Protection of Personal Data -- The European View

by Steve Mathews

A new series of laws are being passed to control the processing of personal information -- including medical information -- inside the European Commonwealth. The author gives an overview of the European view of personal information and examines the implications for healthcare professionals both here and abroad.

In October 1995, the European Parliament approved a Directive[1] for the Protection of Personal Data, which is having profound effects in many countries both inside and outside the European Union (EU). Why? Very little is more personal than healthcare data, and nothing has excited the public more than the thought that such personal information seems to be considered someone else's property -- and may be bought and sold for commercial purposes. Healthcare professionals have always enjoyed considerable trust from their patients. That trust seems under threat in the information age.

Many European states (Germany and France in particular) have strong privacy laws. It has long been recognized that members of the public are not always aware of the power and capability of computer systems. To protect the rights and interests of the European citizen, a new series of laws are being passed to control the collection and processing of any personal information inside the EU and to require equivalent protection of that information if it passes outside the EU borders. Today, the United States is not considered a country offering equivalent protection.

To understand the implications for both healthcare professionals and the applications software industry, you need to understand the European view of personal information. In this context, information is personal if it can be associated with an identifiable living individual (or in a medical context, genetically linked to one).

Concepts behind the Directive

The contents of the Directive have been the subject of considerable debate and political lobbying, not just in the European states but also by many other countries, including the US. At the heart of the Directive are a number of key concepts concerning the collecting and processing of information, both by computers and in paper-based systems. These concepts include:

- Fairness of obtaining information
- Informed consent of the data subject
- Need to process information
- Sensitive information
- Adequate protection of information

These concepts are intended to be used to determine the right and limits for collecting and processing personal information in all EU member states. For countries inside and outside the EU, the last two concepts are having the greatest effects.

Types of Personal Information

The Directive is concerned with personal information -- information related to a living individual. Obviously this can include ordinary items such as date of birth, preference for clothing, credit information, or usual vacation destination. However, the Directive also defines a further special category -- sensitive information, such as:

- Racial or ethnic origin, including skin color
- Religious, philosophical, or ethical persuasion, or lack of one
- Trade union membership

- Health, physical and mental -- past, present, and future
- Drug or alcohol abuse
- Sexual life
- Criminal record(s)

Medical information is clearly listed as sensitive, as is other information which might also be considered relevant to the interests of patient healthcare. Processing information (defined very broadly as collecting, storing, copying, or manipulating) is allowed unless the information is defined as sensitive. If it is sensitive, the Directive states that such information must only be collected and processed when it is essential (and in the case of criminal information, only with authority from and under the supervision of administrators).

Healthcare Exemptions and Restrictions

Medical practitioners and their support staff are, obviously enough, able to collect sensitive information because it is essential for providing treatment, and there is an implied consent from the patient that information may be processed. This should not be considered blanket license to collect and process any and all sensitive information. Information has to be relevant to the purpose (in a medical case, this could be to treat the condition presented). But there is no implied right to use the information for any other purpose without the informed consent of the patient.

Information for the purpose of research is exempt; however, it is required to be made anonymous. This requirement may seem easy to meet if there is no patient identifier, but care may be required to ensure that a patient could not be identified through descriptive material together with the healthcare practitioner or facility identifier.

Patients' Rights

Patients must be asked explicitly if information (not just that defined as sensitive, but any personal data) may be passed to a third party, and they must have the right to refuse unless it is essential to their health or necessary for the prevention or detection of crime. As a result, there may be an implication that computer systems will have to be modified to record patients giving and refusing permission for the processing of nonessential information and to be able to show when information has been passed to other parties.

There does not seem to be a requirement to catalog where individual items of information may have been sent, but there is a need to identify third parties who have received information for processing, particularly if an error has to be corrected.

Patients also have a number of rights. One of these is to be able to demand a copy of any personal information held about them on payment of a reasonable fee (probably between $8 and $20). Such requests must be answered in a reasonable time frame. (There are likely to be some limitations where particular states allow information to be withheld when it would harm the health of the patient.) Another right is the correction of wrong information and the deletion of information that is improperly obtained.

Finally, if a patient is not treated reasonably, or their legitimate complaints are not handled, or if they suffer harm as a result of infringing activities, they will be entitled to ask the courts for relief and damages.

Processing Sensitive Information

Article 8 of the Directive identifies special categories of information as sensitive. Normally these must not be processed unless there is a need created under employment law, rights, and duties for antidiscrimination or health and safety. By the fact that sensitive information has been clearly identified as being special and unusual, the Directive implies that a higher standard of care would be expected of those processing that information from those processing, say, information about goods an individual has purchased, whom they go on vacation with, or their bank account details.

As a result, while healthcare professionals will have access to sensitive information they may have to take care that other staff (administrators, secretaries, or computer staff, including maintenance personnel) do not have the same free access to that information, unless that information cannot be related to a living individual. That will require comprehensive access control and user authentication methods, perhaps with logging systems. It may also create the need for data encryption, where information

is taken out of a medical facility (with good physical security controls) either on a laptop or sent over a communications] medium such as the Internet.

All organizations processing personal data have to identify the "controller" of the system -- again, a person who is the officer of the organization with responsibility for compliance with the law.

The Directive does not spell out what the standard of care has to be. Instead, it states that personal information has to be protected at a level consistent with what is technically reasonable for the state of the art.

Exporting Information

Although there is no extraterritorial legislation, the Directive clearly identifies a difference between processing carried out in European member states and anywhere else in the world. Since all EU states will have equivalent laws there is, of course, no difficulty about processing information in any EU country.

If the controller of the information wishes to process it outside the EU (or wishes to transfer it outside the EU for other processing) he or she may do so only if the destination country is considered to offer equivalent protection to that in the EU. To find out which countries are approved, you will have to check with the data protection commissioner in the country from which you wish to export information.

If the country is not on the approved list, the controller can apply for a specific approval for the receiving organization. That organization will have to be able to convince the commissioner that their security provisions and controls are equivalent to those required in the EU and that they accept the same liabilities as if they were domiciled in an EU member state. If a non-EU organization wishes to offer processing of EU personal data, it will have to provide an EU branch with a declared controller.

When Does All of This Happen?

European Directives come into force three years after they are published. That means all the requirements listed above take effect in October 1998 for computerized records. Equivalent controls over paper records come in three years later and must be fully implemented three years after that.

It also means that from October 1998 it will not be possible to export personal data outside the EU without complying with the Directive. At the time of writing, the US has not been recognized as offering an equivalent level of protection.

Impacts

The short-term impact of that change is that medical groups processing European information outside the EU may find they are unable to do so, and if they do so may be faced with litigation both from the EU commissioners and individual EU citizens. Depending on how computer applications systems have been developed, it may be easier and cheaper to move them into Europe rather than try to get a one-off approval, especially when the approval system has not been developed and tested.

Software applications developers and providers developing in the European market will need to consider whether their products provide adequate security controls, both to prevent disclosure of personal or sensitive information to unauthorized individuals and to prevent authorized users from gaining improper access to information that their role does not require. If cryptography is needed to protect confidentiality or to support patient anonymity, there will need to be standards agreed upon by both commerce and government.

In the longer term there could be many impacts. The US has pending legislation on standards for protecting healthcare data. These may not address the issues of correction and limitations on the ability to transfer to third parties. The standards also may not match up with those being developed and implemented in Europe.

Are There Relevant Standards?

As mentioned above, the US is considering legislation for the security of medical information. There are also standards, advice, and guidance from Federal Information Processing Standards issued by the National Institute for Science and Technology and

standards issued by the American National Standards Institute. These are American standards that are not so well known in Europe.

The International Standards Organization also has created standards for security methods and techniques, but, apart from banking, these have not been focused at vertical industry needs.

The European standards organization, CEN, has a special committee for medical information processing standards, TC 251. Its security group has been working for some time on a standard approach to risk analysis and standard protection measures for healthcare facility systems, and a draft standard is progressing through the system. It has been extensively reviewed in Europe and was presented in the US hearings on medical information security, where it was commended both for thoroughness and not mandating proprietary methods and solutions.

Specific national standards have been developed in Germany and the UK. In Germany the Bundesamt für Sicherheit in der Informationstechnik[2] has published a baseline on detailed security measures for commercial computer systems. In the UK, the British Standards Institute[3] published BS 7799, the standard code of practice for information security management. This has been adopted by the Netherlands and Sweden and is being developed for accreditation starting next year.

Summary

For healthcare professionals, this could become a period of turbulent change where their computer applications and procedures have to be changed, perhaps a number of times. Those changes will not be accomplished free of charge from their suppliers, and any change to the way of running a business means cost.

Healthcare professionals will benefit from direct involvement in the process of ensuring that patients can have confidence in the probity of the computer system. If they do not, then developments will be dominated by technologists and lawyers.

Notes

1 Europe has been debating the need to balance the rights and duties between the private individual, the corporate body, and the state for many years. The citizen in Europe is entitled to expect the same treatment in any member state (the level playing field). This harmonization is achieved by a consensus where common concepts and principles are put into a Directive which is then enacted locally in all member states within three calendar years of the date of the Directive.

2 IT-Grundschutzhandbuch 1997 is available on CD-ROM in German and English for 180 GDM from Bundesanzeiger-Verlag, Postfach 10 05 34, D-50445 Köln, Germany. Telephone: 49 228 9582 369; fax: 49 228 9582 405; e-mail: bestellung@bundesanzeiger.de.

3 BS7700 (1995) is available in paper for 75 GBP for 5 copies from BSI, 289 Chiswick High Road, London W4 4AL, UK. Telephone: 44 181 996 9000; fax: 44 181 996 7448; Web site: http://www.bsi.org.uk.

Steve M. Mathews *is head of consulting for PCSL, specialists in computer information security, with US headquarters in Dallas, TX, and in Europe in Marlow, England. He is a member of a number of standars committees for both information security and electronic data interchange.*

Article citation:
Mathews, Steve. "Protection of Personal Data--the European View." *Journal of AHIMA* 69, no.3 (1998): 42-44.
