Make privacy a cornerstone of your culture

Think about the amount of information and records that you maintain about employees. Now, think about the valuable information you possess about your clients and customers. Do you treat those two groups of data the same when it comes to confidentiality?

Employment attorneys warn that some employers don't. They're taking a substantial risk by plowing more time and effort into protecting client information and shrugging off employee data privacy. One problem hindering the effort is lax supervisor attitudes about the importance of privacy.

The fact is confidentiality can quickly become a legal issue in many workplace decisions and activities. While certain employment-related data obviously must be protected, here are a couple more frequently overlooked employee data categories you should also protect:

Privacy during hiring

During the selection process, you should keep applications, interview notes and references under wraps. But other sources of confidential information exist beyond the personnel file.

With many organizations using 360-degree performance reviews and peer interviewing, managers and co-workers may stumble upon confidential information without knowing it. It's important to stop privacy leaks before they start. How? By teaching everyone involved to keep quiet about information that's shared in interviews and job reviews.

The hiring supervisor or HR should be the only ones who check references. And the results shouldn't be shared with others, especially subordinates, even if the employee helped in the interview process. Subordinates who are part of a search committee should be excused from the discussion when you develop hiring recommendations. Lastly, never allow outgoing employees to oversee the selection process for their replacements.

Privacy in health data

Consider the employee in drug rehab who returns from a leave of absence to find the details of his recovery had been announced at the office. Or say an employee talks over a private health issue with a co-worker only to find the secret spread to others.

Each of these scenarios carries potential legal hazards. When private medical information is disclosed, the employer opens itself to lawsuits under the ADA's confidentiality provision. (Employees don't need to be disabled to file such lawsuits, and former employees can file those suits, too.) And you face additional liability under the Health Insurance Portability and Accountability Act (HIPAA), which requires you to keep such data private and to ensure its security.

That's why it's important to hammer this point home to supervisors and employees: Never disclose medical information about employees or former employees.

Privacy training

"When it comes to confidentiality, the ability to see the facts from another person's viewpoint will be very helpful in preventing problems," says Joan Rennekamp, an HR consultant in Denver who helps attorneys improve their clients' HR practices. "Breach of confidentiality cannot only be a legal problem. Perhaps more importantly, it can create a breach of trust that is difficult, if not impossible, to repair."

Rennekamp says it's crucial to train every staff member on privacy issues. At least annually, management should discuss and review with all employees the types of confidential information they may encounter in their jobs and the proper way to handle it.

"It's not productive for any employee to become the 'rumor mill' for the company, and this point needs to be consistently enforced," she says.

Make privacy a priority

Here are two ways to make confidentiality a priority in the minds of employees and managers, according to Rennekamp:

1. Discuss the concept of "ownership of information." Think of information just as you would a tangible object that has an owner. In that context, if an employee communicates her health problem to a supervisor, the employee still "owns" that information. The supervisor, or any other employee, doesn't have the right to pass along that information unless some overriding concern arises, or unless the owner gives permission.

2. Adopt a policy. Draft written guidance for employees regarding how to handle confidential or sensitive information. Your policy should include descriptions of the types of sensitive information that might become an issue, procedures for protecting information (locked files, passwords, desks cleared each evening, etc.) and procedures for handling media inquiries.

At the same time, draft a policy that explains the level of privacy your staff can expect relating to their own desk, computer, office and any personal items brought to the workplace. By outlining those expectations, Rennekamp says, you'll have a better chance of the privacy mind-set sinking in.

Make privacy a priority for employees

Here are two ways to make confidentiality a priority in the minds of employees and managers, according to Joan Rennekamp, an HR professional at a Denver law firm:
1. Discuss the concept of "ownership of information." Think of information just as you would a tangible object that has an owner. In that context, if an employee communicates her health problem to a supervisor, the employee still "owns" that information. The supervisor, or any other employee, doesn't have the right to pass along that information unless some overriding concern arises, or unless the owner gives permission.
2. Adopt a policy. Draft written guidance for employees regarding how to handle confidential or sensitive information. Your policy should include descriptions of the types of sensitive information that might become an issue, procedures for protecting information (locked files, passwords, desks cleared each evening, etc.) and procedures for handling media inquiries.
At the same time, draft a policy that explains the level of privacy your staff can expect relating to their own desk, computer, office and any personal items brought to the workplace. By outlining those expectations, Rennekamp says, you'll have a better chance of the privacy mind-set sinking in.