

Compliance Plans in Health Care Operations: How to Create and Maximize Their Value

As **health care** lawyers and **consultants**, the point at which we are most frequently contacted by a new client is after notice of a complaint. Occasionally, the complaint is internal – from a disgruntled employee, a patient, or even an anonymous source; other times, the notice is from a government agency that is investigating or, worse, ready to take action. Sometimes the complaint is about fraud – overbilling, upcoding, unbundling, or ordering unnecessary tests; other times, the allegation is a kickback – inducement to encourage referrals; still others, the allegation is one directed at mishandling or mistreatment of a patient.

In the current regulatory climate, health care facilities and professionals need to be ready for such claims before they are made. Federal and state government investigation and enforcement are on the rise. Similarly, more and more health care providers are being subjected to private enforcement, from whistleblower actions to False Claims Act lawsuits. In this environment, it is essential for health care providers to be ready before a complaint is made. Once a complaint is received, if no preparation has been undertaken, the “train” has already gone “off the rails”; the situation is simply one of damage control.

With advance compliance planning, by contrast, health care providers can not only ensure that they are prepared, but can minimize the risk of having problems in the first place. The compliance plan came to prominence as a model of effective prevention of “organizational wrongdoing” through the 1991 Federal Sentencing Guidelines for Organizations (<http://www.ussc.gov/orgguide.htm>), which set forth a framework by which organizations can mitigate their liability for misconduct. While the compliance plan is not specific to the health care industry, the complexity and volume of industry regulations – from HIPAA to Stark to documentation to operational rules – have made compliance planning a virtual necessity for health care providers.

1. Developing a Compliance Plan

The first step in developing is understanding which legal issues present the most risk of noncompliance. Some helpful questions to start with are: which government agencies may come calling on our business? And what are the issues they are likely to care about?

For providers of all types, there are certain common starting points: the Department of Labor may come investigating a complaint from a disgruntled employee; OSHA or California OSHPD may inquire about safety practices (e.g. handling of biohazardous materials); allegations of violations of patient privacy (HIPAA) may bring the federal Office of Civil Rights (OCR). For all providers who participate in the Medicare and Medi-Cal Programs, investigations may come from the Center for Medicare and Medicaid Services (CMS), one of its many contractors, or the Department of Health Care Services (DHCS).

Other regulators vary according to the type of provider. For physician groups, it may be principally the Medical Board of California (MBC), which regulates the individual license to practice medicine, or the Drug Enforcement Administration (DEA), which regulates dispensation of controlled substances. For skilled nursing facilities, it may be the California Department of Public Health (CDPH) for drug recovery facilities, the Department of Alcohol and Drug Programs (ADP); for assisted living facilities, the Department of Social Services (DSS).

It is critical to know not only *who* is regulating your business, but also what power they have. Some regulatory agencies (e.g. OSHA or the MBC) have the power to discipline or, in serious cases, revoke licenses. Others (e.g. CMS or DHCS) have the power to suspend reimbursement or initiate audits to claw back funds that have already been paid. Some agencies can enforce civil monetary penalties; others, such as the federal Office of Inspector General (OIG) or California Bureau of Medi-Cal Fraud and Abuse, may charge criminal conduct; still others may do both. To be prepared, providers need to understand what risks are associated with that particular regulatory authority. This includes not only an appreciation for the range of potential sanctions in the arsenal of the particular agency, but also the enforcement agenda and priorities of that agency.

For health care providers, OIG – the fraud investigative arm of the Medicare Program – provides valuable guidance of what it considers to be the most recurrent issues for every type of health care provider, from skilled nursing facilities to physician groups from home health agencies to hospices. The OIG offers guidance to use the issues for purposes of developing a compliance plan (<http://oig.hhs.gov/fraud/complianceguidance.html>). OIG’s guidance is invaluable in identifying the most common risks associated with particular areas of health care, and in providing a road map of the government’s enforcement agenda. This allows companies

to prioritize, focus appropriately, and do their best to minimize risks.

Once those risks are identified, a compliance plan can be developed. The United States Sentencing Commission, which plays a key role in popularizing compliance plans, identifies the essential elements of a compliance plan:

(1) development of standards and procedures that are reasonably capable of reducing the prospect of wrongdoing and detecting fraud;

(2) ensuring appropriate staffing, including assigning specific, high-level personnel to oversee compliance and receive reports from lower level staff with operational responsibility to assess compliance;

(3) communicating compliance standards and procedures throughout the organization;

(4) monitoring and auditing to detect fraud;

(5) consistent enforcement with appropriate incentives and disciplinary mechanisms, including the option of anonymous reporting and

(6) response to misconduct, including tailoring the compliance plan to address and prevent its recurrence.

For more information, see <http://www.ussc.gov/2007guid/CHAP8.pdf>.

2. Tailoring the Compliance Plan to the Organization

Compliance plans are not cookie-cutter, one-size-fits all documents. It is essential to develop and implement a plan that fits the particular health care provider's organization. While it is helpful to begin with the general guidance specific to the type of health care provider – whether a medical group, a skilled nursing facility, a pharmacy, or any other type, this is only a starting point. To develop a meaningful compliance plan, the provider must assess the billing, operational and legal risks of its specific operation. The size and scope of the program can vary depending on the provider's needs. It is essential to map out the historic problem areas, how those issues are addressed, the personnel and structure that will be exercising oversight.

Critically, resources must be allocated for training and educating employees so that they understand the relevant legal requirements and implement the compliance plan. Since rules are continually evolving, training needs to be an ongoing process. Participation in training should be documented in compliance plan records.

It is also critical to establish an appropriate compliance structure that vests responsibility in the appropriate personnel. For some providers, it may be appropriate to designate internal staff for compliance roles; for others, it may be appropriate to consider a mix of internal staff and an external compliance officer.

In addition to general OIG guidance as to problem areas for various types of providers, it is critical for organizations to assess their own risk areas. Are billings claims an issue? Is the sufficiency of documentation a problem? Are their contracts with third parties that raise Stark and Anti-kickback concerns? It may be helpful to focus the compliance plan by a historic review of issues and by seeking outside guidance. As attorneys, we are frequently asked to assist in this process or to guide employees or consultants in identifying issues.

Above all, it is essential to have a plan that the provider can actually carry out; it may very well be worse to have a compliance plan and not enforce it than to have no plan in the first place. If a plan is perceived by government investigators as being "window dressing," the result may be to antagonize and raise suspicions. As a result, it is critical that health care providers think carefully about what they are committing to do and to follow through on that commitment. Compliance officers need to exercise real supervision and oversight and ensure that policies and procedures are enforced.

3. Testing and Refining the Compliance Plan

Once a compliance plan is implemented, it is essential to evaluate its effectiveness periodically and to identify any shortcomings. The compliance plan itself should contemplate the frequency and types of review to be conducted. Some issues, such as billing and documentation, may be appropriate for more frequent review at intervals throughout each year. Other issues, such as HIPAA

contractual relationships, may be well suited to annual review.

After each periodic audit, the question becomes what to do with the results. To the extent that potential issues have been identified, it is essential to address the matter and to attempt to prevent its recurrence. One question to be considered with legal counsel is whether any problem is sufficiently serious to warrant disciplinary action against the offending personnel, voluntary disclosure to the government, or other action, such as repayment to the relevant program. It is particularly important to ensure appropriate disclosure that may be required by the terms of any agreement with the government or by federal or state regulation. In numerous areas, regulations require reporting of particular kinds of legal violations.

Once particular problems have been addressed, it is critical to turn attention back to the compliance plan and to ask whether it should be updated or revised to address the matter that arose. In so doing, the compliance plan becomes an evolving document as the health care provider learns from experience.

4. Putting the Compliance Plan to Work

Although it can play an invaluable role when a problem arises, the value of a good compliance plan should be manifest in day-to-day operations. Providers should experience fewer denials of claims and fewer complaints. When government auditors review records, the higher quality of documentation should significantly reduce the likelihood of overpayment determinations. Personnel will be better educated and prepared, not merely avoiding problems but actively working to improve the quality of the provider's operations.

A "moment of truth" for compliance plans also comes whenever the provider receives a complaint, whether internal (an employee) or external (the government). It is essential to respond promptly and appropriately in order to demonstrate seriousness. Failure to take internal complaints seriously heightens the likelihood of complaints being redirected to the government and whistleblower lawsuits. Timely and appropriate corrective action, by contrast, increases the possibility of avoiding encounters with the government. Similarly, when dealing with government agencies, serious and prompt response can often improve the chances of a favorable resolution.

The compliance plan should continuously be reexamined to consider whether, in light of the matter that arose, the plan needs revision or, alternatively, whether a particular audit or review is necessary. It is critical to maintain a record of reported complaints and incidents, along with the ensuing evaluation to demonstrate the efficacy of the plan.

Effective compliance planning is an integral part of health care operations. In an environment of abundant regulatory challenges and pitfalls for the unwary, a carefully thought out and appropriately implemented compliance program reduces risk exposure, improves quality, and demonstrates integrity. The expense and effort of compliance is likely to be a fraction of the time and cost associated with a government investigation that might have been prevented.