

# Fostering a Culture of Safety: Crafting an Effective Non-Retaliation Policy



**CJ Wolf** MD, CHC, CPC, CCEP, CIA



The Health and Human Services Office of Inspector General (OIG) recently published General Compliance Program Guidance<sup>1</sup>, and one of the many important sections in the document includes a list of a compliance officer's primary responsibilities. Among these primary responsibilities is the development of policies and programs that encourage personnel to report suspected fraud and other improprieties ***without fear of retaliation.***

It takes dedicated effort to create an organizational culture that makes personnel feel safe enough to report concerns without fearing retaliation. Leadership, messaging, training, and many other actions can help build such an environment. However, one of the most important steps in helping personnel feel safe is the development of a non-retaliation policy.

## Why is it Important?

Anyone who regularly reads the Department of Justice's (DOJ) press releases outlining settlements will notice that a whistleblower is often the first person to alert the government to wrongdoing. Most whistleblowers claim they reported the concerns internally and many say they experienced retaliation for doing so. No doubt, such retaliatory treatment played a part in deciding to blow the whistle. If for no other reason, it is likely in the organization's best interest not to retaliate.

"Among these primary responsibilities is the development of policies and programs that encourage personnel to report suspected fraud and other improprieties *without fear of retaliation.*"

Additionally, when entities sign corporate integrity agreements (CIA) with the OIG, there is almost always a provision in the CIA to establish a disclosure program that allows employees and others to report potential wrongdoing. For example, one recent CIA published by the OIG states: "The Disclosure Program shall prohibit retaliation against Covered Persons relating to use of the Disclosure Program and...shall not retaliate against Covered Persons for use of the Disclosure Program."<sup>2</sup> Following CIA elements before a problem occurs can often prevent it from occurring in the first place.

It is best practice to have a non-retaliation policy. In the OIG guidance document previously referenced, the OIG also says that written confidentiality and non-retaliation policies should be developed and distributed to all employees to encourage communication with the compliance officer and the reporting of incidents of potential fraud and other compliance concerns.

Finally, there is a provision in the False Claims Act protecting employees and others who are engaged in protected activity from retaliation. Aspects of retaliation might include being "discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in the terms and conditions of employment." 31 U.S.C. § 3730(h)(1).

[1] See <https://oig.hhs.gov/compliance/general-compliance-program-guidance/>

[2] See [https://oig.hhs.gov/fraud/cia/agreements/Community\\_Health\\_Network\\_12182023.pdf](https://oig.hhs.gov/fraud/cia/agreements/Community_Health_Network_12182023.pdf)

The OIG also believes this concept of protection is embodied in the provisions of the False Claims Act. They state that whistleblowers should be protected against retaliation and report that in some cases, employees sue their employers under the False Claims Act's qui tam provisions out of frustration because of the company's failure to act when a questionable, fraudulent, or abusive situation was brought to the attention of senior leaders.

If employees and others who are "in the know" fear retaliation, they are not as likely to speak up when compared to organizations with a culture of safety.

## What Should be Included in a Non-Retaliation Policy?

There is no single, right way to create a non-retaliation policy. Much will depend on your organization and its unique circumstances.

For example, some health care organizations might be run by a state, county, or city. These jurisdictions might have their own unique rules and regulations that should be included in the policy.

However, in general, most non-retaliation policies have the following elements:

- An introductory policy statement that demonstrates the organization's

commitment to non-retaliation of individuals who raise concerns in good faith.

- A section on the mechanisms employees and others should use to appropriately report concerns of misconduct or non-compliance.
- Definitions. There are many terms used in these kinds of policies that not everyone is familiar with.
  - For example, it is usually best practice to define or explain ideas like 'good faith,' 'retaliate/retaliation,' 'protected activity,' and examples of retaliation such as intimidation, harassment, discrimination, demotion, ostracizing or other prohibited behaviors.
- A section describing how an individual who feels retaliated against can report their concerns.
- What the organization will do when concerns of retaliation are reported.
  - Most policies include a brief outline of how such reports will be investigated and who will make decisions and determinations of whether retaliation took place.
- Consequences for those who retaliate against individuals.

- In most cases, it is important to state that disciplinary action could include termination of employment.
- The policy owner or responsible party.
- A "last revised" and effective date.
- Signatures of approvers, as appropriate.
- References to any laws, regulations, or other related institutional policies.

"If employees and others who are "in the know" fear retaliation, they are not as likely to speak up when compared to organizations with a culture of safety."

[3] See <https://www.justice.gov/criminal-fraud/page/file/937501/download>

Many non-retaliation policies are approved by a committee or higher-level management group. Those at the highest level of the organization should at least be generally aware of the key aspects of this critical policy.

In addition to having a separate policy, most organizations include a statement in their code of conduct or code of ethics that shows their support of non-retaliation for issues raised in good faith. Such statements also usually show a reference to the actual policy name, title, or policy number.

The following links are to non-retaliation policies from healthcare entities that were easily found through a public internet search. Sharing the links to these policies should not be construed as endorsement of any particular policy or strategy. Rather, the intent is simply to provide examples for compliance professionals to review.

- [https://ippvip.mdanderson.org/OnBaseWebIPPEExternalPRD/docpop/docpop.aspx?KT337\\_0\\_0\\_0=Published&KT377\\_0\\_0\\_0=Y&KT354\\_0\\_0\\_0=Y&KT345\\_0\\_0\\_0=ADM0254&clienttype=html&cqid=142&vieweronlyforsingle=true&chksum=8b79667bfc731aec42e3b56067e6a85e4ac962bb434650697404371efa00506](https://ippvip.mdanderson.org/OnBaseWebIPPEExternalPRD/docpop/docpop.aspx?KT337_0_0_0=Published&KT377_0_0_0=Y&KT354_0_0_0=Y&KT345_0_0_0=ADM0254&clienttype=html&cqid=142&vieweronlyforsingle=true&chksum=8b79667bfc731aec42e3b56067e6a85e4ac962bb434650697404371efa00506)

- <https://hcahealthcare.com/util/forms/ethics/policies/ethics-and-compliance/EC030-a.pdf>
- [https://www.blythedale.org/sites/default/files/content/inline/whistleblower\\_and\\_non-retaliation\\_policy.pdf](https://www.blythedale.org/sites/default/files/content/inline/whistleblower_and_non-retaliation_policy.pdf)

## Other Considerations:

The OIG is not the only entity opining on the importance of non-retaliation. In their Evaluation of Corporate Compliance Programs document,<sup>3</sup> the DOJ instructs their investigating prosecutors to assess whether the company's complaint-handling process includes proactive measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers.

The United States Sentencing Guidelines also state that an effectively working compliance

program will have in place a publicized 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.<sup>4</sup>

The OIG's guidance document that has been referenced previously contains a section for adaptations for large or small organizations.

They acknowledge that small organizations might not have the resources to develop extremely formalized programs and processes. However, even in these circumstances, they emphasize the importance of non-retaliation. They state, "Although a formal disclosure program may not be necessary or appropriate for a small organization, a small entity should ensure that its personnel understand the entity's commitment to compliance and to nonretaliation."<sup>5</sup>

They continue by explaining, "Even in the absence of a formal disclosure program, small entities should have policies in place that require good faith reporting of compliance issues or potential violations of law, outline a process for the investigation and resolution of reported issues or concerns, and prohibit retaliation for good faith reporting."<sup>6</sup> So, even small organizations should have written policies describing their commitment to non-retaliation.

## Conclusion:

If your organization does not have policy work that includes the topic of non-retaliation, they should create it. And, if you do have an existing policy, it might be wise to reassess and determine if it is where it should be.

[4] See U.S.S.G. § 8B2.1(b)(5)(C)

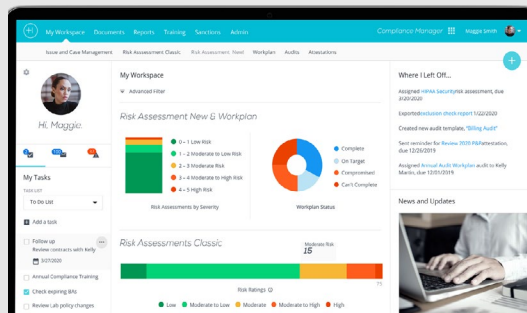
[5] See <https://oig.hhs.gov/compliance/general-compliance-program-guidance/>

[6] See *ibid*



**For more on Healthicity's [Compliance Services and Solutions](https://healthicity.com/compliance), please visit [healthicity.com/compliance](https://healthicity.com/compliance) or call **877.777.3001****

### COMPLIANCE MANAGER



**WATCH ON-DEMAND DEMO**

### RESOURCE CENTER



**EXPLORE FREE RESOURCES**