Security and confidentiality issues from a national perspective

Barry Barber
Security and Data Protection Programme Manager, NHS Executive, Information Management Centre

What do the papers say?

The computer press often includes interesting items about information systems security and these sometimes emerge into the national press, the radio or television. However, I would like to continue the interesting story that Dr Fleur Fisher described in her paper when a radio programme included the story that the Blood Transfusion Authority was going to sell its mailing lists of donors in exchange for some fruit juice and biscuits. I have, of course, no inside knowledge of what, if anything, is intended but the Data Protection Act 1984 established some basic ground rules about how we should protect such data. This proposal as it stands would clearly not be acceptable ethically to blood donors or to the NHS or to the Data Protection Registrar. If it were to go ahead it would be necessary to obtain the express consent of the donors. Data Protection is often a matter of transparency. The Data Protection Principles require that when information is collected, those providing it should be aware of, or told of, the purposes for which it is to be used and there should be no hidden purposes or use of the information.

Data Protection and the associated security issues require eternal vigilance because there are always problems arising somewhere that have to be checked and addressed. The press provides a continual commentary on how someone somewhere did the wrong thing and the ensuing problems provide object lessons from which we can all learn to avoid and defeat the reported unpleasant consequences.

At MEDINFO in Vancouver the Privacy Commissioner for British Columbia described the case of a hospital that tried to incinerate some old medical records on a local beach. The fire was put out initially by the fire service and then by the incoming tide leaving partly burnt records on the beach and in the water. Complaints rapidly reached the local and national press and the chief executive had to leave his post.

The International Medical Informatics Association (IMIA) has had a long interest in the issues of Data Protection and Security, and the European Union has, likewise, developed a serious interest as a result of its programme of Advanced Informatics in Medicine (AIM).
What is security?

Security is concerned with three key issues: confidentiality, integrity and availability. The right information must get to the right person at the right time. Confidentiality is concerned with ensuring that information only gets to somebody who is authorised to receive it. You can have lots of discussions about who is authorised. This is not a technological issue but a professional one. The organisation must be able to show that it has established arrangements for authorising individuals to handle particular sorts of work and for training them to carry out those allocated tasks. The individuals also need to be aware of the limits of their authority. Only if this information is available and can be substantiated is it possible to think of using the modification to the Data Protection Act 1984, under the Criminal Justice and Public Order Act 1994, where procuring the disclosure of personal information by deception is a criminal offence. In order to make this work it is also necessary to modify our Data Protection registrations to reflect the intention that only authorised disclosures should be lawful within the categories of disclosure registered.

Integrity requires that the information is correct and free from accidental or malicious error. The Radiation Treatment Planning System at Stoke on Trent had not been programmed correctly and it was underestimating the dose. This was accidental, a misunderstanding. The unauthorised modification to the drug regime at Arrowe Park Hospital was a deliberate modification and the perpetrator received a jail sentence under the Computer Misuse Act 1990. The trouble with inaccurate information in systems is that it is possible that someone might believe it and do something that might damage the patient. The closer the system is to a wide variety of clinical activities, the greater is the potential for damage to patients. Therefore the security requirements, in terms of the integrity and availability of patient information, must be improved. The reports of inquests in the papers often illustrate the desperate results of inadequate, incomplete or missing information. The EU Directive which will shortly control our use of personal data covers both computer-based and manual information systems.6

What can go wrong?

There are a lot of things that can go wrong. A list made using the CCTA Risk Analysis and Management Methodology (CRAMM) includes the following problems:

- public embarrassment or loss of public confidence;
- personal safety;
- infringement of personal privacy;
- failure to meet legal obligations;
- commercial confidentiality;
- financial loss and
- disruption of activities.7, 8

Clearly the damage to patients is of vital concern, but the other types of damage can also be important. Financial loss and legal penalties are self-evident problems but if an NHS Trust really loses public confidence, because it is believed that the care it provides is sub-standard, then no one will be prepared to be treated there. Major security breaches frequently cause great damage to the organisation concerned. A pattern of worst case scenarios has been developed by Barber, Vincent and Scholes.9
**Appropriate security**

The important issue is that appropriate security should be installed. Too much security is a waste of resources as well as being an unjustified inconvenience for the system users, but too little security implies a casual or negligent approach to the potential risks. If the issue of security came to court one would like to be able to show that appropriate steps had been taken. That is the security measures taken meet the commonly accepted standards, that they meet the risks arising from the information being processed and the purposes for which this processing is being undertaken. Security will never be one hundred percent certain but the arrangements should not be negligent. Having installed an appropriate security regime it is still necessary to be constantly vigilant for new or unexpected vulnerabilities and to block holes in the security arrangements as they are discovered.

In summary, a confidentiality breach may be damaging. However, any loss of integrity or availability may be dangerous and in this sense clinical systems may be safety-related and this will have implications for the processes of designing, building and purchasing systems in the future.

The requirements for the design, testing and certification of Health Care Information Systems will eventually be seen to be as important as the requirements currently laid down for the design, testing and certification of Medical Devices which are set out in the Medical Devices Directive of the European Union.10

**Confidentiality in the NHS**

In some ways we have seen it all before, Dr Fleur Fisher in her paper described the efforts of the inter-professional working group, whose document was published in the Encyclopaedia of Data Protection,11 and the more recent draft bill on confidentiality published by the BMA.12 Before that, the publication in October 1994 of the Sixth Korner Report, from the working party chaired by David Kenny, had similar recommendations.13 Their survey found a high level of extra-ordinary disclosures. That committee suggested that extra-ordinary disclosures should be monitored, logged and published as statistics. The Korner report also included:

- a list of legally required disclosures;
- a policy for the protection of patient data and employee data;
- a draft code of confidentiality and
- confidentiality clauses for contracts.

It is expected that the Department of Health will produce guidance on confidentiality in the NHS and that it will be widely accepted throughout the country and answer some of the questions that are continually being asked. It is expected that we shall be able to build on that guidance in quite practical terms and that the Security and Data Protection programme of the NHS Executive will gradually start to be able to give quite detailed practical advice on associated security topics. There is still some discussion as to whether this confidentiality guidance should be a voluntary code or a statutory one. The Data Protection Registrar believes that it may be necessary to have a statutory code if exemptions in the EU Directive in respect of the processing of Personal Health Data are to be invoked. Further discussion is needed before there is any agreement on this matter, let alone time in the parliamentary timetable to enact the necessary law.
The European setting for data

The origin of the Data Protection Act 1984 and the associated Health Order comes from the UK's ratification of the Council of Europe Convention 108 which is concerned with the protection of individuals with regard to the automatic processing of personal data. The Data Protection Principles in our own Act derive from this convention, which requires that Personal Data shall be:

- obtained and processed fairly and lawfully;
- stored for specified legitimate purposes;
- adequate, relevant and not excessive;
- accurate and where necessary, up-to-date;
- not kept for longer than necessary;
- available to Subject Access;
- have appropriate security.

In addition the convention lists personal health data as a special category of personal data that requires special protection, along with racial origin, political opinions, religious or other beliefs and sexual life. In fact, processing of such data is prohibited unless appropriate safeguards are in place.

At the moment Convention 108 is effectively the world standard, ratified by a number of non-European countries. However, it may be that the number of countries within the European Union that will be controlled by the EU Directive may eventually lead to that Directive becoming a new standard.

The Council of Europe has previously developed a Recommendation on Automated Medical Data Banks. This required that public notice should be given about the establishment of a medical data bank; a concept that made sense in the mainframe era, but not in the current era of networked small computers. It also required the establishment of proper regulations governing the operation of the data banks. The modern way of describing this is that there should be a proper security policy for the data banks which sets out the rules to which its operators must adhere. The convention suggested that there was a need to retain erroneous data, properly marked, so that the clinician could review the treatment process in the light of the information actually held in the patient record. It also suggested that some countries might wish to handle Subject Access via a physician rather than giving the right direct to the patient.

The Council of Europe is in the process of developing a new recommendation on the Protection of Medical Data to update R(81)1.

European Directive 1995 - Data Privacy Rights

In 1994 I was talking about Data Protection to the annual conference of the Hong Kong Health Authority which has 47,000 staff and looks after six million people. At that stage they were talking about Data Protection legislation in Hong Kong; they had an odd situation where many of the medical notes were written in English, most of the nursing notes were written with Chinese characters and they were wondering if they ought to do some translation. I advised them that might be difficult and the real data protection issue was that a Subject Access Request should secure a copy of the data however they were expressed. Thereafter the Data Subject has the basic information and he or she can seek translations or additional medical opinions as appropriate. The
interesting aspect of the Hong Kong approach is the rate of implementation. They were discussing the law in January 1995 and it is being implemented in January 1996.

By comparison, with the European Union's Data Protection Directive [Article 32] we have three years to put national legislation in place from the date of the adoption of the Directive on 24 October 1995. We have a further period of three years before existing automatic processing has to comply and a further six years before data held in manual systems has to comply with the full quality requirements of the Directive. Superficially, it appears that the year 2007 will be a great year for the Reopen Union Data Protection environment. However, these exemptions are not as far reaching as they appear at first sight. Any new automated processing will have to comply as soon as the legislation is brought into force (i.e. not later than 24 October 1998) and hence all systems will have to be adapted so that they can provide the necessary facilities by that date. Regarding manual systems, the exemption only applies to data held when the legislation becomes effective and so all new processing, including amendments, will have to comply straight away. The exemption is for existing material until 2007 does not apply to Subject Access Requests.

Although the UK abstained on the vote, we are certainly bound to upgrade our Data Protection regime as indicated and I believe that it can only be advantageous to our patients and ultimately to the NHS and the general public.

Definitions - Article 2

Many of the definitions in the Directive are quite interesting and there is room for extensive discussion as to the exact meaning of the terms used and of the requirements of the Directive. In some cases it is likely that there will be differences of interpretation between countries within the European Union. Some of the key definitions are outlined as follows:

- **Personal Data** - "any information relating to an identified or identifiable natural person". It is not clear if this includes dead persons or whether this is for national choice.
- **Personal Data Filing System** - "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis". It certainly covers medical records, both automated and manual, and it includes images and sounds. It probably covers personal address books too.
- **Data Subject's Consent** - "any freely given specific and informed indication of his wishes by which the Data Subject signifies his agreement to personal data relating to him being processed".
- **Controller** - "the natural or legal person or public authority, agency or other body which alone or jointly with others determines the purposes and means of processing of Personal Data".
- **Processor** - "a natural or legal person or public authority, agency or other body which processes Personal Data on behalf of the controller".
- **Processing** - the definition is very wide and covers virtually any usage.
Special categories of processing - Article 8

As with Council of Europe Convention 108 the processing of certain categories of Personal Data, relating to race, ethnic origin, religious or philosophical beliefs, trade union membership, health or sex life, is prohibited except unless the processing:

- has explicit consent of the Data Subject;
- is necessary for obligations under employment law;
- is necessary to protect vital interests of the Data Subject or another person where the Data Subject cannot consent;
- concerns the legitimate activities of a non-profit foundation where processing relates solely to members or contacts and there are no disclosures to third parties without consent;
- data made public by Data Subject or necessary for handling legal claims.

In addition, where Personal Data are processed "for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services and where those data are processed by a Health Professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy" this prohibition from processing does not apply. Apart from general practice computing, it would appear that most NHS processing of personal health information is not handled by health professionals and there are no national laws or rules providing an equivalent obligation of secrecy, especially where the processing is 'out-sourced' and not even under direct NHS control.

Article 9 - Processing of Personal Data and Freedom of Expression

There is a curious Article on the processing of Personal Data and freedom of expression. This provides an exemption for journalistic purposes or for artistic or literary expression, but only if privacy and freedom of expression are reconciled. As in many of the European documents there is a balance, but no body knows what that balance ought to be until there have been some test cases.

Information to be given to the Data Subject - Articles 10 & 11

Article 10 deals with the provision of information to the Data Subject, the patient, at the time at which information is collected. If he or she has not got the information already it is seeking to ensure that Data Subjects have a reasonable opportunity to find out what is happening. The information to be given to the Data Subject includes the identity of the data controller and representative, the purposes of processing and further information for fair processing including recipients or disclosure categories, the consequences of failure to reply and the right of access and rectification. Article 11 deals with the question of data obtained from third parties and regulates the provision of information to be provided to the Data Subject either at the time of collection or, in any case, no later than the time at which data is first disclosed to a third party. These requirements are broadly similar to the requirements of our existing UK Act as interpreted by the Data Protection Tribunal, but are somewhat more specific.

This area is quite exciting in UK terms. There have been a lot of discussions centring around the provision of information at the point of the initial contact with the patient,
the issue of rectification of inadequate, initial information if the patient has not been told properly of what is going on - and what control the data subject, the patient, has over disclosure. The European view of "informational self-determination" comes in here. Although the discussion has sometimes become quite heated, it seems to me that there is beginning to be fairly clear agreement as to how our Personal Health Data should be handled.

**Subject Access Rights - Article 12**

Article 12 deals with subject access, rectification and erasure, and the rectification of Personal Data to third parties. These arrangements are similar to our current Data Protection Act, but they prioritise access to "the purposes of the processing, the categories of recipients, to whom the data are disclosed". The Data Subjects interests would be better served by a list of recipients, rather than simply categories of recipients. In addition the requirement for rectifying third party disclosures presupposes the existence of a third party disclosure register - possibly with the names kept in the patient record.

**Data Subject's Right to Object - Article 14**

The Data Subject may object to processing "on compelling legitimate grounds" and this right of objection is specifically clear in respect of Personal Data to be used or disclosed for direct marketing.

**Automated Individual Decisions - Article 15**

There is a clear right to ensure that decisions which significantly affect the Data Subject should not be based solely on automated processing of his data. The individual can demand personal consideration of his situation rather than being bound by some automated, computer programmed decision making.

**Confidentiality of Processing - Article 16**

This article requires that "Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to Personal data must not process them except on instructions from the controller, unless he is required to do so by law". This is a quite unequivocal requirement of confidentiality.

**Security of Processing - Article 17**

Article 17 covers the security of processing and requires the controller to "implement appropriate technical and organisational measures to protect Personal Data against: -

- "accidental or unlawful destruction;"
- "accidental loss or alteration;"
- "unauthorised disclosure or access;"
- "in particular where processing involves transmission of data over a network; and"
- "all unlawful forms of processing".

The security measures "shall ensure a level of security"
• having regard to the state of the art;
• the cost of their implementation;
• appropriate to the risks represented by the processing and
• the nature of the data to be protected".

In effect, this approach is substantially the same as that outlined in the Top Level Security Policy, issued by the NHS Executive, for the NHS. Risk analysis is the key thing; it is concerned to explore what happens when things go wrong and then to put security measures in place to address those problems.

**The use of Personal Health Data for "Non-Core Activities"**

One final area of discussion is the issue of purposes that are not fundamental to the basic activity. The blood transfusion service mentioned earlier provides an example. Giving the names and addresses of blood donors to outside organisations is, clearly, not vital to the process of delivering the blood to patients. Hence, if such a proposal were to reach the stage of serious consideration, the Authority would have to provide the means for donors to opt-out of that arrangement. No organisation has a right to use Personal Data for other purposes over the heads of the Data Subjects who provided the data in the first place for specific purposes - whether or not such sale or usage would provide extra income for the organisation, or reduce the requirement for national funding!

The reformed NHS does not 'own' patient data but rather holds the data in trust for its declared purposes of delivering improved health care.

**Developing security standards**

The British Standards Institute has developed a Standard for Information Security Management, BS7799, which provides a sound business-like basis for addressing security issues. In addition, quite a lot of work is going on within Technical Committee 251 (Medical Informatics) of the European standards organisation, (known as CEN) to provide standards to assist with the implementation of appropriate security within Health Information Systems. A "Password Standard" has been developed, within Working Group Six of TC251, which provides guidance on a safe way of constructing passwords: so that they are much less likely to be guessed or 'cracked'. Most people use passwords and could use them a lot better than they do today. In addition, an extensive series of Risk Analyses using CRAMM has been conducted. This has led to a security classification of Health Information Systems, mainly along the direction of the use of the information - if it is critical to clinical care or treatment, or not. Associated with each security classification is a profile of protection measures that are thought to be appropriate to various systems. It is expected that the Health Care area will utilise appropriate security measures from other sectors as well as developing standards appropriate to its own environment where none exist. Copies of these various standards, and any others under development can be obtained from the Standards Programme at the NHS Information Management Centre.
The next steps in data protection within the UK

The Department of Health is working on the confidentiality guidelines and these will be available early in 1996. They will provide a foundation for NHS arrangements in handling confidential Personal Health Information. These have been long awaited and it will be a great relief when they finally appear. The Executive's Security and Data Protection programme will continue to provide training seminars and to develop both technical and training materials to complement those already produced.21-23

Now that the EU Directive on Data Protection has been finally adopted, the thing to look forward to is the development of UK legislation incorporating the requirements of the Directive within UK law. This must happen before 24 October 1998 but this requirement comes at a difficult time in the Parliamentary timetable: either near the end of the present Parliament or at the beginning of a new Parliament.

The next thing, is that the European Commission is doing some negotiation on the Fourth Framework activities. The NHS Executive is involved in discussions on a number of projects; two of them concern the issues of Data Protection and Security which may be helpful within the UK context. The first is TrustHealth which is exploring the use of digital signatures and Trusted Third Parties across the European Union, and the other project is ISHTAR which is extending and developing SEISMED security guidelines.24-26 So watch this space - I do not think 2020 is the time but much needs to be done earlier than the 2007 deadline for the final phases of implementation of the Directive.

Discussion

Q

Having almost completed the implementation of a mental health system covering both hospital and community, one of the things that we sought, because confidentiality and security issues obviously loomed very large, was some practical guidance from the centre on technical things like "Are modems a suitable means of communication?" and also the softer issues about confidentiality. You talk about the strategy level Ñ the top-level document Ñ is there something in more practical terms which will shortly be available. Or are we individually going to have to ask a risk consultant?

Barry Barber

The NHS Executive has been doing some work with three major HIS sites: Greenwich, The Royal London and the Wirral. This has provided some generic models which tease out the security measures for those sorts of sites. We have held a workshop to present some of the material and are trying to decide how best to make it generally available to the service. There are generic requirements; such as proper access control. There is then another issue - are there specific pieces of software to deal with access control which we all ought to be using? At the moment we have no plans to produce kite marks on particular forms of software, but I have a feeling we do need to move down to the product area in order to give some detailed practical advice. It is a tricky and complicated area, with the commercial considerations but I believe that we shall need to move in that direction in the immediate future.
Q Franca Mongiardi Adviser on Nursing Information, Royal College of Nursing

I have heard rumours that the UK has opted out of the European Directive on Data Protection. Is that true?

Barry Barber

I understand that we abstained when voting on the Directive. However, this does not give us an opt out. There appears to have been more hassle with the Data Protection Directive and it's various drafts than any other previous directive; that is why the discussion went on for so long, but we shall be implementing it and I believe that it will be beneficial to our patients.

Q Franca Mongiardi

If the UK has abstained, what are the implications for UK data protection?

Barry Barber

We fit in and do what the Council of Ministers and the European Parliament have agreed that the European Union will do. We pass national legislation as required by the Directive and we implement it on the timescale set out in Article 32 of the Directive. All the protesting is now over and we are into the process of developing a new Data Protection regime. All new processing will have to comply with the requirements of the Directive by 24 October 1998 at the latest and existing automated processing will have three years from the date at which national legislation becomes effective to be brought into line with its requirements. From that time existing manual records will be open to Subject Access, rectification and erasure but compliance with the other requirements can be delayed until 2007! The Directive offers national governments a number of options in devising their legislation and, of course, we do not know what options will be selected by the UK government Ñ or indeed which government will be doing the selecting. However, it has been assumed that the approach will be to select the minimum required in order to comply and to avoid challenge in the courts as a result of inadequate representation of the Directive in UK legislation.

This new regime will be recognisable but there will be many tweaks and developments, in line with the development of the technology. If you look back over the decade from the 1984 Act and think of what has happened and then of what might happen in the next decade, it is quite clear that we need to keep the ethical and human rights dimensions clearly in view. We need to keep in step with technology and the developments in the delivery of health care if we are to get the benefits everybody else has been talking about. If we don't have sensible arrangements about the confidentiality, integrity and availability of personal health data and how we handle the information, then we don't get the benefits everybody else is trying to achieve. Effective data protection and security are integral and vital parts of that process.

Q Maggie Wheeller Public Health Laboratories, Colindale

A small technical question, when you were trying to define 'person'. Looking to the future, with tissue culture already causing all sorts of copyright and other problems, is a tissue culture living tissue and part of a person? Is it covered, because there is a lot
of medical information which is needed about the person supplying the cells and how is that person protected?

**Barry Barber**

The Bio-ethics Committee of the Council of Europe has been developing a convention in this area. Also, I remember reading a paper which was arguing that we should protect information in the same way and with the same rights as we protect body substances. It is an interesting topic open to a lot of exciting legal discussion. I am not the expert on body tissues but I think that the Council of Europe work would provide a good starting point for best practice.

**Update**

Since this paper was produced the Department of Health has issued its guidance on the confidentiality of patient information, the Information Management Group (IMG) has issued its IM&T Security Manual, the Home Office has issued its consultation on the EU Directive and the Office of the Data Protection Registrar has issued a paper on the issues raised by the EU Directive. 27-30 In addition the Zergo report, commissioned by the IMG, on encryption within the context of the NHS computer-network, has been issued.31

**References**


missing refs 9-31