BODY OF KNOWLEDGE REVIEW SERIES

Risk and Compliance Management

MGMA®

MEDICAL PRACTICE MANAGEMENT
Body of Knowledge Review

3.5 Edition

RISK AND COMPLIANCE MANAGEMENT

VOLUME 5

MGMA
104 Inverness Terrace East
Englewood, CO 80112-5306
877.275.6462
mgma.com

MGMA
Medical Group Management Association®

Body of Knowledge Review Series - Edition 3.5

Volume 1: Operations Management

Volume 2: Financial Management

Volume 3: Human Resource Management

Volume 4: Organizational Governance and Patient-Centered Care

Volume 5: Risk and Compliance Management

Library of Congress Cataloging-in-Publication Data
Names: MGMA (Association), issuing body.
Title: Risk and compliance management.
Other titles: Medical practice management body of knowledge review (3.5 edition) ; v. 5.
Description: Englewood, CO : MGMA, [2019] | Series: Medical practice management body of knowledge review (3.5 edition) ; volume 5 | Includes bibliographical references and index.
Identifiers: LCCN 2019047363 (print) | LCCN 2019047364 (ebook) | ISBN 9781568296999 (paperback) | ISBN 9781568297002 (ebook)
Subjects: MESH: Risk Management | Practice Management | Program Development | United States
Classification: LCC R728 (print) | LCC R728 (ebook) | NLM W 80 | DDC 610.68--dc23
LC record available at https://lccn.loc.gov/2019047363
LC ebook record available at https://lccn.loc.gov/2019047364

Item: 1029
ISBN: 978-1-56829-700-2

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents

Introduction

Risk and compliance management is not a new concept in medical practices. However, there's still a lot of uncertainty on the depth, breadth, and scope of work needed to maintain an effective compliance program. And while many of the same regulations and skills are required for managers in any organization, there are particular nuances specific to the delivery of healthcare in a clinic setting that differentiate the medical practice administrator from his or her peers in other business or healthcare delivery environments. The chapters in this volume follow the blueprint designed by practicing medical practice executives to describe the key competencies, knowledge, and skills required to develop and maintain effective operations in the medical practice.

The major areas of competence in risk and compliance management, as identified by the certified and fellow members of the Medical Group Management Association, are to:

- Create, implement, and maintain a risk management program to provide a safe environment;
- Develop, implement, and maintain policies and procedures to prevent or minimize the impact of adverse events;
- Develop, implement, and maintain a compliance program for federal and state laws and regulations; and
- Comply with necessary accreditation and licensure requirements.

Within each chapter of this volume, these major competencies are further delineated according to the key knowledge and skills required to demonstrate competency as a manager of risk and compliance. A few examples of these supporting skills are the ability to plan for disasters, mitigate and minimize the impact of legal events, provide a safe workplace, and remain in compliance with laws and licenses. These knowledge and skills and many others are explored in detail in the pages that follow.

Chapter 1

Risk Management for a Safe Workplace

Creating a Risk Management Program

Risk management is essential to protect the assets of your organization.[1] These assets include the tangible financial assets as well as the intangible assets of lost opportunity, loss or diminished capability of personnel, loss or diminished usability of property, and loss of reputation and community trust.

Historically, risk management in healthcare has focused on losses incurred solely through medical malpractice.[2] In recent years however, the focus has moved from clinical risk management, concentrated on losses directly related to clinical care, to a broader perspective. This perspective, known as *enterprise risk management*, considers all aspects of the organization's function as integrated components of overall loss exposure.

In this framework, *risk* is synonymous with *capital*. Risk exposure is therefore a direct potential loss of capital. Capital losses can come from operational exposures, financial risks, human capital risks, strategic risks, legal exposures, and technological risks.[3]

Given that risk management cannot be relegated to a set of specific pieces of information but must be examined by parts of the process, this

volume first examines the risk management process and then addresses the related skills and tasks.

The Risk Management Process

To fully appreciate the ramifications and breadth of issues involved in risk management, it is essential to understand the risk management process, which has four essential components:

1. **Risk assessment and analysis**, which is the identification and analysis of exposures;
2. **Loss control**, which is the identification and selection of potential mechanisms for addressing those exposures;
3. **Risk financing**, which is using selected techniques, including financing, for failed control of losses; and
4. **Monitoring,** which means the continuous observation of selected methods for controlling losses for potential improvement.[4]

These components, applied to financial, human, operational, technological, and strategic areas and property across all aspects of the organization, create the constellation that defines the organization's risk management program. They are all related to the executive's ability to assess risks.

Risk Assessment and Analysis

Medical practice executives must ensure that they are aware of all potential risk exposures. As James Reason discusses in his book *Human Error*, every process contains latent errors, many of which are identified as such because our systems rely on consistently perfect human activity.[5] In fact, many processes depend on constant human vigilance and omniscient foresight to prevent all errors. Examples on a grand scale include the lack of coordination of resources early in the tragedy of September 11, 2001, and the disorder that resulted in the loss of lives and chaos after Hurricane Katrina.[6]

On a smaller, but more relevant scale to all practices are the preventable failures that result in medication errors, fires on site, staff member injury, failure of service initiatives, or loss of business productivity as the result of technology failures. In each of those circumstances, the blame is often laid on the person who "didn't follow the policy" or "didn't pay close enough attention." In fact, processes without risk control mechanisms to counter the human factor are fraught with latent errors.

The opportunities for error are frequently aligned through serendipitous occurrences or through a series of small human errors that can ultimately result in devastating outcomes and losses. Reason's Swiss cheese model, often quoted in patient safety literature, is applicable to all aspects of an organization's processes and activities. The alignment of any number of process *holes* can result in risk management exposures. The key is to find and correct those exposures before losses occur.[7]

Risk Control Processes

The most exhaustive way to identify potential exposures in complex systems is through a process, such as a Failure Modes and Effects Analysis (FMEA). This process, which gained popularity through its use in engineering, is designed to examine every step of a process and identify the myriad of ways in which each step could fail, as well as the potential for that failure to be stopped.[8]

Unfortunately, process tools such as FMEA are limited by resources. Such analyses take time. Obvious loss-potential areas may justify the dedication of human capital for this type of intensive analysis. Nonetheless, many processes have the potential to root out problems that will cause equally devastating losses. How then does an organization prioritize the processes that should be reviewed?

Information on exposures that have high loss potential can be gathered from a number of sources. The organization's insurance claims and malpractice loss run reports are basic sources of information. Complaints from patients and/or staff members are another fundamental source of information. Formal risk assessments by outside consultants, self-assessment questionnaires, literature reviews, and insurance

application forms also provide exposure identification. Furthermore, by examining the questions on the insurance application or survey forms, the medical practice executive can ascertain which processes are perceived as high risk by insurers and other surveyors. Finally, by using a simple but effective technique, staff members can list the various processes in each department and then ask "What can go wrong?" for each process. If answered honestly, it will be apparent from the list where loss control mechanisms might be useful.

Loss Control

The next step in the risk management process is to analyze the data and identify the tools that will reduce either the frequency (loss prevention)[9] or the severity (loss reduction)[10] of losses. The potential losses prime for application of these techniques are: (1) those that occur frequently even though the cost per loss may be small (e.g., missed appointments or employee unplanned absences); and (2) those that occur infrequently but are more costly per loss (e.g., medical malpractice claims or equipment failures).

Furthermore, any process that relies heavily on human compliance with complex procedures (or procedures in a complex environment) is subject to great variability and potential error.

Areas in any process that present high variability or high potential for loss should be addressed first. Potential methods to address these issues can be found in the industry literature or through insurance or business consultants.

The key point to remember is that loss control methods are not uniformly applicable in all situations. The unique location, culture, and characteristics of each organization may render a solution a potentially bad fit. Consequently, each solution must be analyzed for its potential latent failures in the given situation.

Risk Financing

Most executives are familiar with the risk-financing vehicles of commercial insurance and self-insured vehicles, such as captives, risk

retention groups, and trusts. What many executives may not fully appreciate, however, is that commercial insurance, although more costly, is effectively a contractual transfer of risk.[11] The risk of loss belongs to the insurer. Consequently, the risk of financial devastation through catastrophic events is minimized for the organization.

The downside to risk transfer is that the insurance company maintains control over what will be covered and retains the ability to increase premiums. Furthermore, the premium paid by the organization is not based solely on the organization's history nor specifically on its loss control efforts but on an aggregate of similar organizations with combined loss experience. Of course, some attention is paid to the organization's specific loss history; however, the cost of overhead and need for margin to the insurance company sometimes outweigh those benefits.

Risk transfer is not bad. For forms of losses that are unpredictable and potentially costly (e.g., automobile, directors' and officers' liability, employment liability, property, key person), commercial insurance is the standard and probably most cost-effective form of risk financing. The organization hopes to never need it. Nonetheless, it would be extremely difficult to predict ultimate losses and to plan for setting aside sufficient funds to cover these losses should they occur.

Self-insurance vehicles are best when there is a known frequency and consistent value of typical losses.[12] The organization must have sufficient funds or reserve set aside to cover those losses. Self-insurance vehicles tend to be less expensive to administer and offer the organization more control over the loss control mechanisms and their effect on the premium.

In addition, there are losses that occur infrequently but result in such large losses that it is better to cover them with more structured forms of risk financing. For minimal losses or extremely infrequent losses, risk financing might include loans, nonfunded reserves, or even payment from the operations budget.

Given the variety of options for risk financing, it is essential that the medical practice executive understand the full array of potential risks faced by the organization and plan accordingly for failure in any arena. Does the organization have a plan to respond to a disaster that affects all technological equipment? Is there a plan should delivery of medical supplies be cut off? Is there a contingency for a loss of water or electricity, for a contagious illness reducing the availability of staff members to care for patients, or for severe weather resulting in patients and staff members being forced to remain in the building for days? What is the plan should an intruder hold staff members hostage, threaten patients, or disrupt the practice in other ways? The number of risks that must be provided for and covered both through procedures and possible risk-financing mechanisms is seemingly unlimited.

Monitoring

Controls that a medical practice puts in place to reduce risk must be continually monitored to see if they are succeeding in reducing the risk. As new controls are implemented, the administrator or risk manager needs to look at each risk and evaluate it. This is an ongoing process that will help determine if controls that are put into place are effective at reducing the risk. Audits are also another way to determine if a risk control is effective. Audits are potent tools to use in areas like staff training. An audit can be performed to see if the safety training for all required users of a piece of equipment was proven effective.

Planning for Safety

Introduction to Employee Safety, Health, and Security

Employers realize the importance of occupational health and safety programs in maintaining a productive and highly efficient workforce. The cost of unsafe and unhealthy conditions in the workplace is substantial considering the lost productivity caused by accidents and illness. In addition, the cost of healthcare benefits to the employer continues to rise, contributing to higher health insurance costs when

employees are injured. The cost of providing safety and training programs is low when compared to the cost of employee accidents, injuries and illnesses, and workers' compensation claims.

More important than the economic aspect of health and safety is the employee's right to work in an environment that does not pose a health hazard or an unreasonable risk of injury. No employer wishes to see anyone harmed by the group's everyday operations, but failure to establish and enforce strict health and safety policies may unintentionally encourage careless practices.

Today, the rise of worldwide disasters and the possible risks to healthcare workers and patients make such policies even more critical.. Issues related to significant exposure to blood, body fluids, and tissues must be addressed, as well as exposure to contaminated needles, instrument punctures, and lacerations. Another growing concern is exposure to hepatitis B and the need to administer the hepatitis B vaccine to those employees involved with direct patient care and specimen handling.

Finally, employers have become aware of the importance of protecting the environment, community, and society in which they work. Employers realize that they are a part of the community and must take a role in protecting and enhancing that community. A record of occupational health and safety problems is a detriment to the employer's image and place within the community.

Employee Safety Laws

The Occupational Safety and Health Act of 1970 (OSH) was passed in part to address some of the inadequacies that were thought to exist in state workers' compensation laws. The law encourages employers and employees to work toward reducing the number of hazards in the workplace. It also stimulates employers and employees to develop new programs, or revise existing ones, and to provide safe and healthful working conditions.

OSH requires that every employer covered by the law provide employees with a place of employment that is free from recognized hazards to life or health. The act further provides that each employee comply with all standards, rules, regulations, and orders issued by the employers to comply with the law.

An employer covered by the act is defined as any person or business who has employees and who is engaged in interstate commerce. The act provides for civil and criminal penalties for violation of the law or regulations issued thereunder.

Numerous state and local regulations also affect health and safety in the workplace. The medical group should be aware of these laws and conform to them.

For customizable policies on exposure control and hazard communication, please refer to the Medical Group Management Association's book, *Operating Policies and Procedures*.[13]

Delegating Safety Responsibilities to an Individual

Most small medical groups choose to select an individual to be responsible for safety in the workplace. Larger medical practices may appoint a safety officer for this role. Regardless of the organizations size, management should develop a comprehensive safety program suited to the group's particular needs and enforced by the compliance or safety officer.

Much of safety and health compliance relies on providing educational safety and health training programs; training programs must be in place and mandatory. A safety committee responsible for all safety and health programs and safety incentive programs are other ways to ensure compliance with regulations. Employees who do not follow the safety policies should be properly disciplined to ensure that safety regulations are followed.

Finally, safety has become an overriding concern in healthcare institutions because they may have patients who are incapable of helping themselves in emergencies. Fire is one of the most dangerous

emergencies in this regard, so a fire plan should be included in the policy manual, and fire safety training should be provided for all employees. Other areas to consider in the safety policy are:

- On-the-job injuries;
- Accident and injury reports;
- Medical emergencies;
- Posting of emergency information;
- Evacuation plan;
- First aid equipment;
- Weather-related alerts;
- Care and use of equipment;
- Violence and terrorism threats;
- Bomb threats;
- Protective clothing;
- Safety inspections;
- Reporting of unsafe conditions;
- Firearms;
- Safety designated areas;
- Safety suggestions; and
- Incentive award programs.

Employee Security

Because of vandalism, pilferage, thefts, bomb scares, terrorism, and major incidences of workplace violence, most group practices realize that securing their facilities has become very important. For example, the theft of business equipment, especially small items, has greatly increased in recent years and is costly to employers. As terrorism and workplace violence continue to affect the lives of employees and employers, security programs have become a priority.

Security programs involve taking precautionary measures to ensure adequate protection of the group practice's property and assets, as well as that of its employees. Many healthcare managers have written and unwritten security rules that range from "the last one out locks up for the night" to contracting security firms for surveillance. A group practice's security needs vary depending on its location, the nature of

its operations, and the number of employees. Some larger groups hire security consultants to develop and administer their security programs.

A typical security program requires all employees to wear identification (ID) badges while at work, which helps prevent unauthorized entry and possible theft. Secured doors to authorized-only areas may involve coded or card locks. More sophisticated security techniques include motion sensors, video surveillance, spot inspections, fingerprint scans, retina scans, or security guards on site. Clearly visible ID badges help to quickly identify unauthorized people on medical group property and help prevent acts of terrorism.

Workplace Violence

Workplace violence is a very real threat in our daily working lives. In 2013, workplace violence accounted for about 17 percent of on-the-job deaths, while the cost associated with those injuries was incalculable.[14] According to the Bureau of Labor Statistics, there were five homicides in the healthcare sector in 2013, with four of those happening in physician offices.[15]

Most attackers and harassers are people the victims deal with on a daily basis. Coworkers and supervisors account for most of the harassers at work; customers, clients, and patients account for the largest group of attackers at work. Typical perpetrators of workplace violence are bitter, dissatisfied people who make threats of violence. Other types include:

- Frustrated employees who are shuffled from low-level tasks to even lower-level tasks;
- Frustrated professionals;
- Those who refuse to accept blame for their own problems;
- Those with pent-up rage;
- Those experiencing substance abuse;
- Those experiencing extreme stress in their personal lives or with their jobs; and
- Those with little or no support systems, such as families or friends.

Characteristics of at-risk work environments include group practices with:

- A strict authoritarian management style;
- Numerous grievances filed;
- Many disciplinary actions and/or terminations;
- Inconsistent, inequitable, or insensitive management;
- Chronic labor-management disputes;
- Multiple injury claims;
- Frequent layoffs and downsizing;
- Disgruntled employees;
- Interpersonal conflicts on the job; and
- Failure to recognize and intervene early in the cycle of violence.

Although this list is not exhaustive, it does illustrate typical factors associated with workplace violence. Experts warn that in most cases where violence has occurred, there were indicators of potential or impending violence before it actually happened. Ineffective or incompetent management contributes to workplace violence by *failing to*:

- Promptly respond to pre-employment warning signs or clues of future violence;
- Admit that a potentially violent situation has occurred;
- Follow up after warning behaviors;
- Communicate an expectation of self-control to the involved employee; and
- Convey that the employee will be held responsible for his or her inappropriate and unacceptable behavior.

The emotional and psychological toll on employees subjected to workplace violence can be devastating. Three out of four workers who have experienced workplace violence report having suffered psychological and emotional distress. As a result, an employer's work effectiveness and productivity may be severely damaged. In addition to physical and emotional costs, workplace violence can have a dramatic effect on an employer's financial resources. Workplace violence also affects workers'

morale and productivity, increases absenteeism, promotes worker turnover, and raises costs for security and workers' compensation.

Risk Exposure Monitoring

Time changes all things. The methods and procedures that work at one time can suddenly no longer fit the organization's practice. The challenge is to remain attuned to the influence of organizational change on loss control methods. Once a method of loss control is chosen, the tendency is to be so hopeful it works that signs of it not working are ignored. Regular monitoring and reevaluation of all loss control methods are therefore a crucial component of risk management.

Standardized times should be scheduled for review of written policies and procedures as well as actual processes as performed in the organization. This ensures that the organization regularly updates all aspects of its risk management program.

Tips for Minimizing OSHA Violations in Your Medical Practice

While daily complaints from employees in your medical practice may not always refer to Occupational Safety and Health Administration (OSHA) violations, it's still important to intervene before OSHA gets involved. These 10 tips will help you enforce OSHA standards in your group practice:

1. **Add OSHA managerial duties to your job description.** As your practice's OSHA safety officer, you need time to accomplish your duties, so it's important that your job description include OSHA responsibilities.
2. **Make sure everyone understands that you wear the OSHA hat.** Encourage staff to bring safety concerns to your attention. Be the go-to person for safety advice and leadership.
3. **Take all complaints seriously.** Keep an open door and open mind to all safety concerns, even if you don't think they're justified. Employees often call OSHA when they

believe management isn't listening. Handle minor issues before they escalate into major problems.

4. **Document everything.** At inspection or incident investigation time, if it wasn't written down, it didn't happen.
5. **Consider safety a value rather than a priority.** Business priorities change over time, but values endure. Since the needs of the moment determine business priorities, safety might not always hold a place at the top of the list.
6. **Make safety compliance a requirement in each employee's job description.** Discipline employees who purposely don't comply. First, document the problem. Then speak with the employee. If the problem persists, document the incident and inform the supervisor. For serious cases, approach senior management and consider termination.
7. **Manage by walking around.** This well-known approach lets you learn if employees merely give lip service to OSHA regulations.
8. **Make annual OSHA training applicable to your practice.** Preview videos and identify areas where you can use examples from your practice to reinforce the education. Keep employees involved; have them voice opinions or demonstrate techniques.
9. **Keep your cool.** Manage OSHA tasks using monthly and annual checklists to organize your duties. Listen to employee concerns, but don't take safety-related criticisms personally.
10. **Remind organizational leaders of the benefits of OSHA compliance.** Part of managing your practice's OSHA safety program is quantifying its contributions, which are fewer injuries, less downtime, reduced workers' compensation claims, and improved employee morale.

Complying with the Hazard Communication Standard

The goal of the OSHA Hazard Communication Standard (HCS) is to "ensure that the hazards of all chemicals produced or imported are evaluated and that information concerning their hazards is transmitted to employers and employees."[16] You can communicate the information through a comprehensive hazard communication program, which should include container labeling and other forms of warning, safety data sheets (SDSs) (formerly material safety data sheets), and employee training.

Information and training are the core elements of a hazard communication program, which is intended to prevent illness or injury from chemical exposure. Training should include education about the HCS, hazardous properties of all chemicals in the workplace, and methods of protection to ensure a safe work environment. Each employee should comprehend and understand the risks associated with any potential exposure.

The hazard communication program is a written plan that describes how an employer will implement and comply with the HCS. This plan will be the initial focus of an investigation if an OSHA compliance officer conducts an inspection and should include a complete list of all potentially hazardous chemicals in the workplace, corresponding SDSs, how the SDSs will be maintained and accessed, and documentation of training and education on labeling use and SDSs.

Each employer must have a designated OSHA compliance officer who is responsible for maintaining an up-to-date list of all hazardous chemicals in the workplace and current SDSs on each of the chemicals in the office. The compliance officer should also determine if the chemical containers are properly labeled and updated.

Employees should know where to access SDSs in the workplace. Detailed procedures for purchasing, receiving, storing, and handling chemicals should be readily available. When a new chemical is introduced in the workplace, employees should be educated about the chemical before it is used. Training can be performed on individual

chemicals if only a few chemicals are used in the workplace or by hazard categories if there are several chemicals.

Medical group practices can learn more about the HCS in *Hazard Communication*,[17] a guide published by OSHA. Exhibit 1.1 is an HCS compliance checklist that can be used in your medical practice.

Exhibit 1.1
Hazard Communication Standard Compliance Checklist

- ☐ Obtain a copy of the rule.
- ☐ Read and understand the requirements.
- ☐ Assign responsibility for tasks.
- ☐ Prepare an inventory of chemicals.
- ☐ Ensure that containers are labeled.
- ☐ Obtain a safety data sheet for each chemical.
- ☐ Prepare a written program.
- ☐ Make safety data sheets available to workers.
- ☐ Conduct employee training.
- ☐ Establish procedures to maintain the current program.
- ☐ Establish procedures to evaluate effectiveness of the program.

Risk and Safety Training

Employee training is imperative. Training should create knowledge of materials and equipment, the known and potential hazards that may exist in the workplace, and how to control or minimize those hazards. No employee should undertake a job until he or she has been properly trained to perform the duties of the job, nor undertake a job that appears unsafe or in which potential hazards have not been minimized. Training should include both instruction and demonstration by

qualified personnel, such as laboratory or phlebotomy supervisors on the use of sharps, fire department personnel on the use of fire extinguishing equipment, and radiation safety officers on the use of dosimetry badges and lead gowns. Practices can also use Web-based broadcasts on safety-related topics.

All new employees should receive training on the general standards of the facility (e.g., fire and evacuation procedures) and job-specific hazards as a part of their orientation. Staff should have additional training when changes in the work environment alter potential or actual safety hazards. Annual training should be provided on all aspects of the safety compliance program. Documentation of this training should include a listing and signatures of the employees present, the date, the type of training, the subjects covered in the training, the person performing the training, and his or her credentials.

These points are the basis for the creation and implementation of the OSHA compliance plan for a medical group practice. The OSHA *Small Business Handbook* provides a thorough primer.[18]

Record-Keeping Legal Compliance

The primary responsibility for ensuring proper storage and retention should include a designated backup should the process owner (e.g., the medical practice executive) be unavailable. The plan should also include a loss control process for electronic backup of important documents. Under most circumstances, it is prudent to retain a copy of important documents at a location that is physically distant from the primary storage location. This should prevent any type of disaster from destroying all copies of significant information. Many organizations keep original documents for the length of the statute of limitations pertinent to the most likely allegations related to the document.

Medical Records

Different regulations and statutes apply to the retention of patient medical records and employee health or OSHA records. Patient medical records are generally retained in accordance with the statute of limitations

for bringing malpractice action as defined by the individual state. Employee records must be retained in accordance with the type of employee health services provided on site. For both types of records, the medical practice should confer with counsel familiar with the applicable statutes.

Record Retention

Record retention is a critical issue in group practices. There are several medical practice concerns as well as legal issues to consider when retaining records. Laws regarding record-keeping vary from state to state. Policies need to be developed to clearly indicate:

- Type of record, such as financial, employee, property, tax returns, medical record, or other;
- Whether the record is electronic or paper;
- Location of the record;
- How long it should be retained;
- Who is authorized to order record destruction; and
- Who should have access to records.

Record-retention policies should be reviewed at least annually to update and consider issues related to compliance.

Using Technology for Recording History

Record-keeping used to be limited to rooms filled with boxes of materials stored where mold, dust, mice, and dampness could destroy them. Today, computers provide the opportunity to maintain records in electronic formats so that environmental changes cannot affect them and space for storage is reduced to a minimum. In addition, computer programs provide the opportunity to format information in standardized ways that are accessible and usable by a variety of people.

Common computer programs include databases that are designed to store many records of a similar nature in a retrievable format. Often databases generate reports that sort and list records that contain specific fields. In addition, spreadsheet software is used universally to display and analyze numerical data and financial records. Presentation programs are used to display reports in a readable format, and word processing

programs are used to generate documents. Although in the past many brands of these types of programs were not compatible, in recent years, the trend has been toward creating programs that can communicate with each other in common formats.

The benefit of using these types of programs for record-keeping is the universality of access. Almost any computer user with a PC-compatible operating system can access, read, and modify records as needed. However, this capability also creates a vulnerability exposure for unauthorized changes to records.

Redlining changes in documents is an effective risk management tool for policies and procedures and other documents that are regularly revised. Redlining marks changes within the document so it is clear when alterations occurred. In litigation, policies and other records are often requested for production during discovery. The presence of redlined documents allows the organization to prove that it is producing the version of the document in use at the time of the alleged malpractice or other allegation.

E-mail is considered an official record in the context of litigation. It is increasingly being demanded as part of the discovery process. The danger of e-mail, however, is the very characteristic that makes it easy to use. The anonymity and informal nature of e-mail tends to elicit casual comments and speculation from writers. These candid communications could cause damage in litigation. Staff members should be cautioned about the official nature of business communication via e-mail. It should not be used for speculation, gossip, or threats.

Online cloud storage is another option, but you should consult with an information technology expert to make sure your files will be encrypted and otherwise secure. When a file is stored in the cloud, that means it is stored on a remote server and accessed by you via the Internet. This makes it easy to access files from anywhere you have an internet connection, allows for the sharing of files with all employees, and keeps your records safe if a catastrophe strikes your office. You will need to decide if the potential security risks of leaving your information in somebody else's control is worth those benefits.

Record System Organization

Despite modern tools, electronic records are not free from destruction. Operating systems are modified, computer programs and compatibilities change, accessibility to older forms of data storage change, and data may be lost. Computers can also break down or be damaged by water, fire, or sabotage. The same loss control mechanisms as for hard copies of important documents, including redundancy of storage, storage in a variety of formats, and segregation of copies, are essential.

In addition to the safeguards of physical separation and redundancy of files, a variety of individuals should have access to the files. It is often prudent to also keep the source documents (such as paper forms) for a period of time commensurate with state regulation. Transcription errors, disputes about the validity of the documentation, and allegations of misrepresentation are likely to arise early in the life of a document. Historical documents provide a framework for decisions but may be called on more rarely in litigation.

Conclusion

Comprehensive risk management plans in patient care can facilitate patient safety initiatives and reduce medical errors. Robust risk management requires extensive preparation and qualified healthcare administrators to develop, implement, and monitor an organization's plan. This is ultimately beneficial to overall patient satisfaction and other bottom-line priorities within the medical group practice. The ability to lead risk management initiatives will help advance the career of practice executives.

Notes

1. G.L. Head and S. Horn, *Essentials of Risk Management*, vol. 1 (Malvern, PA: Insurance Institute of America, 1991), 1.

2. J. McCaffrey and S. Hagg-Rickert, "Development of a Risk Management Program," in *The Risk Management Handbook for Healthcare Organizations*, ed. R. Carroll (San Francisco: Jossey-Bass, 2004), 95.

3. W.R. Ching, "Enterprise Risk Management: Laying a Broader Framework for Health Care Risk Management," in *The Risk Management Handbook for Healthcare Organizations*, ed. R. Carroll (San Francisco: Jossey-Bass, 2004), 3.

4. Head and Horn, *Essentials*, vol. 1, 6.

5. J. Reason, *Human Error* (Cambridge, UK: Cambridge University Press, 1990), 208.

6. C.B. Thomas, "New Orleans Today: It's Worse Than You Think (Time)," Katrina Aftermath (blog), Nov. 20, 2005, www.digitaldivide.net/blog/ katrina05/ view?PostID=9791.

7. Reason, *Human Error*, 208.

8. R.E. McDermott, R.J. Mikulak, and M.R. Beauregard, *The Basics of FMEA* (Portland, OR: Productivity, 1996), 1-5.

9. Head and Horn, *Essentials*, vol. 1, 8.

10. G.L. Head and S. Horn, *Essentials of Risk Management*, vol. 2 (Malvern, PA: Insurance Institute of America, 1991), 13.

11. Head and Horn, *Essentials*, vol. 2, 40.

12. Head and Horn, *Essentials*, vol. 2, 162.

13. Elizabeth W. Woodcock and Bette Warn, *Operating Policies and Procedures: Manual for Medical Practices*, 4th ed. (Englewood, CO: Medical Group Management Association, 2010).

14. "Workplace Homicides by Selected Characteristics, 2011-2013," Census of Fatal Occupational Injuries, U.S. Department of Labor, Bureau of Labor Statistics, www.bls.gov/iif/oshwc/cfoi/work_homicide.pdf.

15. "Workplace Homicides by Selected Characteristics, 2011-2013."

16. "Hazard Communication 1910.1200," Occupational Safety and Health Administration, U.S. Department of Labor, March 26, 2012, www.osha.gov/ pls/ oshaweb/owadisp.show_document?p_table=standards&p_id=10099.

17. Occupational Safety and Health Administration, *Hazard Communication: Small Entity Compliance Guide for Employers That Use Hazardous Chemicals* (OSHA, U.S. Department of Labor 3695-03, 2014), www.osha.gov/ Publications/OSHA3695.pdf.

18. *Small Business Handbook*, Small Business Safety and Health Management Series, OSHA 2209-02R, Occupational Safety and Health Administration, U.S. Department of Labor, 2005, www.osha.gov/Publications/smallbusiness/small-business.html.

Chapter 2

Adverse Event Policies and Procedures

Assess and Procure Insurance Coverage

The healthcare organization is a complex network of exposures. Some exposures can be easily managed and controlled, and some are more insidious. Latent exposures may pass unnoticed until a loss occurs. Furthermore, some exposures are conducive to self-insurance mechanisms, whereas others are better served through commercial insurance. An experienced, qualified insurance broker with expertise in healthcare is the best counsel to ensure that the organization appropriately addresses financing mechanisms for identified risk exposures.

Insurance Requirements and Products

Each medical practice has its own unique needs. A practice with a great deal of computer equipment might want or need a specific rider to cover that equipment. A practice that has a swimming pool to provide physical therapy needs specific coverage for that. In general, the following types of insurance denote the most common kinds of insurance coverage for a group medical practice:

- Professional liability (medical malpractice);
- General liability;
- Property and casualty;

- Directors and officers liability for errors and omissions;
- Workers' compensation (which is not an employee benefit, but a risk control coverage);
- Key person (in small practices);
- Employment liability;
- Environmental;
- Vehicle;
- Helipad (if the organization has one); and
- Business interruption.

Selecting insurance can be overwhelming. Which product offered by which company will provide the best coverage for the organization's specific needs? Would a self-insured vehicle best meet the organization's financial and exposure needs for all or part of the medical malpractice or workers' compensation coverage? As with any major investment, all parts of the insurance relationship should be evaluated.

Many organizations work with a broker to help procure quotes and make decisions. An insurance broker is different from an agent. An *agent* represents a single insurance company. Any insurance bought from that individual will be from his or her company. Using an agent may limit the flexibility in coverage that the practice may want. A *broker* is trained to evaluate the needs of the client and the insurance market. The role of the broker is to find the best coverage and combination for the client's unique needs. Furthermore, the broker has a relationship with the insurers. A broker can negotiate with underwriting to ensure that the client is given the best deal possible for the exposures being insured and the group's comfort with risk.

The role of the underwriter is to assess the exposure the healthcare organization brings to the insurer as the recipient of the risk transfer. The underwriter compares the organization's loss potential with that of similar organizations functioning in similar venues. With that baseline, the underwriter then looks at the specific loss history of the organization to determine the level of risk posed. By using actuarial formulas, the underwriter determines the premium. Other costs are added to the

premium based on the insurance company's overhead as well as the services provided by the insurance company.

A skilled broker can also advise the client if self-insurance is in the client's best interest. Working with the broker and an actuary, the organization can conduct a feasibility study. Sometimes the practice will be approaching readiness for self-insurance but is not yet ready to "take the leap." A broker can design an interim short-term insurance program or stop-loss policy that will allow the practice to assume part of the risk before taking the plunge into full self-insurance.

Risk-Benefit Analysis

Even with a skilled broker, the medical practice executive should be prepared to ask questions and to challenge recommendations. To do this, the executive has to have a handle on the risks and benefits of each type of risk-financing vehicle or policy presented. The executive must understand the cost of risk in the organization and have answers to questions about the present coverage, such as: What insurance coverage is currently in place? What are the limits of coverage? What are the deductibles, both by claim and aggregate? What are the attachment points for each layer of coverage? What losses have been paid from operations, through loans or through unfunded reserves, during the last five years? Are there losses that should have more formal financing to take advantage of present dollar value?

Once the medical practice executive understands the current cost of coverage, the actual practice losses for the last 5 to 10 years should be reviewed. Where did losses occur? Which were the frequent small losses and the less frequent large losses? Were there any unexpected losses? Are there potential losses identified through the risk-assessment process that have not yet occurred but could be devastating to the organization if they should occur? Are there insurance or self-insurance vehicles to prepare for them?

With this information, the executive has a picture of the coverage in place and the exposures that have resulted in losses. The benefits and drawbacks of each type of insurance product must then be weighed.

As discussed earlier, the benefit of commercial insurance is that it is known coverage. The limits are defined in the policy, which is a contract of risk transfer between the medical practice and the insurer. The downside of commercial insurance is its overhead, commissions, and profit loading. The services that are *included* are also encompassed in the premium. Although this might make self-insurance appear to be the only reasonable option, this is not true for every exposure. The cost of some services, such as claims management or risk management, may exceed the rate in the premium. Furthermore, self-insurance requires oversight and administration. The decision to self-insure or to purchase commercial insurance is one of philosophy, convenience, financial capacity, and tolerance for risk.

Organizational Commitment

Regardless of the type of risk-financing vehicle selected, the organization benefits from tight loss control processes. The temptation to diminish loss control when there is commercial insurance must be avoided. When the insurance market is tight and there is very little competition for customers, those practices with the best loss records and the tightest loss control methods will be the ones with choices regarding an insurer. Those with few processes may find insurance difficult to procure or prohibitively expensive.

Reduction of loss exposure is not just the job of the person with risk management responsibility. It requires commitment on the part of the board and administration to provide the necessary resources for loss control. It further requires that physicians understand the benefit of loss control methods to their practice and that time spent participating in risk management activities may directly relate to less time spent defending their practice in lawsuits. Finally, all personnel must realize that risk management is the job of each person in the organization. Although attributed to insurance, true risk management is about people, patients, and staff, as well as maintaining a fiscally viable organization so that the people who work there will continue to have a place to work and to serve others.

Eight Considerations before Purchasing a Medical Malpractice Policy

Medical malpractice insurance is a must-have for any physician, but as many practice managers know, higher coverage limits aren't necessarily a good thing. Experts say that high limits can lead to plaintiffs seeking higher judgments, and because tort reform caps on the amount plaintiffs can be awarded vary from state to state, bigger limits aren't always better.

So how do you determine what level of insurance coverage is appropriate for your practice? Here are eight issues to consider:

1. Understand hospital credentialing and managed care plan requirements.
2. Know your specialty requirements; certain specialties might need to carry higher insurance limits than others.
3. Consider what might happen if a judgment in excess of coverage limits is granted. It is important to be aware of the possible risk of personal liability of the physician if insurance coverage is too small for a judgment against the physician.
4. Find an insurance broker who's familiar with malpractice insurance in your state. Information gathering is imperative.
5. Organizational structure can also offer you some protection; limited liability companies (LLCs) and limited liability partnerships, for example, might give your organization an advantage when it comes to malpractice suits.
6. Be very familiar with the physicians in the practice before purchasing insurance. Physicians fresh out of school typically have lower premiums than physicians who have been practicing for decades or a physician who has had a previous malpractice judgment or settlement.

7. Use networking to reach out to other administrators or managers in your region to determine their experience with specific insurance companies. Referrals and word of mouth are some of the quickest ways to narrow down prospective companies.
8. Practice managers should also familiarize themselves with different types of malpractice coverage, such as tail coverage, claims-made vs. occurrence-made malpractice insurance, and more. Physicians considering moving their organization to a new location may want to consider insurance costs during the decision making because premium rates can vary based on location.

Address Complaints, Grievances, and Claims

Handling Litigation

Although most formal claims will be managed by a claims manager, the medical practice executive must have a working understanding of the implications of pursuing litigation as opposed to settling or finding alternative resolution approaches. Once allegations rise to the level of a claim, there will be financial ramifications, regardless of whether that claim is settled or goes to litigation. Although litigation offers the possibility of victory (in which case no indemnity is paid to the plaintiff), there are still costs for attorney fees, court costs, expert witnesses, and other discovery expenses, as well as organization costs from staff and administration time and resources. In a small claim or a claim that is obviously an error, nobody wins when litigation is pursued. In cases where there is no wrongdoing or negligence (e.g., medical malpractice) under the law, litigation may be the best route.

Alternative Settlements

Litigation is almost always an expensive and protracted process, and other forms of determination are available. In addition to settlement outside of court, alternative resolution processes such as arbitration and

mediation provide less adversarial and time-consuming mechanisms for coming to agreement in disputed situations.

Arbitration can either be binding, meaning that the parties must adhere to the decision rendered, or nonbinding, meaning that the parties are free to accept or reject the opinion rendered and pursue litigation. In contrast to arbitration, mediation involves a process designed to bring both parties to an acceptable decision without going to trial. There are many forms of mediation, which generally are not binding; however, the goal is to reach agreement on an outcome acceptable to both sides of the dispute.

Settling Claims

The settlement of a claim results from the defendant agreeing to the demands of the plaintiff to avoid the cost and difficulties of a trial. There may be some negotiation of the amount to be paid, but settlement is different from mediation in that it is not a process designed specifically to meet the needs of both parties. In fact, settlement is generally favorable to the plaintiff.

In all situations, the cost-benefit ratio of going to court vs. avoiding court must be based on the total cost of litigation compared to the damage created by conceding on any point of the accusation. If the damage to the organization, either financially or in reputation, exceeds the benefit of early resolution, then it is wise to pursue litigation. Many times, however, organizations choose to litigate because of the insult of the allegation or the desire to be seen as justified in their actions without considering the long-term financial and reputation ramifications. Each organization must develop its own philosophy about litigation and alternative forms of resolution.

The philosophy of the organization regarding claims management is an essential part of the relationship with legal counsel. Attorneys are usually paid by the hour (defense counsel) or on contingency (plaintiff counsel). Unless the medical executive is clear about avoiding unnecessary litigation costs and has a philosophy of early resolution when appropriate, legal costs will be a prominent part of the company

budget determination. When working with attorneys, it is wise to develop legal retainer contracts that reward rapid resolution and legal resource use commensurate with the organization's philosophy and financial tolerance.

Develop Relationships with Legal Counsel and Insurance Agents

Laws and their interpretations are insidious. It is more common to be in violation of a legal nuance than to be certain that you are in compliance. Furthermore, the rapid proliferation of legislation at all levels of government, coupled with a focus on patient safety and patient rights, means it is possible for statutes in the same jurisdiction to conflict in some areas. Even within state laws, conflict can exist or be perceived to exist when interpreted by different legal entities.

It is essential for the medical practice executive with risk management responsibility to have a relationship with a respected, ethical, and efficient law firm. The medical group needs an attorney familiar with general legal principles and general business issues. This may be an attorney who serves as the central point for ensuring there are no conflicts among the specialists. This attorney may also be the one who watches out for the best interests of the organization in a general way, keeping an eye on the changes in local, state, or federal law that may be of interest to the organization.

In addition, the medical practice should engage attorneys specifically trained in healthcare and environmental issues, medical malpractice, compliance, employment, real estate, human resource, and contract law. (Some attorneys may specialize in more than one of these areas.) The medical practice executive should work with each of these specialists and have them coordinate with one another to ensure that conflicting perspectives will not create additional risk exposure for the practice.

It is essential that the medical practice executive understand how legal fees are generated and monitor invoices to avoid spending more

on attorneys than they would on the consequences of risk exposure. The responsible professional has an understanding of the legal system and how it works, client rights, and the benefits of lower-cost methods to resolve legal disputes, such as mediation and arbitration. By fully understanding one's rights as a client, as well as the avenues available to the attorney to resolve disputes, the medical practice executive can function as a partner in the legal process instead of as a passive recipient of services.

Identify Your Organization's Vulnerabilities

Practice administrators may not view the legal protection of business assets as their concern, but the sudden economic impact caused by a malpractice judgment against an organization can quickly make it so. Here are some ways practice owners can avoid dangerous errors.

Rich Coverage Makes Physicians Targets

A physician's first line of defense against a lawsuit is open and effective patient communication; malpractice insurance provides backup in the form of defense lawyers. But because of the expense of lawsuits, physicians would be ill advised to rely solely on malpractice coverage.

Let's say you're a personal injury lawyer retained to bring suit against a physician. Before deciding to take the case, you investigate his or her malpractice insurance. A high amount of coverage makes suing the doctor more lucrative. Personal injury lawyers may focus on physicians with generous liability insurance. In fact, most lawyers hope to negotiate pretrial settlements with insurers. Defending a baseless claim still requires the insurer to pay large legal costs, giving an incentive to settle. The following recommended strategies make physicians — and your practice — less attractive to malpractice lawsuits.

Shield Your Group's Assets

Start by protecting your accounts receivables (A/Rs), which are unencumbered and highly liquid. The A/R balance can be pledged to a bank as collateral for a loan, placing the bank ahead of any other creditor, or the loan balance can be kept in an account owned by an LLC. As an asset held outside the practice, it will be exceedingly difficult for a creditor to capture and may provide a secure source for retirement contributions.

An alternative is to sell the A/R balance to a factoring company and place the proceeds in an account held by a separate LLC. The factoring company will charge for the service, but this allows the asset to be safeguarded. Any and all other large business assets should be held in separate LLCs, if allowed by the state (this assumes the practice is structured as an LLC, or at least not as a sole proprietor or partnership). Legal counsel should be consulted when structuring any business entity.

Protect Personal Assets

The same liberal use of LLCs should be applied for depreciating personal assets. By using a family limited partnership or a family LLC, assets are likely to increase in value. Other than separating the asset from the practice — and protecting it from creditors — a 20 percent to 40 percent discount may apply on the value of these assets, with positive estate-tax implications.

Personal assets with considerable liability risk should be in separate LLCs to partition an estate and protect each portion from creditors of other portions.

The personal residence may be an exception to this rule since most states have a homestead exemption. A few protect 100 percent of the home from creditors, but most cover only a small fraction of its value. As long as the home is titled "tenancy by the entirety" (TE) with a spouse, it's protected from creditors of either the physician or spouse.

A physician is not safe from creditors when both the physician and spouse are co-obligors on creditors' accounts. To protect a primary residence, the physician's spouse should not be a partner or owner in the

practice. If both spouses are owners, the homestead exemption and TE titling will not protect their primary residence from creditors.

Keep in mind that by using TE titling as opposed to a separate LLC, the property owners retain the use of the $250,000 capital gains exemption per spouse (lost when the home is placed in an LLC because the physician or spouse no longer own it). Owners must occupy the principal residence for at least two of the past five years to claim the personal-residence capital gains exemption.

Ensure That Qualified Retirement Plans Are Safe

The Employee Retirement Income Security Act of 1974 protects qualified company retirement plans from creditors. However, withdrawn assets are not shielded. Some states have statutes protecting nonqualified plans, such as simple individual retirement accounts (IRAs) and Roth IRAs. Consult with the practice's certified public accountant to ensure that the state protects assets inside nonqualified plans from creditors.

Review Insurance Coverage

Many physician groups are developing strategies to boost patient volume, revenue, and quality to build their practices. When adopting new practice strategies, it is wise to explore and weigh all of the inherent risks associated with them. Finding ways to identify and manage risk will be vital with the implementation of healthcare reform. Seven percent of physicians in 2014 run a direct pay or concierge service, and 13 percent more plan to transition to that type of practice. Seventeen percent of physicians age 45 or younger claim they will transition to that form of practice in the future.[1]

A wide range of industry experts, including insurers, insurance brokers, and practice management consultants, caution that such changes could affect groups' insurance coverage, costs, and exposure to litigation.[2]

Leadership Liability

In the past, it was considered a privilege to serve on the board of an agency or organization. There were few exposures to risk and many benefits. Today boards and officers of corporations are increasingly held personally accountable for their decisions and their actions.

Boards of directors can no longer accept the word of leadership at face value. There is a public duty to conduct due diligence efforts, which include speaking up on issues, recognizing the responsibility to dig beneath the information presented to ensure its validity and veracity, and recognizing that the board members may be held accountable for civil or even criminal penalties if they are found to be derelict in their responsibilities.

Officers and directors are not only responsible for the direct fiscal decisions of leadership, they are also accountable for ensuring compliance with all federal regulations and statutes through the corporate compliance plan. They are responsible for ensuring that the organization does not engage in unethical or illegal conduct in relation to federal funding agencies, including the Centers for Medicare & Medicaid Services or granting agencies. They must ensure that tax number usage, invoices, and contracts are legal and free of anti-kickback or Stark law implications. Furthermore, the board and officers have oversight responsibility regarding structural changes in the organization, including partnerships, mergers, de-mergers, and collaborative relationships.

Ethical organizations will ensure that there is sufficient directors and officers (D&O) liability insurance and that the directors are aware of their personal liabilities beyond the limits of the D&O coverage. The members of the board must have a clear understanding of their personal responsibility for conducting due diligence on decisions they make as well as a complete understanding of the vulnerability of their records and conversations under the rules of discovery. Finally, it is the duty of the organization to ensure that directors are educated on their responsibilities regarding all legal requirements for the organization so they can discharge their duties effectively and appropriately.[3]

Coordinate Disaster Preparedness

What Is a Disaster?

There are a number of definitions for a *disaster*. It can be "an event which causes loss of an essential service or part of it for a length of time which imperils business"[4] or "a calamitous event, especially one occurring suddenly and causing great loss of life, damage or hardship as a flood, airplane crash or business failure."[5] In other words, a disaster is an event that makes normal functions impossible.

Disasters can be natural or human-made. Witness the destruction caused by Hurricane Katrina and the subsequent flooding of New Orleans in 2005 or the Arizona wildfires in the spring of 2006. Human-made disasters can be work stoppages, such as transit strikes in Philadelphia and New York, or the destruction caused by terrorist attacks on the World Trade Center in 2001.

Planning and Preparedness for Catastrophic Events

Losses stemming from natural disasters provide examples of the variability needed in loss control methods. Flood and emergency evacuation processes that worked in Vermont in the ice storm of 2000 were not uniformly applicable to New Orleans in 2005 in the face of Hurricane Katrina. Both were water- and wind-based disasters. Both affected the availability of electricity and potable water. Both affected transportation. Both created temperature conditions that were dangerous to humans (the ice storm resulted in deaths by freezing and collision; the hurricane, in deaths by drowning and heat). Both required evacuation of vast numbers of people from nursing homes and hospitals. However, unlike the aftermath of Katrina, the New England ice storm did not result in potential infectious disease through coliform or mosquito transmission, nor the repair time and the time before people could return to their homes after the ice storm was shorter. Although there is much to be learned from the communication among various agencies, the military, and first responders, such as emergency service personnel, many aspects of the emergency plan do not go far enough to meet the needs of different disasters.

In addition to natural and human-made disasters, increasing attention is being paid to the threat of an infectious disease pandemic. Medical practices should review disaster preparedness protocols and procedures in their organizations and in their communities to be current on the incorporation of pandemic influenza and Ebola preparedness into emergency management procedures and what their own roles and responsibilities would be.

The Department of Health and Human Services and the Centers for Disease Control and Prevention (CDC) publish a number of resources specifically targeted to help medical offices and ambulatory clinics assess and improve their preparedness for responding to pandemics. Medical practices may find that they need to adapt the information and checklists to meet their unique needs.

According to the CDC, medical offices should develop a structure for planning and decision making. The structure should include a planning committee with both clinical (physicians, nurses, and ancillary staff) and administrative (medical practice administrator and support staff) representation, as well as the services of an environmentalist, if possible. One person in the organization, such as the practice administrator, should be assigned responsibility for coordinating preparedness planning for the practice. A point of contact (either someone in the clinic or an outside consultant) should be responsible for answering questions and/or providing consultation on infection control to prevent transmission of communicable diseases. The organizational structure should be described in a written plan.

The plan developed for the practice should be consistent with its existing emergency and disaster plans and with community response plans. No loss control mechanism should be selected without full consideration of the influence of local cultural and environmental conditions on the potential for failure. Even apparently fail-proof plans may fall short because of unforeseen events. The World Trade Center buildings were built to withstand potential encounters with airplanes. However, the World Trade Center was built years before the Boeing 767s, which hit the towers, had even been designed.[6]

Disaster Response and Recovery

To protect the medical group's employees in times of emergency, it is important to create disaster plans. Most buildings have fire escape routes posted on the walls, lighted exit signs, and ceiling sprinkler systems; however, these precautions do not protect human life unless specific guidelines and drills are laid out, communicated to all employees, and practiced on a regular basis.

Since September 11, 2001, most employers have seen the need for emergency and disaster plans for both human-made and natural disasters. Policies should be in place directing supervisors and employees on what to do and how to handle emergency situations. Every employee should be notified about all emergency and disaster guidelines during orientation. Drills should be practiced at least once a year, and more frequently if possible. The policies should also direct employees on how to help patients and visitors reach safety.

Different geographic regions have different threats in terms of natural disasters. In California, for example, an earthquake emergency plan should be drafted to protect employees. Midwestern states should have tornado drills. Hurricane-prone areas should have evacuation plans in place for hurricanes and tropical storms. Every organization should promote "Be Prepared" for disaster programs so employees have emergency provisions and plans for their homes and families.

Tornadoes, fires, electrical storms, and even chemical spills all have the power to damage critical supply lines and make it impossible for a medical practice to function on a normal level. What would happen to a practice if a pipe in an office above were to rupture, pouring water onto the server or file room?

How does a medical practice plan for this type of calamity? These incidents are rare, but the economic effect on the affected practices can be staggering. It is estimated that "30 percent of companies that suffer a catastrophic disaster never get back to business and another 29 percent close within two years of the disaster."[7] Employers look to their medical

practice executives and expect they will provide leadership in this vital area of medical practice administration and oversight.

There are numerous websites, articles, and textbooks written in the past few years that document how to prepare a disaster recovery and business continuity plan. The best practices have been pulled together and refined to make them workable in a medical practice environment.

Here are four keys to disaster management:

1. **Disaster preparedness:** Are you ready for different scenarios that can affect the services you deliver? Have you performed a risk assessment, developed communication strategies, trained management and staff, and performed mock simulations?
2. **Disaster response:** Do you have a strategy for responding to the crisis, including communicating with patients and the community? This includes managing written, verbal, and social media communication.
3. **Post-disaster recovery:** Can you perform an impact assessment, including communicating with your key stakeholders, determining the effect of events on your community, and identifying strategies for repairing or restoring your reputation?
4. **Debriefing:** After the disaster, be certain to meet with your leadership team and board to discuss the disaster and how you handled each step of the process, and then fine-tune your plan for future unplanned events.

Taking the time to develop or refine your plans for responding to a crisis will save you and your organization time and money — and may save your reputation.

What Is a Disaster Recovery Plan?

Disaster recovery planning is multi-faceted. Information technology functions are often the first area of planning to be reviewed. If a

network, server, or personal computer goes down, how does one ensure that the data is recoverable and how quickly can the system get back online? Because most practices rely on practice management software for scheduling, billing, and clerical documentation, medical practice administrators must have a working knowledge of the steps needed to repair systems and recover data.

However, the medical practice executive must review the entire business as part of the planning. If there is no access to the facility and the doctors cannot treat patients, there is no revenue. Without access to the bank, the practice is unable to process payroll or pay bills — or deposit additional funds. If there is no phone service, how do patients contact the practice for emergencies, appointments, or follow-up questions?

A disaster plan consists of precautions to be taken so that the impact of a disaster will be minimized and the organization can resume critical functions. This planning can be divided into a six-stage cycle. The stages are risk assessment, business impact analysis, strategy and business contingency plan development, business continuity plan development, testing, and maintenance.[8]

Risk Assessment

When performing a risk assessment, it is important to look at how the risk might affect the practice and the likelihood of the threat. Although there is a geologic fault running along 14th Street in New York City, it is not the San Andreas Fault. Disaster planning for earthquakes in New York would rank very low on the likelihood scale compared to areas in California and on the West Coast. Even extremes of temperature might have an adverse effect on business.

Internal Control: Guidance for Directors on the Combined Code (also known as the Turnbull Report), published by the Internal Central Working Party of the Institute of Chartered Accountants in England and Wales, provides guidance on the implementation of internal controls, enabling companies to identify and respond to changing risks, both internal and external. The corporate

governance codes recommended in this report published in 1999 are now being established worldwide.[9] These codes help examine the financial, business, compliance, and operational areas of the business and rank the potential risks as high impact/high likelihood, high impact/low likelihood, low impact/high likelihood, and low impact/low likelihood.[10]

Ranking the perceived risks using this methodology, one would be able to put time and effort into projects with potentially significant effect on a medical practice. It is also possible that the final plan may consist of a number of smaller plans allowing several issues to be addressed once and inserted into various disaster recovery plan scenarios. For example, a practice could set up miniature disaster recovery plans to cope with problems such as loss of local and system-wide electricity, loss of system-wide computers, loss of local and system-wide phones, including the T1 and DSL (digital subscriber line), and loss of a transportation network. In doing so, the medical practice would have identified many issues required in most disaster scenarios recovery plans.

Business Impact Analysis

In addition to reviewing potential risks, it is also imperative to look at key performance indicators: the people, knowledge, and equipment that allow a practice to function each day. Without all three elements, the practice cannot function at its optimum level.

There are a number of ways to gather this information. A survey can be sent to various departments or to the individuals responsible for office functions. One can also meet with and interview these individuals one on one. Both methods have been found lacking in gathering accurate and reliable data.

The most effective method of gathering critical information is usually with a survey followed by a group meeting across all functions. This allows personnel to own a process, recognize the impact of a disaster on the individual department or function, and agree to the steps that need to be taken to get the functions back online. For example,

access to coding resources might be used by the physicians and checkout personnel, as well as billing personnel. Billing personnel, however, would probably consider this a critical need while the physicians and other personnel might be more focused on ways to contact patients about appointments.

During the discussions of impact analysis, the question of moving to an alternate site may arise. Disaster recovery plans refer to sites as *hot*, *warm*, and *cold*. A *hot site* is one that is a total standby environment. Unless the practice has an office in another location, on a different power grid and serviced by a different telephone provider, the expense of maintaining this type of site would be prohibitive. A *warm site* is a standby environment lacking only those requirements that can be provided quickly. For example, if there is a loss of power to one area of the building and a conference room is set up with additional phone and computer cabling powered by generator, it could be used in this emergency situation. A *cold site* is a standby location without any hardware available.[11] Without the luxury of having a backup office as a substitute, smaller practices would be forced to a cold site if access to the office is prohibited for any period of time.

Strategy and Business Contingency Plan Development

Once the impact analysis is completed and there is a clearer understanding of the practice's critical processes, the strategy and contingency plan for getting these functions back online should be developed. The plan must clearly identify the tasks that need to be accomplished along with the timeline for progress. It is also imperative that personnel responsible for these tasks be identified as well as the location(s) used, that is, alternate office, home, cold site, and so forth.

This plan must be as detailed as possible if it is to be effective. Sit at a desk with only a computer and a phone and attempt to do a day's work. Within a very short time, you would recognize the little things that are used every day and taken for granted, such as staplers, pens, pencils, sticky notes, and so on.

The methods and procedures for bringing back these critical processes must be documented in the event the persons responsible have been adversely affected by the disaster and are unable to complete their tasks. The plan should cover the possibility that personnel may have other commitments if the disaster is wide ranging. They may have friends and family affected by the disaster or they may be responsible for the care of young children or elderly, sick relatives. If staff members have no access to money or transportation, they may be unable to get to work to assist with practice disaster recovery efforts.

Plan Testing and Maintenance

After the plan has been developed, it is critical that it be tested. Again, the literature demonstrates that only about 40 percent of disaster plans are actually tested. Of the plans that are tested, 80 percent fail in one or more areas. However, testing failure is perceived as a positive outcome, because corrections are made during the testing stage and not discovered in the middle of an actual disaster.

The testing is often the most difficult part of the planning process. Most experts in the field recommend testing part of the plan, in short intervals in case of plan failure. The only time a full-scale disaster drill should be called is when one is assured that all elements will function perfectly.[12]

Critical Processes

After reviewing the outline for developing a disaster recovery plan, look at critical processes that would be similar in almost all medical office practices, regardless of size or specialty. These processes include evacuation, communication, finances, insurance claims, human resources, clinical concerns, servers and information systems, telecommunications, and the physical plant.

Evacuation

If the building is unsafe due to fire, loss of electrical power, or any other reason, there should be a plan to safely evacuate staff, patients, and visitors.

If the practice will not be able to access the premises for a period of time, all deposits and mail containing checks should be removed at the time of the evacuation along with current encounters and chart notes.

If time allows, the servers should be powered down, the previous days' backup tapes taken, and phones forwarded to a remote answering service.

The person designated as the team leader for an evacuation should check the premises to ensure that all patients, visitors, and staff have departed. The staff should meet at a preordained area to ensure that all employees have evacuated and can be accounted for. At this time, further instructions can be delivered to the staff based on the situation.

Communication

Lines of communication must be set up with staff, patients, and vendors as soon as possible after a disaster. The practice administrator or designee should have an employee contact list with home and cellular telephone numbers as well as e-mail addresses. If an employee is hurt during an evacuation, the practice will need emergency contact information readily available. Cloud-based storage can be used to keep this information encrypted off site for easy access after an emergency if the office computer is now unavailable.

Practice executives must have a process to contact patients. This includes a plan to have access to off-site backup data for patient names and phone numbers. An answering service acting as a backup call center can be a good solution if the office is inaccessible.

The practice must also contact vendors to let them know of the emergency and perhaps place orders for replacement equipment. Again these numbers need to be stored off-site. In addition, account numbers, passwords, and other essential information is information that medical

practice executives must always have available at their fingertips in case of an emergency.

Finances

One of the most critical areas to plan for in a disaster is finances. If the office must be closed and patients cannot be seen, there is an immediate effect on cash flow. If the practice does not participate in electronic funds transfer from payers and the mail cannot be delivered, receivables are also affected.

Payroll must still be processed. Business interruption insurance is an excellent strategy to cover employment issues such as payroll and health insurance coverage. A prepared practice executive will make sure this insurance will cover the practice for an adequate time.

Vital practice information, such as managed care contracts, particularly those with carve-out reimbursements, must be accessible from an off-site facility. Contact information must be available so that payers can be alerted, which can help the practice avoid denials caused by untimely filing during this emergency period.

Insurance Claims

Information regarding the practice insurance carriers must be available off site. Commercial insurance covers buildings and contents, whereas business interruption insurance is meant to cover the incremental costs incurred through dislocation. Business interruption insurance does not cover the full cost of getting the practice back to normal working conditions. When formulating a disaster recovery plan, the practice administrator should meet with the insurance carriers and discuss their requirements for damage documentation, their response times, and any policy limitations.

Video and still cameras can be used to document existing property condition and the damage after an event. All damaged materials and equipment should be kept on site until an adjustor provides a release. The insurance carrier should be asked how the replacement value of

an item is determined. Because the practice will need cash to restore operations, it is important to know how quickly claims will be paid.

If the untoward event was caused by a terrorist attack, there should be coverage under the current policy or assurance that it is not excluded under the "act of war" clause. It is important to be aware that property and casualty companies are increasingly reluctant to write policies covering disaster recovery in certain areas of the country.

Human Resources

The most valued resource for a practice is the staff. The needs of staff members must be reviewed and addressed as part of any successful disaster recovery plan. If the disaster has affected a wide area or a significant transportation route, employee issues will need to be resolved. Without alternate routes, employees may be unable to reach the worksite.

Employee photo identification cards or badges may be necessary if there is an untoward event in the building or area because law enforcement may refuse entrance to those without the proper credentials. If the event will deny access to the facility for a period of time, it is important to have license and credentialing information available for affiliate clinical staff.

The most important element for handling human resource issues during a time of disaster is to communicate, plan ahead, and involve the entire staff.

Servers and Information Systems

Information systems is the one area of disaster recovery that most practices have already addressed. Daily backups and redundant systems are standard procedure in today's practices. Employees working in remote locations should have the ability to access the practice network to allow certain employees, such as billers, to work from home for a period of time if the facility is not available.

Practices that use an application service provider (ASP) may have access to their data more quickly because the data and servers are off site

and possibly outside of the affected disaster area. However, it is important to investigate the ASP's disaster plans and ensure access to the medical practice data if they have a disruptive event at the vendor's site.

Telecommunications

Telephones are a practice's lifeline to the outside world. However, phones are commonly attached to computer systems through Voice over IP (VoIP), which means a loss of power may make service unavailable. The practice should have at least one corded phone, available for an emergency, which does not go through their private branch exchange. It could be the fax line, a modem, or the line used for credit card transactions. Plugging a corded phone into that line will allow the practice to make outgoing calls to the answering service and to remotely transfer calls to a working number.

Consider the value of having the practice's answering service or call center being located in a different power grid and telephone service area. The call center might still be functional and able to handle the practice's call volume. The call center must have its own disaster recovery plan, which should be reviewed by the practice.

If systems are up and running, but access to the site is being denied, the message system can be programmed remotely to alert patients of the office problem and options for follow-up.

Physical Plant

When the practice can gain access to the physical plant, the first priority is to contain the damage. Save everything that can be salvaged, tested, or restored, and keep the damaged equipment for the adjustor to review. Maintain an up-to-date fixed inventory list and keep the list accessible remotely. The age and purchase price of the destroyed equipment will need to be documented. Copies of receipts and purchase records will speed the turnaround time on claims.

As part of the recovery plans, research vendors who can respond quickly to assess and contain fire and water damage. Keep the contact names and information for insurance claims. Although items may

look unrecoverable, salvage must be started immediately to prevent rust, corrosion, and mold.

Keep a contact list of all vendors and make video or photo records of the damage incurred. Contact the practice insurance carrier immediately to perform a damage assessment. It may be quicker to replace equipment instead of restoring, but it's usually more expensive. Restoring avoids capital expenditure and improves cash flow. This might be critical because the insured value may be less than the cost of replacement, and it may take months to process claims and receive a damage settlement.

Critical Process Time Frames

After the critical processes for the practice have been established, the next step is to determine how quickly these need to be up and running. First, determine the:

- **Maximum tolerable downtime**, which is the maximum time an organization can tolerate being down;
- **Recovery time objective,** which is the time available to recover;
- **Recovery point objective** (RPO), which is the extent of data lost; and
- **Work recovery time** (WRT), which is the time available to recover data.

Critical process time frames are usually set at (1) 24 hours, (2) three to five days, (3) one to two weeks, and (4) one to two months. Prior to Hurricane Katrina, these time frames worked for most disasters. For example, a practice would want to set the critical process time frame for workable telephones at 24 hours.

Although the practice may want access to servers and computers within 24 hours, the RPO and WRT may be two or three days. These time frames should be reviewed carefully and have realistic expectations. There may be alternative ways to solve the problem by setting up work-around solutions, such as using paper until the systems are back

online. Staff may need to function in different capacities during this time period and staff members may need to focus on damage control and recovery. Other employees may be required to take the information captured on paper and enter this backlog when the computers are back online. Additionally, other staff members may be handling the day-to-day functions of the office.

Along with detailing the time frames to get processes up and running, it is critical that the practice administrator determine when staff members should return to work. Time frames should be set for when the practice's billing, administrative, clinical, and ancillary staff should return.

Tips for Disaster Preparedness

Here are additional tips that William Hineman, MGMA member and former administrator for Cardiac, Thoracic, & Vascular Surgery Inc., Metairie, La., used to help his practice survive Hurricane Katrina:

- Add a provision to your business-interruption insurance policy to include actions by civil authority. Hineman's practice suffered no physical damage (which is what most insurance policies include), but most of its patients lived outside the parish and were blocked from entering.
- Set up an 800 phone number for your staff to use before, during, and after a disaster, because local area codes may be jammed.
- Have a *civilian* exchange e-mail (such as Yahoo) that is not subscriber-based and is accessible from any computer.
- Maintain a corded landline telephone at home (because cordless telephones cannot be charged when the electricity fails).
- Use a payroll vendor that can operate remotely and outside your geographic area.

Conclusion

Developing, implementing, and maintaining policies and procedures will help the organization to prevent adverse events, plan for disasters, and cope with the recovery process when necessary.

Notes

1. "2014 Survey of America's Physicians: Practice Patterns & Perspectives: An Examination of the Professional Morale, Practice Patterns, Career Plans, and Perspectives of Today's Physicians Based on Over 20,000 Survey Responses," Physician's Foundation, September 2014, www.physicians foundation.org/uploads/default/2014_Physicians_Foundation_Biennial_Physician_Survey_Report.pdf.

2. H. Benjamin Harvey and I. Glenn Cohen, "The Looming Threat of Liability for Accountable Care Organizations and What to Do about It," *Journal of the American Medical Association* 310, no. 2 (2013): 141-142, doi:10.1001/jama.2013.7339; S. Jones, "Professional Liability Risks Evolve with Changes in Healthcare System," Insurance Journal (June 2012), www.insurancejournal.com/news/national/2012/06/01/249708.htm.

3. Carter McNamara, "Some Legal Considerations for Board Members," Free Management Library, http://managementhelp.org/boards/liabilities.htm.

4. Andrew Hiles, *Business Continuity: Best Practices*, 2nd ed. (Brookfield: Rothstein Associates, 2004), 3.

5. Aktar Syed and Afsar Syed, *Business Continuity Planning and Methodology* (Canada: SentryX, 2004), 1.

6. "Learning from 9/11—Understanding the Collapse of the World Trade Center," House Committee on Science, World Trade Center, March 6, 2001, http://commdocs.house.gov/committees/science/hsy77747.000/hsy77747_0f.htm.

7. Hiles, *Business Continuity*, 41.

8. Syed and Syed, *Business Continuity Planning and Methodology*, 9.

9. Gary Bennett, "Managing Risk for Clients and for Ourselves. A Bug's Life (and the Turnbull Report)," *Risk Management at PB: Balancing Risk and Reward* 16, no. 51 (January 2002): 3.

10. Hiles, *Business Continuity*, 29.

11. Syed and Syed, *Business Continuity Planning and Methodology*, 108.

12. Hiles, *Business Continuity*, 208.

Chapter 3

Compliance Programming for Federal and State Laws

Developing a Compliance Plan

Corporate Compliance

Corporate compliance is an area that has confused many people because of the number and types of laws that are included in this diverse area. In its simplest terms, corporate compliance is the organization's program to ensure that it meets all relevant federal and state laws as well as the program requirements of federal, state, and private health plans. In actuality, a compliance program also includes the formula for executing and running a compliance program defined by the U.S. Department of Health and Human Services, Office of Inspector General (OIG), and the requirements of agencies that monitor compliance in healthcare.

The OIG-recommended compliance program elements are based on the Federal Sentencing Guidelines.[1] The OIG believes that every hospital and integrated healthcare delivery system, regardless of size, location, or

corporate structure, should apply all of the following elements, modified to fit their unique situations:

- Develop written standards of conduct (often referred to as a *code of conduct*);
- Provide continuing education to all staff members on these standards of conduct; and
- Develop written policies and procedures to promote the organization's commitment to compliance (e.g., medical and business record policies, evaluation of managers on adherence to policies, and monitoring of necessity of care) and to address specific areas of potential fraud, including but not limited to:
  - Incorrect reimbursement;
  - Record falsification;
  - Fraudulent billing and documentation practices;
  - Billing errors;
  - Inadequate documentation of care;
  - Continuation of unneeded or unauthorized care;
  - Inadequate patient information;
  - Client abuse;
  - Patient discrimination;
  - Inadequate safety plan for patients and staff; and
  - Inappropriate acceptance of gifts.

A complete listing of compliance program guidelines can be found on the website of the Health and Human Services OIG in the "Compliance" section.[2]

Complying with Federal, State, and Local Laws and Regulations

Many federal, state, and local laws and regulations affect healthcare organizations. General corporate and business laws affect the structure and operation of medical organizations. Among those are the tax laws that apply to the corporate structure selected by the

organization. Certainly the size of the organization, its anticipated growth, tax goals, and concerns about liability will inform the selection of the most appropriate legal structure. These are areas to discuss with an attorney because of the variability associated with location, partnership relationships, personal and professional liability, the corporate practice of medicine, and state laws.

Laws Pertaining to Collaborations

At times, competitors may collaborate for specific projects or services to enhance their ability to offer services. Most competitor collaborations are time limited, and competition continues in all areas except those affected by the collaboration. In those situations, the relationship is defined by contract, and the parties must ensure that the collaboration does not create antitrust issues.[3] Guidelines for preventing antitrust issues in a variety of joint ventures and other collaborative relationships have been developed conjointly by the Federal Trade Commission and the U.S. Department of Justice in a document called *Antitrust Guidelines for Collaborations Among Competitors*, an important resource for the healthcare executive.[4]

Even more than antitrust concerns, kickbacks and Stark law violations are concerns in collaborative relationships. The anti-kickback statute[5] does not permit a provider to "knowingly or willfully solicit, receive, offer, or pay remuneration for services paid for under any federal health care program."[6] Simply stated, this statute prohibits goods or money from being given in exchange for referrals.

It is easy to see how this could happen innocently in a collaborative relationship: One party agrees to provide the other with office space, a share of profits from medications, durable medical equipment, or services in exchange for referrals to a specific program. Such arrangements are in violation of the anti-kickback statute and carry criminal and civil penalties. Although there are exceptions such as "safe harbor regulations," it is prudent for the organization to have an attorney familiar with the subtleties of healthcare law review any contracts that establish relationships.

Similarly, the Stark law regulations (I and II) prohibit referral by a provider to any entity in which the provider has a financial relationship. Known as the Ethics in Patient Referrals Act of 1989, Stark law I was promulgated in an effort to deter referrals to substandard providers. It also was intended to prohibit over-utilization or unfair competition. Stark law II broadened regulations to include Medicaid patients and all designated health services (not just laboratory services)[7] and was passed in an effort to clarify the provider self-referral prohibitions.

Both Stark law regulations carry civil penalties.[8] These related but distinctly different issues of corporate compliance create dilemmas about appropriate behaviors and business arrangements that must be carefully considered in negotiating any collaborative relationship.

Miscellaneous Laws

Other laws may apply to the medical practice, depending on the size of the practice and the corporate structure. For example, organizations that receive federal funding may be subject to laws such as the Drug-Free Workplace Act of 1988, which requires the employer to notify employees of the regulation prohibiting the use, distribution, manufacture, or possession of controlled substances in the workplace.[9] Other key regulations that may apply include the Occupational Safety and Health Act of 1970, Americans with Disabilities Act of 1990 (ADA), ADA Amendments Act of 2008 (ADAA), Family and Medical Leave Act of 1993 (FMLA), and Employee Retirement Income Security Act of 1974 (ERISA).

Conducting Internal Audits

Monitoring and auditing activities in the medical group practice should be documented with the activity title, its purpose or objective, start and end dates, the metrics measured, and any key findings. Risk assessments help a medical practice set annual goals. The OIG Work Plan helps keep the focus on areas of OIG interest and align monitoring and auditing.[10] Compliance audits of all applicable departments and areas should be done at least annually or more frequently when appropriate.

Quarterly or randomized audits may be necessary if prior audits have detected systemic errors requiring more frequent monitoring.

Report Findings and Apply Corrective Action

When deficiencies or errors are detected in internal or external audits, document the action plan with appropriate follow-up actions, including the project review and end date. A log with compliance issues should be maintained and the practice executive should work closely with appropriate departments to investigate any issues. For example, inappropriate access to a patient's medical record would involve human resources, information technology, the group or department staff directly involved (such as nursing), and the compliance officer.

The investigation needs to be comprehensive, and each group should document the steps performed and support, defend, or remedy the actions associated with the claim. The compliance log helps ensure a level of consistency in handling situations and identifying trends. Any deficiency should be addressed with additional education and communication about the importance of compliance. The leadership team should share topics of concern, not specific cases, to illustrate to staff the organizational policies and procedures to avoid recurrence of violations resulting from misunderstanding or ignorance of the rules and standards.

Disciplinary Action

The compliance plan or practice procedures and policies should indicate when employee retraining or disciplinary action is warranted, up to and including termination. A review may determine that the practice should report a single violation or a pattern of behavior to the applicable agency or authority. As an example, some medical practices have zero-tolerance policies when there is inappropriate access to patient medical records. Any access not related to a business purpose results in termination. In these practices, strong compliance commitments are enforced with employee orientation and onboarding and reinforced with regular communication, training, and education.

Training and Education

The committee should continuously develop an education program that drills down to the physician and employee levels. It should include information and training on how employees perform their jobs in compliance with practice standards, applicable regulations, and the practice's commitment to an effective compliance program. The OIG has created educational materials to explain federal laws on fraud, waste, and abuse, including a physician self-study booklet titled *A Roadmap for New Physicians* with a companion Microsoft® PowerPoint presentation and speaker notes.[11] This presentation can be supplemented with customized training on compliance roles for physicians and staff.

Conclusion

Compliance is everyone's responsibility. Whether it is the fiduciary responsibility for the board members or claims accuracy by the billing staff, the commitment to compliance is organizational and individual.

The compliance process is also dynamic and requires engagement to ensure that groups fulfill all the elements of an effective compliance program. By considering these suggestions, medical practice professionals demonstrate their commitment to corporate compliance.

Notes

1. U.S. Department of Health and Human Services, Office of Inspector General (HHS/OIG) *Compliance Program Guidance for Hospitals*, 63 Fed. Reg. 8987, Feb. 23, 1998, p. 4, https://oig.hhs.gov/authorities/docs/ cpghosp.pdf.

2. "Compliance Guidance," U.S. Department of Health and Human Services, Office of Inspector General, http://oig.hhs.gov/compliance/compliance-guidance/index.asp.

3. R.A. Havlisch, "Emerging Liabilities in Partnerships, Joint Ventures, and Collaborative Relationships," in *The Risk Management Handbook for Healthcare Organizations*, ed. R. Carroll (San Francisco: Jossey-Bass, 2004), 695.

4. *Antitrust Guidelines for Collaborations Among Competitors*, Federal Trade Commission and the U.S. Department of Justice, April 2000, www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-anti trust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf.

5. Anti-Kickback Statute, codified as Criminal Penalties for Acts Involving Federal Health Care Programs, 42 U.S.C. § 1320a-7b.

6. 42 U.S.C. § 1320a-7a.

7. "Stark Law: Information on Penalties, Legal Practices, Latest News and Advice," Stark Law, http://starklaw.org/.

8. "Stark Law."

9. "Drug-Free Workplace Act of 1988: Requirements for Organizations," elaws® — Drug-Free Workplace Advisor, www.dol.gov/elaws/asp/drugfree/ require.htm.

10. "Work Plan," Office of Inspector General, U.S. Department of Health and Human Services, http://oig.hhs.gov/reports-and-publications/workplan/.

11. *A Roadmap for New Physicians: Avoiding Medicare and Medicaid Fraud and Abuse, Physician Education Training Materials*, U.S. Department of Health and Human Services, Office of Inspector General, https://oig.hhs.gov/ compliance/physician-education/index.asp.

Chapter 4

Accreditation and Licensure Requirements

Prior to officially joining any practice — and in many cases, prior to the interview — physicians will need to complete several credentialing processes. These steps are critical for many legal reasons.

The Credentialing Process[1]

Laws in every state and the District of Columbia establish physician licensure requirements for persons practicing medicine. Some jurisdictions prohibit, either through explicit statements in their medical practice acts or through case law, the corporate practice of medicine. This doctrine generally forbids physicians from practicing medicine on behalf of, or in concert with, any organization other than a professional services corporation (or similar corporate entity) for the practice of medicine. In some states, similar limitations are also imposed, to a greater or lesser degree, on other licensed healthcare professionals (e.g., psychologists) delivering services in a corporate setting.

Many states have eased up on this strict prohibition to allow nonprofit hospital service corporations, health maintenance organizations, and certain other enterprises to employ physicians. For example, some states allow employers to hire physicians to provide medical services to their own employees and their dependents at company-sponsored clinics. In other jurisdictions, hospital employment

may be authorized on the grounds that the delivery of medical care is consistent with the hospital's mission.

Legal Requirements

To meet these legal requirements, physicians and their practice managers must take many credentialing steps, some of which are required before physicians can legally practice medicine. These requirements include obtaining the following:

- Employer identification number;
- State tax identification number;
- Medical license for every state in which the physician plans to practice;
- Drug Enforcement Administration (DEA) permit;
- Hospital privileges;
- Payer credentialing after receiving state license and DEA clearance; and
- Medicare and/or Medicaid credentialing.

Credentialing may take many months and some employers will not allow a new physician to begin employment until the physician has received a certificate of completion from residency and all credentialing is complete.

Every physician must have a state license and a DEA permit to practice medicine. Also most practices will not allow a new physician to begin work until the insurance carriers, including Medicare and Medicaid, have credentialed the physician. After the physician has been credentialed, he or she can bill for and receive reimbursement for services rendered.

A physician's training license is not a state license. Physicians must apply for licensure in every state in which they wish to practice. If your group practice has a satellite office in a neighboring state, confirm that the state will allow doctors to practice if they're licensed in a neighboring state and working for an organization with sites in both states.

State medical license and DEA permit applications often take three to four months to complete. Insurance carriers also take three to six months to process applications. Thus, each new physician can face a six- to nine-month process to get every credentialing obligation accomplished. Again, physicians cannot practice medicine without a state license and a DEA permit. All other credentialing requirements, including insurance panel credentials, flow from these two credentials.

Meeting Accreditation Requirements for Physicians and Facilities

In the perception of the public, the primary reason for accreditation and credentialing is to be able to show that an outside, independent body has determined that an organization (or an individual) has been tested and has met standards that prove its level of quality and/or competency within the healthcare field.

For organizations and facilities, the primary accrediting bodies are the Joint Commission on Accreditation of Healthcare Organizations and the Accreditation Association for Ambulatory Health Care. When pursuing accreditation, a practice or healthcare facility should undergo a rigorous multi-day evaluation that addresses all aspects of the operation of the organization and the medical treatment that is being provided.

Within this accreditation process, an organization can expect that evaluations of the following areas will take place:

- Governing bylaws;
- Safety and health procedures;
- Facility design and safety;
- Chart documentation;
- Human resources;
- Quality assurance reviews; and
- Physician and staff credentialing.

The development, implementation, and adherence to documented policies and procedures that delineate and govern the day-to-day

operations of the practice are critical to the successful completion of the accreditation process. This in-depth evaluation is repeated, normally on a three-year cycle, to ensure that the findings of both the initial and subsequent evaluations are still within the expected values that earned the organization its original accreditation.

Failure to meet the expected standards places a requirement on the organization to implement corrective action to address issues that did not meet the standards of the accrediting body. Continued failure to be responsive to and correct deficiencies can result in increasing levels of response and attention from the accrediting body, with the ultimate result being the revocation of the certificate of accreditation.

In addition to these accreditation organizations, other recognized professional organizations provide the means to credential or certify the competency of physicians and administrators. Physicians obtain board certification through the completion of specialty training and the successful passing of comprehensive examinations that test their knowledge and expertise within defined areas of specialization. In many cases, this board certification is required to obtain privileges at hospitals and participation on various insurance carrier provider panels. This board certification is specialty controlled, and retaining certification normally requires the physician to complete a specified number of continuing education credits each year as well as take periodic recertification exams to ensure that the physician has maintained current skills and knowledge within the specialty.

In addition to the professional credentialing organizations previously discussed, physicians are also credentialed by licensed healthcare facilities (e.g., hospitals and nursing homes) and by commercial and noncommercial insurance carriers. Each organization has its own policies and procedures for credentialing providers and confirming and updating those credentials. Each accredited entity has its own regulations that must be followed by the provider, such as proof of advanced life support training or tuberculosis screening.

In the event of noncompliance with the policies and guidelines of the credentialing body, the provider may be subject to progressive

disciplinary action, which may ultimately result in the provider losing credentialed status with the entity. Normally, the provider is advised of the area of noncompliance and is offered the opportunity to implement corrective action within a defined period of time. Failure to implement corrective action or continued violations of the specific policies and procedures may result in progressively stronger disciplinary actions, including suspension and the ultimate termination from the healthcare facility staff or termination from the provider panel of an insurance carrier.

To properly and effectively manage the myriad regulations, licenses, and credentialing requirements of its healthcare providers, it is advantageous for the practice to develop a database that reflects and summarizes all of the requirements so the practice's leadership can easily identify areas of conflict or areas where information requires updating. A simple way to create this database is to use electronic spreadsheets, which can be updated as information changes. Through the use of spreadsheets, a practice can chart the status of the credentialing of individual providers within a health plan or within their group and can maintain an electronic tickler file of when various licenses and certifications are due for renewal. As licenses and permits are updated, the appropriate entities can be notified to avoid any lapse in privileges or credentialing and billing status.

Conclusion

Successful accreditation is only the first step. Ongoing compliance must be a part of the day-to-day operation of the practice. Committee meetings, code blue and disaster drills, ongoing staff training, organization of human resource and administrative documents, quality control studies, and ongoing review are all items that become part of the daily, weekly, and monthly routine. Every aspect of the practice is reviewed during the accreditation process. It offers the opportunity for in-depth analysis of operations. A key individual on staff who is familiar with all departments, skilled at organization, capable with computer documentation, and endlessly patient is vital to successful compliance.

Note

1. Medical Group Management Association, "Credentialing Process." All rights reserved.

Resource List

The following resources are available online. Please visit the MGMA Store at www.mgma.org/store for updates and new products. Members of MGMA seeking assistance locating articles and industry resources on Risk and Compliance Management may contact the MGMA Knowledge Center at infocenter@ mgma.com.

MGMA Compliance Web-Based Fillable Forms

MGMA Compliance Plan Fillable Form, by Marcia Brauchler, Erika Riethmiller, Amy Powers, Christopher Variani, and Daryl T. Smith (2015).

MGMA HIPAA Outpatient Practice Policies and Procedures Fillable Form, by Marcia Brauchler, Erika Riethmiller, and Amy Powers (2015).

MGMA OSHA Medical Practice Compliance Fillable Form, by Marcia Brauchler, Erika Riethmiller, and Daryl T. Smith (2015).

MGMA Washington Connection — eNewsletter

The current year and the previous three years of issues are archived on the MGMA Website.

MGMA Practice Resources Topics and Tools Sections

See the following topic-focused content sections on the MGMA website:

- Compliance and Management
- Physician Practice Assessment (PPA) Studies — member-based research on healthcare policy issues
- Regulatory updates:
  - Affordable Care Act
  - Federal Quality Reporting Programs
  - Health Information Technology
  - HIPAA Resource Center
  - Medicare Payment Policies
  - Red Flags Rule Resource Center
  - Specific Regulations and Compliance Issues
- Risk Management Tools:
  - Bioterrorism Preparedness for Medical Groups
  - Embezzlement Risk Assessment
  - Entrepreneurial Health Care Checklist
  - Medical Emergency Preparedness Resource Center
  - Medical Office Disaster and Emergency Preparedness

MGMA Connection Magazine — Risk Management Focus

Medical Practice Today, published each July, is a review of the annually updated "What Members Have to Say" research, focusing on challenges faced by MGMA members and what they're doing to survive and thrive in today's healthcare environment.

Risk Management issue, published each September, is an array of articles that drill down into specific Body of Knowledge domain topics.

The State of Medical Practice, published each January, is an annual update to the myriad issues medical practice executives will grapple with in the coming year.

MGMA Online Education — Self-Study Courses

Essentials of Risk and Compliance Management. Item # S15RM.

MGMA HIPAA Outpatient Practice Policies and Procedures Online Staff Training. Item # S16HIPA.

MGMA OSHA Online Staff Training. Item # S16OSHA.

Index