Protecting the individual: confidentiality, security and the growth of information systems

Derek Hoy
Health Systems Division, National Health Service in Scotland

Information describes people, relationships, activities or objects. It may betray our privacy if it is made public or damage us if it is inaccurate. IT systems may affect the way an individual is thought of and treated by others, and the relationships between groups of people. In this paper we look at these issues by discussing:

- data protection, maintenance of the accuracy, confidentiality and usability of a system;
- the effects of an IT system on relationships between the individuals and groups within the organisation.

Data protection

The purpose of IT is to make valuable information readily available. The greater the availability, the greater the risk that information may be abused and a breach of privacy will result. For example, a hospital information system might allow a member of staff in one department to inspect the records of a patient in another department. On a larger scale, the information in health records would be of great commercial value for market research, and could be collected and sold easily if restrictions did not make this illegal.

Concern over data protection has been around for much longer than the new technology we are considering; the problems of confidentiality, accurate recording and respect for patients' privacy have always been with nurses. But the power offered by the computer to collect, process and communicate information has resulted in:

- more information being available;
- more possibility of errors in information;
- more reliance by the organisation on information systems for essential functions;
- more interdisciplinary sharing of common information;
- more public concern over abuse of information and privacy.

Before considering data protection, we should mention that other terms are sometimes used to mean the same thing. Data safety, data security, and data integrity have all
been used, but not always in a consistent way. We shall consider data protection under the three headings used by Working Group 4 of the International Medical informatics Association. These are: usage integrity (more commonly 'confidentiality'), data or program integrity, and availability.

**Usage integrity**

This rather awkward term is used to cover those aspects of data protection that relate to how information is obtained and used. More commonly the term confidentiality is used.

The exchange of information is part of our daily lives as we are used to discussing matters relating to our work, home or social life in our conversations with others. We choose what we tell to whom and when, and we accept that this sharing plays an important role in our society.

We choose not to share some things with others and this we call our privacy. We expect that some things we share with others will be for a limited audience only, and this we call confidentiality.

It is this confidentiality and trust which lie at the heart of the nurse-patient relationship and which now require reconsideration when IT systems require nurses to enter information into records over which they have very little control.

With paper systems it is accepted that nurses gather information which might be shared with other professionals if the patient's needs require it. While the patient is in the nurse's care, this information will be kept safely, with access denied to anyone whom the nurse does not consider authorised.

However, if computers are used, the King's Fund Centre has stated that "...the nurse using the machine must further satisfy herself that... there is no breach of' confidentiality by any unauthorised person interfering with the system in any way. " This is clearly impossible if the information being entered in the ward is being passed on electronically for storage in a central databank. A clinical nurse loses all control over this information. Even if it is stored on the ward computer, if that machine has communication links with the outside world, the integrity of information stored there can not be guaranteed by the nurses using it, but they will have to rely on the assurances of technical staff that security is adequate. If the accepted nature of the confidentiality of the nurse-patient relationship is being changed in some way by information technology, nurses must consider whether they should inform the patient of this.

There is now much concern about the abuse of information more centrally, a feature of large databanks which has attracted some criticism. If nurses are responsible for the collection of patient data then the profession can not comfortably ignore its possible use, both archived and live, for research or commercial purposes, and the potential for linking health data to social services, police, taxation, intelligence services and other large computer systems under government control.

The problems of data protection are often viewed as being technical, and answerable by more sophisticated technology. However, cost alone will limit the use of the most expensive protection techniques and, more important, the nature of the problem is
essentially ethical and always will be. Machines cannot make decisions about the limits of confidentiality. Though information technology may not have the answers to such problems, technology and especially organisational factors can present people with ethical problems or help avoid such situations. What you cannot do, you cannot be tempted to do!

Three approaches to data protection have been suggested: hardware, software and organisational.

The hardware approach

Controls over access might include physical barriers such as doors, special locks, locks on individual machines, locking data storage, using storage media which are not easily removable, and control over the use of communication links to the system.

Cards with magnetic stripes similar to bank cards may identify their owner, while 'smart' cards with embedded microprocessors may be used to carry more information. Systems have been developed which can distinguish fingerprints for identification.

The software approach

The most common method of control is the password or Personal Identification Number (PIN). This can identify the user and determine the level of access allowed by the system. For example, a nurse using a care planning system will be allowed access to certain patients only, and any amendments she makes to the plan can be tagged with her identity.

Passwords are commonly abused by being passed between users, left written down beside the terminal, or by the use of easily-guessed words such as "secret".

If authorised users start using the system, but then leave it unattended (for example, a nurse called to deal with an emergency) it may be usable by someone else who may be unauthorised. Systems may monitor the use of a terminal and after a period of inactivity shut it down to prevent this.

Encryption is a technique used to scramble data in the system in a way which makes it incomprehensible unless the 'key' to unscrambling it is known. It may be used for particularly sensitive information such as passwords.

Systems may automatically record their use, and, in particular, unauthorised attempts at access.

The organisational approach

"Organisational factors play a key role in data protection measures. Education has been cited as important in giving high priority to data protection and ensuring staff are aware of the measures required by their system. Strangely, it has been said that overstrict security can have an adverse effect on data protection."

The readiness of an organisation to address data protection is of great importance, as the system's security is only as strong as its weakest link. Careful planning is required for the siting of terminals, printers, data storage and the disposal of unwanted
information such as paper printout. Decisions need to be made about who has access to what, and the convenience of users needs to be balanced against the requirements of confidentiality and the law.

Many users of nursing systems think that portable computers or bedside terminals are essential to allow the potential of these systems to be fulfilled. Portable machines are liable to theft, and both portables and bedside terminals may allow the patient or visitors access to the system. This may be used to advantage, for example by offering health education material or hospital information, but it also increases the chance of attempts at unauthorised access.

**Data and program Integrity**

Health care systems may hold information which is of great importance to the individual and the organisation. If this information is wrong or becomes corrupted in the system it might cause embarrassment, inconvenience, financial problems, or death. For example, if medical prescriptions are made using a computer system, an error in the system software that corrupted a patient's drug regime might have serious results.

Making mistakes is part of the human condition. It makes life more interesting and is important in our creativity. Using a computer simply adds to our ability to get things wrong. Errors made while using a system may be hard to detect as they can appear quite plausible. For example, a wrong menu selection will result in an entry on a care plan which looks correct at first glance, because the grammar and spelling are in order. A computer-based system might detect errors which appear to contradict other data, for example a patient on bedrest having an immersion bath ordered on their care-plan, and may lessen the chance of error by restricting the user's choice based on data already entered.

The legal issues surrounding errors in using computers are uncertain as we await the first test cases to set precedents. It seems likely that if the system has been used for the purpose intended and no fault in its function could be demonstrated, then the user would be liable to litigation. If the system can be proved to have been at fault, then the user may still be liable due to professional accountability, but would then have to sue the system's supplier. Further problems may arise where the system is supplied as an empty 'shell' and the users enter their own data and adapt it to local conditions. See Crabtree and Kostrewski for discussion.

Another source of error in data is system malfunction. Computer scientists are working at improving the error handling capabilities of systems and methods of producing fault-free software, particularly as computers are used for military projects such as the control of nuclear weapons. For the moment, we must accept that any software will have faults which may damage data in our systems causing unexpected results. This damage may not be detected easily. If strange characters appear on a computer screen or a nurse receives a 100% rise in pay it is obvious that something is wrong. However, a fault which exchanges the recording of vital signs between two patients in an intensive care unit may not be so noticeable.

Loss or corruption of information and disruption of care are constant dangers of computer-based systems. Loss or small-scale corruption is a danger of manual
systems also, but large-scale damage, whether accidental or malicious, is a new threat previously only comparable to disasters such as fire.

In larger hospital systems, software development is often required on site as new facilities are added or existing ones changed due to experience. Such development needs to be strictly controlled, for example by insisting that it takes place separately from the system in use, using only copies of data files. In this way, changes may be tested thoroughly without any problems being caused to users.

A further source of interference with a system is the growing use of personal computers, either as stand-alone machines or as 'intelligent' terminals. Individual members of staff may keep data on these machines without it being known to managers and subject to control. These machines, can encourage the use of 'home-made' software, programmed by enthusiastic amateurs, which may have unpredictable consequences if used on patients. Personal computers also offer possibilities for skilled people to use them to attempt unauthorised access to other systems. For example, the computer might be programmed to attempt repeated access using a communications link, generating different passwords each time, until it succeeds.

Unauthorised access to computer systems has long been a sport among computer enthusiasts. Sometimes access alone is not enough, and a few will attempt to interfere with the functioning of the system to publicise their expertise. This interference may be simply a harmless but irritating practical 'joke, for example planting some software in the system which makes the text appear upside-down or presents rude messages on users' screens. Of more concern is the software which damages a system and can spread through it before its effects are detected, the much-publicised computer 'viruses'. These are less likely to be accidentally introduced into a large information system, as their spread is commonly due to individual users bringing in software of unknown origin to use on networked personal computers.

A rigorous policy regarding the use of personal software and attention to maintenance as outlined in the next section will contribute to prevention, or early detection and recovery from such problems.

**System availability**

Information stored in a system may be of vital importance, for example staff pay data; while other data may have been obtained at considerable expense, for example results from costly medical investigations. It may be important that information is available at a particular time, for example patient care plans when nursing shifts changeover, or laboratory data during surgery.

A system must be available in the right place at the right time. Overloading may slow down its response considerably resulting in staff frustration, whilst more serious problems may shut it down altogether. All computer-users live with the fear of their system becoming unusable due to failure of the machine or power supply. Solutions may involve uninterruptable power supplies, backup hardware on constant standby, and certainly should include backup of patient data to ensure none are lost if a problem occurs. Buildings housing important equipment require precautions against fire, such as alarms and automatic sprinkler systems.
Problems are inevitable so measures taken to protect a system will be rewarded sooner or later. Maintenance of a system might involve the following three types of activity.

**Prevention or preparation for problems**

Backup copies of data are essential to allow the restoration of the system if damage occurs. The more frequently this is done, the more up to date they will be. Some systems record all additions or changes made to data following each backup. If a problem occurs the system can be restored by taking the last backup and adding these changes to it up to the point where the problem appeared.

**Early detection of problems**

Regular maintenance may help prevent and detect problems. If data checking or verification can be done this will speed the detection of problems and may limit the damage caused.

**Restoration of the working system**

Analysis of the problem and its causes may allow the prevention of a reoccurrence.

**The principles of data protection**

Concern for data protection has led to many countries using their legal systems to enforce it. Whilst the introduction of data protection law may be due to concern for the rights of a country's citizens, there has also been pressure due to the increasing international trade in data processing. Some countries are attracting trade due to their low labour costs and lack of data protection law. The modern equivalent of the 'sweatshop' has rows of low-paid workers spending long hours at the wordprocessor instead of the sewing machine. This has been tackled by some countries making it illegal to export data to countries where there are not adequate data protection laws. The threat of being excluded from this lucrative international business has helped spread legislation to countries that seemed reluctant to commit themselves.³

The Scandinavian countries were among the first to pass data protection laws. The variations in legislation around the world are mostly due to cultural and political differences, but, even where laws exist, their effectiveness is often disputed by those concerned for civil rights.

Vandermuelen summarises the principles of data protection found in most countries' laws⁵

- Only the information needed is taken, and it must be taken in an honest and legal way.
- The purpose of taking information must be explained to the subject when it is collected.
- The information may only be used for the purpose specified unless the subject’s permission is obtained or it is required by the law.
- Information held must be relevant, correct, complete and up to-date for its purpose.
• The individual has the right to inspect her or his own data and demand correction or deletion of anything that is not correct.
• The existence of the information system must be declared.
• A named person is accountable for the legal operation of the system.
• Security must be adequate to prevent unauthorised reading or alteration of the information.

Protection of staff data

While much of the discussion about data protection rightly focuses on the patient, the same principles apply to data regarding members of staff. The computer has the ability to record who is using it, when and for what. For example, care planning systems usually record the identity of a nurse making additions or alterations. There is the potential to monitor the work done by individuals and even compare the outcomes for patients against the staff who nursed them.

The growing pressure for the measurement of performance and audit of health care makes it increasingly likely that managers will consider using technology for this purpose. This raises the possibility that staff activity may be recorded in ways which go beyond what is known and agreed. Whilst such information may seem useful if staff see a system as policing their activity they are less likely to cooperate and use it effectively. As a result, labour relations may suffer and information in the system may become less accurate and less valuable.

The individual and the system.

The more our society becomes supported and ‘driven’ by IT systems the more it becomes necessary for our behaviour to adapt accordingly, for example the necessity of having a bank account or credit facilities. These effects may be subtle but can be far-reaching. There is a story about a Chinese man whose name in its English form was -, simply ‘U’. He discovered by bitter experience that some airline companies used ‘U’ as a code to mark cancelled tickets. He had to change his name to suit the airlines’ IT systems and ensure trouble-free travels.

Imagine a hospital where, over the years, it has become increasingly difficult to meet the growing demands for care with available money. As a result, managers have introduced a Hospital Information System to improve the allocation of resources. The Nursing Information System includes a care-planning facility which identifies the amount of care required for each patient and the level of skill required to deliver it. Translating this kind of information into more cost-effective action means that staff will be moved around more to meet the demands for care. As a consequence, staff feel they are becoming just ‘a pair of hands’, a number on the computer’s screen, being sent where the system dictates and losing a sense of continuity with patients and other staff.

This kind of problem has been around a lot longer than computers, but, as we have discussed before, computers deal only with representations of things; symbols which form some model of reality with which the machine can deal. If this computer-based view of the world dominates the thinking of the system’s users then people will cease to be seen as people, but in whatever way the system represents them: a number, name, Diagnosis Related Group, dependency category, staff grade, pay scale etc.
Information technology systems are becoming essential in the attempts to quantify care requirements and cost the services provided. The patient is increasingly seen as a consumer of these services. The nature of existing information systems seems to encourage this view with the emphasis being on those aspects of care that can be measured, bought and sold. This may seem overly pessimistic, but problems like these stem from the users' lack of understanding of the information with which they are dealing. For a manager whose only contact with patients or staff is through the computer screen it seems inevitable that she will start to see things through the distorted eye of the computer. The more this manager has contact with the real world, the more she will understand just what these numbers, names and statistics mean, and the more effectively she will be able to use this information. The nurse using a care-planning system must fully understand what she sees on the screen as she makes suitable selections on the computer. She must know the patient and the appropriate nursing care or the plan becomes a meaningless ritual of words and tasks.

**Interdisciplinary issues**

The process of developing and introducing an IT system will change an organisation and affect the interests of groups of workers within it. New ways of working may become apparent when people look closely at what they do, or those with power in the organisation may take advantage of a new system to introduce different methods or reallocate staff. Any change is likely to have effects that were never planned.

The resulting system may describe and shape activities and relationships that are quite different to what happened before. For example, a hospital's nursing information may have come from middle managers who collected it from wards, and then did some processing before taking it to the central administration. An IT system might collect ward information at source, pass it electronically to the centre and process it automatically. In this way, there are changes in the way people work together, and the work that they do.

Automation in industry has done much to deskill or remove employees altogether. Already there are factories where all mechanical work is done by computer-controlled machines, serviced and supervised by a few remaining humans. Fears about robot nurses appearing in our hospitals may be a little far-fetched, but any change in working practice may enhance or diminish nursing skills. It is tempting to consider this argument to be similar to the use of electronic calculators by children. Whether or not calculators reduce mathematical skills depends on how the subject is taught. If children learn the basic concepts, the machine can remove the drudgery and may improve the grasp of higher concepts if difficult calculations can be done more quickly and accurately. For nurses, a Fostering system may produce staffing rota quickly and easily, but the nurse using it must still scrutinise the results and use judgement to decide if they are acceptable.

However, a computer is much more sophisticated than a calculator and allows far greater variation in how tasks are performed. A care planning system may offer standard care plans which limit and direct the nurse, or it may encourage the use of judgement by prompting and even questioning the user. A good system would allow the skilled nurse to produce a comprehensive and individualised plan in less time.

The integration of information systems used by different disciplines may cause some overlap in activities. If information is gathered only once instead of many times, then
who will collect it? It may be easy to distinguish between most medical and nursing information, but doctors and nurses who aim for a holistic view of their patients or clients are now more interested in information about social background, support services etc. A system which introduces a shared record will require some redefinition of roles.

Issues which bring different disciplines together in negotiation are sure to cause trouble. Within an organisation various groups will have their own interests. Some will cooperate, others may be in competition at times, trying to increase or at least maintain their relative power. With the introduction of an integrated computer-based system these groups are brought together making this "...essentially a political event" according to Willcocks and Mason. They discuss a system called PROMIS, the Problem-Orientated Medical Information System. Although this system was based around a medical record for each patient, it was used by other disciplines as well. It was particularly popular with nurses, who liked the increased availability of patient information and found that the system allowed greater use of their discretion in making decisions without requiring the approval of medical staff. Pharmacists could monitor drug therapy more closely and radiologists used the system to become more involved with diagnosis. Hospital physicians were the only group who were not impressed, claiming that the system was time-consuming, detrimental to care and upset staff relationships. Willcocks and Mason suggest that this reaction was due to the doctors finding that their records had become open to scrutiny, allowing other staff to question their practice and even alter the record. The shift to a team approach meant some sharing of the power traditionally held by the physicians and in this case it seemed hard for them to accept.

The way information moves around an organisation will tell us much about the balance of power. Equating knowledge with power is not quite as simple as it sounds. Communication theory tells us that too much information is as bad as too little, as it overloads the receiver. A nurse who describes a procedure to a patient in great detail using very technical terms is likely to confuse and simply emphasise the patient's lack of knowledge and control.

As well as the amount of information, the way it is presented may have great influence over the receiver. In Braten's theory of model-power, model-strong people ill tend to see things more clearly, whether they are right or wrong in their assumptions. Model-weak groups may find it more difficult to comprehend the information they receive, and may be unduly influenced by it. Consider the example of a hospital which has become increasingly influenced by its model-strong accountants, with model-weak nurses less sure about the service they provide, and the importance of those aspects of care that are difficult to justify in terms of cost-effectiveness. An IT system is introduced with the main aim of costing care to individual patients and this is reflected in the way information is entered and presented. It results in a very cost-conscious culture which begins to influence the way the nurses relate to their patients.

The growing use of IT systems has led to increasing reliance on them; if the system stops working, the organisation may grind to a halt. Some groups of staff may become essential for the operation of the system, giving them a degree of power, for example, clerical workers who type in medical records, or the technical staff who keep the system operating. However, whilst conflict is part of our daily life, cooperation is required if we are to get any work done. So long as the various
disciplines involved in health care jealously guard their own information, there will be repetition of data and difficulty for the manager who has to co-ordinate the service to the patient. IT demands the integration of different information systems to realise its potential for cutting wasteful repetition and improving communication. Enforced sharing of information between disciplines is a likely result and may become one of the main benefits of the new technology. It has been observed that computer-based communications may mask clues to the users' status and be a social leveler.  

Giving people some freedom of choice may appear democratic, but real power lies in defining what choices will be available. Robins and Webster argue that IT increases the ability of those with power to extend their control over others, because "... it's development - whom, in what circumstances, in what form - hinges on power, on the power to buy, to define, to initiate, and to design technological innovations. "

If political issues affect the work we do, then nurses are faced with two important questions: who has this power, and what are their motives in using it?

References

Further reading

Winner L. Autonomos Technology: Technics-out-of-Control as a Theme in Political Thoughts. Cambridge, Massachusetts: MIT Press, 1977,