INTERNATIONAL STANDARD

ISO 22857

First edition
2004-04-01

Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health information

Informatique de santé — Lignes directrices sur la protection des données pour faciliter les flux d'information sur la santé du personnel de part et d'autre des frontières

Reference number
ISO 22857:2004(E)

© ISO 2004

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

This document is a preview generated by EVS

© ISO 2004

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

 © ISO 2004 – All rights reserved

Contents

Page

This document is a preview generated by EVS

© ISO 2004 – All rights reserved

This document is a preview generated by EVS

 © ISO 2004 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 22857 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

This document is a preview generated by EVS

© ISO 2004 – All rights reserved

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 manipulated 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 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 the boundaries of these purposes and consents.

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

There is a wide range of organisations that might be involved in receipt of personal health data from another country for example

— healthcare establishments such as hospitals;

— pharmaceutical companies involved in research;

— contractors remotely maintaining health care systems in other countries;

— organisations holding educational data bases containing, for example, radiological images with diagnoses and case notes;

This document is a preview generated by EVS

 © ISO 2004 – All rights reserved

— companies holding banks of medical records for patients from different countries;

— organisations involved in international health-related e-commerce such as e-pharmacy.

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 are protected from unauthorised access in storage or transmission;

— the number of persons who have authorised access;

— the nature of the personal health data;

— 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 will normally be necessary to ascertain the required level of security measures.

In addition to the standards bodies ISO, IEC, CEN and CENELEC, there are four major trans-national bodies that have produced internationally authoritative documents relating to security and data protection in the context of trans-border flows

— the Organisation for Economic Co-operation and Development (OECD);

— the Council of Europe;

— the United Nations (UN);

— the European Union (EU).

The primary documents from these bodies are

— OECD “Guidelines on the Protection of Privacy and Trans-border flows of Personal Data” [1];

— OECD “Guidelines for the Security of information Systems” [2];

— Council of Europe “Convention for the Protection of individuals with regard to Automatic Processing of Personal Data” No. 108 [3];

— “Council of Europe Recommendation R(97)5 on the Protection of Medical Data” [4];

— UN General Assembly “Guidelines for the Regulation of Computerised Personal Data Files” [5];

— EU Data Protection Directive on the protection of individuals with regard to the processing of personal data and free movement of that data [6].

Annex A provides a brief summary of the key aspects of these documents.

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 may exist which lay down a duty on medical practitioners to safeguard confidentiality.

This document is a preview generated by EVS

© ISO 2004 – All rights reserved

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.

Annex B comprises a brief outline of the key national standards or other documented requirements and of the legislative position concerning data protection in a range of countries.

Personal health data can be extremely sensitive in nature and thus there is extensive guidance and standards available both nationally and internationally on various administrative and technical 'security measures' for the protection of personal health data (see Annexes C and D).

This International Standard seeks to draw on, and harmonise, data protection requirements relating to the transfer of personal health data across international boundaries as given in authoritative international documents. It also seeks to take into account a range of national requirements so as to avoid, as far as practicable, conflict between the requirements of this International Standard and national specifications.

This International Standard applies, however, solely to transfer of personal health data across national borders. It explicitly does not seek to specify national data protection requirements. The creation of a set of requirements aimed at being acceptable to all countries, whether they be transmitting or receiving personal health data to/from other countries, inevitably means adopting the most stringent of requirements. This means that organisations in some countries would need to apply extra or more severe data protection requirements when transmitting to, or receiving personal health data from, other countries than might be necessary for handling such data within their own boundaries. Although that might be the case, that does not mean that those extra or more severe requirements must be applied to solely national applications.

Articles 25 and 26 of the EU Data Protection Directive lay down the conditions under which transfer of personal data from an EU Member State to a non-EU Member State is permitted. CEN Standards [11] [12] provide guidance on meeting such conditions and on a high level security policy which importers of personal health data from EU Member States should implement. This International Standard seeks to be consistent with both these CEN standards.

This document is a preview generated by EVS

© ISO 2004 – All rights reserved

Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health information

This document is a preview generated by EVS

1 Scope

This International Standard provides guidance on data protection requirements to facilitate the transfer of personal health data across national borders. It does not require the harmonisation of existing national standards, legislation or regulations. It is normative only in respect of international exchange of personal health data. However it may be informative with respect to the protection of health information within national boundaries and provide assistance to national bodies involved in the development and implementation of data protection principles. The International Standard covers both the data protection principles that should apply to international transfers and the security policy which an organisation should adopt to ensure compliance with those principles.

Where a multilateral treaty between a number of countries has been agreed e.g. the EU Data Protection Directive, the terms of that treaty will take precedence.

This International Standard aims to facilitate international health-related applications involving the transfer of personal health data. It seeks to provide the means by which data subjects, such as patients, may be assured that health data relating to them will be adequately protected when sent to, and processed in, another country.

This International 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.

National privacy and data protection requirements vary substantially and can change relatively quickly. Whereas this International Standard in general encompasses the more stringent of international and national requirements it nevertheless comprises a minimum. Some countries may have some more stringent and particular requirements and this should be checked.

2 Normative references

This International Standard does not contain normative references.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply. They seek to be consistent with similar terms in other international documents.

NOTE Throughout the text, the word “he” should be understood to mean “he or she” and the word “his” to mean “his or her”.

3.1
the application
the international application to which this International Standard is being applied unless obviously to the contrary

3.2
Commission
European Commission unless obviously otherwise

© ISO 2004 – All rights reserved