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

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

EESTI STANDARDIKESKUS

EESTI STANDARDI EESSÕNA **NATIONAL FOREWORD**

Käesolev Eesti standard EVS-EN 14484:2004 sisaldab Euroopa standardi EN 14484:2003 ingliskeelset teksti. Käesolev dokument on jõustatud 18.05.2004 ja selle kohta on avaldatud teade Eesti standardiorganisatsiooni ametlikus väljaandes. Standard on kättesaadav Eesti standardiorganisatsioonist.	This Estonian standard EVS-EN 14484:2004 consists of the English text of the European standard EN 14484:2003. This document is endorsed on 18.05.2004 with the notification being published in the official publication of the Estonian national standardisation organisation. The standard is available from Estonian standardisation organisation.

Käsitlusala: This 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).	**Scope:** This 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).

ICS 35.240.80

Võtmesõnad: data, data security, data transfer, definition, definitions, english language, european communities, health protection, information exchange, information interchange, languages, medical informatics, medical sciences, medicine, public health

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 14484

December 2003

ICS 35.240.80

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 personelles de santé couvertes par la directive européenne sur la protection des données personelles - 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 **4**

Introduction **5**

1 Scope **9**

2 Normative references **9**

3 Terms and definitions **9**

4 Abbreviated terms **10**

5 The European Data Protection Directive (see annex A) **11**
5.1 General 11
5.2 General aims: (Article 1) 11
5.3 Scope: electronic and non-electronic (Article 3) 11
5.4 Principles relating to data quality (Article 6) 11
5.5 Criteria for legitimacy (Article 7) 11
5.6 Special categories of processing, including personal health data (Article 8) 12
5.7 Information to be given to the data subject (Article 10) 12
5.8 Right of access to data (Article 12) 12
5.9 Right to object (Article 14) 12
5.10 Security of processing (Article 17) 12
5.11 Judicial remedies, liability and sanctions (Articles 22, 23 and 24) 13
5.12 Supervisory Authorities (Articles 28 and 18) 13
5.13 Working party on the protection of Individuals with regard to the Processing of Personal Data 13
5.14 Transfer of personal data to Third Countries 13

6 Requirements for the transfer of personal data to third Countries. **13**
6.1 General 13
6.2 Principles (Article 25) 13
6.3 Ensuring transfers are permissible 14
6.4 Grounds by which transfers to third countries are permissible 14

7 A Security Policy for third countries **16**
7.1 The requirement 16
7.2 The purpose of the security policy 16
7.3 The ‘level’ of the security policy 16

8 High Level Security Policy: general aspects **17**
8.1 Levels of abstraction in ensuring security 17
Generic principles 17
8.3 Non-generic Principles 17
8.4 Guidelines 18
8.5 Measures 18
8.6 Elements of a High Level Security Policy 18

9 High Level Security Policy: the content **18**
9.1 Principle One: overriding generic principle 18
9.2 Principle Two: chief executive support 19
9.3 Principle Three: documentation of Measures and review 19
9.4 Principle Four: Data Protection Security Officer 20
9.5 Principle Five: permission to process 20
9.6 Principle Six: information about processing 21
9.7 Principle Seven: information for the data subject 23
9.8 Principle Eight: prohibition of onward data transfer without consent 23
9.9 Principle Nine: remedies and compensation 24
9.10 Principle Ten: security of processing 25

9.11 Principle Eleven: responsibilities of staff and other contractors 26
9.12 Principle Twelve: adequacy of third country data protection 26
9.13 Principle Thirteen: additional EU Member State particular requirements 27

10 Rationale and Observations on Measures to support Principle Ten concerning security of processing 27
10.1 General 27
10.2 Encryption and digital signatures for transmission to the third country 27
10.3 Access controls and user authentication 27
10.4 Audit Trails 28
10.5 Physical and environmental security 28
10.6 Application management and network management 28
10.7 Viruses 28
10.8 Breaches of security 28
10.9 Business Continuity Plan 28
10.10 Handling particularly sensitive data 28
10.11 Standards 29

11 Personal health data in non-electronic form 29

Annex A (normative) **EU Data Protection Directive 30**

Annex B (informative) **Useful sources of advice 50**
B.1 EU Security projects 50
B.2 CEN/ISSS 50
B.3 Non-CEN Standards 50
B.4 Selected web sites 51

Annex C (informative) **Model declaration 52**

Bibliography 54

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 an 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 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 form 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