

DIN EN 14484

ICS 35.240.80

**Medizinische Informatik –
Internationaler Austausch von unter die EU-Datenschutzrichtlinie
fallenden persönlichen Gesundheitsdaten –
Generelle Sicherheits-Statements;
Deutsche Fassung EN 14484:2003, Text in Englisch**

Health informatics –

International transfer of personal health data covered by the EU data protection directive –
High level security policy;

German version EN 14484:2003, text in English

Informatique de santé –

Transfert international des données personnelles de santé couvertes par la directive
européenne sur la protection des données personnelles –

Politique de sécurité de haut niveau;

Version allemande EN 14484:2003, texte en anglais

Gesamtumfang 60 Seiten

Normenausschuss Medizin (NAMed) im DIN

Die Europäische Norm EN 14484:2003 hat den Status einer Deutschen Norm.

Nationales Vorwort

Diese Norm enthält unter Berücksichtigung des Präsidialbeschlusses 13/1983 die Englische Fassung der Europäischen Norm EN 14484:2003. Diese Europäische Norm wurde in der WG III „Security, Safety and Quality“ des CEN/TC 251 „Medizinische Informatik“ erarbeitet. Der Fachbereich G „Medizinische Informatik“ und insbesondere die Mitarbeiter des Arbeitsausschusses G 4 „Sicherheit“ des Normenausschusses Medizin (NAMed) im DIN haben an der Erarbeitung mitgewirkt.

English version

**Health informatics - International transfer of personal health data
covered by the EU data protection directive - High level security
policy**

Informatique de santé - Transfert international des données
personnelles de santé couvertes par la directive européenne
sur la protection des données personnelles - Politique de
sécurité de haut niveau

Medizinische Informatik - Internationaler Austausch von
unter die EU-Datenschutzrichtlinie fallenden persönlichen
Gesundheitsdaten - Generelle Sicherheits-Statements

This European Standard was approved by CEN on 13 November 2003.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Contents

Page

Foreword	5
Introduction	6
1 Scope.....	10
2 Normative references	10
3 Terms and definitions	10
4 Abbreviated terms.....	11
5 The European Data Protection Directive (see annex A).....	12
5.1 General.....	12
5.2 General aims: (Article 1).....	12
5.3 Scope: electronic and non-electronic (Article 3)	12
5.4 Principles relating to data quality (Article 6)	12
5.5 Criteria for legitimacy (Article 7).....	12
5.6 Special categories of processing, including personal health data (Article 8).....	13
5.7 Information to be given to the data subject (Article 10).....	13
5.8 Right of access to data (Article 12)	13
5.9 Right to object (Article 14)	13
5.10 Security of processing (Article 17).....	14
5.11 Judicial remedies, liability and sanctions (Articles 22, 23 and 24).....	14
5.12 Supervisory Authorities (Articles 28 and 18)	14
5.13 Working party on the protection of Individuals with regard to the Processing of Personal Data.....	14
5.14 Transfer of personal data to Third Countries.....	14
6 Requirements for the transfer of personal data to third Countries.	14
6.1 General.....	14
6.2 Principles (Article 25)	14
6.3 Ensuring transfers are permissible.....	15
6.4 Grounds by which transfers to third countries are permissible	15
6.4.1 General.....	15
6.4.2 Members of the EEA	15
6.4.3 Depersonalisation of data	15
6.4.4 Consent	16
6.4.5 Subject to contract clauses	16
6.4.6 Claiming adequacy of data protection	17
7 A Security Policy for third countries.....	17
7.1 The requirement.....	17
7.2 The purpose of the security policy.....	18
7.3 The 'level' of the security policy.....	18
8 High Level Security Policy: general aspects.....	18
8.1 Levels of abstraction in ensuring security.....	18
8.2 Generic principles.....	18
8.3 Non-generic Principles	19
8.4 Guidelines	19
8.5 Measures.....	19
8.6 Elements of a High Level Security Policy.....	19
9 High Level Security Policy: the content	19
9.1 Principle One: overriding generic principle	19
9.1.1 General.....	19
9.1.2 Principle One, Guideline One: fundamental rights and freedoms	19
9.1.3 Principle One, Guideline Two: information about doubts	20

	Page
9.1.4 Rationale.....	20
9.1.5 Observations as to Measures.....	20
9.2 Principle Two: chief executive support.....	20
9.2.1 General.....	20
9.2.2 Principle Two, Guideline One: alignment with local practice	20
9.2.3 Principle Two, Guideline Two: organisational arrangements	20
9.2.4 Principle Two, Guideline Three: regular HLSP review.....	20
9.2.5 Rationale.....	20
9.2.6 Observations as to Measures.....	20
9.3 Principle Three: documentation of Measures and review	21
9.3.1 General.....	21
9.3.2 Principle Three, Guideline One: staff information.....	21
9.3.3 Rationale.....	21
9.3.4 Observations as to Measures.....	21
9.4 Principle Four: Data Protection Security Officer.....	21
9.4.1 General.....	21
9.4.2 Principle Four, Guideline One: Data Protection Security Officer and organisation as a processor.....	21
9.4.3 Principle Four, Guideline Two: Data Protection Security Officer and organisation as a controller.....	21
9.4.4 Principle Four, Guideline Three: Data Protection Security Officer qualification for office.....	21
9.4.5 Rationale.....	21
9.4.6 Observations on Measures.....	22
9.5 Principle Five: permission to process.....	22
9.5.1 General.....	22
9.5.2 Principle Five, Guideline One: unambiguous consent to transfer	22
9.5.3 Principle Five, Guideline Two: explicit consent to processing.....	22
9.5.4 Principle Five, Guideline Three: limitation to the purposes consented.....	22
9.5.5 Principle Five, Guideline Four: conditional consents.....	22
9.5.6 Principle Five, Guideline Five: review of information concerning consent.....	22
9.5.7 Rationale.....	22
9.5.8 Observations regarding Measures.....	23
9.6 Principle Six: information about processing	23
9.6.1 General.....	23
9.6.2 Principle Six, Guideline One: documentation about consented processing	23
9.6.3 Principle Six, Guideline Two: quality of data collected and processed.....	23
9.6.4 Principle Six, Guideline Three: accuracy of data processed	23
9.6.5 Principle Six, Guideline Four: Data Retention and Destruction Policy.....	23
9.6.6 Principle Six, Guideline Five: data subjects' access to their data	23
9.6.7 Principle Six, Guideline Six: objection to processing	23
9.6.8 Principle Six, Guideline Seven: rectification, erasure and blocking	23
9.6.9 Principle Six, Guideline Eight: identification of transferred data	24
9.6.10 Principle Six, Guideline Nine: action on notification of the death of a data subject.....	24
9.6.11 Principle Six, Guideline Ten: direct marketing	24
9.6.12 Principle Six, Guideline Eleven: re-personalisation of de-personalised data	24
9.6.13 Observations on Measures.....	24
9.7 Principle Seven: information for the data subject.....	25
9.7.1 General.....	25
9.7.2 Rationale.....	25
9.7.3 Observations on Measures.....	25
9.8 Principle Eight: prohibition of onward data transfer without consent.....	25
9.8.1 General.....	25
9.8.2 Principle Eight, Guideline One: assuring protection for onward transfers	25
9.8.3 Principle Eight, Guideline Two: HLSP for onward transfers	25
9.8.4 Principle Eight, Guideline Three: Disclosure Register	25
9.8.5 Rationale.....	25
9.9 Principle Nine: remedies and compensation.....	26
9.9.1 General.....	26

	Page
9.9.2 Principle Nine, Guideline One: investigation of complaints.....	26
9.9.3 Principle Nine, Guideline Two: independent arbitration.....	26
9.9.4 Rationale	26
9.9.5 Observations on Measures	26
9.10 Principle Ten: security of processing	26
9.10.1 General.....	26
9.10.2 Principle Ten, Guideline One: risk analysis	26
9.10.3 Principle Ten, Guideline Two: encryption during transmission	27
9.10.4 Principle Ten, Guideline Three: proof of data integrity and authentication of origin	27
9.10.5 Principle Ten, Guideline Four: access control and user authentication.....	27
9.10.6 Principle Ten, Guideline Five: Physical and Environmental Security	27
9.10.7 Principle Ten, Guideline Six: application management	27
9.10.8 Principle Ten, Guideline Seven: network management	27
9.10.9 Principle Ten, Guideline Eight: virus controls	27
9.10.10 Principle Ten, Guideline Nine: reporting breaches of security	27
9.10.11 Principle Ten, Guideline Ten: Business Continuity Plans	27
9.10.12 Principle Ten, Guideline Eleven; audit trails	27
9.10.13 Principle Ten, Guideline Twelve: handling particularly sensitive data	27
9.10.14 Rationale and observations on Measures	27
9.11 Principle Eleven: responsibilities of staff and other contractors	28
9.11.1 General.....	28
9.11.2 Principle Eleven, Guideline One: informing staff and other contractors	28
9.11.3 Principle Eleven, Guideline Two: instruction and training	28
9.11.4 Principle Eleven, Guideline Three: staff and contractor contractual obligations	28
9.11.5 Rationale	28
9.11.6 Observation on Measures	28
9.12 Principle Twelve: adequacy of third country data protection	28
9.12.1 General.....	28
9.12.2 Rationale	28
9.12.3 Observations on Measures	28
9.13 Principle Thirteen: additional EU Member State particular requirements	28
9.13.1 Rationale	29
9.13.2 Observations on Measures	29
10 Rationale and Observations on Measures to support Principle Ten concerning security of processing	29
10.1 General.....	29
10.2 Encryption and digital signatures for transmission to the third country.....	29
10.3 Access controls and user authentication.....	29
10.4 Audit Trails.....	30
10.5 Physical and environmental security.....	30
10.6 Application management and network management.....	30
10.7 Viruses	30
10.8 Breaches of security	30
10.9 Business Continuity Plan.....	30
10.10 Handling particularly sensitive data.....	30
10.11 Standards.....	31
11 Personal health data in non-electronic form.....	31
Annex A (normative) EU Data Protection Directive	32
Annex B (informative) Useful sources of advice	53
B.1 EU Security projects	53
B.2 CEN/ISSS.....	53
B.3 Non-CEN Standards	53
B.4 Selected web sites	54
Annex C (informative) Model declaration	55
Bibliography	57

Foreword

This document (EN 14484:2003) has been prepared by Technical Committee CEN/TC 251 "European Standardization of Health Informatics", the secretariat of which is held by SIS.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2004, and conflicting national standards shall be withdrawn at the latest by June 2004.

Annex A is normative. The annexes B and C are informative.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and the United Kingdom.

Introduction

In the health context, information about individuals needs to be collected, stored and processed for many purposes, the main being:

- direct delivery of care e.g. patient records;
- administrative processes e.g. booking appointments;
- clinical research;
- statistics.

The data required depends on the purpose. In the context of identification of individuals, data may be needed:

- to allow an individual to be readily and uniquely identified e.g. a combination of name, address, age, sex, identification number;
- to confirm that two data sets belong to the same individual without any need to identify the individual himself e.g. for record linkage and/or longitudinal statistics;
- for statistical purposes but with the end desire positively to prevent identification of any individual.

In all of these circumstances data about individuals are now, and will increasingly in the future, be transmitted across national borders or be deliberately made accessible to countries other than where they are collected or stored. Data may be collected in one country and stored in another, be processed in a third, and be accessible from many countries or even globally. The key requirement is that all this processing should be carried out in a fashion that is consistent with the:

- the purposes and consents of the original data collection and, in particular;
- all disclosures of personal health data should be to appropriate individuals or organisations within these purposes and consents.

International health-related applications require health-related data to be transmitted from one nation to another across national borders. That is very evident in telemedicine or when data are electronically dispatched for example in an email or as a data file to be added to an international database. It also occurs, but less obviously, when a database in one country is viewed from another for example over the Internet. That application may appear passive but the very act of viewing involves disclosure of that data and is deemed 'processing'. Moreover it requires a download that may be automatically placed in a cache and held there until 'emptied' - this also is processing and involves a particular security hazard.

There is a wide range in the types of third country organisation that might be involved in receipt of personal health data from an EU Member State for example:

- healthcare establishments such as hospitals;
- pharmaceutical companies involved in research;
- contractors remotely maintaining health care systems in EU hospitals;
- companies holding educational data bases containing for example radiological images with diagnoses and case notes;
- companies holding banks of medical records for patients from different countries.

In all applications involving personal health data there can be a potential threat to the privacy of an individual. That threat and its extent will depend on:

- the level to which data is protected from unauthorised access in storage or transmission;
- the number of persons who have authorised access;
- the nature of the personal health data stored;

- the level of difficulty in identifying an individual if access to the data is obtained;
- the difficulty in obtaining unauthorised access.

Wherever health data are collected, stored, processed or published (including electronically on the Internet) the potential threat to privacy needs to be assessed and appropriate protective measures taken. Some form of risk analysis should be undertaken to ascertain the required level of security measures.

In addition to the standards bodies CEN, CENELEC, ISO and IEC there are three major trans-national bodies that have produced internationally authoritative documents relating to security and data protection:

- the European Union (EU);
- the Organisation for Economic Co-operation and Development (OECD);
- the Council of Europe;
- the United Nations (UN).

The primary documents from these bodies are:

- EU Data Protection Directive "on the protection of individuals with regard to the processing of personal data and free movement of that data" [1];
- OECD "Guidelines on the Protection of Privacy and Trans-border flows of Personal Data" [2];
- OECD "Guidelines for the Security of Information Systems" [3];
- Council of Europe "Convention for the Protection of individuals with regard to Automatic Processing of Personal Data" No. 108 [4];
- "Council of Europe Recommendation R(97)5 on the Protection of Medical Data" [5];
- UN General Assembly "Guidelines for the Regulation of Computerised Personal Data Files" [6].

The means and extent of the protection afforded to personal health data varies from nation to nation [7]. In some countries there is nation-wide privacy legislation, in others legislative provisions may be at a state level or equivalent. In a number of countries no legislation may exist although various codes of practice or equivalent will probably be in place and/or 'medical' laws which lay down a duty on medical practitioners to safeguard confidentiality.

Although privacy legislation in different parts of the world may mention personal health data, frequently there is no legislation specific to health except perhaps in relation to government agencies and/or medical research.

The EU Directive on Data Protection (see text in annex A) aims to create uniform legislative data protection provisions throughout the EU. The Directive also applies to non-community countries of the European Economic Area by virtue of the EEA Treaty Decision 83/1999 of 25 June 1999. The majority of countries of Central and Eastern Europe and Cyprus which are applicants to become members of the EU, are also looking to introduce legislation in conformance with the Directive.

The Directive makes it permissible for personal data to be passed across EU borders. However, the transfer of personal data from an EU country to a non-EU country is controlled by Articles 25 and 26.

In essence, subject to specific 'derogations', Article 25 allows transfer of personal data to a third country only if that third country ensures an 'adequate level of protection'.

The 'adequacy of protection' is to be assessed (Article 25.2) in the light of all the circumstances with 'particular consideration' to be given to particular factors including:

- the nature of the data;
- the purpose and duration of the proposed processing operation(s);
- the rules of law applying;
- the professional rules and security measures which are complied with;
- the country concerned.

In the health context personal health data can be extremely sensitive in nature and is recognised as such by the Directive. There is extensive guidance available both nationally and internationally on 'security measures' for the protection of personal health data (see annex B).

As noted above there is in many countries a mix of general and specific legal or quasi-legal requirements covering personal health data protection plus professional codes covering ethical aspects including safeguarding confidentiality. These two aspects may not necessarily be consistent and may in some aspects be in conflict. This European Standard, although referring to both, deals primarily with the legal context deriving from implementation of the Data Protection Directive. Ethical codes generally contain material that goes beyond formal legal requirements. The guidance in this standard should not diminish compliance with such more extensive documents. Indeed ensuring conformance with legal rules is only one aspect of ensuring confidentiality is protected. In that context it should be noted that the European Group on Ethics in Science and New Technologies [8], is of the opinion that "personal data should be considered in the framework of the rights of personality, even if in some cases they may be subject transactions" and, "since personal data continue to reflect the data subject's identity, they cannot be treated as entirely separate from him/her". The Group observed that consequently "some countries regard sensitive personal health data as inalienable to protect the dignity of the individual". The International Medical Informatics Association is in the process of developing and accepting a code of ethics for health information professionals [18].

Article 26 of the Directive details the 'derogations' under which an EU Member State may permit transfer of personal data to a third country without an adequate level of data protection. The full list is in annex A. The derogations include where:

- the data subject has given his unambiguous consent;
- it is necessary to protect the data subject's vital interests;
- the "controller adduces adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals"; "such safeguards may in particular result from appropriate contract clauses".

Under Article 29 of the EU Directive an EU Working Party, on the Protection of Individuals with regard to Processing of Personal Data, was created. Its findings provide important interpretations and views on the Directive.

EN 14485, *Health informatics - Guidance for handling personal health data in international applications in the context of the EU data protection directive* [9] provides guidance on the general measures that should be taken to render permissible transfer of personal health data from an EU Member State or another country.

These general measures comprise guidance for ensuring that such transfers are permissible under the Directive. Whilst it indicates the actions that a non-EU organisation should take to render such transfers permissible, the standard does not make explicit the essential elements that such an organisation should include in its security policy covering these types of international applications.

This standard addresses these aspects and provides guidance on the policy which an organisation in a non-EU country should adopt to demonstrate compliance with the measures necessary to make permissible the transfer of personal health data to it from an EU country in the context of the EU Directive.

This standard is based on the premise that all organisations processing personal health data in international applications should reflect all of their obligations under the EU Data Protection Directive in their security policies. It would be of considerable benefit to data subjects, which for health data includes patients, if all such organisations had a high level security policy addressing these matters which:

- made clear the organisation's expectations of all its staff involved in the processing of personal health data in an international application (often expressed in contracts of employment);
- was available to any data subject on request;
- was part of the documentation which would assist in reassuring an EU Supervisory Authority of an organisation's compliance with the Directive;
- would help reassure other bodies with which the organisation was associated in the context of health data.

Whereas the Directive renders it permissible for personal health data to be transferred to other EU Member States (strictly also EEA Member States), data controllers nevertheless have the obligation to ensure EU/EEA

organisations have implemented necessary requirements for processing. A high level security organisation policy standard will assist EU controllers in:

- specifying and assessing the adequacy of the data protection provisions of others with whom they are dealing;
- demonstrating to others the adequacy of their own provisions.

Article 25 of the Directive prohibits the transfer of personal data to non-EEA countries unless they have adequate data protection provisions in the context of the Directive. Article 26 details allowable derogations in the context of that prohibition.

Those EU organisations seeking to engage with organisations in non-EEA countries in international applications involving personal health data, will at least need to assure themselves that the non-EU party:

- is in compliance with any measures which will ensure adequacy of their data protection in the context of the EU Directive (these go beyond solely technical security aspects); or
- will ensure compliance with the terms of any derogations available.

The High Level Security Policy which this standard addresses will assist:

- EU organisations in laying down conditions on non-EEA parties to render permissible the transfer of personal health data;
- non-EU organisations in complying with the requirements of the Directive in the context of the transfer of personal health data to them from an EEA body.

1 Scope

This European Standard provides guidance on a High Level Security Policy for third country organisations and is restricted to aspects relevant to personal health data transferred from a compliant country to a third country (see definitions).

This European Standard provides guidance on the High Level Security Policy which should be adopted by third country organisations involved in international informatics applications which entail transmission of person health data from an EU Member State to a non-EU Member State whose data protection is inadequate in the context of the EU Data Protection Directive [1]. Its purpose is to assist in the application of the EU Directive.

The European Standard does not provide definitive legal advice but comprises guidance. When applying the guidance to a particular application legal advice appropriate to that application should be sought.

Whereas this guidance will be useful in the formulation of a high level policy for EU organisations, its scope is restricted to organisations in third countries (see definitions).

2 Normative references

Not applicable.

3 Terms and definitions

For the purposes of this European Standard, the following terms and definitions apply. Where a term is defined in the EU Data Protection Directive (Article 2) that definition is used for the purposes of this European Standard. In countries in which the EU Directive has not been implemented, other definitions for these terms may be in use and may have a legal status and therefore care should be taken in utilising this standard in those circumstances.

3.1

identifiable person

person who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

3.2

compliant country

country whose legislation complies with the EU Data Protection Directive and is recognised as such by the European Commission

3.3

controller

natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law

3.4

data subject

identified or identifiable natural person, which is the subject of personal data

3.5

personal data

any information relating to an identified or identifiable natural person

3.6**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 allowing easy access to the personal data

3.7**personal health data**

any information relevant to the health or sex life of an identified or identifiable natural person

3.8**processing of personal data**

processing any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

3.9**processor**

natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

NOTE In the definition of a third party in 3.15 below, the processor is distinguished from "the persons who under the direct authority of the controller or processor, are authorised to process the data". This implies that employees per se are not processors. This is the approach taken by some implementations of the Directive e.g. in the UK.

3.10**recipient**

natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry are not regarded as recipients

3.11**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

3.12**third country**

country not bound by the legal requirements of the EU Data Protection Directive

3.13**third party**

any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data

3.14**Commission**

Commission of the European Communities unless obviously otherwise

3.15**high level security policy**

High Level Security Policy for organisations in third countries which process personal health data from EU Member States.

4 Abbreviated terms

The following abbreviated terms are used:

EEA	European Economic Area;
EU	European Union;
EU Directive	EU Data Protection Directive 95/46/EC [1]
EU WP	EU Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of the EU Directive;
HLSP	High Level Security Policy;
OECD	Organisation for Economic Co-operation and Development;
UN	United Nations.

5 The European Data Protection Directive (see annex A)

5.1 General

The following picks out the requirements of the Directive that are most pertinent to this standard. The requirements are summarised. The full text (annex A) shall be used for definitive and complete meaning.

5.2 General aims: (Article 1)

Article 1 states that “Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data” and “shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection”. The Directive’s scope is thus more than solely technical data protection. Its result is that Member States may not restrict or prohibit the free flow of personal data between Member States for reasons of protection afforded by the Directive.

5.3 Scope: electronic and non-electronic (Article 3)

The Directive applies to the processing of personal data wholly or partly by automatic means AND to processing other than by automation. It therefore applies to data on paper as well as in electronic form and the Directive requires, inter alia, that appropriate security measures should be applied to these data also.

5.4 Principles relating to data quality (Article 6)

The controller shall ensure that personal data is:

- processed fairly and lawfully;
- collected for explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive for the purpose;
- accurate and, where necessary, kept up to date;
- kept no longer than is necessary.

5.5 Criteria for legitimacy (Article 7)

Personal data may be processed only if one of a number of criteria is met. These include that:

- the data subject has unambiguously given his consent;

- processing is necessary to protect the vital interest of the data subject;
- processing is necessary for the performance of a contract to which the data subject is party.

5.6 Special categories of processing, including personal health data (Article 8)

Subject to exceptions, it is prohibited to process "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of data concerning health or sex life".

Thus personal health data is in a special category and can be processed only if one of several conditions is satisfied. These include that:

- the data subject has given explicit consent;
- processing is necessary to protect the vital interests of the data subject.

However the prohibition on processing personal health data does not apply "where processing of the data is required 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".

5.7 Information to be given to the data subject (Article 10)

The controller must provide the data subject with specified information including:

- the identity of the controller;
- the purposes of the processing;
- any further information which is necessary for processing such as:
 - the recipients of the data;
 - the existence of the right of access to, and the right to rectify, data concerning him.

5.8 Right of access to data (Article 12)

The controller must guarantee to the data subject the right:

- to obtain, without constraints, at reasonable intervals and without excessive delay or expense:
 - confirmation as to whether data relating to him is being processed, and any other recipients;
 - communication to him of data undergoing processing and their source;
- to rectify, erase or block processing of data which does not comply with provisions of the Directive e.g. is inaccurate.

5.9 Right to object (Article 14)

The data subject must have the right:

- to object, on compelling legitimate grounds, to the processing of data relating to him. Where the objection is justified the controller may no longer process those data;
- to object to processing of personal data relating to him for the purpose of direct marketing and to be informed before such data is first disclosed to any third party for such purposes.

5.10 Security of processing (Article 17)

The controller must:

- implement appropriate technical and organisational measures to protect personal data in particular where the processing involves the transmission of data over a network. These measures shall have regard to the state of the art and the cost of their implementation and shall ensure a level of security appropriate to the risks and the nature of the data;
- where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect to technical security and organisational measures and must ensure compliance;
- ensure that processing by way of a processor is governed by a contract or legal act binding the processor to the controller stipulating in particular that the processor shall act only on instructions from the controller. The contract must be in writing or equivalent form.

5.11 Judicial remedies, liability and sanctions (Articles 22, 23 and 24)

- every person shall have the right to a judicial remedy for any breach of the rights guaranteed to him;
- any person who has suffered damage as a result of unlawful processing or any act incompatible with the Directive is entitled to receive compensation from the controller;
- each Member State must lay down the sanctions to be imposed in case of infringements of the Directive.

5.12 Supervisory Authorities (Articles 28 and 18)

Each Member State must appoint an independent Supervisory Authority with powers to investigate, intervene and to engage in legal proceeding. A controller must notify his Supervisory Authority before carrying out processing. Member States may exempt controllers from this requirement in certain circumstances e.g. if the controller appoints a personal Data Protection Official responsible for ensuring, in an independent manner, that the Directive's provisions are implemented.

5.13 Working party on the protection of Individuals with regard to the Processing of Personal Data

(Articles 29 and 30)

The above Working Party was created through the Directive and its opinions provide significant interpretations.

5.14 Transfer of personal data to Third Countries

Articles 25 and 26 deal with this aspect and are considered in detail in Section 6.

6 Requirements for the transfer of personal data to third Countries.

6.1 General

The following is a précis of the requirements in the Directive. For the full text see annex A.

6.2 Principles (Article 25)

Transfer of personal data from an EU Member State to a third country may take place only if the third country ensures an adequate level of protection.

The adequacy of protection shall be assessed in the light of all the circumstances. Particular consideration is to be given to the nature of the data, the purpose of processing and the rules of the law, both general and

sectoral, in force in the third country and the professional rules and security measures compiled with in that country.

The Commission is empowered to negotiate a remedy wherever a third country is judged not to ensure an adequate level of protection.

Derogations including standard contract clauses (Article 26)

Transfer of personal data is permissible under certain conditions (derogations) including where:

- the data subject has given his consent unambiguously;
- the transfer is necessary for the performance of a contract between the data subject and the controller;
- the transfer is necessary in order to protect the vital interests of the data subject.

It is also permissible where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. Such safeguards may result from appropriate contract clauses. The Commission proposes to adopt standard contractual clauses that offer sufficient contractual safeguards [10] where the recipient in the third country is a processor (but not a controller).

6.3 Ensuring transfers are permissible

No transfer of personal health data may take place from an EU Member State to a non-EU country unless permitted by the Directive. EN 14485, *Health informatics - Guidance for handling personal health data in international applications in the context of the EU data protection directive* [9], deals in detail with the options for ensuring transfers are permissible and should be referred to as a companion to this standard. This standard is based on the premise that, by whatever means, transfers are permissible and deals with the security policy that the third country recipient organisation should adopt to ensure and demonstrate compliance. However, since the elements of that policy have a dependence on the manner by which transfers have been rendered permissible, a brief summary is given below but without the rationale and background of the companion standard [9].

6.4 Grounds by which transfers to third countries are permissible

6.4.1 General

Annex C comprises a "Model Declaration of Grounds upon which Transfer of Personal Health Data is regarded as in compliance with the EU Data Protection Directive", taken from the companion standard [9]. It provides a succinct summary of the different grounds.

6.4.2 Members of the EEA

These countries may be regarded as equivalent to EU Member States as far as this standard is concerned. Countries recognised as having adequate data protection provisions

The Commission might find that a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. For example this has been found for Hungary and Switzerland [11], [12]. Such countries can be regarded as equivalent to EEA countries and EU Member States as far as this standard is concerned.

6.4.3 Depersonalisation of data

The EU Directive defines personal data as "any information relating to an identified or identifiable natural person". An identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

A solution to problems of transferring personal health data to third countries is to render the data non-personal. This may often be referred to as rendering data 'anonymous'. However the perception of anonymisation varies. In the context of this standard "anonymisation" therefore means rendering data 'non-personal' in the context of the EU Directive's definition of "personal data".

An "identifiable person" includes one who can be identified "indirectly" by reference to "one or more of the factors specific to him". Clearly such factors comprise more than name and address. A data subject may for example be identifiable by a combination of any one or more of age; sex; race; occupation; postal/zip code; income group; physiological or mental state; family characteristics etc. Additionally in the context of some health applications, images e.g. photographs, dental records, radiographs or traces such as EEGs may have details which, taken alone or together with other data such as specialty and/or identity of health organisation, would render the data as person-identifiable and thereby as personal data.

Such combinations of data elements may render as personal, data that may otherwise have been considered as purely statistical. Postal/Zip Codes provide a very effective way of locating an individual within a small group. Similarly this may also occur through small numbers e.g. the number of women having triplets could be extremely small in even a large geographic area.

Rendering data non-personal thus requires attention to considerable detail. The Database Inference Problem is always theoretically soluble given sufficient resources and access to other relevant information. However, adequate anonymisation can frequently be achieved by withholding obviously identifying information and ensuring that the recipient does not seek to re-identify individuals or to disclose the anonymised information wider than is necessary for the purposes for which it has been agreed that it can be used.

Correspondingly statistical information concerning health can often, given the resources and reference to other data bases which may be in the public domain, reveal the identity of an individual. Clearly criteria based on the concept of excessive effort in relation to the necessary security and sensitivity of the data need to be applied to such statistics. In this context Paragraph 26 of the EU Directive's preamble states that:

"Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable".

Any assurance given to a data subject concerning the rendering of data as non-personal should address the matter of risk of identity being revealed in relation to the level of effort required to do so. The extent and cost of such resources will vary with time as technology advances.

6.4.4 Consent

Transfer of personal health data to a third country is permissible if "the data subject has given his consent unambiguously to the proposed transfer". (Article 26 (1)).

In some applications such as telemedicine obtaining a patient's consent will be practicable. However for some applications, such as a shared international data base of radiological images with case notes, obtaining consent at a point which may be some time after the image was acquired for a different purpose, may be difficult. However consent for one purpose is not consent for another.

"Consent" needs to be "freely given, specific and informed". "Unambiguous consent" must therefore be on the basis of knowledge of any matters which may be relevant particularly if these matters might weaken the rights that would have been obtained had consent not been given. Thus the data subject will need to know not only that a transfer of personal health data to a third country is involved but also what that entails.

6.4.5 Subject to contract clauses

If the 'controller' can "adduce adequate safeguards" through "appropriate contract clauses" then transfer of personal health data to a third country is permissible. This is not a straightforward matter (see companion standard [9]). The Commission has proposed standard clauses [10] but these apply only where the third country recipient is solely a 'processor'. In many circumstances the recipient may need to be, or at times act as, a 'controller' in his own right. For example the provision of independent professional advice in telemedicine consultations almost certainly renders the professional concerned or his organisation a data 'controller'.

If the data is in a special category then the data subject must be informed before transfer. Personal health data is in a "special category".