COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2018
Non-retaliation

By Patrick Hogenbirk, CCEP

Patrick Hogenbirk (patrick_hogenbirk@yahoo.com) is Director, Global Compliance & Privacy at Owens & Minor in Richmond, VA and Cincinnati, OH.

Non-retaliation is such an important aspect of a compliance program, I have made it a cornerstone component in the programs that I have been involved with implementing. It has always been the first policy that I implement, and surprisingly, in my 20 years in Compliance, it has rarely been in existence. The focus has always been on non-retaliation during harassment situations, which—while extremely important—is simply too narrow a focus.

As compliance professionals, we need to think about our people first—both the people we manage, but also the people we serve—the employees, contractors, and vendors who work with and for our company. They need to know that if they report an issue, ask a question, or are involved in an investigation, we have their back, and they are not going to be retaliated against.

I have addressed this compliance need by first creating a policy on non-retaliation. That policy should outline why non-retaliation is important and why it is essential for the legitimacy of our compliance program. Of course, as we are all aware, a policy is not enough. We need to communicate and embed non-retaliation into our program and include it in training, communication, and in every talk.

The basics

As you will see below, I am providing the basics of a policy for non-retaliation. I have generalized the policy to give you a start. You will need to have your general counsel, outside counsel, and employment attorney review it. The basics have served me well and have provided associates under my watch with a comfort level that allows them to report, ask a question, cooperate in investigations, become involved in a whistleblower activity, or cooperate with a government agency, all knowing that we have their best interest in mind.

The policy purpose

This is a critical component of the policy and simply lays the groundwork for your policy. I wanted to be direct with our audience and let them know that we take retaliation seriously in our company. Again, it is a cornerstone element of our compliance program and critical for people to understand. A model policy might look like this:

> This document establishes (company name)'s policy prohibiting retaliating against, threatening, or punishing anyone who reports a possible compliance issue (violation of the code of conduct, company policy, government regulations, or the law) in good faith, or anyone who cooperates during an investigation or engages in other conduct protected by law or under this policy. Teammates who violate this policy will be subject to disciplinary action, up to and including termination of employment.

Under applicability and scope, as detailed below, we expanded our policy to include vendors who work in our facility in addition to employees, contractors, etc. Third parties and customers are important groups to include, because they might also be impacted by retaliation. As an example, I was once contacted by a soda vendor who lost a contract with the company after they reported an unsafe act within the facility. An investigation uncovered a level of retaliation from the facility manager who switched vendors after the report. The manager was disciplined, and the vendor was reinstated.

The policy is only as good as the communication channels around it. For customers (e.g., a customer who might witness inappropriate behavior), you might want to create a communication method (e.g., a brochure) and a reporting mechanism for them to use. In addition, creating a "vendor code of conduct" is always a good idea. It can communicate the process of reporting and help a vendor understand their responsibilities to your company.

Applicability and scope

A model policy should include clear definitions, such as:

> This policy applies to all associates. For purposes of this policy, "associates" are defined as employees as well as contracted/temporary workers. This could include vendors who work in our facilities (e.g., pest control, maintenance, or cleaning companies).

Under the policy statement, this component of the policy stipulates the specifics of what associates can and cannot do:

Associates may not retaliate, threaten or punish anyone who, in good faith, engages in protected actions under this policy. All forms of retaliation are prohibited, including any form of discipline, reprisal, intimidation, or other form of retaliation for participating in any activity protected by law or this policy. Protected conduct includes, but is not limited to, the following:

- Filing a good faith internal complaint (written or oral) with <department name> specifically identifying an unlawful or unethical practice;
- Filing a good faith complaint of an unlawful practice with the appropriate country or federal or state enforcement agency, such as filing a harassment or discrimination charge with the U.S. Equal Employment Opportunity Commission (EEOC) or reporting a potential safety issue to your manager;
- Participating or cooperating in good faith in an internal investigation related to an allegation of an unlawful practice or policy violation;
- Participating or cooperating in good faith in an external proceeding related to an allegation of an unlawful practice or policy violation;
- Requesting an accommodation or leave under the Americans with Disabilities Act, Family and Medical Leave Act, or state leave or anti-discrimination statute;
- Filing a worker's compensation claim; or
- Reporting an unsafe act.

Unlawful practices may include alleged ethical, compliance, or legal violations under any applicable country, federal, or state law. Examples include:

- Healthcare fraud and abuse (such as anti-kickback provisions, false claims, etc.),
- Harassment/discrimination,
- Wage and hour dishonesty,
- Safety and health violations,
- Financial irregularities,
- Foreign Corrupt Practices Act or International Anti-Bribery and Fair Competition Act infringements,
- Dishonest sales practices,
- Healthcare non-compliance,
- Improper disclosure of the company's confidential or proprietary information,
- Improper use of company assets,
- Conflicts of interest,
- Privacy or HIPAA violations, or
- Violations of government contract requirements.

Standards and procedures

When you outline the standards and procedures of the policy, it's important to call out what a "bad faith" report consists of. It should be defined and understood by the organization. Although I have never experienced a bad faith report, they do exist, and they can negatively impact your organization unless action is taken against the reporter. The elements of the standards and procedures of a policy include:

1. Reporting
    a. This is where we specify how and when to report and that we will take the report seriously and confidentially.
2. Observing or experiencing retaliation
    a. I specified a number of days in the policy, because I wanted immediate action to occur from the associate. We give associates three days to report.
3. Investigating alleged prohibited retaliation
4. Responding to a bad faith report
    a. "Teammates are prohibited from making a bad faith report, which means the teammate knew the report was false or misleading. If the company determines that a report was made in bad faith, the teammate may be subject to disciplinary action, up to and including termination."

b. We spell out the definition to ensure associates understand what a bad faith report looks like.