THE HARTFORD

Loss Control TIPS

Technical Information Paper Series

*Innovative Safety and Health Solutions*SM

E-Mail Liability Concerns

Most businesses today have some electronic mail (e-mail) capability; and most find it to be an extremely efficient way to communicate. However, users and managers should be aware of potential risk management issues concerning the use, storage, and deletion of electronic mail messages and other forms of electronic communications. Electronic communications are of concern in the areas of employment practices, personal privacy, and many forms of litigation.

Develop a Program

The first and most important step in reducing the liability associated with e-mail is to develop and implement a program to address the risks. Document the program and distribute it to all employees who use e-mail. Establish policies and include them in employee handbooks. Be sure that employee orientation programs address the policy, and require employees to sign off that they have read and understand the program. Review the program periodically and update it as necessary. A legal advisor should review current policies and procedures as part of this process.

Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) of 1986 prohibits the unlawful intentional interception of wire, oral, and electronic communications. It also prohibits the unlawful intentional access to such communications while they are in electronic storage. The law began as the "anti-wiretapping" act, designed to combat the eavesdropping excesses of the Watergate scandal in the late 1960s. The law now deals with electronic communications, including:

- Electronic mail
- Digitized transmission
- Video teleconferences

Thus, it would seem that companies who provide their employees with such things as voice mail, e-mail, or video-conferencing would violate the ECPA if they monitored these communications. However, the law recognizes the legitimate needs of businesses to monitor such communications and, therefore, allows for the interception of electronic communications or access to stored electronic communication when "one of the parties has given prior consent." The concepts of prior consent and the employees' expectation of privacy are key to drafting appropriate policies and procedures regarding the company's ability to monitor electronic communications.

Legitimate Reasons for Monitoring Electronic Communications

Employers have legitimate reasons for monitoring electronic communications, including:

- Monitoring employee performance
- Detecting employee misconduct
- Reducing liability arising from employee acts[1]

Monitoring Employee Performance

Employers may monitor employee performance to determine productivity, quality of work, and customer satisfaction. For example, if you call your bank to inquire about your balance, you may hear a message that states that the call may be recorded for quality control purposes.

Detecting Employee Misconduct

Employers may monitor electronic communication to detect employee misconduct such as gambling or improper disclosure of company information. If the employer were not permitted to monitor electronic communications for this purpose, employees could share company secrets simply by sending e-mail.

Reducing Liability Arising From Employee Acts

Employees can place the company at risk from liability in a number of ways such as downloading illegal or sexually offensive materials from the Internet, making inaccurate or untrue products claims, or engaging in illegal activities via a computer or other electronic communication devices.

Programs and Policies for Business Use of Electronic Communications

Programs and policies that cover employee use of e-mail, voice mail, the Internet, and other forms of electronic communications should include, but not necessarily be limited to, the following[2]:

1. The program should include statements that indicate that:

- ☐ Employees' use of e-mail, voice mail, Internet access, and other forms of electronic communication are subject to management review. This will reduce employees' expectation of privacy with regard to electronic communications.
- ☐ Employees' use of electronic communications is limited solely to legitimate business purposes.
- ☐ Although the company may provide for individual passwords, the passwords can and may be overridden by the company and its authorized personnel.
- ☐ Employees who violate the company policies and procedures related to electronic communications are subject to disciplinary action, up to and including termination of employment.

2. The program should include statements that prohibit:

- ☐ The use of electronic communications that is contrary to state/federal/local laws.
- ☐ Inappropriate messages and information. This would include telling offensive jokes and the distribution of other offensive materials, pictures, etc.
- ☐ Any use of electronic communications that could damage the company's/organization's reputation or put it at risk for legal action.
- ☐ Distribution via electronic communications of company proprietary information.
- ☐ The use of others' passwords or the accessing others' messages, except by authorized personnel for legitimate business purposes.

3. The program should be published as part of the company policies and procedures and in employee handbooks.

4. Employees should be required to sign off that they have read and understood the program. Sign off statements should be kept on file.

The program should also contemplate that there could be a need to access electronic information as part of the discovery process in a litigation proceeding. Although employees regularly delete electronic information, especially e-mail, the information is often still stored on the company system. As such, it can become discoverable in a litigation. Because of this, information that reflects poorly on the company, or that could be interpreted as discriminatory, can be particularly damaging. Therefore, companies must implement a program to regularly eliminate unnecessary data. In doing so, the company must also be aware of situations that could lead to charges of spoliation of evidence in an on-going litigation proceeding. Human resource managers and others who manage the company's information should work with the company's legal advisor and technology experts to determine what information to store, for how long, and why.[3]

In her article " What If Your E-mail Ends Up in Court?," (*Workforce*, July 1998), Brenda Paik Sunoo offers "8 Tips to Stay Out of Trouble." She cautions that the employer should memorize these facts to help the company stay out of trouble:[4]

- ☐ Legally archived or deleted messages can be acquired by a court of law or government agency in regard to antitrust, discrimination, termination, or copyright infringement investigations.
- ☐ E-mail is not the place for discussing sensitive issues, such as suspicions, employee performance, hiring, or firing. If you do use this venue for such issues, always consider it a formal and permanent form of communication.
- ☐ Stating a negative opinion or feeling about an employee while using e-mail lends merit in a legal proceeding related to discrimination or termination.
- ☐ Prosecuting attorneys count on the fact that your e-mail archives will be ripe with incriminating information. They want you to be careless with your e-mail; disappoint them.
- ☐ Certain comments, suggestions and even graphics delivered by e-mail to others can give merit to a harassment claim.
- ☐ Be careful what you write about others. You can't control who will read your documents.
- ☐ Downloading and viewing graphics that are personal in nature are not appropriate at work.
- ☐ Common sense will usually tell you what you should or should not do. If you even wonder if something is inappropriate – don't do it.

Conclusion

Employers must develop programs to address the liability risks associated with electronic communications. The program must comply with the provisions of the Electronic Communications Privacy Act. Employers have legitimate reasons for monitoring electronic communications, including monitoring employee performance, detecting employee misconduct, and reducing the potential liability arising from employee acts. Such monitoring is permitted as long as employees give prior consent and there is no expectation of privacy. The program should be disseminated to all employees. Training should be provided, with appropriate employee sign-off. Legal review of the program policies and procedures and periodic updating is critically important to reduce the exposures in this area.

Notes

1. Noonan, Robert. *Personnel Law Update,* 1998.
2. Ibid.
3. Sunoo, Brenda Paik. "What If Your E-mail Ends Up in Court?" *Workforce* 77 (7): 36-41, July 1998.
4. Ibid.

For more information, contact your local Hartford agent or your Hartford Loss Control Consultant.
Visit The Hartford's Loss Control web site at http://www.thehartford.com/corporate/losscontrol/