitted over an electronic network.

- HIPAA Breach Notification Rule - requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

- A breach is an impermissible use or disclosure under HIPAA that compromises the security or privacy of the protected health information.

    - Covered entities must assume that any breach is an impermissible use or disclosure of protected health information unless it can prove that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

        - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

        - The unauthorized person who used the protected health information or to whom the disclosure was made;

        - Whether the protected health information was actually acquired or viewed; and

        - The extent to which the risk to the protected health information has been mitigated.

- Notice of Privacy Practices - notice that provides a clear, user friendly explanation of individuals' rights with respect to their personal health information and the privacy practices of health care providers.

- Unsecured Protected Health Information and Guidance

    - Practices must only provide breach notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of HHS in guidance.

        - For data at rest, use encryption processes that are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.

- For data in motion, use encryption processes which comply, as appropriate, with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

- For media on which the PHI is stored or recorded, destroy in one of the following ways:

    - Shred or destroy paper, film, or other hard copy media in a manner such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

    - Electronic media must be cleared, purged, or destroyed in a manner consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI cannot be retrieved.

o HIPAA Civil Money Penalties

HIPAA Violation	Minimum Penalty	Maximum Penalty
The practice or person did not know and, by exercising reasonable diligence, would not have known that it/he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violations due to reasonable cause and not to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violations due to willful neglect and was corrected during the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violations due to willful neglect and was not corrected during the required period the practice or person liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

- HIPAA Criminal and Money Penalties

Type of Violation	Penalties	Prison
Knowingly obtains or discloses PHI in violation of HIPAA	Up to $50,000	Up to one year in prison
Offenses committed under false pretenses	Not more than $100,000	Up to five years in prison
Offenses committed with intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm.	Not more than $250,000	Not more than ten years