# DIN EN 14485:2004-03 (E)

**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**

## 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

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

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**