Study Guide: Risk and Compliance Management

Below is a brief outline for the course

It is the responsibility of the physician practice to provide a safe physical, clinical and technical environment for all visitors, staff and patients. In many instances, the safety of persons entering the physician practice has already been dictated by multiple federal and state regulations. Examples of regulations affecting staff, visitors and patients include:

- The Fair Labor Standards Act (FLSA)
- Title VII of the Civil Rights Act of 1964
- Americans with Disabilities Act (ADA)

Facilities - The safety of the physical environment affects visitors, staff and patients. One of the first areas to review is evaluation of the space for fire hazards. This includes:

- Sprinkler systems
- Active and working fire alarms
- Current fire extinguishers
- Evacuation maps which are prominently posted for all to see
- All egresses are clear
- Exit signs are adequately lit
- Emergency lighting is present and in good working condition
- There are no boxes or papers within 18 inches of the ceiling

You must also have a procedure which clearly delineates how evacuation is to take place. This should include:

- Designated staff members responsible for different parts of the evacuation
- Ensuring patients and visitors have left the space
- Ensuring staff are out of the office
- Collecting and removing any cash or checks
- Shutting down and backing up (if needed) the practice management system or electronic health record

It is imperative to have an annual fire drill so that all staff members practice their roles in the event of a fire and know what procedures they must follow. A simple acronym for a fire police is R.A.C.E.

R: Rescue individuals in the facility
A: Activate the alarm – call the fire department
C: Contain the fire – close doors
E: Extinguish if able to or Exit the facility

Likewise, the physician practice should have formalized procedures for weather-related emergencies as well as facility emergencies involving such matters as electricity, natural gas and toxic and hazardous substances.

Environmental factors also need to be closely reviewed and monitored. For example, slippery floors are a great cause for concern in physician practices, especially with patients who may already be debilitated. You will also want to review your parking lot for blind spots or areas of your building that require maintenance.

HIPAA is another area of concern with respect to safety. In this case, you are looking at safeguarding the patient’s and the employee’s health information. This takes the form of both physical means (such as keeping patient information in an area which is not visible to the general public, or discussing patient information in a private area) as well as technical means (ensuring passwords for all computers, encoding of patient-sensitive material).
The staff should be constantly vigilant for any physical factors which could present a safety risk. This includes the potential for workplace violence. If an employee perceives a threat from a co-worker, patient, visitor or superior, it is imperative that the appropriate procedure be followed. This may mean notifying a manager or, when appropriate, security or police.

**Personnel** - There are multiple federal and state laws which affect personnel. Some of the more prominent regulations include, but are not limited to, the following:

- Americans with Disabilities Act of 1990 (ADA): This act prohibits discrimination against people with disabilities in employment, transportation, public accommodation, communications, and governmental activities. It requires that reasonable accommodations for accessibility and employment must be made in public places and business, including medical practices.

- Civil Rights Act, 1964: The act prohibiting discrimination based on race, color, religion, sex, national origin, physical and mental handicaps and age. The Civil Rights Act of 1991 expanded individual protections to include sexual harassment.

- Employee Retirement Income Security Act (ERISA) of 1974: This act sets federal requirements for pension and employee benefit plans to include employer health plans. It addresses plan design issues and discrimination within a benefit plan. Employers are allowed to determine the medical costs of their own group and to self-fund the risk of employee medical costs. In addition, the act provides that the employer is not subject to premium tax or mandated benefits.

- Fair Labor Standards Act of 1938 (FLSA): The act establishing minimum wage, overtime pay, recordkeeping, and child labor standards affecting full-time and part-time workers in the private sector and in federal, state, and local governments and defining which employees are exempt from minimum wage and overtime restrictions.

- Family and Medical Leave Act of 1993 (FMLA): The act allowing employees up to 12 weeks of unpaid leave within a 12-month period for a serious health condition, the birth or adoption of a child, or caring for a relative with a serious illness. Employees are eligible if they have worked for the company or practice for more than one year, for 1,250 hours over the previous 12 months, and if there are at least 50 employees within the organization.

- National Labor Relations Act of 1935 (NLRA): Defines unjust labor practices for both employers and employees; provides mechanism for complaint hearings; and defines mechanisms through which employees can select a union. Also set up the national labor Relations Board for enforcing the Act’s provisions.

- Occupational Safety and Health Act of 1970 (OSHA): Established the Occupational Safety and Health Administration; the federal agency responsible for assuring the safety and health of workers by setting and enforcing standards and encouraging continual improvement in workplace safety and health.

- Workers’ Compensation: An employer funded, state regulated program providing insurance coverage for work-related injuries and disabilities.

**Medical Records** - Medical records can make or break a legal case. It is imperative that the physician document legibly, thoroughly and accurately the service which was provided. The medical record should document not just the therapeutic plan, but also the rationale behind the plan as well as the patient’s response to the treatment. The medical record provides an avenue for the providers to show medical necessity and complexity by documenting the clinical thought processes behind decision-making. The rule which has been upheld in courts time and time again is, “if it wasn’t documented, it wasn’t done.” The medical record must be able to stand alone as a sole reflection of the service provided.

Documentation in the medical record should include any discussions with the patient regarding test results, whether positive or negative. It should also include any discussions with other healthcare providers, educational materials which have been reviewed by the patient, telephone calls with the patient, and the patient’s compliance or non-compliance with the treatment plan.
In general, the medical record should not be altered. However, if an error has been made within the record, it should be struck out with a single line so that the writing is still legible under it, and initialed by the person making the correction. If the physician needs to make an addendum to the record, the addendum should be dated and timed at the time when the addendum is made.

Incident reports should not be a part of the medical record as these are viewed as administrative documents and may not be discoverable. However, an adverse event should be documented thoroughly within the medical record, including any treatment which was provided.

**Records Retention** - When thinking about records in a practice, one usually thinks about medical records. But, there are countless other records. Problems associated with records and information include storage, cost, the amount of time needed to sort them and potential legal issues. One must always consider privacy and confidentiality, especially under the requirements of HIPAA when dealing with records. The development of a reasonable and consistent records-retention policy is important for any practice.

The retention policy outlines how long records should be kept. The first step is to understand the records. There are many federal and state statutes that have specific retention periods for different kinds of records. Records retention may also be a condition of compliance and participation in federal and state programs. Some regulations require record keeping without mentioning how long they should be kept. When your state regulations differ from federal regulations, always keep the records for the longer period.

Statutes of limitation must also be considered when creating a retention policy. Government agencies may not require records to be stored, but the records may be essential in the case of a lawsuit. At a minimum, records should always be kept for the length of the statute of limitations. The disposition of medical and other records after a patient’s discharge, transfer or death, is also covered under state and federal regulations. The federal statute of limitations for civil penalties is six years. The False Claims Act allows claims to be brought for up to seven years after an incident and sometimes up to 10 years. HIPAA requires providers to retain authorization forms and complaint records for six years. To help preserve confidentiality, both for the patient and practice, business and clinical records should be destroyed by shredding or similar methods. If you have outstanding questions about destroying a record, consult your attorney.

- To create a records retention policy, it is advisable to consult with an attorney in your state. Keep in mind:
  - Why is the information necessary?
  - What are the legal requirements for storing the records?
  - Do they fall under HIPAA?

Establishing and maintaining policies and procedures is critical to the protection of the organization. These should cover a vast array of situations and should be reviewed annually for necessary changes. All staff should have at least annual training and updates on these policies and procedures.

Ensuring that the practice is covered by the proper insurance is another imperative when attempting to reduce your financial liability. Types of insurance you may want to consider are:

- Malpractice
- General Liability
- Property and Casualty
- Directors and Officers Liability
- Workers’ Compensation
- Employment Liability
- Environmental
- Motor Vehicle
- Business Interruption

In many cases, what you do before a legal case occurs can very much influence the outcome. For example, if you continuously perform a risk assessment, have a risk manager, have a risk committee that meets quarterly to review patient issues, and review all incident reports which are submitted, your chances for having a large settlement are much less than if you had no risk management program identified whatsoever.

Good patient relations, employee training and quality assurance programs also help mitigate risk of liability, or control the financial loss should a legal event occur.

**Policies and Procedures** - Policies and procedures need to be in place to ensure the safety of all. Moreover, the administrative and physician leadership of the practice need to be committed to upholding the policies and procedures, taking any violations seriously. Policies should include the following:

- A training manual and training schedule for all employees with respect to the standards and policies of the practice. Training should be provided at new employee orientation and should be refreshed annually for all staff.
- Designation of an OSHA safety officer. In many smaller physician practices, the responsibilities of OSHA will usually fall to the practice administrator or lead clinical supervisor.
- Provision and use of personal protective equipment where appropriate.
- Ensure appropriate care of the employee or patient in the event of an incident, then, proper follow-up documentation (e.g., incident report) and a discussion on future prevention.
- Ensure compliance with safety policies; include this information in the employee’s job description and annual performance evaluation.
- The use of checklists and logs for equipment, medications, etc.

Prevention of incidents is essential in any safety program. Prevention can occur in many different forms. It is critical that all equipment be properly maintained and tested regularly. Developing a good relationship with patients and listening to their concerns could mitigate risk of future patient actions. It is imperative to document all incidents and potential incidents and then implement follow-up action plans. In addition, providing an environment which is not punitive with respect to the reporting of incidents enables a practice to truly view risk potential with a critical eye.

**Insurance** - In any physician practice, insurance coverage with the appropriate type and amount of insurance is paramount. Determining which type of insurance is needed, however, can be an overwhelming task. If you are not an expert in insurance, it is important to build a relationship with someone who can help you to determine the appropriate type of insurance, the amount of insurance required, and whether self-funding is an alternative to commercial insurance.

One option is to look to consult with an insurance broker. An insurance broker reviews the physician practice and determines its needs. The broker then reviews the various policies that are available in the insurance market, and chooses the option which is the best fit for the practice. In the process of performing the review, the insurance broker, with your assistance, will perform a risk/benefit analysis. This ensures that those areas which are the highest risk for legal action are covered appropriately by the insurance.

**Risk Management Program** - One way to reduce the impact of exposure to legal events is to have a documented risk management program. A solid program includes risk assessments that are reviewed by a risk manager, who then implements an action plan for those issues that have been identified. Also, the minutes of quarterly risk committee meetings that indicate the committee’s knowledge and input on identified issues, help to show that the physician practice takes its risk management responsibilities seriously.
The risk manager should be responsible for not only reviewing risk assessments, but also investigating every incident report, patient complaint and employee grievance.

Peer review of medical procedures by physicians is another way to mitigate the risks of litigation. This indicates the practice has a culture that focuses on quality patient care.

**Personnel Training** - Personnel should be thoroughly trained on providing patients with an experience that exceeds their expectations. Customer service applies to everyone in the practice - telephone staff, front desk receptionists, clinical staff, billers and physicians. Patients tend not to sue the people they like. If you can put a good face on the physician practice, it will reduce the risk of legal action in the event of an adverse result.

In addition, staff should be knowledgeable about “no tolerance” policies and procedures. They also should be made aware of the “chain of command” with which to report such occurrences. Just as with patients, a culture of caring, acceptance, and treating each person as an individual, will help mitigate any potential legal events regarding personnel policies.

**Public Relations** - Establishing an excellent relationship with patients is critical in reducing the risk of litigation. When patients feel as though they are being cared for and listened to by the entire staff and physicians, they are more likely to forgive untoward results or events.

The relationship should begin with communication. Patients should be notified of what to expect during their visit at the physician practice. If a physician is late, the patient should be told this upon checking in and then given the option to wait or to reschedule. If payment is expected at the time of service or if the patient has any outstanding balances, this also should be communicated to the patient as well as the method of payment accepted. All procedures, regardless of how minor (e.g., taking vital signs) should be communicated to the patient. Although you and your staff may know the routine throughout the office very well, the patient does not and needs to be guided so as not to feel uncomfortable in the situation.

Any time informed consent is required, the patient should be very clear as to the risks involved in the procedure. In this manner the patient has forewarning as to what may occur as a result of the procedure. Informed consent should include the most frequent or severe risks as well as any risk which may become more likely due to the patient’s physical condition. Alternatives should also be discussed. The discussion of the informed consent must be clearly documented in the patient’s medical record, including what was discussed and whether the patient verbalized an understanding of the risks and alternatives. Again, if this is done consistently with all patients requiring informed consent, it will show the culture of the physician practice to be one of quality care.

**What to Do if You Get Sued** - In the event that you are contacted about a pending lawsuit involving a patient, you should first pull the medical record, make copies of it, and secure the original in a locked area where it cannot be tampered with. No changes should be made to the original medical record after a legal action has been initiated.

The risk manager should be notified immediately to pull any incident reports or meeting minutes regarding this patient. In addition, your attorney and malpractice carrier should be notified of the lawsuit. The attorney may have additional requirements, including, but not limited to, speaking with the physician and any staff who have been involved, reviewing the medical record, and reviewing the malpractice insurance policy (or whichever insurance policy would cover the untoward event if it does not involve medical malpractice).

In many cases, the attorney will want to settle out of court in order to reduce the costly nature of a trial. If the case goes to trial, half of the claim may be for legal costs. Arbitration may be less costly than incurring the legal bills associated with a trial.
Establish a Plan for Disaster Response and Recovery - Disasters to physician practices can occur from many different sources and can be internal or external. A disaster is considered any type of scenario which prevents the practice from functioning in a normal manner. Recently, several disasters have brought into focus the necessity for physician practices to have a disaster recovery plan in place: the terrorist attacks of September 11, 2001 on the World Trade Center in New York City, Hurricane Katrina of August 23, 2005 in the Gulf Coast and Hurricane Sandy of October 22, 2013 on the East Coast. Examples of internal disasters include, but are not limited to:
- Fire
- Burst pipes
- System or computer failures
- Labor strikes
- Computer viruses

Examples of external disasters include, but are not limited to:
- Weather-related shut-downs
- Transit labor strikes
- Electrical power outages
- Epidemics or pandemics
- Massive wild fires
- Acts of terrorism

The establishment of a disaster recovery plan should involve several steps:
- Determine which areas of the physician practice are at greatest risk in the event of an internal or external disaster.
- Perform a business impact analysis.
- Develop a disaster response and recovery plan.
- Test the plan frequently.
- Update the plan at least annually.

Determining Areas of Risk - Where is the physician practice at highest risk during a disaster? The answer to this question will change depending upon the type of disaster. For this reason, you may be developing several different disaster recovery plans for a variety of situations.

The first order of business in any disaster is to ensure that patients are safe and cared for. That said, you have other factors to consider. Employees may face very real personal losses during this time. Ensuring that personnel are well cared for is also a priority. This includes psychological, financial and physical safety. In addition, it may also be necessary to ensure the safety of the employee’s family so that the employee can concentrate on the job at hand.

It's also important to review the financial aspects of the physician practice. How long can a practice close its doors without having the influx of revenue? Every day that a physician practice is closed means lost revenue.

A disaster recovery plan must take into account all aspects of the physician practice: communications, personnel (including who holds what knowledge), finances and the actual facility.

Performing a Business Impact Analysis - A business impact analysis will enable you to determine which functions and processes are the most critical to bring back up quickly in the face of a disaster. In other words, what is the critical path for each of the possible disasters identified?

For example, if a physician practice has a devastating fire which guts the entire facility it becomes critical to find an alternative location in which to begin seeing patients. If a medical group uses a practice management
system for scheduling and its computers go down, it becomes critical to have a plan that includes some type of paper back-up.

Through this process, you will be able to define priorities and determine the impact on all aspects of the business. Again, depending upon the scenario, this could mean loss in personnel, loss of the facility, loss of equipment or loss in communication.

**Developing a Disaster Response and Recovery Plan** - In developing a disaster response plan, you must clearly delineate the step-by-step protocols which should be followed. This should include the personnel responsible for the task, as well as back-ups for those personnel in case the primary employee is unable to assist with the task. In addition, time frames and equipment requirements need to be identified.

Below is a sample of questions which should be addressed in the policies and procedures within a disaster plan. Several different situations should be considered when developing the plan. For example:

- What will happen to the physician practice if you need to evacuate immediately?
- Do you have personnel identified along with their responsibilities for ensuring that all of the patients are no longer in the facility?
- If you perform procedures, how will you ensure the safety of the patients in those situations?
- If you have cash, checks or credit card receipts at the front desk or business office, who is responsible for ensuring that they are removed?
- What happens to the computers or servers?
- Is there a protocol in place for shutting them down or having them backed up on a nightly basis in an off-site location?
- Do you have a location off-site for employees to meet following an emergency?
- Do you have a chain of command if key personnel are unable to perform their duties?
- Do you have an alternative facility which could be used as a back-up?
- If you need to obtain equipment quickly, do you have vendors who can respond immediately to your needs?
- Which functions within your office can occur with limited equipment and which require an immediate replacement?
- Do you have an inventory of your equipment (including receipts, pictures and videos) off-site to provide to your insurance company?

**Questions with respect to communications:**

- Do you have a list of contact information (home telephone numbers, cell phone numbers, e-mails, work phone numbers) for all staff, physicians, vendors, insurance agents, bankers, and payroll?
- Do you have at least one line within the practice which is not affected by a power outage?
- Can your answering service serve as a call center and communicate directly with you in the event of a disaster?
- Is your answering service located within the same geographic region as you so that if your phones go out, theirs will as well?
- Do you have a phone tree for communicating with the staff?

**Questions with respect to finances:**

- How will patients be able to pay their co-pays and balances due if the computers are down?
- Is there a fire-proof and water-proof safe for key financial records?
- Is there a duplicate of key financial records kept off site?
- How will you provide for payroll in the event of a disaster?
- Do you have copies of your managed care contracts off-site?
- Do you have copies of your insurance policies off-site?
- Do you have business interruption insurance?
- Exactly what does your insurance cover?

Questions related to technology and records:
- Do you have a list of other healthcare providers in your area that could provide you with information regarding your patients (pharmacies, hospitals, other physicians)? (Many practices still have paper charts.) Because you need this information in the provision of patient care, you are not in violation of HIPAA and therefore are not required to obtain an authorization for release of information from the patient.
- Do you have a list of passwords for the computers in an off-site location and with more than one key personnel who is knowledgeable about them?
- Do you have back-up for some of your other business functions such as transcription, financial statements, accounting systems, or clinical / research databases?

Testing the Plan
- In testing your disaster plan, you will want to test it for various individual scenarios, rather than trying to test all possible scenarios at one time. You will want to ensure that key personnel within the practice take part in the test. In addition, you will want to walk through the test for certain situations with your banker and insurance agent to ensure that you have addressed critical issues from their standpoint as well.

Updating the Plan
- The disaster response and recovery plan should be reviewed at least annually or when there is a change in key personnel. In addition, any changes to contact information should be updated immediately as they occur. The plan should be reviewed in-depth with the staff at least on an annual basis. Each staff member should be aware of their critical role in the event of a disaster, and should practice it at least once per year.
- The diligence required to keep the plan current may seem burdensome in light of all of the other responsibilities you may have, but it will be invaluable in the face of a true disaster.

Purpose of a Compliance Plan
- The purpose of a compliance plan is to define the legal and ethical conduct of employees and to:
  - Provide a mechanism to detect, correct and/or prevent possible violations
  - Promote and create awareness across the organization about the importance of compliance
  - Prevent fraud, abuse and waste
  - Scope of a Compliance Plan

The corporate compliance plan should identify the entity that it applies to, including the group and any legal entities owned by the group or its partners. Examples might include a building corporation, joint-venture arrangement and a diagnostic center.

**Developing Policies and Procedures** - Any physician practice must have policies and procedures to allow the compliance plan to become operational. Areas to be addressed in the policies and procedures include:
- The role of the compliance officer
- The training and education required for both new employees at orientation and ongoing annual training
- Monitoring (routine checks and balances) and auditing (a more formal review and analysis) of systems to detect when breaches in the policy or procedures have occurred. For example, you can perform periodic record reviews, spot checks of logs used, review of reports, and so on.
important in the auditing and monitoring process that steps are clearly defined and results detailed. In addition, any action plans developed to correct issues must be documented.

- Plan enforcement and the steps the practice will take to discipline staff and physicians who do not comply (i.e., a disciplinary process).
- The communication plan for reporting issues which have been uncovered
- The process whereby an employee, visitor or patient can bring to light an issue (either anonymously or identified) without fear of retaliation or retribution
- A grievance procedure for employees
- The process by which an uncovered issue is investigated. This could include an internal review as well as hiring an objective outside party, such as a consultant or attorney, depending upon the magnitude of the issue
- Background checks and reference checks for any potential candidate for employment within a practice, including physicians and staff. This includes checking the state medical board for sanctioned physicians
- Conducting risk assessments. A physician practice must continually review its potential for risk in all areas of the practice. These issues can be revealed through formalized processes such as patient satisfaction surveys or benchmarking of billing data. Anonymous tips from inside or outside the organization or complaints from patients or employees are also legitimate sources for assessing risk.

**Compliance Officer** - Every organization should have an individual who serves as the corporate compliance officer. This person is responsible for assuring that the entity complies with the law. The duties and responsibilities of the compliance officer are considerable and should include:

- Overall leadership of the compliance program
- Ensuring compliance with state, federal and local regulations
- Evaluating and investigating issues brought to them
- Conducting timely, thorough investigations and, when necessary, corrective actions
- Developing and assuming responsibility for maintaining current policies that pertain to compliance
- Conducting and directing audits to monitor performance and adherence to the organization’s compliance plan
- Providing forums for training and education of staff and physicians
- Maintaining knowledge of current state, federal and local regulations that affect the operation of the medical group

**Education and Training** - It is the responsibility of the compliance officer and organization’s leadership to see that all employees have compliance plan training. The compliance officer should ensure that:

- All employees receive a copy of the plan
- All employees learn about changes to the plan on an ongoing basis.
- New employees participate in an orientation program that includes training on the compliance plan
- All employees sign an acknowledgement that they have received the information about the compliance plan
- All employees reaffirm their knowledge of the plan and again sign an acknowledgement

The compliance plan should be maintained with the organization's policies and procedures. If available, the compliance plan should be posted on the organization's intranet site.

**Compliance and Standards of Conduct** - This section outlines the daily actions of employees. Generally, compliance standards incorporate brief descriptions of prohibited conduct and legal violations. Examples include:

- No employee shall make or receive payments regarded to referrals
- No employee shall knowingly submit claims for health care services that were not appropriate or provided
- No employee shall participate in any scheme intended to defraud payers or any government agency
- No employee shall make false statements regarding claims for payment
- No employee shall falsify or conceal facts that pertain to a potential issue or violation
- Employees shall not knowingly retain funds paid for services that were not appropriate or not provided
- No employee shall retaliate against another employee who reports a potential violation that results in an investigation

**Compliance Procedures** - A process to report suspected violations needs to be incorporated in a compliance plan. This process should be clear, and employees should know to whom they need to report violations. Typically, these individuals would include:

- Immediate supervisor
- Senior administrative staff or officer
- The organization’s designated compliance officer
- Corporate counsel

In a larger setting, an organization should consider establishing a compliance hotline. The number and information about the line should then be made available to all employees. If an organization has evening or weekend hours, leaders may need to consider other individuals who might be appropriate to take the calls or reports from employees. Ultimately, all issues should be reported to the organization’s compliance officer. This individual assumes responsibility for any investigation, follow-up and corrective actions.

**Employee Responsibility** - All employees of the organization are required to abide by the compliance plan and any associated policies. Employees have a duty to report possible violations and cooperate fully with any investigation. In addition, employees need to be familiar with the contents of the compliance plan and participate in all educational programs as offered.

**Monitoring and Auditing** - The compliance officer establishes a plan to monitor and audit the performance of the organization as it pertains to the compliance plan. Some audits may be ongoing. Others may be periodic, based on changes in regulations or the operations of the organization. Any such review should be directed by the compliance officer. Depending on the size and the structure of the organization, all findings should be reported to the compliance committee and the organization’s governing body. Problems and appropriate corrective actions may require additional expertise in the form of legal counsel.

**Corrective Action** - If an audit or investigation determines corrective actions are necessary, the compliance officer should be responsible for:

- Responding to all pertinent parties
- Reporting findings to the compliance committee, governing body and other leaders
- Serving as the contact/point person, in conjunction with legal counsel, state or federal officials
- Developing a plan to correct issues, time lines for doing so, and assigning responsibility for the plan's implementation
- Ensuring the corrective actions are implemented by appropriate individuals
- Implementation of a Compliance Plan

The implementation of a compliance plan requires acceptance and commitment from the senior leadership of a practice, including the physicians. Aside from having policies and procedures in place, extensive training will need to occur for all levels of employees. Implementation may require a change in culture which can be difficult for employees to accept. Therefore, it is important for you to have a change management plan as well.

The practice may lose some of its employees who are unable or unwilling to adopt the necessary procedures required for the compliance plan. Difficult decisions may need to be made by senior leadership with respect to some employees.
Change is never easy for a business. However, adopting a culture of no tolerance for harassment, discrimination, and other personnel-related issues as well as for questionable patient safety practices will greatly reduce your risk of liability. In the end, it will also make for a better work environment for employees and an atmosphere that promotes quality care.

Objectives (Self check):
- Develop and implement a risk management plan for the practice.
- Discuss which areas of the practice that require a risk management plan.
- Define a plan for the physical records.
- Define a plan for personnel.
- Identify the applicable regulations.
- Discuss the plan for medical records.
- Discuss what should be included in a medical record.
- Identify how record retention fits into the plan.
- Identify the statutes of limitation.
- Implement policies and procedures to manage the impact of adverse legal actions.
- Review the practice’s insurance and ensure proper coverage.
- Identify possible insurance types.
- Create a risk management plan.
- Identify a risk manager.
- Define a training program for personnel.
- Discuss the procedure if the practice is sued.
- Create a plan for damage control and recovery.
- Determine risk areas in the practice.
- Perform a business impact analysis.
- Develop a recovery plan.
- Define recovery areas.
- Design a compliance program for federal and state law requirements.
- Determine the purpose and scope of the compliance program.
- Discuss compliance specific policies and procedures to implement.
- Identify a compliance officer.
- Discuss the importance of a compliance officer.
- Discuss the items included in standards of conduct policy.
- Define the parts included in the standards of conduct policy.