DEUTSCHE NORM

März 2004

DIN EN 14485

ICS 35.240.80

Medizinische Informatik – Anleitung zur Verwendung von persönlichen Gesundheitsdaten in internationalen Anwendungen vor dem Hintergrund der EU-Datenschutzrichtlinie; Deutsche Fassung EN 14485:2003, Text in Englisch

Health informatics –
Guidance for handling personal health data in international applications in the context of the EU data protection directive;
German version EN 14485:2003, text in English

Informatique de santé –
Guide pour manipuler des données personnelles de santé dans des applications internationales dans le contexte de la directive européenne sur la protection des données personelles;
Version allemande EN 14485 : 2003, texte en anglais

Gesamtumfang 79 Seiten

Normenausschuss Medizin (NAMed) im DIN

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

Die Europäische Norm EN 14485:2003 hat den Status einer Deutschen Norm.

Nationales Vorwort

Diese Norm enthält unter Berücksichtigung des Präsidialbeschlusses 13/1983 die Englische Fassung der Europäischen Norm EN 14485:2003. 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.

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 14485

December 2003

ICS 35.240.80

English version

Health informatics - Guidance for handling personal health data in international applications in the context of the EU data protection directive

Informatique de santé - Guide pour manipuler des données personnelles de santé dans des applications internationales dans le contexte de la directive européenne sur la protection des données personelles

Medizinische Informatik - Anleitung zur Verwendung von persönlichen Gesundheitsdaten in internationalen Anwendungen vor dem Hintergrund der EU-Datenschutzrichtlinie

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

© 2003 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN 14485:2003 E

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

Contents

Page

Foreword 5
Introduction 6
1 Scope 9
2 Normative references 9
3 Terms and definitions 9
4 Abbreviated terms 11
5 General solutions to exchanging personal health data between compliant and non-compliant countries 11
5.1 General approach 11
6 Judging the adequacy of data protection 12
6.1 General 12
6.2 Content Principles 12
6.3 Procedural/Enforcement Mechanisms 14
6.4 Third Countries that have ratified the Council of Europe Convention 108 14
6.5 Industry self-regulation 15
7 Making adequate provisions 16
7.1 Introduction 16
7.2 Meeting the "Content Principles" 16
7.3 Providing for the "Procedural/Enforcement Mechanisms" 17
7.3.1 General 17
7.3.2 Providing redress 17
7.3.3 Support and help to data subjects 17
7.3.4 Adequate compliance 18
7.3.5 Onward transfers 18
7.3.5 Direct marketing and sale of data 18
7.4 Overriding law 18
8 Permissible derogations, Articles 26.1 and 26.2 19
8.1 Article 26.1 19
8.1.1 General 19
8.1.2 Consent 20
8.2 Article 26.2 20
9 Anonymisation 20
9.1 Definition of personal data 20
9.2 Rendering personal data anonymous 21
10 Notification to Supervisory Authorities 21
10.1 Introduction 21
10.2 Implementation of Articles 18 to 20 21
11 Steps in establishing an international application with adequate data protection safeguards from the view point of an EU data controller 22
11.1 Introduction 22
11.2 Step One: Can the data be non-personal? 22
11.3 Step Two: Is the recipient third country an EEA country? 23
11.4 Step Three: Is the recipient country recognised by the Commission as having adequate data protection provisions? 23
11.5 Step Four: Is the recipient organisation in compliance with arrangements formally recognised by the Commission as providing adequate data protection provisions? 24

Documents
Document Sharing Hub
Full document details: DIN EN 14485:2004-03

Page

11.6 Step Five; If the recipient third country is not EEA, has it signed the Council of Europe Convention 108? ... 24
11.7 Step Six: Is the recipient country applying to become a member of the EU? ... 24
11.8 Step Seven: Can adequacy of data protection be established? ... 24
11.9 Step Eight: If adequacy of data protection cannot be established can the derogations in Article 26.1 provide a solution? ... 24
11.10 Step Nine: If adequacy of data protection cannot be established can the derogation in Article 26.2 regarding contractual clauses provide a solution? ... 26
11.11 Step Ten: If transfer of personal data health data to the recipient third country is permissible has the recipient implemented adequate security measures and can the application proceed? ... 26

12 Steps in establishing an international application with adequate data protection safeguards from the viewpoint of a non-EU data controller ... 26
12.1 Establishing data protection adequacy in the EU ... 26

13 Model contract clauses ... 27
Published models ... 27

14 Security measures ... 27
14.1 Introduction ... 27
14.2 General security ... 28
14.3 Security contracts with processors and with controllers in non-compliant countries ... 28
14.4 Security policy ... 28
14.5 Risk analysis ... 29
14.6 Security organisation and allocation of duties ... 29
14.7 Reporting of security incidents or breaches ... 29
14.8 Staff and contractor contracts ... 29
14.9 Training and awareness ... 30
14.10 Transmission of data ... 30
14.11 Limitations of purpose and access ... 30
14.12 Onward transfers ... 30
14.13 Audit trails ... 31
14.14 Loss, damage and destruction ... 31
14.15 Business Continuity Plans ... 31
14.16 Network Security ... 31
14.17 Patients Rights ... 31
14.18 Compliance ... 32
14.19 Standards ... 32

15 Declaration of grounds on which transfers are to take place ... 32
15.1 Statement of grounds ... 32

Annex A (informative) Key primary international documents on data protection ... 33
A.1 EU Data Protection Directive ... 33
A.1.1 General ... 33
A.1.2 Coverage ... 33
A.1.3 Rules for lawfulness of processing ... 33
A.1.4 Special categories of processing ... 34
A.1.5 Data subject's rights ... 34
A.1.6 Security of processing ... 35
A.1.7 Supervisory Authorities ... 35
A.1.8 Remedies and sanctions ... 35
A.1.9 Transfer of personal data to third countries ... 35
A.2 Organisation for Economic Co-operation and Development (OECD) ... 36
A.3 Council of Europe ... 36
A.4 United Nations General Assembly ... 37
A.4.1 General ... 37
A.4.2 Principles concerning minimum guarantees that should be provided in any national egislation ... 37

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

Page

A.4.3 Application of the Guidelines to personal data files kept by governmental international organisations 38

Annex B (informative) **Text of Articles 25 and 26 of the EU Data Protection Directive** 39
B.1 Article 25: Principles 39
B.2 Article 26: Derogations 39

Annex C (informative) **Text of Article 28 of the EU Data Protection Directive** 41

Annex D (informative) **Questionnaire for Assessing Data Protection Adequacy** 43

Annex E (informative) **Safe harbour privacy principles** 49

Annex F (informative) **Standards and sources of advice** 52
F.1 EU Security projects 52
F.2 CEN/ISSS 52
F.3 Non-CEN Standards 52
F.4 Selected web sites 53

Annex G (informative) **Model Declaration of Grounds upon which Transfer of Personal Health Data is Regarded as in Compliance with the EU Data Protection Directive** 54

Annex H (informative) **Model contractual clauses for controller to controller transfers to a country with inadequate data protection provisions** 56
H.1 Introduction 56
H.2 Model standard contractual clauses 57

Annex I (informative) **Model contractual clauses for controller to processor transfers to a country with inadequate data protection provisions** 67
I.1 Introduction 67
I.2 Model standard contractual clauses 68

Bibliography 76

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

Foreword

This document (EN 14485:2003) 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.

The annexes A, B, C, D, E, F, G, H and I 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.

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

Introduction

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

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

The data required will depend 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 with the 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.

International health-related applications will require health-related data to be transmitted from one nation to another.

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 the other 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.

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

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);

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

•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].

Annex A provides a synopsis of the key documents published by these bodies.

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 legislature provisions may be at a state level or equivalent and in a number no legislation may exist although various codes of practice or equivalent will probably be in place.

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 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 passing of personal data from any one of these conforming nations to another ('third') country is controlled by Articles 25 and 26 of the Directive the full text of which is in annex B. 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.

In the health context personal health data can be extremely sensitive in nature and is so recognised by the Directive. However rules of law specific to health are not common with the exception perhaps of medical research. Nevertheless 'professional rules' applying to the medical and other healthcare professions concerning the protection of patient confidentiality are present in most countries with significant 'penalties' associated with non-compliance. There is in addition extensive guidance available both nationally and internationally on 'security measures' for the protection of personal health data (see annex F and clause 2).

In many countries therefore there is a mix of general and specific legal or quasi-legal requirements covering 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 context deriving from implementation of the Data Protection Directive. Ethical codes often 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 to the Commission [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”.

Documents
Document Sharing Hub
Full document details: DIN EN 14485:2004-03

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 B. They 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 freedom of individuals and as regards the exercise of the corresponding rights; 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 and these are frequently referred to in this standard.

This standard provides guidance on measures that should be taken to protect personal data in applications which involve transfer of personal health data across national boundaries and in particular between EU and other countries which conform to the EU Directive, and those which may not. In that context it considers the use of contract clauses to achieve adequate safeguards.

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

1 Scope

This European Standard provides guidance on data protection for those involved in international informatics applications which entail transmission of person health data from an EU Member State to a non-EU Member State. Its purpose is to assist in the application of the EU Directive on Data Protection [1].

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.

2 Normative references

Not applicable.

3 Terms and definitions

For the purposes of this European Standard, the following terms and definitions. Where a term is defined in the EU Data Protection Directive [1] 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

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

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 should not be 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
the Commission of the European Communities unless obviously otherwise

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

4 Abbreviated terms

The following abbreviated terms are used:

EEA	European Economic Area;
EU	European Union;
EU Directive	EU Data Protection Directive 95/47/EC [1];
EU WP	EU Working Party on the Protection of Individuals with Regard to Processing of Personal Data set up under Article 29 of the EU Directive;
OECD	Organisation for Economic Co-operation and Development;
UN	United Nations.

5 General solutions to exchanging personal health data between compliant and non-compliant countries

5.1 General approach

Article 25.1 of the EU Directive prohibits the transfer of personal data from an EU Member State to a third country unless the latter ensures an adequate level of protection. Article 25.6 provides that the Commission may find that a third country does ensure an adequate level of protection but meanwhile decisions on the adequacy of protection must be made by the data controller taking advice from his Supervisory Authority.

This clause considers the general approach for reaching a position whereby transfer of personal health data from an EU Member State to a non-EU country would be permissible.

Article 25 defines the 'derogations' (exemptions) within which an EU Member State may transfer personal data to third country which is judged not to ensure an adequate level of protection. The full text of these derogations is in annex B. Each of them may be very relevant to personal health data including in particular the conditions that:

- the data subject has given his consent unambiguously to the proposed transfer (26.1(a));
- the transfer is necessary in order to protect the vital interests of the data subject (26.1(e)).

Additionally Article 26.2 provides that a Member State may authorise such transfers if the controller adduces adequate safeguards through 'appropriate contract clauses'.

The general solutions to exchanging personal health data between nations are therefore as follows.

If the exchange is between EU Member States or other compliant country transfers are permitted.

If the exchange is between an EU Member State and a non-EU Member State the controller in the EU Member State should first establish whether the Commission has determined, through Article 26.6, that the data protection provisions in the non-EU State are adequate. If that is not the case then the following steps should be taken.

1 Determine whether the Commission has made any findings.

2 Determine whether the appropriate Supervisory Authority has made any findings.

3 Assess whether the protection in the non-EU State could be considered as adequate.

4 Assess whether a solution exists in the permissible derogations (exemptions) in Article 26.1.

5 Assess whether a solution can be found in the derogation allowed in Article 26.2 i.e. a contractual solution.

In practice a combination of 1, 2 3 and 4 may be the most appropriate solution.

AVA Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

6 Judging the adequacy of data protection

6.1 General

The EU Working Party (EU WP) has taken a view on assessing the adequacy of data protection of third countries [9]. The underlying principles, which the EU WP expounds for judging adequacy can be applied both to the third country as a whole and to the particular institution such as a hospital involved in the international application. Thus it may be possible to address any deficiencies in a country's data protection provisions through Article 26 derogations applied to the application itself, for example through contract clauses. Indeed even where a third country's data protection provisions in a particular aspect appear satisfactory, it may still be wise to reinforce the provisions through contract clauses.

These are two essential elements of adequacy:

- the adequacy of the data protection provisions in the storage and processing of the personal health data within a recipient's institution and the obligations placed on those responsible for them;
- the means for ensuring that such provisions are followed in practice and for ensuring the rights of data subjects.

The EU WP refers to these as "Content Principles" and the "Procedural/Enforcement" Requirements.

6.2 Content Principles

An examination of a range of international laws, rules, Codes of Practice and Guidelines reveals a high degree of consensus on the essential rules which should be applied in protecting personal health data within and between institutions. Clause 14 of this Standard deals with such content rules and procedures. The EU WP "Content Principles" are:

1 **the purpose limitation principle** - data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the EU Directive (see below).

2 **the data quality and proportionality principle** - data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed (subject to exemptions in Article 13).

3 **the transparency principle** - individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11.2 and 13 of the EU Directive (see below).

4 **the security principle** - technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

5 **the rights of access, rectification and opposition** - the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the EU Directive (see below).

6 **restrictions on onward transfers** - further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26.1 of the EU Directive.

Documents
Document Sharing Hub
Full document details: DIN EN 14485:2004-03

Additional principles applying to specific applications are:

- **sensitive data** - where "sensitive" categories of data are involved (those listed in Article 8 of the EU Directive and which include health: see below) additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing;

- **direct marketing** - where data are transferred for the purposes of direct marketing, the data subject must be given the opportunity to prevent his data being used for such purposes at any stage;

- **automated decisions in the sense of Article 15 of the EU Directive (see below):** in general the individual should have the right to prevent decisions being taken about him which have legal effects concerning him or have significant effects on him based solely on automated processing of data. There are some exceptions in relation to contracts where there are safeguards. Where such decisions are involved, individuals have the right to know the logic involved in these decisions.

The essence of the Articles referred to above are:

- Article 13 permits Member States to adopt legislative measures to restrict the scope of the obligations and rights provided for in a number of the Directive's Articles which bear on almost all of the 'Content Principles'. This is permitted if such a restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, and important economic or financial interest, or the protection of the data subject or the rights and freedoms of others;

- Article 11.2 stipulates that when data are collected from one other than the data subject, information need not be provided to the data subject if this proves impossible, involves a disproportionate effort, or if the recording or disclosure of the data is expressly required by law;

- The sensitive categories of data in Article 8 are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, data concerning health or sex life, and data relating to offences, criminal conviction or security measures;

- Article 15 states that "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."

The EU WP makes clear that the "Content Principles" are regarded as a minimum list and 'not set in stone'. The degree of risk to the data subject will determine the precise requirements in a particular case and may require additions to the list or even a reduction.

In the context of personal health data it should be noted that Article 8 regards health as "sensitive" data. Also in applying Principle (4) Security, some applications such as telemedicine may require sender and recipient to have both "controller" and "processor" roles, for example when sharing an electronic patient record.

The Directive is silent on the question of requirements to safeguard the confidentiality of personal data on the death of the data subject. The manner in which this aspect is handled in national legislation varies e.g. in the UK Data Protection it applies only to living persons.

However there are many circumstances where the health records of a dead individual could reveal personal health data relevant to some other individual and be of detriment to them. The records may refer explicitly to other individuals e.g. members of the dead person's family. If an individual died of a condition deriving from an inheritable genetic deficiency, his records may reveal matters relevant to his offspring.

Partners in an international application will need to come to an explicit agreement about what to do in circumstances of death. That agreement may depend on the countries involved and how they treat health records e.g. laws or rules which may apply to length of time health records must be retained after death. Different property

Documents
Document Sharing Hub
Full document details: DIN EN 14485:2004-03

rights may also apply e.g. if a patient is the legal owner of his records then on death such records may be part of his estate and subject to probate.

Since a patient's permission to allow his personal health data to be processed and passed to a third party, may depend on what would happen to such data should he die, patients should be informed of any arrangements made concerning the handling of such data on his death.

Whereas the list in this clause was compiled with a view to transfers of personal data from an EU Member State to a third country in the context of the EU Directive, they may equally satisfy third countries when transferring in the opposite direction.

6.3 Procedural/Enforcement Mechanisms

Even if the "Content Principles" are built into the rules for processing, storage, transfer etc of personal health data, the rights' of individuals will not be assured unless the rules are followed and, if not, individuals have an effective form of redress.

Whereas a number of international and national documents, for example from the Council of Europe [4] [5], the OECD [2] [3] and the UN [6], agree upon the essence of the requirements concerning the rights of individuals, the means for ensuring their effectiveness varies substantially.

The EU Directive ensures that the means for ensuring effectiveness are imbedded in law. It, for example, requires creation of Supervisory Authorities with monitoring and complaint investigative functions, and provisions such as liability sanctions and remedies.

Many national and international guides and rules, whilst they may exhort similar rights for individuals:

- may not be so comprehensive;
- may not require enshrinement in law;
- may not cover all health sectors e.g. may cover only the public sector.

Thus to judge adequacy of data protection in a third country requires assessment of the judicial mechanisms in place. The EU WP considers that such an assessment should achieve the following objectives.

1. To deliver a good level of compliance with the rules (no system can guarantee 100 % compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important part in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

2. To provide support and help to individual data subjects in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

3. To provide appropriate redress to the injured party where rules are not complied with. This is a key element, which must involve a system of independent adjudication, or arbitration, which allows compensation to be paid and sanctions imposed where appropriate.

In terms of personal health data these general objectives are considered further in clause 11 of this standard.

6.4 Third Countries that have ratified the Council of Europe Convention 108

Most of the countries that have ratified this Convention are already bound by the EU Directive as members of the EU or EEA. However there are some that are not, e.g. Slovenia, Hungary and Switzerland.

Documents
Document Sharing Hub
Full document details: DIN EN 14485:2004-03

The EU WP has considered whether countries that have ratified the convention can be considered as affording adequate protection in the context of Article 25.1.

With respect to the six minimum "Content Principles", Chapter One of the Convention could be regarded as meeting the first five. However it does not restrict transfer of personal data to a third country theoretically allowing a compliant country being used as a "staging post" to a country without adequate protection.

In respect to "Procedural/Enforcement Mechanisms" the Convention does require its principles to be embedded in domestic law which if implemented would ensure a reasonable level of compliance and redress for data subjects where there is non-compliance. However there is no obligation to establish institutional mechanisms for independent investigation of complaints.

The EU WP's preliminary conclusion was that transfers of personal data to countries that have ratified Convention 108 could be presumed to be allowable under Article 25.1 provided that:

- the country in question has appropriate mechanisms to ensure compliance, help individuals and provide redress (such as an independent Supervisory Authority with appropriate powers);
- and the country in question is the final destination of the transfer unless the onward transfer is to an EU country or other destination offering adequate protection.

6.5 Industry self-regulation

Article 25.2 refers to "professional rules and security measures which are complied with in a third country" as an element in assessing adequacy of data protection.

The EU WP have considered this aspect under "self-regulation" and specifically in the context of self regulatory codes or similar they being "a set of data protection rules applying to a plurality of data controllers applying to the same profession or industry sector the context of which have been determined by members of the industry or profession concerned". Doctors are specifically recognised as one such profession.

For self-regulation, such as through a code, to be regarded as adequate protection the same criteria of "Content Principles" and "Procedural/Enforcement Mechanisms" need to be applied. In particular this would require a high assurance of compliance by the professions or sector covered by a code; adequate penalties for non-compliance; and redress for any data subject suffering damage including "distress" in the legal sense.

The EU WP concluded that:

- for a self-regulatory instrument to be considered as a valid ingredient of "adequate protection" it must be binding on all the members to whom personal data are transferred and provide for adequate safeguards if data are passed on to non-members;
- the instrument must be transparent and include the basic content of all core data protection principles;
- the instrument must have mechanisms which effectively ensure a good level of general compliance. A system of dissuasive and punitive sanctions is one way of achieving this. Mandatory external audits are another;
- the instrument must provide support and help to individual data subjects who are faced with a problem involving the processing of their personal data. An easily accessible, impartial and independent body to hear complaints from data subjects and adjudicate on breaches of the code must therefore be in place;
- the instrument must guarantee appropriate redress in cases of non-compliance. A data subject must be able to obtain a remedy for his/her problem and compensation as appropriate.

In the health sector, codes of one form or another often exist compiled by the caring professions or others. In the area of medical research such codes may have a judicial or quasi-judicial force. In other contexts such as

Documents
Document Sharing Hub
Full document details: DIN EN 14485:2004-03

healthcare this is less likely to be the case. Compliance of any code with the "Content Principles" would need to be examined since full compliance will probably not be assured.

The medical profession will normally in a country have a strong ethical code of practice that will include a requirement to safeguard patient confidentiality. There will usually be sanctions for breaches, including the possibility of losing the licence to practice. However such ethical codes and the confidentiality aspects are unlikely to encompass the data protection "Content Principles". If a code embodying "Content Principles" does exist it may not be inherently linked to the primary ethical code. Such combinations are therefore unlikely to fulfil all the requirements of "adequacy" but may fulfil most of them leaving deficiencies to be addressed through other measures, e.g. contractual.

7 Making adequate provisions

7.1 Introduction

Articles 17.2 and 17.3 of the EU Directive state:

- the Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures;

- the carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

  –the processor shall act only on instructions from the controller;

  –the obligations set out in Article 17.1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

In formulating a contract between parties in an EU Member State and a non-compliant State(s), the same objectives would apply. A contract confined to parties in the EU is executed within the full legal context of the EU Directive and the more general framework of Community Law. Where this is not the case, a contract must go further and compensate for any inadequacy in data protection in the non-compliant country.

In all provisos for transferring data to a non-compliant third country, the test of adequacy must include both the "Content Principles" and the "Procedural/Enforcement Mechanisms".

Article 17.2 and 17.3 relate to the responsibilities between a data controller and a processor. However in many health applications such as telemedicine, it will be necessary for the recipient to process the data in a manner which he chooses i.e. to act as a data controller in his own right. Such controller to controller relationships require extra provisions.

7.2 Meeting the "Content Principles"

Many countries and/or health institutions within them will be subject to some set of data protection rules. In general there is a widespread commonality in these rules and with the "Content Principles" but perhaps without specific restrictions on transfers to other non-compliant countries or organisations. Arriving at a situation which meets "Content Principles", is thus the easier step. Providing for effective "Procedural/Enforcement Mechanisms" can be more difficult because the sanctions of the law applicable in the transferer's country may not be possible to implement in the recipient's country.

Documents
Document Sharing Hub
Full document details: DIN EN 14485:2004-03

7.3 Providing for the "Procedural/Enforcement Mechanisms"

7.3.1 General

"Procedural/Enforcement Mechanisms" should:

- deliver a good level of compliance with the "Content Principles";
- provide support and help to individual data subjects in exercising their rights;
- provide an appropriate redress to an injured party.

7.3.2 Providing redress

The EU WP identifies three basic contractual approaches to enable a data subject to attain redress.

Approach one, is for the EU transferer to restrict the recipient to being simply a sub-contracted processor who, as a result, would have no autonomous decision-making powers. The transferer, as data controller, would specify in detail what the processor is to do and only to do. Since the transferer, being an entity in an EU Member State, remains totally responsible for the data transferred, he is liable to the law of that Member State and thereby automatically liable, under such law, for any damage resulting from unlawful processing no matter where undertaken. However circumstances will frequently occur e.g. in sharing electronic patient records in telemedicine, where the recipient in the non-compliant country is not solely providing data processing services. It may often be necessary for the recipient to have freedoms to process data as he sees fit and thereby effectively becoming a controller in his own right. In this case further safeguards will be required.

Approach two, is for the transferer to enter into a separate contract with the data subject stipulating that the transferer will remain liable for any damage caused by actions of the recipient. Such a contract could, for example, be made at the time data was obtained from the data subject and the issue of the transfer should be addresses then.

In both of these two approaches it would be for the transferer to pursue the data recipient for breach of contract if he sought to recover any damages paid to a data subject.

The third approach depends on the legal system applying to contracts in the country in question. Some legal systems allow third parties (i.e. those not party to the contract) to claim rights under the contract. This could, with an open published contract between transferer and recipient, provide satisfactory subject rights.

7.3.3 Support and help to data subjects

Under Article 28 of the EU Directive each Member State must establish a Supervisory Authority empowered to monitor compliance and investigate complaints. The full text of Article 28 is in annex C. However such functions of a Supervisory Authority are limited to the territory of its Member State (although, through Article 28.6, an Authority in one Member State may be requested to exercise its powers by an Authority in another Member State).

Where personal data is transferred to a third country, a data subject will have no such authority to which to turn. An equivalent institutional mechanism will be required.

An approach could be a contractual or other mechanism condition under which the recipient would permit the appropriate EU Supervisory Authority to investigate any data subject's complaint to the extent it felt appropriate, (if necessary through an agent in the recipient's country). However the Supervisory Authority, not being party to the arrangement, may not be able itself legally to invoke this process in the event of a complaint. A means to overcome this problem would be for the transferer to require the recipient to enter into a legally binding agreement direct with the Supervisory Authority to permit such investigation. Whether any Supervisory Authority would be prepared to take on these tasks is open to question.

An alternative would be a contract or other mechanism between the data subject and the transferer under which investigative mechanisms were agreed which the data subject could legally invoke. Such mechanisms, to be

Documents
Document Sharing Hub
Full document details: DIN EN 14485:2004-03

satisfactory, would require independence of investigation by a competent authority with perhaps means for independent binding arbitration.

7.3.4 Adequate compliance

Compliance with adequate data protection provision is ensured in EU Member States and other compliant States through the provisions of the EU Directive. Whereas a contract or other arrangement may be satisfactory in the requirements laid upon the recipient in a non-compliant country, and there may be satisfactory means for investigation and redress, this in itself does not ensure adequate compliance. Whether adequate compliance will in practice be attained, will in part depend on what penalty the recipient may suffer in a case of non-compliance.

In the medical and other caring professions an obligation to preserve confidentiality with the possible ultimate penalty of losing the licence to practice goes some way towards a solution. Contracts of employment may also carry the obligation to safeguard patient confidentiality with associated penalties but these are not uniform or standard. However safeguarding confidentiality of personal health data in the context of professional ethical codes and/or contracts of employment may fall short of ensuring compliance with the six "Content Principles".

7.3.5 Onward transfers

The sixth "Content Principle" is that transfers of personal data by the recipient of the original data should be permitted only where the second recipient is also subject to the rules affording adequate protection.

Any contract or other arrangement would need to ensure this. Where an arrangement is with a single recipient organisation, such as a hospital, with no requirement for onward transfer this can readily be achieved. However considerable complications will occur in some health applications such as telemedicine involving the need for the original recipient to consult further with other parties the identity of which may be unknown at the time of any contract or other arrangement being made.

7.3.5 Direct marketing and sale of data

One of the additional aspects of the "Content Principles" is that where data is transferred for the purpose of direct marketing, data subjects have the unequivocal right to prevent the use of their data for direct marketing. This will need to be assured particularly in the context of personal health data being regarded as sensitive data in a special category. Utilisation of personal health data, such as prescription data, in a purely commercial context may be permissible in some countries. This should be prohibited unless the data subject has explicitly consented, or the personal health data has been anonymised (rendered non-personal) before transfer. Such anonymisation will need to be to the satisfaction of the transferer acting under the requirements of the EU Directive.

Obviously if the original recipient passes personal health data to another party, that party shall be prohibited from using it for direct marketing unless all necessary conditions, including consent, are met to the satisfaction of the EU transferer.

7.4 Overriding law

General or specific laws in a third, non-compliant country may include requirements, in particular circumstances, for the recipient of a data transfer to disclose data to another party e.g. the police, law courts, disease surveillance authority, security services.

These laws may override any agreements or contract provision and it may, in some circumstances, be illegal for the data controller to reveal to the data subject that access has been granted e.g. police investigations. Such laws exist in the EU and the EU Directive recognises this in Article 16 which requires that personal data be processed only "on instructions from the controller, unless he is required to do so by law". The circumstances under which this is permissible is given in Article 13 namely where such legislative measures are necessary to safeguard:

(a) national security;

(b) defence;

(c) public security;

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

Personal health data is sensitive data in a special category and the problem of overriding laws is therefore of particular concern. It will not be sufficient for the transferer and recipient simply to satisfy themselves that data which the recipient may be forced to disclose falls into one of the above categories. Everyone living under the jurisdiction of signatory States to the Council of Europe Convention on Human Rights and Fundamental Freedoms [14] is guaranteed certain rights and freedoms. These rights are backed up by an investigatory Commission on Human Rights and the Court of Human Rights established in Strasbourg. It should be noted that the whole architecture of Data Protection in Europe [4] [5] derives from Article 8.1 of the Convention on Human Rights and Fundamental Freedoms which guarantees that:

"Everyone has the right to respect for his private and family life, his home and his correspondence." Article 8.2 then goes on to make certain specific exceptions to the exercise of this right.

Where personal health data is being sent to an EU Member State from another country, the non-EU transferer will equally wish to be assured that the circumstances whereby such data shall be disclosed in the EU is acceptable.

These are difficult matters which require careful checking prior to an EU transferer notifying his appropriate EU Supervisory Authority of the proposed application (see clause 10).

An understanding of the position in the recipient's country regarding overriding laws will be an important aspect in obtaining informed consent from a data subject. Where legally permissible, data subjects should be informed of such exceptional accesses as soon as practicable after they have occurred.

8 Permissible derogations, Articles 26.1 and 26.2

8.1 Article 26.1

8.1.1 General

Annex B contains the full text of Article 26.1. This lists the conditions under which transfer of personal data is allowed to a third country that does not ensure an adequate level of protection. The conditions include:

- the data subject has given his consent unambiguously to the proposed transfer; or
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

Documents
Document Sharing Hub
Full document details: DIN EN 14485:2004-03

In health terms the transfer of personal health data may well, on occasions, be "necessary in order to protect the vital interests of the data subject", e.g. where an individual falls seriously ill outside the EU.

However in the context of this standard the most significant of the permissible derogations is probably where the data subject has "given his consent unambiguously to the proposed transfer".

8.1.2 Consent

To be permissible consent must be unambiguous and apply to the proposed transfer.

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. 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, and 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 non-compliant country is involved but also what that entails. That will include:

- any possible deficiencies in compliance with the "Content Principles" and "Procedural/Enforcement Mechanisms";
- any means by which such deficiencies will be addressed including any weaknesses in these means such as redress;
- any rights which the non-compliant country has to force the third country recipient to disclose data and any other aspects of overriding laws.

Of obvious relevance to a data subject will be the nature of the personal health data to be transferred and the ease with which the data subject's identity might be accessed or evident. Anonymised personal health data are unlikely to be of concern but the perception of what constitutes "anonymous" needs to be addressed.

The data subject will need to be made aware of the means available to him for exercising his rights and the processes involved in exercising them e.g. in relation to pursuing a complaint, obtaining redress etc.

8.2 Article 26.2

Article 26.2 of the EU Directive see (annex B) provides a derogation whereby personal data can be sent to a third country without adequate data protection if "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". Furthermore such safeguards may in particular result from contractual clauses. Through Article 26.4, the Commission can decide that certain standard contractual clauses offer sufficient guarantees and, should the Commission so decide, EU Member States must abide by that decision. The Commission has published such standard contractual clauses both for controller to controller transfers (annex H) and controller to processor transfers (annex I).

9 Anonymisation

9.1 Definition of personal data

The EU Directive defines personal data as "any information relating to an identified or identifiable natural person ('data subject'). 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".

Documents
Document Sharing Hub
Full document details: DIN EN 14485:2004-03

9.2 Rendering personal data anonymous

A solution to problems of transferring personal health data to non-compliant third countries is to render it 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 which may otherwise have been considered as purely statistical. This may also occur through small numbers e.g. the number of women aged 90 plus in even a large geographic area could be extremely small.

Rendering data non-personal thus requires attention to considerable detail.

Any statistical information concerning health can, given the resources, 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.

10 Notification to Supervisory Authorities

10.1 Introduction

Each EU Member State must create one or more public authorities, known as "Supervisory Authorities", responsible for monitoring applications in their country (Article 28).

An EU data controller must notify his Supervisory Authority before carrying out a processing application (Article 18). Article 18 to 20 lay down the requirements for, and content of, notification and the criteria where checks must be made prior to an application commencing. Notification can in some circumstances be simplified.

The notification arrangements may be simplified or exempted where national law allows the controller to appoint a Data Protection Official to ensure, in an “independent manner”, the internal application of the Data Protection measures and to keep a register of the processing operations. In such circumstances any such Data Protection Official would be closely involved in the development of contracts and/or other arrangements between the controller and any controller in a non-compliant country to which personal health data were to be transmitted.

10.2 Implementation of Articles 18 to 20

The manner in which Articles 18 to 20 has been implemented in EU Member States may vary substantially [15]. Exemptions to notification may be allowed in different circumstances and the areas where simplification of notification is allowed may also vary.

Documents
Document Sharing Hub
Full document details: DIN EN 14485:2004-03

However given that personal health data is particularly sensitive in a special category notification can generally be assumed to be required.

Additionally Article 26.3 requires an EU Member State to inform the Commission and the other Member States of any authorisation which it grants to allow personal data to be transferred to a non-compliant country by virtue of the contractual derogation (Article 26.2). Notification can therefore be expected to be a requirement for international applications involving personal health data.

11 Steps in establishing an international application with adequate data protection safeguards from the view point of an EU data controller

11.1 Introduction

This chapter gives guidance on steps to be taken by an EU data controller seeking to establish an international application with an organisation based in another country (the recipient country) which may involve transfer over a network.

The steps are to establish the means by which transfer of personal data health data to another country would be permitted under the EU Directive. However it should be noted that simply because it is permissible to send personal data to another country, this will not relieve the EU data controller of the responsibilities given in Article 17 namely:

- "that Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

- that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures;

- that the carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

  – the processor shall act only on instructions from the controller;

  – the obligations set out in Article 17.1, as defined by the law of the Member State in

    which the processor is established, shall also be incumbent on the processor.

- that for the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in Article 17.1 shall be in writing or in another equivalent form".

These matters are considered in clause 14.

11.2 Step One: Can the data be non-personal?

There are many applications where data does not need to be personal i.e. identifiable. There are obvious advantages if data can be de-personalised before transmission. For example data need not be personal for creating a World Wide Web shared international educational database of clinical images with diagnostic commentaries and perhaps presenting conditions.

Documents
Document Sharing Hub

Full document details: DIN EN 14485:2004-03