Take Steps to Protect Your Employees' Personal Information

As identity theft continues growing, one of the main treasure troves that criminals covet is employee data. After all, it typically contains your staff's personally identifiable information and other information that should not fall into nefarious hands.

This kind of data theft can happen through brute force hacking, e-mail phishing campaigns and even your own employees making off with the data. Appropriated personally identifiable information can be sold on the dark web or used by the thieves themselves to steal people's identities, open credit accounts and even bleed their bank accounts dry.

If someone does gain access to personnel files, you could be on the hook for penalties, responsible for notifying all affected parties and expose yourself to legal liability.

Fortunately, there are steps you can take to keep your employees' information from falling into the wrong hands.

Keep your records secure

Start with the low-hanging fruit: Paper records. Files containing personal information should be kept in a sturdy filing cabinet or secure location, with access limited to the individual who is chiefly responsible for maintaining the files and one member of upper management.

As for data stored on a server, make sure that it is protected with a password that only staff who need to access information can reach. Have secure servers that use encryption. Stay on top of patches for your software.

Set policies and procedures

Besides securing your personnel's data, you also need to have in place policies and procedures for handling the information. It should start with which data the company will protect and how it will be protected.

Your policies should prohibit unauthorized copying, sending, viewing or use of personal employee information. Policies should state who is authorized to access the information and the consequences of accessing it if not approved.

These policies should be in writing and disseminated among your staff. Consider holding a meeting to go over the policies, including the steps you take to protect their data.

Restrict access to those who need to know

Permit access to employee files on a need-to-know basis only.

For example, a manager should have access to their subordinates' employee performance metrics, number of absences from work and performance reviews. But they should not have access to their Social Security numbers, medical history, insurance information and other private information that Human Resources may keep.

Keep an access log

Keep a log of each time someone accesses files containing sensitive employee data. The information collected should include who accessed the data, when they accessed it and why. Keeping this log may require purchasing new software that can track these functions.

You should review the logs regularly to identify any suspicious activity.

If you learn that someone may have accessed employee records without authorization, you should investigate the incident immediately. If you discover one of your staff has access the files, you should discipline them in accordance with your policies.

Inform all affected employees accordingly and offer to pay for credit monitoring for them.

Due to the sensitivity of the matter, you may be required by state or federal law to notify regulators. It would be wise to call your attorney to find out what your obligations are under state laws.

The takeaway

It's paramount that employers take all steps necessary to protect their employees' sensitive information. Failure to do so could lead to identity theft, and a degree of financial liability on your part.

You may even be sued for failing to protect the information.

One final note: There has been a lot of talk about the Health Insurance Portability Accountability Act in light of the COVID-19 pandemic and the protection of individuals' medical records.

HIPAA does not apply to employee health information maintained by an employer.

It applies only to "covered entities," which are defined as:

- Health plans
- Health care clearinghouses, and
- Health care providers that electronically transmit certain health information.

That said, if you possess health information about employees, you should take steps to protect that information.

*This material was created by Insurance Newsletters and authorized for use by Brown & Stromecki Agency

###