COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2024
Internal Reporting Systems

By Greg Radinsky,[1] JD, MBA, CHC, CCEP; Shon C. Ramey[2] ; Michael A. Morse,[3] Esq., CHC; Jeffrey M. Klink[4] ; David Childers,[5] CCEP; Joseph Agins[6] ; and Amy Block Joy,[7] PhD

A hallmark of an effective compliance program is having robust internal reporting systems. The Office of Inspector General (OIG) stresses that its compliance guidance is intended to assist healthcare providers and suppliers develop internal controls that promote adherence to applicable federal and state laws.

A key aspect of an organization's internal controls is an internal reporting system to detect potential areas of noncompliance with federal and state laws and an organization's policies. In fact, the OIG cites responding promptly to detect offenses and undertaking appropriate corrective as one of the seven elements of an effective compliance program.

The Federal Sentencing Guidelines

An internal reporting system is necessary in order to comply with the OIG's guidance and the U.S. Federal Sentencing Guidelines. The U.S. Federal Sentencing Guidelines specify that organizations should "take reasonable steps...to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation."[8] Without such a system, employees and other stakeholders are forced to seek government involvement to resolve a serious compliant about noncompliance with a regulation or law.

While a functioning reporting system alone is a core requirement of any compliance program, the implementation of how an organization investigates inquiries is just as important. Some organizations require their employees to report potential wrongdoing to their compliance department, supervisor, or hotline. It is critical that an organization retain skilled compliance professionals to investigate potential wrongdoing and do so in an expeditious manner. It is an industry best practice to track the completion rate of appropriately closing out hotline calls. If an organization is either slow to respond to a complaint or does not conduct a thorough investigation, employees and other stakeholders will lose faith in the reporting system and resort to more litigious avenues to pursue their issue.

An internal reporting system has several other benefits. Detecting an offense early can serve as a preventative measure and help an organization mitigate an issue before it reaches a crisis level. Accordingly, an internal reporting system can allow an organization time to review and investigate a matter and self-report it to the federal government instead of the government identifying the issue first and conducting a potentially costly investigation. A robust and effective internal reporting system will also build trust with the organization's employees and other stakeholders and can enhance employee engagement.

If a company is under investigation, having an internal reporting system will be regarded as an essential element of the organization's compliance program. It is important for the organization to retain documentation of its internal reporting system if requested to provide information to a regulatory body. The organization may be requested to provide certain information about a particular complaint and also may be requested to show a log of its inquiries, including the time period each matter was open.

Fear of Retaliation and Intimidation

Retaliation is a big fear of employees when considering reporting an issue to Compliance. What does it mean to be retaliated against? The verb *retaliate* means “to repay in kind.”[9] Retaliation is revenge, reprisal, retribution, or getting even (e.g., an eye for an eye). The Ethics Resource Center defines retaliation as “...a negative consequence experienced by an employee for reporting observed misconduct.”[10]*Nolo’s Free Dictionary of Law Terms and Legal Definitions* uses a similar definition: “punishment of an employee by an employer for engaging in legally protected activity.”[11]

The negative consequence or punishment is typically an adverse employment action: getting fired, demoted, or laid off; reduced salary or reduced time; reassignment, relocation, or being transferred; and forced resignation. Other harmful results include reputation damage, property damage, and physical injury; exclusion from decision-making and meetings; and abuse, harassment, and/or humiliation from supervisors and coworkers. Many also suffer from failed advancement, negative evaluations, and heavy-handed monitoring.

Merriam-Webster Dictionary defines intimidate as “to make timid or fearful: frighten especially: to compel or deter by or as if by threats.”[12] Intimidation is often associated with bullying, threatening behavior, and coercion. While non-retaliation is critical, so is non-intimidation. Employees must feel comfortable raising a concern in addition to having comfort that, once they raise the concern, they will not be retaliated against. Every organization should have a non-retaliation policy that employees can easily access. See the **Resource: Sample Non-Retaliation Policy** after this article.

As an example, the State of New York felt this was so important that it made applicable healthcare providers certify that they maintain a non-intimidation and non-retaliation policy. A non-intimidation and non-retaliation policy is the “Eighth" element in the New York Office of Medicaid Inspector General’s mandatory compliance program for Medicaid providers.

If employees fear reporting an issue, it can severely hamper the effectiveness of an organization’s internal reporting systems (e.g., hotline) and the overall effectiveness of its compliance program. Often there is a correlation between employee perception of a retaliatory environment and the number of hotline calls an organization receives. It is common for organizations to receive a higher percentage of anonymous hotline calls if an organization has or is perceived to have a retaliatory environment.

Employee Hotlines

Employee hotlines are an extremely practical and inexpensive solution to what are often complex problems. The use of hotlines often is able to put an end to small problems before they become major ones, thus saving a company a significant amount of time and money. Because they act as deterrents, hotlines also mean that employees are less likely to behave in unethical ways.

Hotline service providers often offer a variety of features, some of which may not be necessary or beneficial for the organization deciding to implement. Defining and developing a reporting solution begins with an analysis of your organizational complexity. Some primary considerations are your organization’s size, industry, operational geographies, and operational style: centralized or decentralized, union or non-union, weak culture or strong culture. Additional primary considerations are complexity or magnitude of programs, operations, transactions; extent of manual processes or applications; and historical significance of risk. Decide what features would be best suited for your organization. The biggest benefits that hotlines offer to organizations are the ones that are intrinsic to their existence—detection, deterrence, and defense. Additional features, such as case management, might be great for larger companies, but smaller companies may decide that this feature isn't worth the expense.

Hotline reports should not be limited to reports of fraud and abuse. An important aspect of any good reporting solution is the ability for stakeholders to inquire about their potential actions when confronted with an ethical dilemma or to express a concern for something they believe may be occurring. It is also important to provide feedback to the reporting stakeholder as to what they can expect from the reporting process and, if you have other reporting or support vehicles in place, where and how to use them. It is important to structure the hotline system to receive actionable reports and shift frivolous concerns or other such feedback to more appropriate venues.

The most common areas of reporting for a hotline are:

- Industry-specific regulatory risks such as coding and billing, Stark, and EMTALA
- Health Insurance Portability and Accountability Act (HIPAA) and confidentiality concerns
- Conflicts of interest
- Policy/procedure violations
- Corruption, theft, and fraud
- Finance and accounting concerns
- Information or asset misuse and access
- Customer/partner/competitor concerns, including the Foreign Corrupt Practices Act (FCPA)
- Equal opportunity/affirmative action matters
- Environmental, health, and safety concerns
- Harassment and other Human Resources (HR) issues
- General inquiry/questions