8

Privacy, security and confidentiality

JO LUCK

This chapter provides health professionals with an overview of the security risks to health information systems and available countermeasures.

When describing the important assets of a health care facility, people list the buildings, equipment, finances and personnel. But rarely do people think of the information held by the hospital as being an asset. Yet the information is a very valuable asset. Hospitals would not be able to function for very long without access to the data held in their health information systems. The value of the information is equivalent to the amount of money it would cost to recreate the health information system in the event of the computer files being completely corrupted or destroyed. If the system had not been backed up adequately, it may mean that the files could never be fully restored. No hospital would be able to afford such a loss. In the event of clinical systems the non availability of information could place a person’s life in jeopardy.

The concepts of security and privacy in health information systems are distinct but inextricably linked, liked siamese twins. The distinction can be expressed as follows, security is the protection of computers from people, and privacy is the protection of people from computers. The maintenance of privacy and security are two of the goals of a health informatics system, (Robinson, 1994). They can be achieved through the adoption of various policies and procedures. This chapter discusses various policies and procedures which will serve to protect the computers, data and people associated with health information systems.

Security of health information systems is an important issue because information technology (IT) has removed many of the inherent erstwhile safeguards. The consequences of a breach of security have become more serious. Hospitals have become more highly dependent upon their information processing and communications systems. Ultimately, management carry the legal responsibilities for computer security.

The major security concerns are the impact on the hospital of security events which will affect:

- Availability of data and services: the extent to which the ability of the organisation to provide a service will be affected by the loss or degradation of a given information processing or communication facility or the loss of a given set of data.

- Authentication and integrity of data: the extent to which the ability of the organisation to provide a service will be affected by the accidental corruption of a given set of data or the malicious corruption of a given set of data or the acceptance of a given set of data which did not originate from its purported source.
- Confidentiality of data: the extent to which the ability of the organisation to provide a service will be affected by the disclosure of a given set of data to an unauthorised person.

One can never reduce the risk of these security concerns to zero. But as the clinical information in health information systems is so important to the health care process, one must find a balance between the risks and medical effectiveness. This chapter will outline the basic steps to take to try and preserve the availability, integrity and confidentiality of data stored in health information systems. The bibliography contains a list of books and articles that will give you a more in-depth coverage of the security process.

Physical security

Physical security is; “that part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorised access to equipment, facilities, material and documents and to safeguard them against espionage, malicious damage, theft or interference.” (Caelli, 1992)

The physical vulnerabilities to security can be disasters (both natural and artificial), human vandals, interception by an outsider and unauthorised access and use. A natural disaster can be defined as any event that is an act of God or the result of environmental or natural causes that are not avoidable or predictable. While it is virtually impossible to prevent natural disasters from affecting computer centres, measures should be taken to assess the potential risk. By proper planning damage and destruction can be lessened. Some of the disasters to be considered include floods, water, fire, power loss, power surges, heat and humidity, (Forcht, 1994) and in some locations earthquakes or cyclones. It is also advisable to insure the computer centre against such disasters.

Floods generally are the result of natural causes such as storms, cyclones, tides and waves. Floods can also be the result of artificial (or man-made) disasters, such as broken water pipes, sewerage pipes or sprinklers. The damage to the computer system may result from rising water, as a result of flood water rising up through the floor or it can result from falling water, caused by overhead sprinkler systems being activated or water pipes breaking. If located in a flood prone area, the computer centre should never be located below ground or even on the ground floor. To prevent damage from falling water, large plastic sheets should be kept in the computer centre to allow employees to cover the computers quickly if needed. It would be advisable to have a policy that stated that all computers should be covered when not in use.

Fire is a much more serious problem than flooding, because it usually happens much more quickly than flooding and is a bigger threat to human life. It is important to devise a fire drill for the computer centre and to practise to ensure that the plan is up to date and effective. The placement of the computer in the building is important. A windowless room with fire-proof doors and nonflammable walls may prevent the fire from spreading into the room. The building should also be fitted with fire and smoke detectors and ideally they should be linked directly to the fire service, (Forcht, 1994).

Computers need a constant, pure supply of electricity. After a direct power loss, all computation needs to cease immediately. The information systems also need to be able to recover from a premature shut-down, back-up and recovery procedures should be in place. For certain time-critical applications, such as systems that monitor a patients' vital signs, loss of service may be intolerable, even resulting in the death of patients. In these cases alternate complete power supplies must be available. One protection against power loss is an uninterruptible power supply. Another problem is the "cleanness" of the power. Instead of the voltage on the line being constant, it may have many brief fluctuations such as drops and spikes or suges of current. These variations in the voltage can be destructive to sensitive electrical equipment. Simple devices called surge suppressors can filter the electricity supply to the computers, (Pfleeger, 1989).

Excessive heat or cold can also be destructive to sensitive electronic equipment. The only effective way to deal with extremes in temperature is to turn the system off. Changes in temperature are usually gradual therefore there will be adequate time to take evasive action. It is desirable to house computing equipment in rooms that enable the temperature, humidity and airborne pollutants, such as dust to be controlled.

What do you do after a crisis? The key to successful recovery is adequate preparation before the event. The most important asset is data, physical items can be more easily replaced, therefore be prepared, backup your data and programs regularly. A backup is a copy of all or part of a file to assist in reestablishing a lost file. Computer centres should do a complete backup regularly, for example once a week at the same time every week. In a complete backup, everything on the system is copied. During the week the computer centre should do selective backups. In a selective backup, only the files that have been changed or created since the last backup are saved. The backups should be stored in a fire and water resistant safe. A copy should also be stored off-site to allow the information systems professionals to recreate the system if the centre were to be completely destroyed.

It is important that data and programs stored on personal computers are backed up as well as the data and programs stored on maniframe computers. Personal computers tend to be overlooked when preparing a backup schedule for the computer centre.

Organisations should also guard against the physical presence of people who are not users. Unauthorised visitors can cause three problems, theft of machinery or data, destruction of machinery or data, and viewing sensitive data. Three approaches can be taken to prevent theft, prevent access, prevent portability or detect exit.

The oldest access control is a guard, the second oldest access control is a lock. Both of these still provide simple effective security for access to computing facilities. But there are also various authentication devices that are available to control access to a computer centre. Users can be identified based on; what things they know (for example, passwords), what objects they possess(for example, smart cards), what characteristics they have (for example, fingerprints). The best authentification procedures will combine all three. A password is a code word or phrase assumed to be known only to the user and the system. A smart card is a plastic card, about the same size as a credit card, that has an embedded microchip. These cards can be used to restrict access to authorised individuals at specific entrances, during specified hours of particular days. Biometric devices or personal characteristic recognition devices, is the recognition of some personal (physical) characteristic of the user. There are systems available that will recognise voice patterns, the blood vessels of the retina, palm prints, finger prints and handwriting characteristics.

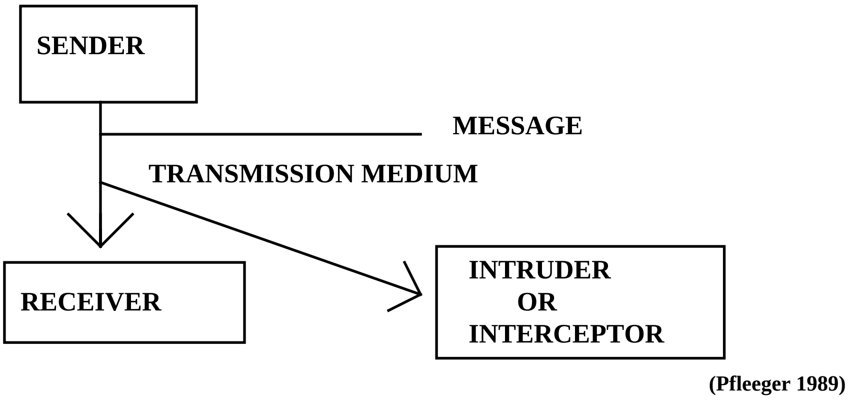
The disposal of sensitive media is important to prevent it being read by unautorised personnel. Data should be destroyed so that it cannot be read after disposal. This can be done by using shredders, disintergrators and incinerators.

Computer systems accessible by dial-in modem ports represent a major vulnerability in your system. The system should be protected by security controls such as dial-back connections, complex authentication schemes handled before connection to the computer and silent modems.

Cryptography

When information is transmitted along a communications line there is a need to protect it. The most common method used is encryption. Encryption is the process of encoding a message so that the meaning of the message is not obvious and decryption is the reverse process. Alternately, the terms encode and decode or encipher are used instead of the verbs encrypt and decrypt, (Pfleeger, 1989). You also need to be able to authenticate the source of the data and authenticate the data itself.

Cryptology is the science of disguised or secret communications. Cryptology is divided into two main areas, cryptography and cryptanalysis. Cryptography means hidden writing, the practice of using encryption to conceal text Cryptanalysis are the methods used to break down or solve the encrypted message, (Pfleeger, 1989). The problem in sending messages is that the message can be interrupted, intercepted, modified or fabricated. Figure 1 shows a message being intercepted.



(Pfleeger 1989)

Figure 8.1 Interception of a message

The two basic methods used in encryption are transposition, which means that the letters of the plain text (original, intelligible message text) are jumbled, and substitution, where the letters of the plain text are replaced by other letters, numbers or symbols.

The encryption key is the cryptographic key used for encrypting and decrypting the data. The decryption key reverses the process at the receiving end. The encryption algorithm is a sequence of rules or steps, generally expressed in mathematical terms, used to encrypt a message. If any of these components are compromised during the transmission of the message, the protection of the message being protected is severely weakened, (Forcht, 1994). The encryption process is illustrated in figure 8.2.

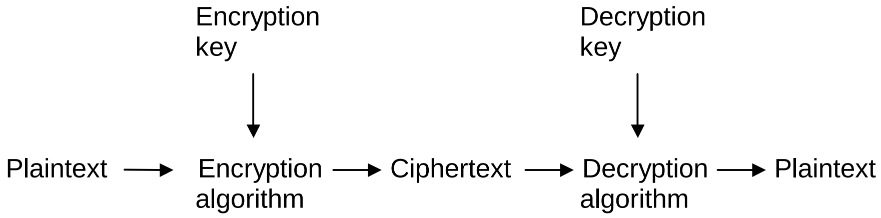


Figure 8.2 The encryption process

Encryption is used to ensure the secrecy (privacy) of messages, interceptors will not be able to read the message unless they have access to the encryption key and algorithm. The integrity of messages sent along tranmission lines can be checked by decrypting the message. If the message cannot be decrypted then some corruption of data has occured and the message should be resent.

Message authentication is ensured by the use of digital signatures. Documents are normally authorised by somebody signing the paper. In computer systems you don't have a tangible object on which to sign your name, only electronic signals. A digital signature is a protocol that produces the same effect as a real signature. It is a sequence that only the sender can make but other people can easily recognise as belonging to the sender. Like a real signature, a digital signature is used to authorise aggreement to a message. They must be unforgeable and authentic. It is also desirable that they be unalterable and not reusable. These conditions can be met using a cryptographic sealing function that includes a date stamp to prevent reuse, (Pfleeger, 1989).

Computer viruses

Computer viruses are a special kind of threat to the health information system. The definition of a virus is a piece of code present on the system without consent of the owner, which is capable of moving from one computer to another, has the potential capability of destroying or altering files and has the capability to deny services to legitimate users.

Viruses are written for a number of reasons:

- Viral code published in books
- Virus construction software is available
- Virus exchange bulletin boards
- Greater awareness and understanding of computers
- Cost of equipment decreasing
- Standardisation of equipment
- Challenge
- Intrigue
- Fun
- Malicious intent

- Recognition
- Financial benefits

There are three types of malicious code, a virus, trojan horse and a worm. A virus is a propagating program that attaches to files and programs and may have time/logic bomb functions, examples are; stoned, brain, friday the 13th, and michelangelo. There are several types of viruses, boot sector virus, program attaching virus, data virus and source code virus. Viruses with time bomb/logic bomb features are triggered by specific circumstances, for example, the Friday the 13th virus is triggered when the system date is the 13th of the month and is a Friday. There are several different activation methods for viruses with time/logic bombs, for example, time, date, percentage of disk space used, number of executions, programmers name removed from payroll file.

A trojan horse is an apparently useful program that has additional hidden functions. It can hide something within its code that can be destructive to the user. For example, a trojan horse program could use the owners file access privileges to copy, misuse or destroy data, format discs, overwrite files or cause the system to crash The effect of trojan horse is to copy confidential files, formatting disks, overwrite files and cause the system to crash.

A worm is a propagating program that propagates through a network. It does not require carrier program, as the program is self-contained. It may contain malicious code, for example, the internet worm. The internet worm infected thousands of sun and vax machines on a unix network in the United States in 1988.

All operating systems are susceptible to viral attack. Only complete isolation provides complete protection from virus attacks. It is important to find a balance between the level of protection and inconvenience to the user. There are three types of anti-virus programs, virus specific products, detection programs, and prevention programs.

Virus specific products locate and remove *known* viruses. They may be able to restore damage/changes done by the virus. They need to be updated regularly to be effective and they should contain a list of viruses detected. An example is Mcfee associates scan program. Detection programs detect damage done some time after it occurs. Notification occurs only when the detection program is run. Prevention programs are memory resident programs, that is, they are active in the computers memory whenever the computer is turned on. Potential viral actions are brought to the user’s attention, the user may allow or disallow the action. They are useful against trojan horse programs. They need to be configurable to the users environment. Users must be aware that they can be bypassed by clever programming.

Is there a cure for computer viruses? It is possible to detect known viruses, but it is impossible to guarantee that a section of code is not a virus. A virus may spread faster than it can be destroyed. It is possible that reinfection will result if any instance of virus remains. There are a number of steps you can take to limit the risk:

- Keep a series of regular backups
- Write protect all possible disks
- Archive all original software
- Assign one boot diskette to each machine
- Never boot from a floppy disk

- Obtain public domain and shareware software from reputable sources
- Always scan new software before using it
- Reboot machine correctly - that is, not using <ctrl-alt-del> or the reset button
- Initiate security procedures to reduce risk
- Be alert to system changes (Caelli, 1992)

Risk analysis and security planning

Risk analysis is the study of the risks of doing something. Every computer user accepts the risk that a storage device will fail, losing all the stored data. Controls can reduce the seriousness of the threat. For example, banning all food and drinks from the computer room can reduce the threat of damage to the computer by food being spilt. A large organisation such as a hospital can not easilty determine the risks and contols of their computing facilities. For this reason, an organised approach to analyzing risks is required.

Following such a study safeguards would be recommended which will reduce the likelihood of a security event, for example, fire proofing, or reduce the impact of an event, for example, fire extinguishers, or reduce the cost of the event, disaster recovery insurance. Note that the emphasis is not on protecting against all possible mishaps but rather concentrating on those which would have the most impact on the organisation.

Some of the steps in performing a careful risk analysis are to determine exposures to risk, assess the potential harm of risks, identify possible controls and the cost of installing these controls. Risk management involves developing and implementing a security plan. See figure 3. Reasons for performing risk analysis are to improve awareness of security issues, identify assets, vulnerabilities and controls, improve the basis for making decisions and to justify expenditures on security, (Pfleeger, 1989).

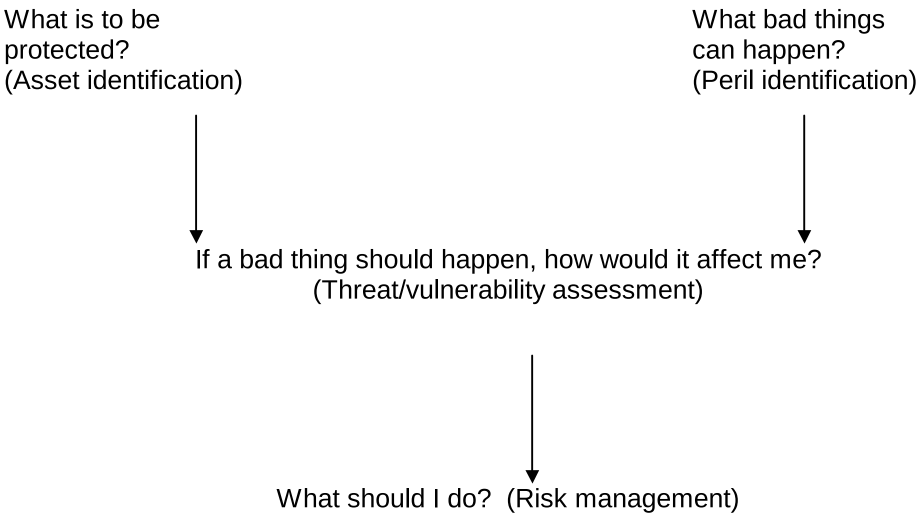

What is to be protected? (Asset identification)
What bad things can happen? (Peril identification)
If a bad thing should happen, how would it affect me? (Threat/vulnerability assessment)
What should I do? (Risk management)

Figure 8.3 Risk analysis and management

The basic steps in doing a risk analysis are as follows:

- *Identify assets*, do an inventory of the system, ie, hardware, software, data, people, documentation and supplies

- *Determine vulnerabilities*, what are the effects of natural and physical disasters? effects of outsiders? effects of wilfully malicious insiders? effects of unintentional errors? One vulnerability can affect more than one asset or cause more than one type of loss. See table 1, for an example of how to organise the consideration of threats and assets.
- *Estimate likelihood of exploitation*, how frequently an exposure could be exploited.
- *Compute expected annual loss*, the cost of each incident is difficult to determine, you will have to rely on data collected by insurance companies, observed data for a specific system, and talking to other people experienced in the field. The annual loss expectancy is calculated using the following formula:

  Annual loss expectancy (ALE) = Loss of incident X the number of inceidents per year.
- *Survey applicable controls and their costs*, new controls needed if expected loss is *too high*, identify new controls on *per exposure* basis.
- *Project annual savings of control*, compute true cost/(savings) from implementation of new controls, the effective cost of new control = actual cost of new controls minus reduction in annual loss expectancy.

Table 8.1 Assets and vulnerabilities

Asset	Confidentiality	Integrity	Availability
Hardware			
Software			
Data			
People			
Documentation			
Supplies			

The types of controls that are available are:

- Cryptography
- Secure protocols
- Program development controls
- Program execution environment controls
- Operating system protection features
- Identification
- Authentication
- Secure operating systems
- Database - access controls, reliability controls and inference controls
- Network controls
- Physical controls

There are a number of packages available to automate the risk analysis process. One of the best known packages is CRAMM (CCTA Risk Analysis and Management Methodology), it is the preferred risk analysis method of the British Government (Barber and Davey 1992).

A security plan is a document that describes how a company will address its security needs. The plan should be subject to periodic review and revision as the security needs of the organisation change. It should identify and organise the security activities for a computing system. The plan should contain, the security policy for the organisation, a description of the current status of security, recommendations for security controls, a listing of who is responsible for each security activity, a timetable identifying when security functions are to be done, and a statement of intention for periodic review of the security plan, (Pfleeger, 1989).

Privacy and confidentiality

The previous sections of this chapter have discussed matters dealing with the security and quality of data. This section looks at issues such as data content, access, control and ownership of data. Recent developments in medical information technology are putting enormous strain on the ability of existing standards, laws and regulatory mechanisms to deal with these issues in respect of the ethical handling of sensitive medical data. Existing standards, laws and regulatory mechanisms are suited to a materially based data-technology. The advent of electronic data storage, handling and processing has significantly altered the way data is collected, stored and distributed. The changes involve more than technology alone. There has been an alteration in the role and function of patient records in health care delivery as well as in the ontological and epistemic status of the patient records themselves. This has serious implications for the ethical use of medical data (Kluge, 1994).

In Australia the Commonwealth government has legislated on privacy and confidentiality through the Privacy Act 1988. This law is applicable to all Commonwealth government departments and their agencies. Pivotal to the Privacy Act is the concept of Information Privacy Principles (IPPs) which are set out in section 14 of the Act. The IPPs are set out in the same order as the information is likely to be handled by the keeper of the records. IPPs 1 to 3 deal with the collection and solicitation of information, IPPs 4 to 8 broadly relate to the storage, security and access to information, IPPs 9 and 10 look at the use of information by the keeper of records and IPP 11 focuses on the limitations placed upon disclosure of information, (Tucker, 1992). For a discussion of the IPPs and Health Information systems see the article by Hardie (1994) listed in the bibliography.

A number of statutory provisions relating to confidentiality in Health Information systems can also be found in the Health Services Act (1991) and the Commonwealth government’s Freedom of Information Act (1982). Some Australian States also have their own Freedom of Information Acts.

Various security vulnerabilities in health information systems were identified in this chapter. The effect of security breaches on hardware, software, data and people was explored, and some of the measures available to protect the security and integrity of health information systems described. The chapter also included a discussion regarding to need for disaster planning and recovery, and explained why it is important to do a risk analysis of the computer system. Finally the role of ethical decision making in the use of health information systems was considered.

References

Caelli, W. 1992, Lecture notes for ITN502 Computer Security, QUT: Brisbane

Caelli, W. 1989, *Information Security for Managers*, M Stockton Press: United Kingdom

Forcht, K.A. 1994, *Computer security management*, Boyd & Fraser Publishing Company, Massachusetts

Kluge, E. H., 1994, "Health information, privacy, confidentiality and ethics", *Caring for Health Information: Safety, Security and Secrecy*, Eds. B. Barber, A. R. Bakker and S. Bengtsson, Elsevier Science, International Journal of Bio-medical Computing: Ireland

Pfleeger, C.P. 1989, Security in Computing, Prentice-Hall, Englewood Cliffs, N.J.

Robinson, D. M., 1994, "Health information privacy: without confidentiality", *Caring for Health Information: Safety, Security and Secrecy*, Eds. B. Barber, A. R. Bakker and S. Bengtsson, Elsevier Science, International Journal of Bio-medical Computing: Ireland

Tucker, G., 1992, Information Privacy Law in Australia, Longman Professional: Melbourne.

Bibliography

Andrews, G. & Wilkins, G. E. J., 1992, "Privacy and the computerised medical record", The Medical Journal of Australia, Vol. 157

Barber, B. and Davey, J., 1992, "The Use of the CCTA Risk Analysis and Management Methodology [CRAMM] in Health Information Systems", *in MEDINFO '92 proceedings of the seventh world congress on medical information, Geneva*, eds K. C. Lun, P. Degoulet, T. E. Piemme & O. Reinhoff, Elsevier Science Publishers: North-Holland, Amsterdam.

Bayne, P.J., 1984, *Freedom of Information*, Sydney: The Law Book Company Limited

Bengtsson, S. and Solheim, B. G., 1992, "Enforcement of data protection, privacy and security in medical informatics", *in MEDINFO '92 proceedings of the seventh world congress on medical information, Geneva*, eds K. C. Lun, P. Degoulet, T. E. Piemme & O. Reinhoff, Elsevier Science Publishers: North-Holland, Amsterdam.

Borovits, I. 1984, *Management of Computer Operations*, Prentice-Hall, Englewood Cliffs, N.J.

Caelli, W. 1989, *Information Security for Managers*, M Stockton Press, United Kingdom

CCH Australia Limited, 1984, *Guidebook to Commonwealth Freedom of Information*, Sydney: CCH Australia Limited.

Chadwick, P., 1985, FOI How to use the Freedom of Information Laws, Melbourne: Age

EDP Auditors Association, 1987, *Microcomputer Control Guide*, EDP Auditors: Sydney

Forcht, K.A. 1994, *Computer security management*, Boyd & Fraser Publishing Company, Massachusetts

Freedom of Information Act 1982 (Commonwealth)

Freedom of Information Act 1992 (Queensland)

Hardie, D., 1994, “Health Information and the Information Privacy Principles”, *Informatics in Healthcare - Australia*, May, Vol 3, No 2.

Harrison, K. & Cossins, A., 1993, *Documents, dossiers and the inside dope*, Sydney: Allen & Unwin Pty Ltd

Hughes, G. 1991 *Data Protection in Australia*, Sydney: The Lawbook Company

Kallman, E.A. & Grillo, J.P. 1993, Ethical Decision Making and Information Technology: An introduction with cases, Mitchell McGraw-Hill: New York

Knight, P., & Fitzsimons, J. 1990, *The legal Environment of Computing*, Prentice-Hall, Englewood Cliffs, N.J.

O’Connor, K., 1993, “Information Privacy Issues in Health Care and Administration”, *Informatics in Healthcare - Australia*, September, Vol 2, No 4.

NSW Health Department, Code of practice: Privacy and confidentiality of data collection, NSW Health Department: Sydney

OECD, 1980, *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data*, Paris: Organisation for the Economic Co-operation and Development

Pfleeger, C.P., 1989, *Security in Computing*, Prentice-Hall: Englewood Cliffs, N.J.

Privacy Act 1988 (Commonwealth)

Queensland Health Guidelines for Information Technology System Security, 1992, Information Systems Strategy Unit, August.

Robinson, D. M., 1992, “A legal examination of format, signature and confidentiality aspects of computerized health information”, in *MEDINFO ‘92 proceedings of the seventh world congress on medical information*, Geneva, eds K. C. Lun, P. Degoulet, T. E. Piemme & O. Reinhoff, Elsevier Science Publishers: North-Holland, Amsterdam.

Standards Australia Draft Guidelines, 1993, Information security and personal privacy protection in health care information systems, Standards Australia: Sydney

Storey, H., 1973, *Infringement of Privacy and its Remedies*, The Australian Law Journal, Vol 47, September

Tucker, G., 1992, *Information Privacy Law in Australia*, Longman Professional: Melbourne.

Waller, A. A., 1991, “Legal aspects of computer-based patient records and record systems”, in *The Computer-based patient record*, eds R.S. Dick & E.B. Steen, National Academy Press, Washington DC.