Second edition
2013-12-15

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

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 22857:2013(E)

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

Contents

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 215, *Health informatics*.

This second edition replaces the first edition (IO 22857:2004), which has been technically revised.

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;

— insurance;

— clinical research; and

— population health.

A classification of purposes for processing personal health information is given in ISO/TS 14265 [15].

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); and

— for any purpose, but where identifiable data are not required, the objective should be to prevent such identification of the individual.

In all of these circumstances data about individuals are now, and will increasingly in the future, be transmitted across national/jurisdictional borders or be deliberately made accessible to countries/jurisdictions other than where they are collected or stored. Data may be collected in one country/jurisdiction and stored in another, be manipulated in a third, and be accessible from many countries/jurisdictions 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/jurisdiction 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. The same circumstances may arise when data are passed across jurisdictional boundaries.

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

— healthcare establishments such as hospitals;

— research databanks held in one country but both fed and accessed in others;

— contractors remotely maintaining health care systems in other countries;

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

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

— organisations involved in international or cross-jurisdictional 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 authorized access;

— the nature of the personal health data;

— the level of difficulty in identifying an individual if access to the data are 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 will 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 Organization 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] and jurisdiction to jurisdiction. 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 legislation may not 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, integrity and availability.

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 .

This International Standard seeks to draw on, and harmonize, 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/jurisdictional borders. It explicitly does not seek to specify national or specific jurisdictional data protection requirements. The creation of a set of requirements aimed at being acceptable to all countries/jurisdictions, whether they be transmitting or receiving personal health data to/from other countries/jurisdictions, inevitably means adopting the most stringent of requirements. This means that organisations in some countries/jurisdictions would need to apply extra or more severe data protection requirements when transmitting to, or receiving personal health data from, other countries/jurisdictions 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 internal national/jurisdictional applications.

This International Standard does not specify whether consent should be implicit or explicit or whether or not it should be in writing or equivalent. Neither does it deal with what measures should be taken where the data subject is unable to give meaningful consent for whatever reason. Such matters may be specified in the regulations of the country/jurisdiction of the data exporter or be a matter of custom or culture in that country/jurisdiction. The consideration that ideally applies to these aspects is that consent is given according to the expectations which a data subject would have in giving that consent in the context of any regulations, customs or cultures that apply to the data subject.