INTERNATIONAL STANDARD

ISO 22857

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

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Abbreviated terms **3**

5 Structure of this International Standard **3**

6 General principles and roles **3**
6.1 General principles 3
6.2 Roles 4

7 Legitimising data transfer **4**
7.1 The concept of "adequate" data protection 4
7.2 Conditions for legitimate transfer 5

8 Criteria for ensuring adequate data protection with respect to the transfer of personal health data **6**
8.1 The requirement for adequate data protection 6
8.2 Content principles 6
8.3 Procedural/enforcement mechanisms 9
8.4 Contracts 10
8.5 Overriding laws 11
8.6 Anonymisation 11
8.7 Legitimacy of consent 12

9 Security policy **12**
9.1 General 12
9.2 The purpose of the security policy 12
9.3 The "level" of security policy 13
9.4 High Level Security Policy: general aspects 13

10 High Level Security Policy: the content **14**
10.1 Principle One: overriding generic principle 14
10.2 Principle Two: chief executive support 15
10.3 Principle Three: documentation of measures and review 16
10.4 Principle Four: Data protection security officer 16
10.5 Principle Five: permission to process 17
10.6 Principle Six: information about processing 18
10.7 Principle Seven: information for the data subject 20
10.8 Principle Eight: prohibition of onward data transfer without consent 20
10.9 Principle Nine: remedies and compensation 21
10.10 Principle Ten: security of processing 22
10.11 Principle Eleven: responsibilities of staff and other contractors 23

11 Rationale and observations on measures to support Principle Ten concerning security of processing **24**
11.1 General 24
11.2 Encryption and digital signatures for transmission to the data importer 24
11.3 Access controls and user authentication 24
11.4 Audit trails 25
11.5 Physical and environmental security 25
11.6 Application management and network management 25
11.7 Malicious software 25
11.8 Breaches of security 25
11.9 Business continuity plan 25

11.10 Handling very sensitive data 26
11.11 Standards 26
12 Personal health data in non-electronic form 26
Annex A (informative) **Key primary international documents on data protection 27**
Annex B (informative) **National documented requirements and legal provisions in a range of countries 32**
Annex C (informative) **Exemplar contract clauses: Controller to controller 37**
Annex D (informative) **Exemplar contract clauses: Controller to processor 44**
Annex E (informative) **Handling very sensitive personal health data 53**
Bibliography 55

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 (ISO 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.

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

1 Scope

This International Standard provides guidance on data protection requirements to facilitate the transfer of personal health data across national or jurisdictional borders.

It does not require the harmonization of existing national or jurisdictional standards, legislation or regulations. It is normative only in respect of international or trans-jurisdictional exchange of personal health data. However it can be informative with respect to the protection of health information within national/jurisdictional boundaries and provide assistance to national or jurisdictional bodies involved in the development and implementation of data protection principles.

This International Standard covers both the data protection principles that apply to international or trans-jurisdictional transfers and the security policy which an organization adopts 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 and trans-jurisdictional health-related applications involving the transfer of personal health data. It seeks to provide the means by which health data relating to data subjects, such as patients, will be adequately protected when sent to, and processed in, another country/jurisdiction.

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 can 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/jurisdictions may have some more stringent and particular requirements.

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.

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
application
process involving international/jurisdictional data transfer to which this International Standard is being applied unless obviously to the contrary

3.2
Commission
European Commission unless obviously otherwise

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

3.4
data subject
identified or identifiable natural person, which is the subject of personal data

3.5
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

3.6
EU Directive
EU Data Protection Directive[6] unless stated otherwise

3.7
identifiable person
one 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

3.8
participants
data exporters and data importers

3.9
personal data
any information relating to an identified or identifiable natural person

3.10
personal health data
any personal data relevant to the health of an identified or identifiable natural person

3.11
primary controller
controller who is the data exporter responsible for all matters relating to ensuring consent of the data subject to the transfer of his personal health data to another country/jurisdiction

3.12
processor
natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

3.13
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, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

3.14
data importer
natural or legal person, public authority, agency or any other body located in one country/jurisdiction which receives data from a data exporter in another country/jurisdiction

3.15
data exporter
natural or legal person, public authority, agency or any other body located in one country/jurisdiction which sends data to a data importer in another country/jurisdiction

3.16
data protection security officer
officer appointed by the controller to ensure, in an independent manner, compliance with the HLSP and the measures that support it

Note 1 to entry: The term "data protection security officer" used in this document covers roles such as "data protection officer" and "information security officer" found in specific organizations.

4 Abbreviated terms

The following abbreviated terms are used

EEA	European Economic Area
EU	European Union
HLSP	High Level Security Policy
OECD	Organization for Economic Co-operation and Development
UN	United Nations

5 Structure of this International Standard

This International Standard is structured as follows:

— Clause 6 lists some general principles reflecting those in international documents on this subject and deals with the main roles of data importers and exporters, and data controllers and processors.

— Clause 7 introduces, in general, the two main requirements for a transfer of personal health data to be legitimate in the context of this International Standard and on which the remainder of the International Standard is based; namely consent and adequacy of data protection.

— Clause 8 deals in detail with these two main general requirements, lays down all the criteria for adequacy and takes further the concept of consent.

— Clause 9 requires the data importer to have a high level data protection policy in place and explains what is meant in this International Standard by "high level".

— Clause 10 lays down the detailed requirements for a high level policy which will ensure the criteria for adequacy of data protection are actually ensured.

— Clause 11 provides detailed requirements for those aspects of a data importer's policy which relate to the administrative and technical means for ensuring security of data processing.

— Clause 12 deals with personal health data in non-electronic forms.

6 General principles and roles

6.1 General principles

The general principles are as follows:

— Participants shall protect the fundamental rights and freedoms of natural persons regarding their rights to privacy with respect to the processing of personal health data.

— The responsibilities and accountability of participants shall be explicit and transparent to data subjects.

— Consistent with maintaining security, data subjects shall be able to gain appropriate knowledge of, and be informed about, the existence and general extent of measures, practices and procedures for the security of the application involved in the processing of personal health data relating to them.

— The application and the security of the application shall respect the rights and legitimate interests of all affected parties.

— Security levels, costs, measures, practices and procedures shall be appropriate and proportionate to the value and degree of reliance on the application and the severity, probability and extent of potential harm to a data subject.

— Measures, practices and procedures for the security of an application shall be coordinated and integrated with each other and with other measures, practices and procedures of the participants in the application so as to create a coherent system of security.

— Participants shall act in a timely coordinated manner to prevent and respond to breaches of security regarding the application.

— The security measures relating to the application shall be reassessed periodically.

— The security of the application shall be compatible with the legitimate use and flow of data and information in a democratic society.

6.2 Roles

6.2.1 Data exporters and data importers

An exchange of personal health data across an international or jurisdictional border involves a 'data exporter' responsible for transmitting the data from one country/jurisdiction and a 'data importer' which receives the data in another country/jurisdiction. Each has obligations to the other.

A 'data exporter' shall not transfer data to a 'data importer' unless the 'importer' complies with the relevant parts of this International Standard.

A 'data importer' shall not participate in an application unless the 'data exporter' complies with the relevant parts of this International Standard.

6.2.2 Controllers and processors

A 'data controller' has the responsibility to determine the purpose and means of processing whereas a 'processor' processes the data on behalf of a controller and according to instructions from a controller (see definitions). Each participant in an application shall be designated either as a 'controller' or as a 'processor'.

NOTE Since control of data may be transferred to another jurisdiction the 'data controller" and 'data exporter' may be the same entity as may be the 'data controller' and 'data importer'.

7 Legitimising data transfer

7.1 The concept of "adequate" data protection

This International Standard is based on the concept of ensuring "adequate" data protection in transferring personal health data across national or jurisdictional borders. It is the responsibility of the data exporter to ensure adequacy of data protection implemented by the importer.

While "adequate" protection includes satisfactory administrative and technical security measures for the protection of data, it encompasses other substantial matters.

A data subject will expect that the rights he has come to expect regarding his personal health data will be respected by any importer when such data are transferred to another country/jurisdiction. The extent and nature of the rights which a data subject will have come to expect will depend on the country/jurisdiction in which he resides and its culture. If it is known or suspected that such rights might not be respected by a data importer, the data subject will expect to be fully informed so as to be able to consent or otherwise to a transfer proceeding. On the other hand a data subject will, in some circumstances, expect data to be transferred even where data protection may not be "adequate" in the terms of this International Standard (e.g. where his vital interests are concerned in a health emergency).

Data subjects will expect personal health data to be protected during the process of transfer and for a data importer to have "adequate" safeguards in place when it is received. Those safeguards would include administrative security and technical measures to encompass for example access controls, data integrity, audit trails, data accuracy etc. They will also expect the importing organization to have staff competent and trained in the handling of personal health data. The expectation will be that the data importer will have in place a security policy covering such matters.

Data subjects will additionally expect to know what is happening to their data, to have access to it if necessary and to have the opportunity to address any perceived inaccuracies.

A data subject will expect to have given consent to a transfer and to have been fully informed on matters relevant to that consent.

Finally, data subjects will expect to be able to make a complaint if the terms under which a transfer has taken place seem to have been breached and for such a complaint to be investigated impartially and, if necessary, by an independent body. Where the data subject suffers damage through a breach in conditions they will expect to be able to pursue redress in a defined and fair manner.

This International Standard addresses all these matters under the umbrella of ensuring "adequate" data protection. It details the criteria for ensuring "adequate" data protection (Clause 8) and the content of a high level security policy which a data importer would be expected to implement to ensure that "adequacy" of data protection was in practice ensured (Clauses 9, 10 and 11).

7.2 Conditions for legitimate transfer

7.2.1 Consent as a condition of transfer

Personal health data shall not be transferred unless the data subject has unambiguously given his consent excepting where the transfer is deemed necessary by the controller to protect the vital interest of the data subject, or where permitted by law. This fact should be made known to individuals and citizens in both a general and a specific way.

Principles and data requirements for consent are given in ISO/DTS 17975.[16]

7.2.2 Conditions for transfer

In addition to unambiguous consent, personal health data shall not be transferred to a data importer unless either the importer ensures an adequate level of protection (see Clause 8) or one of the following conditions apply:

a) the data subject has given his consent unambiguously to the proposed transfer in the knowledge of the inadequacies that exist (note that although 7.2.1 requires consent in all circumstances, the requirement here is that such consent must be with the knowledge of the inadequacies that cause the participants to resort to this condition - see also 8.7); or

b) 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

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another party; or

d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

e) the transfer is necessary in order to protect the vital interests of the data subject; or

f) 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; or

g) where the controller adduces sufficient guarantees through appropriate contractual clauses examples of which are given in Annexes C and D.

NOTE Subclause 8.4 makes it a requirement that in all cases "the application shall be governed by a contract between the participants" but is essentially silent on the form that such a contract should take. However where (g) above applies, particular attention needs to be paid to the contract to ensure it covers any inadequacies in data protection which would otherwise apply such as in matters of redress, investigation of complaints etc. It is for this reason that the examples in Annexes C and D are given.

8 Criteria for ensuring adequate data protection with respect to the transfer of personal health data

8.1 The requirement for adequate data protection

A controller shall not transfer personal health data to a data importer unless the importer provides adequate data protection. There are two essential elements of adequacy.

— **Content principles:** The adequacy of the data protection provisions in the processing of the personal health data by the data importer and the obligations placed on those responsible for them.

— **Procedural/enforcement requirements:** The means for ensuring that such provisions are followed in practice and for ensuring the rights of data subjects.

8.2 Content principles

8.2.1 General

The content principles are given in 8.2.2 to 8.2.7.

8.2.2 The purpose limitation, data quality and proportionality principle

In the context of the application and subject to the allowable exemptions given in 8.2.8, personal health data shall be

a) processed fairly and lawfully;

b) transferred for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purposes for which they are transferred and/or further processed;

d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were transferred or for which they are further processed, are erased or rectified;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were transferred or for which they are further processed. Participants may agree to personal health data being stored for longer periods for historical, statistical or

scientific use provided such use does not impact on the data subject. However the data subject shall be informed of any such agreement.

8.2.3 The transparency principle

In the context of the application and subject to the exemptions in 8.2.8 the data subject shall be provided with the following information:

a) the identity of the data exporter and the data importer and of his representative, if any;

b) the purposes of the processing for which the data are to be transferred;

c) the existence of the rights of access to, and the right to rectify, any data in the application which relates to him;

d) liabilities, remedies and sanctions in respect to any breaches of his rights;

e) the retention period of the data particularly relating to medico-legal requirements and any policy regarding the death of a data subject;

f) any matter which may affect his giving of consent to the transfer;

g) any other information which this International Standard specifies.

8.2.4 The rights of access, rectification and opposition principle

In the context of the application, and subject to the exemptions in 8.2.8, the data subject shall have the following rights:

a) to obtain without constraint at reasonable intervals and without excessive delay or expense, as specified or determined by the applicable (possibly legal) authority

– confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the data importers or categories of data importer to whom the data are disclosed,

– communication to him in an intelligible form of the data undergoing processing and of any available information as to their source;

b) as appropriate to have rights to rectification, erasure or blocking of data the processing of which does not comply with the provisions of this International Standard, in particular because of the incomplete or inaccurate nature of the data;

c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort;

d) to object at any time on grounds relating to his particular situation to the processing of data relating to him. Where there is a justified objection, the processing instigated by the controller shall no longer involve those data.

8.2.5 Restrictions on onward transfer principle

Further transfers of the personal health data by the importer of the original data transfer shall not be permitted unless the second data importer (i.e. the importer of the onward transfer) also affords adequate protection in accordance with 7.2 and other relevant requirements of this International Standard.