

Risk Management 8

Risk Management (cont'd)

What is our exposure for defamation claims?

Recently, employers and employment attorneys have focused their attention on potential defamation claims arising from references given on former employees. The potential for such an action arises when a former employee does not get hired and blames the former employer. However, these suits are not limited to reference situations. An employee can accuse the employer of defamation for what its officials say to each other, to other employees, customers, and third parties during administrative hearings, evaluations, and exit interviews. In many cases, employees bringing wrongful discharge suits also make the associated claim of defamation. Many organizations have responded to the fear of defamation claims by limiting their comments. Some employers will not give employees the reasons for their discharge, or limit outgoing references to a simple statement verifying the basic employment information (employment dates, positions, and most recent salary).

The failure to be honest about the reasons for termination acts as an invitation to the employee to file a wrongful discharge suit. Employees who are not told the reasons they are being let go may assume a discriminatory reason.

While reducing the chances that an employee will make a defamatory statement about a former employee, the adoption of a "name, rank and serial number" reference policy enables poor performers and dangerous employees to move freely from one employer to another. "Neutral" references for dangerous or potentially dangerous individuals leave the organization vulnerable to claims alleging the negligent "failure to warn." Also, if an organization receives a favorable reference for an employee whose former employer had documented deficiencies, the new employer may have grounds for a negligent referral claim. All organizations face this dilemma and should evaluate the risks of defamation carefully. Additional insight on the subject of defamation may be helpful as a nonprofit considers its communications and employment policies.

For nonprofit organizations, the defamation risk also extends to its clients. Nonprofits often handle sensitive information, such as medical histories, criminal records or job histories that could be defamatory. Every organization has a duty to properly handle and use this information. An employee or volunteer who has access and knowledge of information that he or she does not have a legitimate reason for handling or knowing, creates a liability exposure for the organization.

Defining Defamation

Defamation is any language, spoken or written, that tends to lower the esteem of an individual within any respectable group. Slander is a spoken defamatory comment, while libel is defined as a written defamatory communication. In order for a plaintiff to prevail in an action alleging defamation, he must prove that:

1. The defendant (in this context, the employer) intentionally made a false and defamatory statement;
2. The statement was made to one or more third party;
3. The third party understood the statement's meaning; and
4. The plaintiff was injured by the communication or it is the type of communication where the law does not require proof of injury.

Defenses To Defamation

The availability of several defenses makes it very difficult to win a lawsuit alleging defamation. There are two fundamental defenses to a defamation claim: truth and privilege. Truth is an absolute bar against recovery even if the statement is defamatory and made with malice. Therefore, if an employee of a nonprofit informed a third party that a former employee of the nonprofit was a convicted rapist, while the statement is clearly defamatory, if it were true, the defamed party would be unable to recover damages from the nonprofit.

Privilege is the second principal defense to defamation. The privilege defense may protect the organization from liability when a statement is made in good faith and for a legitimate purpose, even if false or defamatory. Privilege can be either "absolute" or "qualified." "Absolute privilege" applies when public policy or the administration of justice requires complete immunity. In this regard, absolute privilege applies to witnesses in legislative, executive and judicial proceedings, such as EEOC and unemployment compensation hearings.

"Qualified privilege" bars recovery by a plaintiff when the organization makes the communication in good faith to someone with a legitimate interest in hearing it. Employee references generally fall within the qualified privilege defense unless a reviewing court determines that the organization abused the privilege. An organization abuses the privilege when the speaker makes the comment with "malice" or there is excessive publication. The courts usually find malice when the communication is made with ill will, spite, hatred or an ulterior motive, or when an employer makes a statement with the knowledge of its falsity or reckless disregard for the truth.

Excessive publication is when the communication is made to people without a legitimate interest or "need to know." The number of people who receive the communication is immaterial unless at least one of them did not have a "need

to know."

Managing the Risk of Defamation Claims

Due to the qualified privilege defense for employment references, nonprofits have a good chance of mounting a successful defense in a suit alleging defamation and based on statements made about former employees. The existence of a valid defense, however, does not stop an individual from filing a defamation claim. Also, remember, defamation cases go beyond references. Anytime an organization official is talking about an employee, volunteer, or client to another party, there is the potential for a defamation action. Every organization can adopt policies and procedures to minimize the chance of a defamation charge. A summary of suggested practices follows:

1. Limit Access to Personnel and Client Files.

Keep all personnel and client files under "lock and key," either physically or with limited computer access. Only persons with a legitimate "need to know" should have access to personnel and client files. The "qualified privilege" defense only applies when the recipient had a legitimate need to know and the organization's personnel acted in good faith.

2. Develop and Follow a Reference Policy.

Develop an organizational policy for providing references. The policy should require written permission or authorization from the former employee, volunteer, or client to release the information. The authorization should include a "hold harmless" provision. Designate which employees can provide references and train them in the legal and proper way to give references. However, inform all employees of the policy and whom to refer the requests to for handling. Some organizations will only respond to written requests for references. This policy enables the nonprofit to verify the identity of the person requesting the information and determine that the requester has a legitimate interest in the information. Some nonprofits use a "Reference Form" instead of oral or written references. A Reference Form is a document that the organization prepares prior to the departure of an employee or volunteer. The former employer sends the form to any organization requesting a reference. The form contains a section where the employee or volunteer can indicate his or her disagreement with any of the statements made. With a reference form, the person knows what the organization is going to say before he or she leaves.

3. Adopt a Confidential Information Policy.

Although it seems like common sense, the nonprofit needs to remind some employees and volunteers of the precautions required when working with confidential information. The policy should identify the types of information that is confidential and how the person should handle the information. Also, remind

employees, volunteers and clients that not all intraorganizational communications are privileged. Both parties must "need to know" the information in order for the privilege to apply.

Summary

Nonprofit organizations face unique defamation exposures. Potential claimants include volunteers and clients in addition to employees. Given the commitment of most nonprofits to help -- not harm -- people, the importance of guarding against defamation is paramount. With simple precautions and monitoring, a nonprofit can protect its stakeholders from the effects of defamation as well as the organization itself against the financial and other costs associated with defending a defamation suit.

What is our risk for an invasion of privacy claim?

As computer technology, the "information superhighway," and state-of-the-art telemarketing schemes intrude into our lives, many people are increasingly concerned about the right to privacy. People are more conscious of their desire to avoid the encroachment of government and business into their daily lives. Every nonprofit should recognize this fact and the attendant risks of possessing and handling confidential information.

Defining invasion of privacy

The concept of invasion of privacy emanates from three principal sources. The first source is the Fourth Amendment of the United States Constitution. The Fourth Amendment protects against "unreasonable searches." However, the amendment has limited affect on privacy concerns. The prohibition on "unreasonable searches" only applies to searches by a governmental entity, agent or instrument of a governmental entity. The limitation does not apply to private employers, except in California, where an employer must show a "compelling reason" for searching an employee or their work space.

Invasion of privacy claims can also arise from statutory provisions. Federal and state statutes shield and protect employees from invasions of privacy. Such laws are often a part of anti-discrimination legislation including laws that limit employers' access to and use of credit histories, criminal histories, political activities, medical information, and surveillance activities.

Finally, common law and tort theories of negligence and outrageous contact are often the basis of invasion of privacy complaints. Four types of invasion of privacy claims exist under common law:

Unreasonable intrusion upon the seclusion of another. The following three elements must exist before a plaintiff can prevail on an unreasonable intrusion

tort claim:

1. The intrusion, physically or otherwise, upon the solitude or seclusion of another must be intentional.
2. The intrusion must be into the private affairs or concerns of another.
3. The intrusion must be highly offensive to a reasonable person.

Appropriation of another's name or likeness.

Unreasonable publicity given to another's private life.

Publication that unreasonably places another in a false light before the public.

Activities That May Lead to Invasion of Privacy Claims

Standing to file a lawsuit alleging invasion of privacy is not limited to employees. Anyone who believes that the nonprofit has intentionally intruded into their "seclusion" can file a claim. While the greatest risk facing a nonprofit in this area is from employee claims, a nonprofit cannot forget its responsibilities to and the risks associated with volunteers and clients.

Invasion of privacy charges often arise from searches of people, their personal belongings and their work space; electronic monitoring (phone calls, computer activities and files); surveillance; the maintenance of personal records (especially medical files); and various forms of testing (drug and alcohol, psychological and genetic). These activities are generally legal when undertaken in a non-offensive manner and with a legitimate business purpose.

The Nonprofits' Insurance Alliance of California (NIAC), a liability insurance pool for California nonprofits, reports that 3% of all claims filed under Directors' and Officers' Liability policies allege invasion of privacy. While this statistic illustrates the relative infrequency of claims alleging invasion of privacy as compared to other sources of D&O claims (such as claims alleging wrongful termination), most lawsuits against nonprofits require considerable financial resources and long periods of time to defend. As a result, minimizing the likelihood of these claims is an appropriate strategy for a nonprofit committed to preventing the erosion of its assets.

Risk Management Techniques

Limiting Expectations of Privacy

For a plaintiff to win an invasion of privacy action, the intrusion must be intentional, into another's private affairs, and highly offensive to a reasonable person. Employees' expectation of privacy is a factor the courts consider in determining if an action is unreasonable. Therefore, employers should inform employees about the "lack of privacy" in some work areas. "Open areas" generally include those areas related to work and generally within the

employer's control. Due to the variety of situations, establishing a uniform standard for employee privacy is impossible. Typically, an office occupied by one person with floor-to-ceiling walls is considered more private than an office shared by three employees. Consequently, each organization must create its own policies and procedures.

A nonprofit's office policies and procedures may act to reduce an employee's expectation of privacy. Some policies to consider are those concerning electronic mail, computer usage, disk storage, telephone usage, drug testing, lockers and personal belongings searches, as well as others that may be unique to your organization. If the organization will monitor phone calls, computer work or conduct video surveillance, it should notify all employees of these practices. In addition, the organization must base its policies on a legitimate business purpose.

Access to Medical Information

Medical information is a particularly sensitive subject. Keep all medical information and histories in limited access files that are separate from personnel files. Besides security concerns, separate medical files reduce exposure for discrimination claims. An organization can only reveal employee medical information in three ways. First, nonprofit can disclose the information to a supervisor who needs to know to accommodate the employee's special needs. Next, management can release medical information to emergency medical personnel when responding to an emergency. Lastly, an employer can release medical data to comply with government requests. Medical files should only be accessible to those who "need to know" such information.

Investigations and Surveillance

Another aspect of the privacy issue is the nonprofit's procedures for investigating suspected employee theft or other activities that may lead to the search of an individual or his or her work space or belongings. Nonprofits should always consult legal counsel before establishing or revising such procedures. It is also appropriate to consult legal counsel and possibly law enforcement agencies before conducting a search or surveillance. Many suits arise from forced or coerced searches that are highly offensive.

Releases

Another risk management technique is to secure a waiver or release from all employees, volunteers and clients regarding the use of their names and likenesses. Many nonprofits print brochures or advertisements, have videos or sponsor web sites that contain pictures of employees, volunteers, and clients. A nonprofit may be subject to an invasion of privacy claim if it did not secure the subject's permission to use their likeness. The misappropriation is particularly

important when dealing with children since the organization may be exposing them to potential harm.

Summary

Invasion of privacy claims are rare, but they do occur. A nonprofit should carefully review its policies and procedures to ensure that it is protecting the rights of employees, volunteers, and clients. The involvement of legal counsel is always appropriate when addressing the issue of privacy rights. Your agency should strive to balance the rights of others against the organization's needs and commitment to conduct its operations safely.