CNPS – Cyberlaw

By Ann Tapp, Professional Liability Officer

Introduction

Many nurses use the Internet at home for personal matters, and at work to do research, access information and communicate. This novel communication tool is convenient, efficient and has opened many doors for us, but not without legal risks. It is important to be aware of the legal risks involved when using the Internet, and to take a number of simple risk management precautions to decrease your employer's and your own potential liability exposure. In this article, three areas of cyberlaw will be addressed.

Cybercrime

The first area involves cybercrime. Cybercrime refers to a large group of computer-related crimes including fraud, forgery, unauthorized access to computer services or systems, unauthorized copying of computer programs, cyberstalking and computer sabotage by means of worms or viruses 1 .

Why should cybercrime be a concern for nurses? It can be a concern from two perspectives. The first relates to potential criminal liability. For example, if a nurse intentionally sabotages a computer system by spreading a computer virus that nurse could be charged with the offence of unauthorized use of computers under section 342.1 of the *Canadian Criminal Code*. And, if that same nurse wilfully destroys, alters data or interferes with the lawful use of computer data, the nurse could also be charged with mischief in relation to the data (s. 430[1.1] *Canadian Criminal Code*). If convicted of these offences, the nurse would have a criminal record and could be subjected to a maximum penalty of 10 years imprisonment.

The second concern is economic. These types of crimes can be financially costly for individuals and organizations. For example, one of the most famous recent viruses, the Lovebug, was released in May of 2000 and circled the globe in very little time. It was estimated that the repair costs to corporations worldwide would be in excess of $10-billion 2 . Because of the risk of damage to either your personal computer or an organization's own computer system from an incoming virus, or liability for passing on a virus, this matter must be treated seriously. In addition to using security technology including firewalls, anti-virus software, intrusion detection tools and authentication services, many businesses are closely examining their existing insurance policies to determine if they have appropriate coverage for losses caused by cybercrime or computer viruses. If they do not, some of these businesses are purchasing additional insurance coverage for such potential losses.

Privacy

The second area relates to privacy. There have been numerous articles in the media involving cyberterrorists hacking into confidential computer networks like the White House, the Pentagon, the Center for Strategic and International Studies (CSIS) and banks. At a personal level, these events have heightened our awareness of the vulnerability of our personal information.

To combat these legitimate privacy concerns, the federal and some provincial governments in Canada have developed, or are in the process of drafting, new privacy legislation to better protect the personal information of Canadians. On 2 January 2001, Canada's new federal electronic privacy law, the *Personal Information Protection and Electronics Documents Act* 3 (PIPEDA) took effect. The intent of this legislation is to protect an individual's privacy by setting basic rules on how businesses compile and share both paper and electronic records. PIPEDA will first affect only federally regulated private sector organizations such as banks, telecommunications and transportation companies and any other business that discloses personal information outside a single province, both nationally and internationally for consideration. By 1 January 2004, this legislation will cover health care information and will apply to any organization in the course of commercial activities within a province or territory, unless the province or territory has enacted substantially similar legislation.

To meet these new legislated requirements, organizations, including hospitals, will be required to establish a privacy policy and rules governing both the internal and external access to personal information. As nurses, you may become involved in the development and implementation of these policies. Safeguards that should be included in those policies include 4 :

- limiting the categories of personal information or the types of files that may be accessed by various employees or groups of employees
- creating security systems to restrict access to only authorized personnel
- creating systems to track access to and disclosure of personal information
- establishing protocols to approve and record "non-routine" access and external requests for information
- establishing protocols to approve and record "non-routine" access and external requests for information
- establishing security measures to protect personal information when it is copied, transmitted electronically or by facsimile
- developing standards for maintaining the accuracy of information and deleting information when it is no longer required ?

Internet Misuse in the Workplace

The third area relates to Internet misuse in the workplace. As a nurse, you may wonder how this relates to

you. With the current staffing you are too busy to access the Internet - let alone use it for personal reasons. Although you may be very busy on your shifts, there are some nurses who do find time to access the Internet for personal use. Just how frequently does this happen? A Canadian poll conducted by the Angus Reid Group Inc. reveals that 34 per cent of the respondents had Internet access at work and of those individuals 78 per cent said that they log onto the Internet for personal reasons. These same employees spent an average of eight hours online per week and at least two hours for personal reasons. This accounted for 26 per cent of their Web surfing time at work, or a total per annum, of 800 million hours of personal surfing time 5 .

Not only is the time spent on these sites an issue, but the type of sites accessed is also a concern to employers. What type of sites do employees access? A second United States (U.S.) Angus Reid poll indicates the following breakdown of sites accessed by American employees who engage in personal online surfing at work: 89 per cent accessed research or search engines; 75 per cent checked headlines such as news and sports; 67 per cent shopped around or did online price checking without making purchases; 49 per cent checked out the stock market in general or how personal investments were doing; 45 per cent made online purchases; 22 per cent played online games; 14 per cent did online banking; and 11 per cent viewed adult sites 6 .

These reports have increased the awareness of employers about the prevalence of personal usage of the Internet during working hours. Needless to say, employers are concerned about the impact on work productivity and potential liability exposure because of the type of Web sites their employees are accessing and the use they are making of that information. To address these issues most organizations are developing guidelines and policies to deal with Internet work usage.

Many employees believe that, even though these Internet usage policies exist, visiting personal Web sites during working hours is a personal matter without any potential legal consequences. This is incorrect. In Canada, the courts have upheld the employer's right to set standards relating to computer usage and to discipline employees for breaching those standards. And, there have been cases where breaching an employer's Internet usage policy has resulted in disciplinary action by the employer and even termination of employment.

In one labour arbitration case 7 , for example, a Respiratory Technologist (RT) was assigned to work in an adult intensive care unit (ICU) which was completely computerized. One of the programs available on this computer system to obtain access to the Internet was Netscape Navigator. A visitor informed the nursing unit manager of the ICU that employees were accessing the Internet for non-business purposes at work. An investigation revealed that a number of non-identifiable employees had accessed the Internet for non-business related purposes and viewed sites depicting pornography and violent images. A decision was made to discontinue access to the Internet in ICU and to monitor all computers in that department for

Internet access. Two memos were sent to the staff informing them of the new policy. One month after the new policy was in place, an audit revealed that an unknown person had accessed the Internet on two consecutive nights from a vacant patient room located in a remote corner of the ICU. A security-installed hidden camera in the room revealed the RT using the computer. As part of the hospital's investigation, the information on the video tape and the computer access records were cross-referenced and revealed that the RT had accessed the Internet to view pornographic sites. Because the RT used the Internet for non-business purposes and failed to be honest about the use during the investigation, the hospital terminated the RT's employment. The RT grieved the termination, but an arbitration panel upheld the termination and dismissed the grievance.

Conclusion

To limit some of the potential legal risks related to using the Internet health care organizations should consider: educating staff about the legal risks related to Internet use; developing written policies related to Internet use, privacy and confidentiality; conducting periodic audits; enforcing the policies; and reviewing their liability coverage for claims related to Internet use.

References

1. Ramiall, V. Of viruses and worms: Cybercrime is on the rise, *The Lawyer's Weekly*, August 17, 2001.
2. Whaley, F. Data security's weak links Lovebug illustrates importance of local laws, *Corporate Times*, December 2000, 10(109), 16.
3. R.S.C. 2000, c.5
4. Latest Developments on Personal Information, INFO EXPRESS, Ogilvy Renault, April 2000.
5. Ipsos Reid, Public Release Date July 4, 2000, online: Ipsos Reid http://www.ipsos-na.com/news/pressrelease.cfm?id=1058
6. Ipsos Reid, Public Release Date May 19, 2000, online: Ipsos Reid http://www.ipsos-na.com/news/pressrelease.cfm?id=1031
7. *Calgary Regional Health Authority v. Health Sciences Assn. of Alberta (Dickinson Grievance)* [1999], A.G.A.A. No. 66 (QUICKLAW).

Note: This article has been reprinted with permission from *Canadian Nurse*, April 2002.