M
ost physicians and other health care practitioners strive to provide ethical, high-quality patient care. Their ability to do so relies on the trust of patients in practitioners’ professionalism and medical expertise. In no small measure, trust is at the heart of good patient-provider relationships.

Modern health care occurs in a complex, dynamic system that relies on many moving parts to function effectively. Notably, the health care system must follow federal and state regulations, professional and organizational standards, insurance rules, and other business requirements.

In this context, trust rests on the expectation that medical practices will protect patient privacy, keep accurate records, submit proper claims for payment, and otherwise meet various administrative and organizational responsibilities.

Under the Patient Protection and Affordable Care Act of 2010 (ACA), health care providers must have a compliance program for enrollment in Medicare, Medicaid, and Children’s Health Insurance Program services. Further, health care providers must comply with the requirements for privacy and security, workplace safety, waste, fraud and abuse, medical records and documentation, coding, human resources, and other key practice areas.

Up to Standard
To fulfill these wide-ranging rules and requirements, health care providers and organizations should have a practice compliance plan to ensure their adherence to all legal, ethical, and professional standards. “Compliance plans and programs generally apply to everyone in health care,” says David J. Zetter, PHR, SHRM-CP, CHCC, president and lead consultant of Zetter HealthCare in Mechanicsburg, Pennsylvania. “Every health care provider and organization is required to have [annual and ongoing] compliance training and education in specific areas. For instance, OSHA [Occupational Safety and Health Administration] safety training has to be done on an annual basis. This includes an OSHA safety walk-through. HIPAA [Health Insurance Portability and Accountability Act of 1996] training on privacy and security rules to protect patient...
A well-trained staff and an organizational culture that encourages open communication, feedback, and good-faith reporting.

Another integral aspect of compliance is internal monitoring and regular audits of the practice or organization’s activities, including billing and claims processes. How is the practice measuring up in terms of compliance? Are there areas of potential risk that employees identify? Medical practices need to conduct regular audits, chart reviews, and other assessments to flag areas or operational procedures where there is room for improvement. Monitoring and auditing can be done in-house, under the supervision of a designated compliance officer, or outsourced to a health care consulting service with the appropriate expertise.

The compliance plan should be adapted to the practice’s needs and purpose. “What’s health information has to be done prior to any new employee seeing, speaking to, or treating patients. This [training] also should be done annually. The practice will need to be able to show proof that its employees have completed these required annual trainings.”

Zetter notes that many health care practices and organizations have not yet established a compliance plan. Regardless, providers must comply with ACA rules and regulations applicable to most of their essential practice and claims responsibilities.

Rather than another administrative burden, an effective practice compliance plan can assist practices in reducing billing or other reporting errors and improve practice efficiency and productivity while reducing costs. The likely result is a medical practice that is better equipped to support quality patient care.

In this sense, a health care compliance plan adopted by a practice or organization should represent the group’s best strategic effort toward fulfilling its various compliance program’s requirements. The plan—built on internal policies and procedures—should help the practice promptly identify and resolve compliance violations, issues, and problems before they worsen.

While federal agencies have not adopted a definitive standard for compliance models, seven fundamental elements for an effective health care compliance program are essential, according to the Office of the Inspector General (OIG):

1. Implementing written policies, procedures, and standards of conduct
2. Designating a compliance officer and compliance committee
3. Conducting effective training and education
4. Developing effective lines of communication
5. Conducting internal monitoring and auditing
6. Enforcing standards through well-publicized disciplinary guidelines
7. Responding promptly to detected offenses and undertaking corrective action

Written policies and procedures are the starting point of a compliance program. These should be straightforward and accessible to everyone in the practice. Strong communication among physicians, managers, and staff is also essential to effective compliance activities. The ability to identify and solve issues as they arise requires a well-trained staff and an organizational culture that encourages open communication, feedback, and good-faith reporting.

Another integral aspect of compliance is internal monitoring and regular audits of the practice or organization’s activities, including billing and claims processes. How is the practice measuring up in terms of compliance? Are there areas of potential risk that employees identify? Medical practices need to conduct regular audits, chart reviews, and other assessments to flag areas or operational procedures where there is room for improvement. Monitoring and auditing can be done in-house, under the supervision of a designated compliance officer, or outsourced to a health care consulting service with the appropriate expertise.

The compliance plan should be adapted to the practice’s needs and purpose. “What’s
specifically included in a compliance plan will depend on the type of business and services it [provides],” says Zetter, a past president of the National Society of Certified Healthcare Business Consultants. “For instance, if you’re a primary care practice and you don’t do imaging, you’re not going to need to have a compliance plan that covers how imaging is done or how you pay your providers for imaging services. … Every compliance plan has to be detailed and specific to the practice it’s written for. You cannot borrow some other group’s compliance plan and put it in place in your practice. That will not work.”

Two particularly critical areas of compliance involve OSHA and HIPAA requirements. For example, OSHA has key standards for hazard communication, bloodborne pathogens, electrical hazards, fire safety, and more.⁴

Similarly, health care providers must comply with the HIPAA Privacy and Security Rules. These rules safeguard the confidentiality of protected health information and the security of electronic protected health information, respectively.⁵

On Good Author-ity
An effective compliance effort requires an engaged and educated workforce and participation from everyone in the practice. Having an active leadership commitment is essential.

For this reason, the OIG recommends that medical practices designate a health care compliance officer to lead the program. The compliance officer should be someone who can supervise the overall effort, ensuring that everyone in the practice adheres to the rules and regulations that govern the practice. In larger medical practices or organizations, the compliance officer may be a full-time position and function as part of a compliance committee. In solo or small group practices, the practice manager or a designated staff member may fill the position, managing the compliance program and their regular work assignments.

“There is no one way to do it, but I believe that the compliance officer should be someone who is able to identify what the applicable federal and state rules are for their practice,” says Kathryn I. Moghadas, RN, CLRM, CHCC, a health care consultant at Associated Healthcare Advisors in Winter Springs, Florida. “They should be able to interpret those rules, understand how they apply to the practice, and have the skill to stay current and familiar with any changes in the rules.”
A designated compliance officer in a large practice or organization may have a master’s degree in health administration or related education or experience. However, the compliance officer can come from a range of backgrounds. A skilled compliance officer should be someone who understands the overall practice plan and its challenges, advises Moghadas. “In my opinion, a practice manager, medical assistant, or other staff member can be a compliance officer, as long as they’re capable of learning the rules and requirements,” she remarks. “They just need to have a good background in understanding what they’re looking for regarding these issues. The big challenge is to consistently apply what you know. So, what does the regulation state? If it states that you cannot do something, then don’t do it. And you stay firm on the rules, you maintain the standard regardless.”

Notably, the compliance officer should be someone who can learn from their own—and the practice’s—mistakes, suggests Moghadas. “Everybody believes that you need to be a subject matter expert to do this type of work,” she says. “Nearly everything I’ve learned about compliance has come from making mistakes. I wish I could say I was smart enough to not make mistakes, but what I can say is that a lot of wisdom has come after the fact from making mistakes and then having to fix the problem.”

In this sense, Moghadas, author of Medical Practice Policies & Procedures, emphasizes the value of teachable moments. When mistakes or breaches occur, accountability is necessary, as is learning how to proceed constructively. “I often see compliance looked at as the heavy hand—the arm that comes down and bangs somebody on the top of the head,” she observes. “That approach doesn’t serve anybody—all it does is demoralize people in the situation.”

Moghadas cites an example to make her point: “A practice I worked with once sent protected health information via an unsecured [public] email system to one of their business associates. The email included a patient’s Social Security number, date of birth, address, and phone number. The problem was they had a secure email system that they failed to utilize,” she explains. “Instead [of berating the person responsible], we … say, ‘As a result of doing this, the penalties for this type of a breach would have been X amount of dollars.’”

“What you want is for people to remember what the rules are. It’s a teachable moment. So, the rules state that you need to have and use a secure email system. Using that secure system is going to make sure that patient information does not get breached. So, let’s use our mistake now to help everyone learn,” says Moghadas.

Fortunately, federal and state agencies and different licenses involved in compliance provide regular updates and online information on compliance rules and regulations, reports Moghadas. “The compliance officer should be reading these notices and updates [to see] what they are saying,” she says. “If they see some kind of rule change being made in one area, especially if it has to do with patient safety, patient identification, or any type of tactile skills involving patient care, they can usually expect to see it adopted throughout the whole spectrum of different services.”

Regarding their reporting responsibilities, the compliance officer should be independent of the legal or financial leadership of the medical practice or organization to avoid any potential conflict of interest.

By the Book
Managers must stay on top of the practice’s compliance issues, according to Viviane Potucek, CMA (AAMA), a practice manager for the Hospital for Special Surgery in Stamford, Connecticut. For Potucek, this means being organized, delegating responsibilities appropriately, and accurately documenting the practice’s compliance activities and requirements.

“As office managers, we are usually very busy,” observes Potucek. “We oversee the whole practice, and there is always a lot to do. In this position, we also know how the smallest issue can become a bigger problem down the line. So, when it comes to compliance, you really have to watch it very closely. Whenever it is appropriate, the manager should delegate and designate certain people to cover particular compliance areas. You might assign someone to be your right-hand person to oversee HIPAA processes, for example. Another person can
cover OSHA. This way you have a go-to person who can be responsible for a specific area.”

Training and accountability are also cornerstones of an effective compliance program, says Potucek. “It’s important to keep up with the training for the staff,” she says. “Generally, I think most training for staff should be mandatory. Everybody has to be informed. ... If someone breaks the rules, or should they try to take shortcuts that could possibly endanger another coworker or a patient, they have to be held accountable with a disciplinary action. But then we also have to make sure that whatever caused a breach is addressed so it doesn’t happen again.”

Practice organization is particularly essential for OSHA safety requirements, says Potucek. Under OSHA rules, health care facilities must maintain a Safety Data Sheet (SDS) with information on the safe handling of on-site chemicals. The SDS includes instructions on using personal protective equipment, first aid and spill cleanup procedures, and related safety issues. OSHA requires that the SDS materials be readily available to employees who are properly trained in how to read, understand, and access the data sheets.7

“The [SDS] folder can be a printout or electronic,” explains Potucek. “It’s [crucial] because every single chemical that we have in the office requires a printout for the [SDS]. If there’s an exposure and you are trying to look for the folder and don’t know where it is, it’s a problem. Or if a compliance officer shows up and is doing an audit and you can’t find the folder, the situation can become very hectic.”

“As a manager, I think it’s important to get organized and know where everything is,” says Potucek. “You should have a compliance checklist to help you with this. You can do some checklists on a weekly or monthly basis. For example, there is an eyewash station that has to be checked at least once a week to make sure it’s functioning. So, who is doing that? Who is responsible? Where is that being documented? You really need to have all the compliance-related information and materials organized so it is all easily available.”

OSHA safety training covers a range of issues, such as the handling and disposing of needles, handling of chemicals, proper labeling of instruments, and other concerns. “A hot topic during [the COVID-19 pandemic] has been personal protective equipment—where to find it, when to use it, and what type of equipment to use,” adds Potucek. “What do we need to know about gloves, goggles, and gowns? There are also discussions of specific protocols for cleaning and so on.”

With HIPAA education, Potucek says managers should emphasize to staff how easily breaches of patient confidentiality can occur. “Everyone who works in health care should keep in mind how conversations and discussions about patients amongst the staff can become a breach,” she says. “If two staff members who share a mutual patient are in an elevator, for example, they shouldn’t be having a conversation about that patient where it’s possible another patient or somebody from outside the organization could overhear what they’re saying.”

A breach of protected health information could involve any piece of information that pertains to a patient, cautions Potucek. “It doesn’t have to be the full name, the date of birth, [or] phone number—anything that links that patient to that information is protected health information,” she says. “You have to be careful how you use that information when you’re talking about a patient.”

A compliance committee keeps Hospital for Special Surgery practices informed and trained on their ongoing compliance requirements. “All updates—all the new information on what we have to do—is communicated to employees either via email or through the annual trainings they put together,” reports Potucek. “The trainings typically involve interactive videos that include illustrations, easy-to-understand examples, and tests that we take at the end of each module to prove that we understand the material.”

In the past, employees often needed to complete training requirements in group sessions, but today employees typically complete their compliance training individually and online. “It’s all electronic now, and each employee accesses the hospital’s organizational intranet platform to complete all their assigned training modules,” says Potucek. Whatever someone’s level of experience or knowledge, the annual training can be very useful, according to Potucek: “Even if you have been doing the training for years and know the materials well, it’s always helpful to have a refresher once a year.”
Finally, the hospital’s compliance training modules can encompass a long list of available topics. “In 2021, our compliance training list included fire safety and utility systems, fostering an LBGTQ inclusive environment, hazard materials, [and more],” explains Potucek. “The trainings cover specific issues like what to do if there is a fire, how to evacuate the building, and when and how to use a fire extinguisher.”

For the Record
While the terms are often used interchangeably, compliance programs and compliance plans have different meanings. “Normally, when we talk about a compliance program, we’re talking about how to educate and train staff,” notes Zetter. “But that is a distinct part of a compliance plan. The latter encompasses much, much more. A compliance program is more often an online system that allows the practice to educate and train their staff in the areas they are required to be compliant in, such as HIPAA, OSHA, corporate and Medicare requirements, waste, fraud, abuse, and other areas.”

As an experienced compliance adviser, Zetter also wants medical practice managers to know that maintaining accurate records of their compliance activities is crucial. “A compliance plan has to be documented, written down, and specific to the practice operation, the providers, staff, and all of the services the practice or organization provides,” says Zetter. “For instance, the practice needs to be documenting any HIPAA violation or accidental breach of somebody’s protected health information. … It’s necessary to document this in your minutes or even in the monthly team meeting to show that you discussed a situation where there was a breach. These teaching moments also help demonstrate the practice’s efforts at ongoing compliance training.”

Zetter recalls his experience with one large multispecialty practice whose compliance officer had drafted but never used two different compliance plans: “One of
the plans was in a binder we found in a file cabinet that was probably drafted 15 years prior. It looked brand new. The other one was on a shelf that was probably drafted later. It wasn't updated, and you could tell it had never been utilized. There were no minutes from compliance meetings. Every practice will sometimes have issues with HIPAA disclosures. Yet if you try to find the disclosure logs and they don’t exist, you know there's a problem.”

To be successful at health care compliance does not mean being perfect, but it does mean the medical practice or organization is strongly committed to compliance with its practice’s rules, regulations, and standards.

A successful approach to the compliance challenge means the practice leadership and staff will do their best to address compliance violations and issues when they arise to mitigate future risks and improve the quality, safety, and integrity of their organizational operations.

References

HIPAA Security Checklist
Complying with the HIPAA Security Rule is complicated due to its multifaceted nature. This checklist provides a practical approach to help health care businesses understand the HIPAA priorities:

1. Start with the big picture before looking at specific details.
2. Understand when the rule applies.
3. Appoint qualified individuals to handle compliance.
4. Remember to use a firewall, antimalware protection, strong passwords, and multifactor authentication.
5. Create a map of patient data — both how it is stored and accessed and how it flows through the practice.
6. Understand the difference between required and addressable specifications.
7. Apply a systematic approach by identifying threats, conducting reviews, and evaluating solutions.
8. Encrypt data to prevent breaches.
9. Keep a schedule for ongoing reviews.
10. Seek expert help when necessary.