HRM
SERVICES

Access to Confidential Employee Data

By Jodi Schafer, SPHR, SHRM-SCP | HRM Services | www.WorkWithHRM.com

October 2021

QUESTION: We have an employee who gained access to confidential employee information. How should we respond to the employee and prevent this from happening again?

ANSWER: When thinking about data security, we often think about protecting customer or patient data, including adhering to HIPAA or FERPA regulations, depending on the industry. Businesses sometimes don't put enough emphasis on also protecting employee private information, which if shared, poses a serious risk to the company. Confidential employee data includes personal data such as social security numbers, addresses, and marital status, as well as employment information such as salary, benefits, and background checks. Performance review information, administrative data such as timesheets and tax forms, and job termination data should also be kept confidential.

When you think about security, you may think about networks, firewalls, and password storage systems. While this technical infrastructure is critically important, they are only one part of keeping data secure. Cybersecurity experts have learned that people and their habits are the biggest risk and most challenging to manage. One misstep by an employee can expose the company to damages, financially and reputationally. Also, these incidents can create distrust among employees.

Start by investigating the incident. Hold a conversation (and document it) with the employee who gained access to the confidential information. Make it clear that the information they accessed was confidential and they are not to share it, in any form, with anyone else. Also ask, if you don't already know, how they gained access to the information. Was it saved in a folder that they happened across? Or did the employee actively seek out the information? The consequence for the employee will differ drastically depending on these details. Also ask if they know of any other employees who saw the information so you can understand the scale of the breach. Once you have more information, you need to address the situation with the employee(s) and also within your systems, policies, processes, and safeguards to prevent it from happening again.

Depending on the details, there may be no consequence to the employee. In fact, they may have helped your company by notifying you of the issue so you can put new measures in place. If the circumstances indicate that the employee intentionally accessed the information and/or shared it with others, you may decide to formally reprimand the employee and document it in their file. If their job position regularly interacts with confidential data, you may consider whether they are a good fit for the role and/or decide to shift their responsibilities.

One of the most important steps is to put stronger policies and procedures in place to prevent this incident from happening again. You may choose to do an internal audit, where you check all access points to your Human Resource Information System (HRIS), payroll, and accounting systems and personnel files/documents to make sure only those who need access, have access. This may also include reviewing files in your document storage system to make sure there are no confidential data accessible. These processes need to be done for both hard copy and digital depending on the set up of your data storage.

Cybersecurity is one of the biggest concerns for businesses these days. The experts say it is not a matter of “if” but “when” companies will have a breach, whether it is internal or external. Partnering with a strong IT company that specializes in security is also worth the investment, as is procuring a cybersecurity insurance policy to protect your business when incidents occur.

In addition, employee education about data security is well worth the investment. Employees are your best line of defense for protecting data. After your policies and procedures are finalized, train employees and involve them in implementing safeguards. This builds ownership and commitment to keeping confidential data safe.