

# HR Brief

Human Resources tips brought to you by  
**Henriott Group**

April 2016

## EEOC Proposes Revised Guidance on Retaliation

The Equal Employment Opportunity Commission (EEOC) has [proposed](#) revised enforcement guidance on unlawful workplace retaliation. The proposed guidance will make it easier for employees to assert claims of retaliation, as an employee will only have to establish a “convincing mosaic” of circumstantial evidence to prove retaliation.

All of the laws that the EEOC enforces make it illegal to fire, demote, harass or otherwise “retaliate” against applicants or employees because they complained to their employers about discrimination on the job, filed a charge of discrimination with the EEOC, participated in an employment discrimination proceeding (such as an investigation or lawsuit) or engaged in any other “protected activity” under employment discrimination laws.

When an employee makes a claim of retaliation, there are three essential elements that the employee must be able to demonstrate:

- That he or she engaged in a protected activity—opposition to discrimination or

- participation in the complaint process;
- That he or she experienced an adverse employment action, such as being demoted or terminated; and
- That there is a causal connection between the protected activity and the adverse action.

Under current EEOC guidance, a causal connection exists when there is direct evidence that retaliation was a motive for the adverse action. Typically, the adverse action must have occurred within a relatively short period of time after the employee engaged in the protected activity in order to prove that the protected activity was motivation for the adverse action.

The EEOC’s proposed guidance would require an employee claiming retaliation only to “demonstrate a causal connection between the prior protected activity and the challenged adverse action by... [showing] a ‘convincing mosaic’ of circumstantial evidence that would support the [retaliation claim].”

The proposed guidance states that any “bits and pieces” that may infer retaliation must be considered. Also, the guidance would not require that the adverse action have taken place shortly after the protected activity, and it even indicates that retaliation may be established when the adverse action takes place years after the engagement in protected activity.

Employers may want to consider reviewing anti-retaliation policies and conducting refresher training. In addition, be prepared to thoroughly document non-retaliatory reasons for disciplining any employee who has engaged in a protected activity.

## DID YOU KNOW?

Wearable technology devices continue to grow in popularity. According to the global technology analyst company, [CCS Insight](#), more than 400 million wearable devices will be in use by 2020.

HR professionals must consider adopting or amending workplace policies in order to address wearable technology in the workplace. For example, many of the wearable devices that are now available make it easy for employees to record video and audio without others’ knowledge, raising privacy and trade secret concerns.

Consider the risks and opportunities that wearable technology introduces to the workplace and develop policies that protect both employer and employee interests.

## IRS: Payroll and HR Targets of New Phishing Scheme

The IRS has issued a [bulletin](#) to alert payroll and HR departments that they may be targeted in an email phishing scheme that requests employees’ personal information.

This tax season, cyber criminals have been sending phishing emails to payroll and HR professionals claiming to be the CEOs of the companies. The emails contain the actual names of the companies’ CEOs and request a list of employees and their personal information, including Social Security numbers and dates of birth.

Several payroll and HR departments have mistakenly sent payroll data, including employees’ Forms W-2, to cyber criminals after receiving one of these phony emails.

According to the IRS bulletin, some of the details contained in the emails include a request for an updated list of employees and their personal information, or a request for individual 2015 Forms W-2 and an earnings summary of all staff for a review.

Don’t become a victim of this scam: Before responding to a request for personal employee information from a company executive, double check who the sender is. If the request truly is from a member of the executive team, he or she shouldn’t have an issue with your diligence in protecting employees’ information.