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 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

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*.

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;

— 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.

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.

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

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

3.3
controller
the 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
the 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
the 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
the 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

3.12
processor
a 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, organisation, 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
a natural or legal person, public authority, agency or any other body located in one country which receives data from a data exporter in another country

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

4 Abbreviated terms

The following abbreviated terms are used

— EEA European Economic Area;

— EU European Union;

— HLSP High Level Security Policy;

— OECD Organisation 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 assured.

— 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

— 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 co-ordinated 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 co-ordinated 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 border involves a 'data exporter' responsible for transmitting the data from one country and a 'data importer' which receives the data in another country. 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 authority 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'.

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 borders.

Whilst “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 is transferred to another country. The extent and nature of the rights which a data subject will have come to expect will depend on the country 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 organisation 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 assured (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 necessary to protect the vital interest of the data subject.

7.2.2 Conditions for transfer

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 sub-clause 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 a third 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 E and F.

NOTE Sub-clause 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 E and F 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

The content principles are given in sub-clauses 8.2.1 to 8.2.6.

8.2.1 The purpose limitation, data quality and proportionality principle

In the context of the application and subject to the allowable exemptions given in sub-clause 8.2.7, 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 should be informed of any such agreement.

8.2.2 The transparency principle

In the context of the application and subject to the exemptions in sub-clause 8.2.7 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 is 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.

8.2.3 The rights of access, rectification and opposition principle

In the context of the application, and subject to the exemptions in sub-clause 8.2.7, the data subject shall have the following rights:

a) to obtain without constraint at reasonable intervals and without excessive delay or expense

- 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.

8.2.4 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 sub-clause 7.2 and other relevant requirements of this International Standard.

8.2.5 The security principle

Technical and organisational security measures shall be taken by the data importer that are appropriate to the risks presented by the processing.

8.2.6 Additional principles applying to specific circumstances

Direct marketing: The data subject shall have the right to object, on request and free of charge, to the processing of personal data relating to him which the participants anticipate being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses. Data subjects shall be informed of this right.

Death of the data subject: The way in which the confidentiality of personal health data is handled after the death of a data subject varies in national legislation e.g. the UK Data Protection Act applies only to living persons. However there are many circumstances where the health records of a dead individual could reveal personal health data relevant to some other individual and be of detriment to them. The records may refer explicitly to other individuals e.g. a member of the dead person's family. If an individual dies of a condition deriving from an inheritable genetic deficiency, his records may reveal matters relevant to his offspring.

Participants in the application shall come to an explicit agreement about what to do in circumstances of death. That agreement may depend on the countries involved and how they treat health records e.g. any laws or rules which may apply to the length of time health records must be retained after death. Different property rights may also apply e.g. if a patient is the legal owner of his records then after death such records may be a part oh his estate and subject to probate. Since a patient's permission to allow his personal health data to be processed and passed to a third party may depend on what would happen to such data should he die, patients shall be informed of any arrangements made concerning the handling of such data after his death.

8.2.7 Exemptions to content principles

Participants may agree exemptions to content principles 8.2.1, 8.2.2, 8.2.3 (a), (b) and (c), where the exemption constitutes a necessary measure to safeguard

a) national security;

b) defence;

c) public security;

d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

e) an important economic or financial interest of a participant's country, including monetary, budgetary and taxation matters;

f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

g) the protection of the data subject or of the rights and freedoms of others.

Where participants agree to any exemption the data subject shall be informed as part of the giving of his consent unless so doing is contrary to the law applying to the data exporter.

8.3 Procedural/enforcement mechanisms

8.3.1 General

Even if the "content principles" are built into the rules for processing, storage, transfer etc of personal health data, the rights of individuals will not be assured unless the rules are followed and, if not, individuals have an effective form of redress.

Whereas a number of international and national documents, for example from the OECD [1] [2] the Council of Europe [3] [4] and the UN [5], agree upon the essence of the requirements concerning the rights of individuals, the means for ensuring their effectiveness varies substantially.

Some countries ensure that the means for ensuring effectiveness are embedded in law through Data Protection/Privacy Commissioners or equivalent with monitoring and complaint investigative functions, and legal provisions such as liability, sanctions and remedies. An example is the EU Member States.

Many national and international guides and rules, whilst they may exhort similar rights for individuals

— may not be so comprehensive;

— may not require enshrinement in law;

— may not cover all health sectors e.g. may cover only the public sector.

Thus to judge adequacy of data protection provided by a data importer requires assessment of the judicial and other mechanisms in place. Such an assessment shall achieve the following objectives:

— To deliver a good level of compliance with the rules (no system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important part in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

— To provide support and help to individual data subjects in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

— To provide appropriate redress to the injured party where rules are not complied with. This is a key element, which must involve a system of independent adjudication, or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

8.3.2 Ensuring compliance with the rules

A means for ensuring compliance with the rules is for a controller transferring the data to require the importer to have a clear security policy for the handling of transferred personal health data which encompasses

— the organisational and technical security measures necessary to ensure adequacy of data protection as required by this International Standard;

— measures to ensure compliance with the policy including the penalties or sanctions which can be applied in the case of a breach.

Clauses 10, 11 and 12 specify the requirements of such a policy.

8.3.3 Providing redress

A data subject shall be able to obtain appropriate redress for damage caused to him as a result of any act incompatible with the requirements of this International Standard.

This may best be achieved through a contractual approach three examples of which are given below [8].

Approach one is for the data exporter to restrict the data importer to being simply a sub-contracted processor who, as a result, would have no autonomous decision-making powers. The data exporter, as data controller, would specify in detail what the processor is to do and only do. The data exporter therefore remains totally responsible for the data transferred and may thereby be automatically liable under his national laws for any

damage resulting from a breach no matter where undertaken. The data subject thereby may have no lesser rights to redress them than if the breach occurred within his own country. However circumstances will frequently occur e.g. in sharing electronic patient records in telemedicine, where the importer is not solely providing data processing services. It may often be necessary for the data importer to have freedoms to process data as he sees fit and thereby effectively become a controller in his own right. In this case further safeguards will be required.

Approach two is for the data exporter to enter into a separate contract with the data subject stipulating that the data exporter will remain liable for any damage caused by actions of the data importer. Such a contract could, for example, be made at the time data was obtained from the data subject and the issue of the transfer should be addressed then.

In both of these two approaches it would be for the data exporter to pursue the data importer for breach of contract if he sought to recover any damages paid to a data subject.

The third approach depends on the legal system applying to contracts in the country in question. Some legal systems allow third parties (i.e. those not party to the contract) to claim rights under the contract. This could, with an open published contract between data exporter and data importer, provide satisfactory subject rights.

A data subject shall be informed of his rights of redress as part of his giving consent to the transfer.

8.3.4 Support and help to data subjects

A data subject shall have the right to instigate an objective investigation of a complaint regarding a breach of his rights which shall include, where a complaint cannot otherwise be resolved, investigation and/or arbitration by an independent, competent body.

As an example a number of countries have legally constituted bodies which are empowered to monitor compliance with data protection law and to investigate complaints e.g. Data Protection Commissioners. If a data subject in one country is able legally to instigate an investigation by such a body in the importer's country, then this could comprise the means for meeting the requirement for independent investigation.

An equivalent institutional mechanism may be achieved through a contractual condition under which the data importer would permit the Data Protection Commissioner (or equivalent) in the data subject's country to investigate a complaint (if necessary through an agent in the importer's country).

An alternative could be a contract between the data subject and the data exporter under which investigative mechanisms are agreed which the data subject can legally invoke.

A data subject shall be informed as to his rights to have a complaint investigated.

8.4 Contracts

The carrying out of processing in the application shall be governed by a contract between the participants, even where the data importer is solely a processor.

The extent and content of the contract will depend on the extent to which the data importer needs to demonstrate adequacy of data protection in the wide sense of this International Standard.

Where the data importer is solely a processor the contract may primarily be devoted to binding the processor to the controller/exporter and to ensuring that the processor acts only on instructions from the controller. Where the data importer is a controller the extent of his responsibilities will be greater and thereby the more the contract will need to address the assurances that the importer gives to the exporter.

8.5 Overriding laws

General or specific laws in a country may include requirements, in particular circumstances, for the importer of data to disclose data to another party e.g. the police, law courts, security services. These laws may override

any contract provision and it may, in some circumstances, be illegal for the data controller to reveal to the data subject that data access has been granted e.g. police investigations. The circumstances under which such restrictions in rights may occur are illustrated by sub-clause 8.2.7.

Data subjects shall be informed of the possible consequences of any such overriding laws or national practices at least to the extent of a listing such as that in sub-clause 8.2.7. Where there are doubts these shall be revealed. Where legally permissible, the data subject should be informed of such exceptional accesses as soon as practicable after they have occurred.

8.6 Anonymisation

8.6.1 General

A solution to problems of transferring personal health data across national borders can be to render it non-personal. Rendering data non-personal shall be achieved in the context of the definition of personal data as given in this International Standard.

8.6.2 Rendering data non-personal

This International Standard defines personal data as “any information relating to an identified or identifiable natural person”. An identifiable person is “one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

Rendering data non-personal is often referred to as anonymisation. However the perception of anonymisation varies. In the context of this International Standard “anonymisation” therefore means rendering data 'non-personal' in the context of this International Standard’s definition of “personal data”. An “identifiable person” includes one who can be identified “indirectly” by reference to “one or more of the factors specific to him”. Clearly such factors comprise more than name and address. A data subject may for example be identifiable by a combination of any one or more of age; sex; race; occupation; postal/zip code; income group; physiological or mental state; family characteristics etc. Additionally in the context of some health applications, images e.g. photographs, dental records, radiographs or traces such as EEGs may have details which, taken alone or together with other data such as specialty and/or identity of health organisation, would render the data as person-identifiable and thereby as personal data.

Such combinations of data elements may render as personal, data that may otherwise have been considered as purely statistical. Postal/Zip codes provide a very effective way of locating an individual within a small group. Similarly this may also occur through small numbers e.g. the number of women having triplets could be extremely small even in a large geographic area.

Rendering data non-personal thus requires attention to considerable detail. The database inference problem is always theoretically soluble given sufficient resources and access to other relevant information. However, adequate anonymisation can frequently be achieved by withholding obviously identifying information and ensuring that the data importer does not seek to re-identify individuals or to disclose the anonymised information wider than is necessary for the purposes for which it has been agreed that it can be used.

Correspondingly, statistical information concerning health can often, given the resources and reference to other data bases which may be in the public domain, reveal the identity of an individual. Clearly criteria based on the concept of excessive effort in relation to the necessary security and sensitivity of the data need to be applied to such statistics (see fifth bullet of sub-clause 6.1).

Any assurance given to a data subject concerning the rendering of data as non-personal shall address the matter of risk of identity being revealed in relation to the level of effort required to do so. The extent and cost of such resources will vary with time as technology advances.

8.7 Legitimacy of Consent

Clauses 7.2.1 and 7.2.2 refer to “unambiguous consent”.

"Consent" needs to be "freely given, specific and informed" (see definitions). "Unambiguous consent" must therefore be on the basis of knowledge of any matters which may be relevant particularly if these matters might weaken the rights that would have been obtained had consent not been given. Thus the data subject will need to know not only that a transfer of personal health data to another country is involved but also what that entails. It should be noted that consent for one purpose is not consent for another.

When seeking unambiguous consent the data subject shall be provided with information specified in this International Standard and any other information which might affect his decision.

NOTE 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 national regulations of the country of the data exporter or be a matter of custom or culture in that country. The consideration that should apply to these aspects is that consent should be 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.

9 Security policy

9.1 General

A data controller transferring personal health data to another country will need to be assured that the data importer has in place the necessary organisational and technical security measures adequately to protect the transferred data i.e. an adequate security policy where security includes confidentiality, integrity and availability. The sub-clauses below give the requirements relating to protecting transferred data: full details of security management generally are given in ISO 17799 (see Annex C).

A data importer who is a controller shall have in place a security policy which

— ensures that the terms of the contract (sub-clause 8.4) between the exporting controller and the data importer are met;

— complies with all sub-clauses of clauses 9, 10, 11 and 12 of this International Standard.

A data importer who is solely a processor shall have in place a security policy which

— ensures that the terms of the contract (sub-clause 8.4) between him and the data exporting controller are met;

— complies with all sub-clauses of clauses 9, 10, 11 and 12 of this International Standard.

9.2 The purpose of the security policy

The purposes of the security policy for data importers is

— to provide assurance to the data controller exporting the data;

— and to provide assurance for data subjects that the provisions of this International Standard will be met by a data importer.

9.3 The "level" of security policy

This International Standard provides guidance on a High Level Security Policy (HLSP) for data importers. Sub-clause 9.4.6 describes what is meant by "High Level".

9.4 High Level Security Policy: general aspects

9.4.1 Levels of abstraction in ensuring security

Security can be viewed on four distinct levels [9]. These are illustrated below in Figure 1. This International Standard is concerned with high level policy. The figure and the following clauses explain what is included in the meaning of 'high level'.

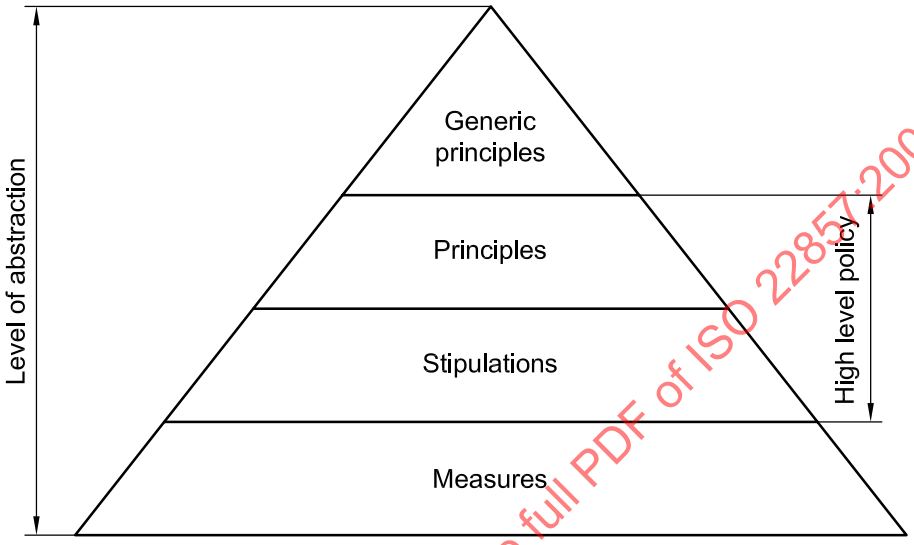


Figure 1 — Levels of abstraction

9.4.2 Generic principles

“Generic Principles” derive from the culture of the society that provides the environment which drives perceptions about human rights and privacy. How such rights are perceived vary across the globe. For example the EU Data Protection Directive [6] derives from a west-European democratic culture specifically those of the EU member States. It thereby derives from an environment that is encompassed by the European Convention on the Protection of Human Rights and Fundamental Freedoms [10]. The latter applies not just to the EU or only to Europe. Other regions of the world may have other overarching conventions or equivalent.

The importance of this is demonstrated by matters such as ‘overriding laws’. The EU Data Protection Directive as an example permits EU Member States to restrict the scope of the obligations and rights provided in the Directive in circumstances such as where it is necessary to safeguard such matters as national or public security; defence; investigation of criminal offences; an important economic or financial interest of a Member State (see sub-clause 8.2.7). Other countries may also have legal provisions of a similar type that might override any organisational rules on data protection. Such overriding laws may be different and/or more extensive than in the exporter's country and may be based on a different view of human rights. These matters will have to be accounted for in obtaining consent to transfers and need to be recognised in an organisation’s security policy.

9.4.3 Non-generic principles

Non-generic ‘principles’ result when generic principles are considered in a specific national or local administrative environment. For example they will be specific to an organisation but be influenced by the generic principles, i.e. influenced by the culture or legislation of the country in which the organisation is located.

9.4.4 Stipulations

'Stipulations' derive from the 'principles' and are the specific operational steps that should be followed in order to fulfil a specific principle. They point out what must be done to fulfil a principle but not how it must be done.

9.4.5 Measures

'Measures' result when stipulations are considered in a specific environment. They specify in detail what must be done to fulfil a stipulation.

9.4.6 Elements of a High Level Security Policy

A High Level Security Policy shall comprise the two middle layers of abstraction namely principles and stipulations.

An HLSP shall therefore be based on 'Generic Principles' and be complemented by specific 'Measures' within a particular organisation.

This International Standard concerns guidance on an HLSP and therefore does not deal with Measures which are very much more organisation dependent. However an indication as to Measures which should back-up stipulations is given.

10 High Level Security Policy: the content

10.1 Principle One: overriding generic principle

The High Level Security Policy (HLSP) shall make clear, as an overriding generic principle, that the personal health data to which the HLSP applies derives from a country other than the importer's and that the data subjects expect their rights to be safeguarded to the extent they experience in their own country.

10.1.1 Principle One, Stipulation One: fundamental rights and freedoms

The data importer shall determine from the data controller what statement he wishes to have included in the HLSP regarding the data subject's overriding fundamental rights and freedoms. That statement shall be included in the HLSP. As an example, where the exporter is in an EU country, reference would be made to the European Convention on the Protection of Human Rights and Freedoms [10] and the EU Directive on Data Protection [6].

The aim of the HLSP shall be to safeguard these rights as prescribed by the exporter.

10.1.2 Principle One, Stipulation Two: information about doubts

Where there are any doubts that such fundamental rights can be guaranteed, these shall be made known so that data subjects can be fully informed and give consent or otherwise.

10.1.3 Rationale

Not all nations subscribe to a declaration of human rights and freedoms and as such there may be overriding laws or practices in the importer's country which are inconsistent with that expected by the data subject. An example might be the right for public authorities to access patient records in circumstances that would be unacceptable to the data subject. Where this is known, or suspected, the data subject has the right to know and decide what to do as a consequence.

10.1.4 Observations as to Measures

A short statement on the data subject's overriding expectations regarding rights and freedoms shall be given. As an example, in the case of EU data subjects, a short summary of the substance of the EU Directive should be available for staff awareness.

10.2 Principle Two: chief executive support

The HLSP shall be endorsed by the chief executive of the organisation and shall be available on request and free of charge to any data subject or other legitimate enquirer.

10.2.1 Principle Two, Stipulation One: alignment with local practice

The HLSP shall, as far as practical, be expressed in a manner consistent with the general data protection policy of the data importer's organisation. Where this is not so, this shall be explicitly recognised.

10.2.2 Principle Two, Stipulation Two: organisational arrangements

The importing organisation shall establish an appropriate organisational structure to support the HLSP.

10.2.3 Principle Two, Stipulation Three: regular HLSP review

The HLSP shall be reviewed at regular intervals that shall not exceed two years.

10.2.4 Rationale

A policy which does not have the backing of the chief executive is less likely to ensure compliance by staff and less likely to command respect from data subjects. Policies and measures which depart significantly from the general practice of an establishment are more likely to encounter non-compliance.

10.2.5 Observations as to Measures

Endorsement simply by virtue of the chief executive's signature is weak: a personally written preface is preferable and his personal observation of its requirements is essential.

Additional endorsement by senior clinical staff such as the chief medical officer is desirable: this can be achieved in association with Measures.

10.3 Principle Three: documentation of Measures and review

The HLSP shall be backed by documented Measures to ensure compliance with the principles and stipulations and these shall be reviewed at regular intervals which shall not exceed one year.

10.3.1 Principle Three, Stipulation One: staff information

The Measures shall be structured so as to be applicable to the staff who receive them.

10.3.2 Rationale

Staff need to know exactly what to do and what not to do. Measures should be tailored to suit the staff who are expected to implement them e.g. measures applicable to clinical staff may not be relevant to administrative staff. Most staff do not need to know the exact details of most technical security Measures.

10.3.3 Observations as to Measures

The documented Measures may usefully take the form of codes of practice.

10.4 Principle Four: Data Protection Security Officer

A Data Protection Security Officer shall be appointed to ensure, in an independent manner, compliance with the HLSP and the Measures that support it.

10.4.1 Principle Four, Stipulation One: Data Protection Security Officer and data importer as a processor

Where the data importer is solely a processor of personal health information, the Data Protection Security Officer shall ensure that no processing of data is undertaken other than as specified by the controller transferring the data and in accordance with the contract that must govern that specification.

10.4.2 Principle Four, Stipulation Two: Data Protection Security Officer and data importer as a controller

Where the data importer is a controller in his own right, the boundaries to be respected in the processing of the personal health data shall be specified and agreed with the primary controller exporting the data. The Data Protection Security Officer shall ensure compliance with these.

10.4.3 Principle Four, Stipulation Three: Data Protection Security Officer qualification for office

The Data Protection Security Officer shall have the necessary skills and experience in safeguarding personal health data to undertake his duties and shall have the necessary authority delegated by the chief executive or person with similar authority.

10.4.4 Rationale

Often an importing organisation processing personal health data will need itself to determine the necessary purpose and means of processing. For example, in telemedicine/teleconsulting the importing clinical professional will require maximum discretion in consulting with other professionals and for keeping results in an appropriate electronic or paper patient record accessible to other authorised persons. This will normally require the professional or the organisation to act as a controller rather than solely as a processor.

The Data Protection Security Officer requires authority derived from top management. Preferably that should be the chief executive but others such as the chief medical officer may be satisfactory.

10.4.5 Observations on Measures

The Data Protection Security Officer shall have clear terms of reference and his authority to audit and investigate compliance shall be made clear in Measures.

10.5 Principle Five: permission to process

Except as allowed in sub-clause 7.2.1 no processing shall be undertaken without assurance that the data subject has appropriately consented (see sub-clause 7.2.1 and 7.2.2 (a)) and only in compliance with such consent.

10.5.1 Principle Five, Stipulation One: unambiguous consent to transfer

Appropriate assurance shall be sought and obtained e.g. from the primary controller exporting the data that the data subject has as appropriate given “unambiguous” consent for the transfer of personal health data to the importer’s country and for the processing of personal health data about him.

10.5.2 Principle Five, Stipulation Two: limitation to the purposes consented

Processing of personal health data shall be limited to the purposes for which consent has been given. Such purposes shall be documented.

10.5.3 Principle Five, Stipulation Three: conditional consents

If any data subject makes consent conditional and those conditions are accepted by the data importer, the conditions of consent shall be appropriately associated with the individual's personal health data and Measures taken to ensure compliance.

10.5.4 Principle Five, Stipulation Four: review of information concerning consent

Information provided to data subjects as part of the process of obtaining informed consent shall be made known in relevant Measures. Such information shall be reviewed at regular intervals not exceeding one year to ensure that the information remains correct and that no other information should be added.

10.5.5 Rationale

Data subjects must give unambiguous consent to transfer of personal health data about them except when transfers are in the vital interests of the data subject such as health emergencies.

Consent must be informed. Thus data subjects will need to be provided with all relevant information if consent is to be valid and much of that information will need to be provided by the data importer. Any information provided for this purpose shall be documented and kept up to date. Information will include, where applicable, such matters as

— overriding laws or practices which allow external authorities to have access to the data such as law enforcement or security services, external clinical audit or investigations;

— absence of ethical professional codes with relevance to privacy;

— measures taken to ensure adequacy of data protection in circumstances where data protection is inadequate in the context of this International Standard.

Where the data importer is unclear about such matters, for example overriding laws and practices, that fact shall be made known.

10.5.6 Observations regarding Measures

If any conditions surround consent they must be reflected in relevant Measures. Measures must ensure processing is limited to the purposes for which consent has been given.

10.6 Principle Six: information about processing

Data subjects' rights to information about processing, to safeguards concerning data quality, to access their data and to object to processing shall be assured in accord with this International Standard.

10.6.1 Principle Six, Stipulation One: documentation about consented processing

The purposes for which the data subject has consented to the processing of his personal health data shall be explicit and documented and no processing which is incompatible with those purposes shall take place.

10.6.2 Principle Six, Stipulation Two: quality of data collected and processed

Personal health data which are collected and processed shall be adequate, relevant and not excessive in relation to a data subject's agreed purposes.

10.6.3 Principle Six, Stipulation Three: accuracy of data processed

Steps shall be taken to ensure that personal health data are collected and recorded accurately and kept up to date where necessary.

10.6.4 Principle Six, Stipulation Four: Data Retention and Destruction Policy

There shall be an organisation Data Retention and Destruction Policy which is communicated to data subjects and is compatible with their consented purposes including that personal health data shall be kept for processing for no longer than is necessary for a data subject's agreed purposes.

10.6.5 Principle Six, Stipulation Five: data subjects' access to their data

Arrangements shall be made to recognise requests from data subjects for access to their data and to ensure that they can be complied with within any legal time-scales and without excessive expense.

10.6.6 Principle Six, Stipulation Six: objection to processing

A data subject shall have the right to object to the processing of data about him and, where that objection is justified, further processing of that data shall cease if the data subject so requests.

10.6.7 Principle Six, Stipulation Seven: rectification, erasure and blocking

Where a data subject believes that his data are inaccurate or incomplete, or where the provisions of this International Standard and/or any undertaking given by the data importer are not being complied with, he shall be allowed to have his personal data rectified, erased or blocked.

Where there is a difference of opinion in respect of the personal data that cannot be resolved objectively, the data subject's view of those data shall be recorded and processed alongside his other personal data.

10.6.8 Principle Six, Stipulation Eight: identification of transferred data

All personal health data transferred to the importer shall be identified as such.

10.6.9 Principle Six, Stipulation Nine: action on notification of the death of a data subject

On being notified of the death of a data subject, the agreement required by clause 8.2.6 shall be enacted.

10.6.10 Principle Six, Stipulation Ten: direct marketing

Personal health data shall not be used for direct marketing without the explicit consent of the data subject.

10.6.11 Principle Six, Stipulation Eleven: re-personalisation of de-personalised data

If personal health data is transferred to the importer on the basis of it being non-personal health data (anonymous data: see sub-clause 8.6), Measures shall be adopted to ensure that identity is not accidentally or deliberately revealed by any processing, including association with other data bases. Where appropriate a 'small numbers' policy shall be formulated.

10.6.12 Rationale

The purposes for which a data subject has given consent must be documented so as to be available to any relevant staff and to ensure that it is not used for any other purpose. In healthcare establishments such as hospitals, personal health data may routinely be used for audit, statistics, financial and statistical returns to national or regional authorities, to third parties for reimbursement, to public health authorities for disease surveillance. None of these may be applicable to the purposes for which the data was transferred and, unless agreed otherwise by a data subject, Measures need to be in place to prevent it being unwittingly used for these purposes.

Staff cannot be expected to comply with the HLSP and Measures supporting it unless they know that the data being used is subject to special constraints – hence the need for it to be identifiable as such.

The requirement that personal health data be retained no longer than necessary for the purposes agreed by the data subject, could cause problems. Importing countries may have requirements to retain health records for a minimum period of time. The data importer may wish to retain records containing personal health data for a substantial time for statistics, audit and in case of legal challenge or complaint. If this is so, then the data subject's consent to these purposes shall be obtained.

Difficulties of the same nature may arise in erasing data if a data subject dies unless agreement to do otherwise is obtained in advance: hence the need for an explicit Data Retention and Destruction Policy.

A data subject's rights to information on data being processed concerning him will cause difficulties unless a process has been created in advance. In a hospital, for example, data about a person may be held in a number of departmental systems and notes making tracing difficult unless the hospital has a comprehensive electronic patient record system.

Similarly a request to erase data may not be executable because of medicolegal requirements to hold all data for audit and investigation of complaints. The data subject should be informed of this when giving consent. An appropriate way to proceed may be to archive the data and block any further processing except for controlled access for essential medicolegal purposes.

10.6.13 Observations on Measures

Measures will need to include a process for handling subject access requests promptly and for the procedures to be followed in the event of death of a data subject.

Measures to deal with the safeguarding of 'non-personal' data will depend on the risk. Appropriate techniques exist for handling the small numbers 'inference' problem [ref. 9 vol.2 pp 272-277].

10.7 Principle Seven: information for the data subject

The data subject shall be informed of the identity of the data importer, the purposes of the processing; any other party to which his personal health data may, or will be, transferred; his rights to object to processing; the complaints procedure; third party arbitration and investigation arrangements; rights to redress and how to pursue them; any information which may affect a data subject's consent which might not otherwise be obvious to him. Information provided shall be documented and stored.

10.7.1 Rationale

Whereas the passing of this information to data subjects may be the responsibility of the controller transferring the data, much of it derives from the data importer. In particular it should be noted that a data subject needs to be provided with all the information that might affect his consent to transfer of data. It is incumbent therefore on the data importer to think through all the circumstances that may affect a data subject's privacy and fundamental freedoms in any way that a data subject would not expect.

Categories of importers of personal health data could include persons other than clinicians and health professionals e.g. finance administration for billing or clerical data input staff.

10.7.2 Observations on Measures

Measure shall include review of the information provided at regular intervals that shall not exceed one year.

10.8 Principle Eight: prohibition of onward data transfer without consent

Transfer of personal health data from the data importer to another party shall not take place without the consent of the controller transferring the data and the data subject's consent unless it is necessary in order to protect the vital interests of the data subject or another person where, and only for so long as, the data subject cannot physically or legally consent. Any other party in receipt of such data, except where it is solely for the purposes of transmission, shall provide adequate data protection.

10.8.1 Principle Eight, Stipulation One: assuring protection for onward transfers

The adequacy of data protection afforded by the 'other' party shall be judged in the context of this International Standard.

10.8.2 Principle Eight, Stipulation Two: HLSP for onward transfers

The 'other' party shall comply with or implement an HLSP that complies with this International Standard.

10.8.3 Principle Eight, Stipulation Three: Disclosure Register

A Disclosure Register of transfers to other parties shall be held and maintained.

10.8.4 Rationale

If personal health data is passed to another party, the data subject will expect no less data protection to apply.

It may often arise that a clinician may wish to seek the views of a colleague in another institution. If such further consulting with a particular colleague/institution is a regular feature of the processing then the 'other' institution should implement an HSLP in full. However if the arrangement is occasional and limited to just one or two healthcare professionals lesser, but still formal, arrangements should suffice.

In any circumstance the data subject's consent will be required. However it will not always be possible to predict what other health professionals in 'other' institutions will need to be consulted. In these circumstances the data subject's consent may be sought for a category of persons which could be other clinicians in another institution if that is necessary to meet the purposes of processing to which the data subject has consented. This shall not be abused and any risks to privacy shall be revealed.

If the 'other' party is, or is likely to be, in a country other than the importer's, then many more and complex considerations will apply. The adequacy of data protection established at the outset for the data importer may not apply. This may also be the case if the data are to be transferred from one state in a country to another state with, for example, different data protection laws.

10.8.5 Observations on Measures

Measures shall include the procedures to be followed if personal health data are to be transferred to another party.

10.9 Principle Nine: remedies and compensation

A data subject shall have the right to judicial or other equivalent remedy for any breach of his rights and to compensation for any damage resulting.

10.9.1 Principle Nine, Stipulation One: investigation of complaints

There shall be mechanisms open to data subjects for investigation of complaints independent of the data importer.

10.9.2 Principle Nine, Stipulation Two: independent arbitration

There shall be mechanisms open to data subjects for independent arbitration in the case of unresolved disputes.

10.9.3 Rationale

These mechanisms will need to be in place as part of establishing adequacy of data protection. They may be complex but shall be documented and made available to data subjects in a form and language which will enable the data subjects to understand how, and in what circumstances, they can be initiated.

The documented mechanisms shall include any implications or limitations that may arise if personal health data is transferred to another party who then causes breach of rights such as a consultation with another health professional in another institution.

10.9.4 Observations on Measures

Measures associated with this principle will often require legal input.

10.10 Principle Ten: security of processing

Personal health data shall be protected against accidental or unlawful destruction or accidental loss, alteration, and unauthorised disclosure or access, and against all unlawful forms of processing.

10.10.1 Principle Ten, Stipulation One: risk analysis

Security Measures shall be appropriate to an assessment of the risks.

10.10.2 Principle Ten, Stipulation Two: encryption during transmission

Personal health data transmitted between the data exporter and the data importer shall be encrypted.

10.10.3 Principle Ten, Stipulation Three: proof of data integrity and authentication of origin

Personal health data transmitted between the data exporter and the data importer shall be subject to security services guaranteeing data integrity and authentication of origin.

10.10.4 Principle Ten, Stipulation Four: access control and user authentication

There shall be effective access controls for the processing of personal data and users of systems shall be adequately authenticated.

10.10.5 Principle Ten, Stipulation Five: Physical and Environmental Security

Subject to the requirements of the delivery of effective healthcare, effective physical and environmental security measures shall be taken.

10.10.6 Principle Ten, Stipulation Six: application management

All applications processing transferred personal health data shall be managed by someone knowledgeable and competent in respect of that application.

10.10.7 Principle Ten, Stipulation Seven: network management

All networks under the direct control of the importer and processing transferred personal health data shall be managed by someone knowledgeable and competent in respect of that network.

10.10.8 Principle Ten, Stipulation Eight: virus controls

Effective virus controls shall be installed to prevent malicious software from compromising the integrity of transferred personal health data or of systems handling them.

10.10.9 Principle Ten, Stipulation Nine: reporting breaches of security

All staff and information system users concerned with transferred personal health data shall be taught to recognise and report breaches of information security to the Data Protection Security Officer. The respective responsibilities of the data exporter and data importer towards the data subject in the event of interference with data referring to the data subject shall be clear as shall be the measures for handling the consequences.

10.10.10 Principle Ten, Stipulation Ten: Business Continuity plans

Arrangements shall be made for the processing of personal data to be carried on by the data importer in the event of the failure of processing systems.

10.10.11 Principle Ten, Stipulation Eleven; audit trails

Tamper-proof audit trails shall be maintained for all transferred personal health data.

10.10.12 Principle Ten, Stipulation Twelve: handling particularly sensitive data

Where personal health data is particularly sensitive, a rigorous risk assessment shall be undertaken and any special Measures necessary shall be strictly implemented. Examples of such data are personal genetic data and data concerning sexually transmitted diseases (see Annex G).

10.10.13 Rationale and observations on Measures

The rationale and observations on Measures relating to security of processing are considered in Clause 11.

10.11 Principle Eleven: responsibilities of staff and other contractors

All staff and other contractors working for the data importer and expected to be involved in processing of transferred personal health data shall be informed of their responsibilities and be capable of exercising them.

10.11.1 Principle Eleven, Stipulation One: informing staff and other contractors

Staff and other contractors involved in processing personal health information shall be informed of the HLSP and be provided with Measures to enable them to comply with the HLSP.

10.11.2 Principle Eleven, Stipulation Two: instruction and training

Staff and other contractors involved in processing personal health data shall receive instruction and/or training as appropriate to their responsibilities. Training material shall be reviewed at regular intervals not exceeding one year. Training shall be repeated at appropriate intervals.

10.11.3 Principle Eleven, Stipulation Three: staff and contractor contractual obligations

The obligations of staff and contractors to comply with Measures to implement the HLSP should be incorporated in their contracts of employment or terms of contract.

10.11.4 Rationale

Staff may already have received instruction or training in data protection in general. However staff involved with transferred personal health data must understand any additional or amended procedures.

10.11.5 Observation on Measures

A short explanatory document, which may act as a training document, should be produced.

11 Rationale and Observations on Measures to support Principle Ten concerning security of processing

11.1 General

Principle 10 (sub-clause 10.10) requires the data importer to protect data against “accidental or unlawful destruction or accidental loss, alterations, and unauthorised disclosure and access and against all unlawful forms of processing”.

These requirements shall apply also where the processing involves the transmission of data over a network.

Importers such as health organisations handling personal health data will probably already have in place measures to protect such data. These measures shall however be reviewed to check that they will ensure compliance with this International Standard and with the requirements of the controller transferring the data.

Measures shall be appropriate to the risks presented by the processing and the nature of the data to be protected. To ensure that Measures are appropriate to the risks a formal risk analysis should be undertaken.

It is not within the scope of this International Standard to specify detailed Measures that must back Principles (sub-clause 9.4.6). The observations below shall not therefore be taken as a full or adequate specification of the administrative and technical Measures required.

Measures shall be to the satisfaction of the controller transferring the data.

11.2 Encryption and digital signatures for transmission to the data importer

Having regard to the state-of-the art and the cost of implementation, encryption shall be used for electronic transmission of personal health data between the data exporter and data importer together with digital signatures in a form that will ensure integrity and authentication.

The strength of the encryption algorithms shall be appropriate to the risks and may be limited by national regulations. Some countries may require key escrow or legal access to keys for law enforcement or national security purposes. Data subjects should be aware if this applies.

11.3 Access controls and user authentication

One way to control the integrity of personal data held in information systems is for there to be an effective signature for all data entry, editing and manipulation and for all activity to be logged and audited. Physical control in terms of time and place can provide the first line of defence but proof of identity is required to ensure that no unauthorised activity occurs. The medical case notes are signed for similar reasons.

Passwords are the most frequently used arrangements for access control and user authentication but this is the lowest form of authentication. It can me made much more effective by the adoption of requirements such as those specified in CEN ENV 12551 (see Annex C) but more effective smart card and biometric systems are becoming available and these should be considered. Digital signatures can also be used to assure that information has not been tampered with and that the individual sending it has been authenticated.

11.4 Audit trails

Tamper-proof audit trails will be essential if a data subject’s rights to an independent investigation are to be guaranteed. The Measures will need to be sufficiently robust to withstand legal actions for redress or application of sanctions. Where possible only the Data Protection Security Officer should have access to these audit trails.

11.5 Physical and environmental security

Physical security is required to keep those who have no need to have access to systems away from them but also to ensure that measures are taken to prevent, alleviate or recover from the effects of things such as, flood, lightning strike, electricity failure, robbery. There will also be the need for adequate environmental measures to ensure that the systems continue working within their specified range of environmental conditions.

11.6 Application management and network management

Detailed technical support may be provided by an outside organisation but the local management must have access to someone who understands each application system and who can handle the basic training, management and trouble-shooting. Supporting measures should include adequate application documentation and training materials. This applies to applications and networks. Network configuration and firewall management are vital aspects of system security.

11.7 Malicious software

Attacks by malicious software are one of the most frequent forms of attack on information systems and web sites. As well as leading to a denial of service, such attacks can destroy or corrupt personal health data held by the organisation. Controls shall be updated not less frequently than monthly.

11.8 Breaches of security

The Data Protection Security Officer will have access to material on current security problems and will know about some of the key issues within the importer's organisation. However unless the details of security breaches across the organisation are reported in a central fashion, no-one will be aware of the totality of the threats facing the organisation and be able to start addressing them.

This requirement to report breaches of security can usefully be built into training programmes and the reporting should be on a non-threatening basis to encourage reporting, at least some of which will arise simply from operator error.

11.9 Business Continuity Plan

It is necessary for the organisation to be able to continue with its business such as the diagnosis and treatment of its patients even when disaster overtakes its processing facilities. There needs to be a clear assessment of the disasters that need to be accommodated and proper plans need to be drawn up, tested and documented for use if such disasters arise. It is too late to invent the plan when the problems have arisen. The consequences of various forms of system failure should be part of risk analysis. The development of a Business Continuity Plan is a significant project that depends on the processing that is undertaken. It should be tested and updated regularly.

11.10 Handling very sensitive data

Whereas all personal health data is sensitive some will be regarded by data subjects as extra sensitive such as data referring to sexually transmitted diseases, abortions etc. Also the increasing use of genetic/genomic information for the diagnosis and treatment of patients as well as its use for police and security purposes demands that these data shall be kept particularly secure from inappropriate disclosure. The most recent current advice on the handling of personal genetic data is included within the Council of Europe's Recommendation R(97)5 on the Protection of Medical Data [4]. However this is an area of active current research.

Wherever personal health data is suspected as possibly being very sensitive to a data subject the data subject shall be consulted regarding the nature of any possible extra security precautions and any agreed extra precautions shall be implemented. Annex G provides advice on what might be regarded as "very sensitive".

11.11 Standards

ISO and CEN security standards should be observed wherever an electronic transfer of person health data occurs. A list of applicable standards is given in Annex C. Annex D provides a list of other sources of useful advice.

12 Personal health data in non-electronic form

Compliance with the substance of this International Standard is required for personal health data in non-electronic forms also. For example non-electronic personal health data shall be transmitted between data exporter and data importer only through a mode offering security appropriate to risk. This may require a special courier arrangement.

It should be noted that non-electronic personal health data may take forms other than paper such as radiographs, ECG traces, specimens and these data need equally effective physical security.

Annex A
(informative)

Key primary international documents on data protection

A.1 EU Data Protection Directive

For EU countries the most significant document on data protection is the EU Data Protection Directive [6]. The twin objectives of the Directive are to protect the fundamental rights and freedoms of natural persons and to promote the free movement of personal data under that protection.

A.1.1 Coverage

Whereas the Directive makes reference to health data, its provisions are general and cover all sectors and applications, whether private or public. It applies to both manual and paper files and computer records. Personal data includes any information that applies to an identifiable person whether directly or indirectly, e.g. through one or more factors specific to an individual such as an identification number, physical characteristic, geographic indicators of residence etc.

A.1.2 Rules for lawfulness of processing

Personal data must be

— processed fairly and lawfully;

— adequate, relevant and not excessive in relation to purpose;

— accurate and kept up-to-date;

— kept identifiable for no longer than necessary for the purpose;

— collected for specified, explicit, legitimate purposes and not further processed in a way not compatible with those purposes.

Personal data may be processed subject to certain conditions e.g. only if

— the data subject(s) has given their 'unambiguous consent';

— or it is necessary for a contract to which the data subject is a party;

— or it is necessary for legal compliance;

— or it is to protect the vital interests of the subject;

— or for the performance of a task in the public interest.

A.1.3 Special categories of processing

Subject to some exceptions Member States must prohibit the processing of personal data revealing

— racial or ethnic origin;

— political opinions;

— religious or philosophical beliefs;

— trade union membership, and

— the processing of data concerning health or sex life.

In the context of this annex the most significant exception is in Article 8, Clause 3, which states that:

> "The prohibition does not apply where processing of the data is required for the purposes of
>
> — preventative medicine;
>
> — medical diagnosis;
>
> — the provision of care, or treatment;
>
> — or the management of healthcare services; and
>
> — where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy."

Member States are obliged to "determine the conditions under which a national identification number or any other identifier of general application may be processed."

A.1.4 Data subject's rights

The data subject must be provided with a minimum of information when data is collected, including

— the identity of the body which holds and controls the processing of the data;

— the purpose of processing;

— the recipients, or categories of recipients, of the data;

— other information to guarantee fair processing.

Where data processing is of personal data not collected from the data subject, the latter must still be provided with this information. There are exceptions in particular circumstances e.g. where processing is for statistics or specific research and the provision of the information would involve disproportionate effort.

Data subjects must have the right to know whether data about him/her is being processed and, if so, what data and for what purpose. They must have the right to have data erased or block its processing if not in accord with the Directive. In this case third parties to which the data has been supplied must be informed and must also erase and block processing (subject to disproportionate effort). However the rights of access may be restricted in the case of statistics and scientific research, as in Article 13 Clause 2 of the Directive which states that:

> "Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the [access] rights provided for in Article 12 when data are processed solely for the purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics".

A.1.5 Security of processing

Article 17 lays down obligations regarding security. Clause 1 states:

> "Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves transmission of data over a network, and against all other unlawful forms of processing.
>
> Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

When processing is carried out on behalf of the data controller, the processors must provide the same guarantees of security and that must be "in writing or an equivalent form".

A.1.6 Supervisory Authorities

Each Member State must have an independent public Supervisory Authority responsible for monitoring implementation of the Directive and with which any person may lodge a 'claim' concerning protection of his rights. The authority must have investigative powers and effective powers of intervention. Data controllers must notify the Supervisory Authority before commencing processing. Notification can be simplified or exempted by a Member State in certain circumstances including where an independent data protection 'official' is appointed for ensuring the Directive is enforced, and for keeping a register of processing operations. There is a specified minimum content for a notification, which must include any proposed transfers to third countries.

A.1.7 Remedies and sanctions

Data subjects must have access to 'judicial remedy' from the data controller for any breach of rights if harm has been inflicted.

A.1.8 Transfer of personal data to third countries

Article 25 of the Directive requires that Member States may not transfer personal information to a third country unless it ensures an adequate level of protection. Clause 2 states:

> "The adequacy of the level of protection afforded by a third country shall be assessed in the light of all circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."

Where the Commission finds a third country does not have adequate protection it can require Member States to prevent transfers, and it can enter into negotiations with that third country (Clauses 4 and 5).

However transfer to a third country that does not ensure adequate protection is allowed by Article 26 in particular circumstances e.g.

— where the data subject has unambiguously consented;

— it is necessary for the performance of a contract agreed by, or in the interest of, the data subject;

— it is necessary for the protection of the vital interests of the data subject.

A.2 Organisation for Economic Co-operation and Development (OECD)

Membership of OECD comprises 24 countries. Its most authoritative documents in the data protection area are a matter of guidance - not directives or laws. There are general guidelines on security [2] and guidelines on protection of privacy which deal with trans-borders flows [1]. The latter includes eight basic principles.

1) **Data collection limitation:** The collection of personal data should be limited. Personal data should be obtained by fair and lawful means and where appropriate, with the knowledge or consent of the data subject.

2) **Data quality:** Personal data should be as accurate, complete, and up-to-date as required for the purposes for which they are used.

3) **Purpose specification:** Individuals should be told why personal data are being collected at the time of collection. The data should only subsequently be used for this purpose or compatible purposes.

4) **Use limitation:** Personal data should not be disclosed or used except as allowed under the Purpose Specification Principle, with the individual's consent, or as required by law.

5) **Security safeguards:** Reasonable security precautions should be used to protect against unauthorised access, use, destruction, modification, or disclosure of personal data.

6) **Openness:** Policies and procedures relating to personal data should be easily obtained. Descriptions of personal data collections and contact information for those responsible for the collections should also be freely available.

7) **Individual participation:** Individuals should have the right to confirm whether an individual or organisation holds data about them, to view such data in a timely and reasonable fashion, and to be given reasons (and be able to dispute) any denial of these rights.

8) **Accountability:** A data controller should be made accountable for implementing the above principles.

A.3 Council of Europe

The Council of Europe's membership is wider than the EU. Council of Europe Conventions have the status of international treaties and Recommendations from the Council of Ministers of the Council of Europe under the various conventions have significant strength although individual citizens do not necessarily have the legal power to enforce their implementation in specific cases. In data protection terms, Recommendations of the Council of Europe provide significant guidance to the Supervisory Authorities. Convention 108, “For the protection of Individuals with regard to the automatic processing of personal data” [3] provided the basis for the European Directive. It addresses automated processing primarily but allows extensions for participating States to apply the same principles to non-automated processing and to provide the same protection to legal persons or groups of individuals as well as to identified or identifiable individuals. Recommendation R(97)5 “On the Protection of Medical Data” [4] recommends that governments of signatory States:

> “take steps to ensure that the principles ... in ... this Recommendation are reflected in their law and practice” and “ensure wide circulation of the principles ... in ... this Recommendation among persons professionally involved in the collection and processing of medical data.”

It covers

— legitimate processing;

— provision of information to patients;

— consent to processing and the right to object;

— subject access and rectification;

— security;

— disclosure of personal data;

— trans-border data flows.

There is particular attention to genetic data.

A.4 United Nations General Assembly

A.4.1 General

The UN has issued “Guidelines for Regulation of Personal Data Files” [5]. The UN Guidelines leave the procedures for implementing regulations concerning computerised personal data files to the initiative of each State subject to a number of “orientations” the essence of which is given in sub-clauses A.4.2 and A.4.3.

A.4.2 Principles concerning minimum guarantees that should be provided in any national legislation

1) **Lawfulness and fairness:** Information should be collected in fair, lawful ways not to be used contrary to the Charter of the UN.

2) **Privacy:** files should be kept up-to-date and accurate.

3) **Purpose specifications:** purpose and use of files should be specified and legitimate, and brought to the attention of the person concerned. None should be disclosed for incompatible purposes without consent and data should be kept no longer than necessary.

4) **Interested-person access:** there should be rights of access, rectification and erasure.

5) **Non-discrimination:** subject to 6 below, data likely to give rise to discrimination should not be compiled examples being racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs, membership of an association or trade union.

6) **Power to make exceptions:** departures from 1 to 4 may be authorised only if necessary to protect national security, public order, public health or morality or to protect the rights and freedoms of others. Exception to Principle 5 may be authorised only within the limits of the International Bill of Rights.

7) **Security:** appropriate measures must be taken to protect files from loss, damage, unauthorised access, fraudulent misuse and viruses.

8) **Supervision and sanctions:** the law shall designate the authority responsible for supervising observance of the Principles. It should have appropriate independent authority. Violations should attract criminal or other penalties with appropriate individual remedies.

9) **Trans-border flows:** if two countries have comparable safeguards to protect privacy, information should be able to circulate freely between them. Where this is not so the restrictions on flow should be limited to those necessary to protect privacy.

10) **Field of applications:** the Principles should apply in the first instance to all public and private computerised files. Optionally, subject to appropriate adjustments, they should apply to manual files.

A.4.3 Application of the Guidelines to personal data files kept by governmental international organisations

The Guidelines should apply to government international organisations and each organisation should designate an authority statutorily competent to supervise observance.

A derogation from the Principles may be provided when the purpose of the file is the protection of human rights and fundamental freedoms of an individual.

Annex B
(informative)

National documented requirements and legal provisions in a range of countries

B.1 Australia

AS 4400-1995 Australian Standard - *Personal Privacy Protection in Health Care Information Systems*

Australian Privacy Amendment (Private Sector) Act 2000

National Principles for the Fair Handling of Personal Information, Office of the Privacy Commission, Australia, Revised edition January 1999

Information Privacy, Code of Practice, New South Wales Health, 1996

B.2 Canada

COACH Guidelines for the Protection of Health Information (2001) - Canada

Canadian Personal Information and Electronic Documents Act 2000

B.3 Europe

Member States of the European Union are subject to the EU Data Protection Directive [6] (i.e. Austria, Belgium, Denmark, Eire, Finland, France, Germany, Greece, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden and U.K). Member countries of the European Economic Area (EEA) which are not also EU Member States are similarly covered by virtue of the EEA Treaty Decision 83/1999 of 25 June 1999 (i.e. Iceland, Liechtenstein and Norway).

The EU Commission has the power to recognise the data protection provisions of other countries as providing data protection equivalent to the EU Data Protection Directive. This has been done for Hungary [13] and Switzerland [14].

Applicants to become members of the EU will also need to comply with the EU Data Protection Directive.

B.4 Japan

JIS Q 15001:1999, *Requirements for compliance program on personal information protection* <http://privacymark.org/ref/jisq15001.en.html>.

The Government Officials Act Article 100: Officials must not divulge a secret which they know in the course of their duty even after retirement.

The Local Officials Act Article 34: Officials must not divulge a secret which they know in the course of their duty even after retirement.

The Criminal Law Article 134: Offence for a medical doctor, pharmacist, medical products trader, midwife, … to divulge without good reason a secret known in the course of duty.

The public health nurse, midwife and nurse Law, The consulting radiologist Law, The dental technician Law, The emergency medical technician Law, The speech and hearing technician Law, all create an obligation to keep, and an offence to divulge, a secret.

The Administrative Agency holding and computer processing related Personal Information Protection Law: imposes duties for processing and creates offence to disclose personal data known through work or to use it for unjust purpose.

The Administrative Agency holding Information Release Law: deals with the responsibilities for protecting personal information when disclosing administrative documents.

The Personal Information Protection Law (Draft under discussion): will be based on principles such as to acquire properly, to ensure accuracy, to take security measures, to provide for owner's participation (notification of purpose of use, disclosure, prohibition and correction).

Security and Privacy Requirement for Remote Servicing, Joint NEMA/COCIR/JIRA Security and Privacy Committee, July 11, 2001.

Security and Privacy Auditing in Health Care Information Technology, Joint NEMA/COCIR/JIRA Security and Privacy Committee, July 11, 2001.

B.5 New Zealand

Health Information Privacy Code 1994, Privacy Commissioner, New Zealand

B.6 UK

BS 7799-1:2000 Part 1, *Code of Practice for Information Security Management*, British Standards Institution, London

BS 7799-2:2002 Part 2, *Specification for Information Security Management Systems*, British Standards Institution, London

Data Protection Act 1998

Access to Health Records Act 1990

Common Law of Confidentiality

Confidentiality: National Health service (NHS) Code of Practice – July 2003 (Department of Health, England)

Use and Disclosure of Health Data – May 2002 (Office of the Information Commissioner)

B.7 USA

USA Health Insurance Portability and Accountability Act, 1996

An Inventory of Healthcare Information Standards, ANSI/HISB, January 1997

ASTM E 1762, *Standard Guide for Electronic Authentication of Health Care Information*

ASTM E 1869-97, *Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records*

ASTM PS 115-99, *Provisional Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*

Safe Harbor Privacy Principles [15] - US Department of Commerce - July 21, 2000

Annex C
(informative)

Relevant ISO and CEN Standards

C.1 ISO

ISO/IEC 17799:2000, *Information technology — Code of practice for information security management*

ISO/IEC TR 13335, *Information technology — Guidelines for the management of IT Security*

— *Part 1: Concepts and models for IT Security*

— *Part 2: Managing and planning IT Security*

— *Part 3: Techniques for the management of IT Security*

C.2 CEN

ENV 12924:1997, *Medical informatics — Security categorisation and protection for healthcare information systems*

ENV 12388:1996, *Medical informatics — Algorithm for digital signature services in health care*

ENV 13608:2000, *Health informatics — Security for healthcare communications*

— *Part 1: Concepts and terminology*

— *Part 2: Secure data objects*

— *Part 3: Secure data channels*

ENV 13729:2000, *Health informatics — Secure user identification — Strong authentication using microprocessor cards*

ENV 12251:2000, *Health Informatics — Secure user authentication for health care — Management and security of authentication by passwords*

Annex D
(informative)

Sources of advice

D.1 References

"Guidelines for the Security of Information Systems", OECD, OECD/GD(92)190 Paris, November 1992

SEISMED Consortium, "Towards Security in Medical Telematics", ed Barber B et al, vol. 27 in Studies in Health Technology and Informatics, IOS Press, Amsterdam, 1996, ISBN 90 5199 246 7

"Data Security for Health Care" ed the SEISMED Consortium, in Studies in Health Technology and Informatics, IOS Press, Amsterdam, 1996:

— Management Guidelines vol. I ISBN 90 5199 264 5

— Technical Guidelines vol. II ISBN 90 5199 265 3

— User Guidelines vol. III ISBN 90 5199 266 1

TrustHealth 1 and 2, EU DG XIII Fourth Framework Health Telematics Projects, HC1051 and HC 4023, 1996 – 1999

Handbook of Standards for Security and Privacy – Healthcare Deliverable 4 EU MEDSEC project, EU DG III Health Care Security and Privacy in the Information Society EU DGIII, ISIS programme, 1997 – 1998

SEMRIC, Secure Electronic Medical Information Communication, EU DG III, ISIS programme, 1997

Initiative on Privacy Standardisation in Europe (IPSE), Discussion Draft, September 2001

The CRAMM User Guide, 29 March 2001, The CCTA Risk Analysis and Management Methodology, CRAMM, software version 4.0, The CRAMM Manager, Insight Consulting Ltd, Churchfield House, 5 The Quintet, Churchfield Road, Walton on Thames, KT12 2TZ [the user guide is included with the software]

Communicating Health Information in an Insecure World, ed. Bakker AR, Barber B, Pellikka RT K & Treacher A, International Journal of Bio-Medical Computing, vol. 43, pp. 1-152, Supplement October 1996 Amsterdam

Common Security Solutions for Communicating Patient Data, ed. Bakker AR, Barber B, Ishikawa K & Yamamoto K, International Journal of Bio-Medical Computing, vol. 49, pp. 1-137, Supplement October 1998 Amsterdam

Security of the Distributed Electronic Patient Record, ed. Bakker AR, Barber B, Moehr J, International Journal of Bio-Medical Computing, Vol. 60 pp. 1 – 237, 2000

D.2 Selected web sites

ISO TC 215 Health Informatics

<http://isotc.iso.ch/livelink/livelink.exe?func=ll&objId=529137&objAction=browse&sort=name>

OECD - <http://www.oecd.org/>

Council of Europe - <http://www.coe.int/>

CEN TC 251 Health Informatics - <http://www.centc251.org/>

ASTM (American Society for Testing and Materials) - <http://www.astm.org/>

CEN/ISSS including Initiative for Privacy Standardisation in Europe (IPSE) - <http://www.cenorm.be/isss>

European Union INFOSEC programme - <http://www.cordis.lu/infosec>

ISHTAR EU Security Projec - <http://www.ishtar.org.uk/>

European Commission Data Protection - <http://europa.eu.int/comm/internal_market/en/dataprot/>

EU Article 29 Working Party - <http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm>

Annex E
(informative)

Exemplar contract clauses: Controller to Controller

E.1 Introduction

Given below is an example of a contract suitable for controller-to-controller transfers (see sub-clause 7.2.2 g)).

E.2 Attribution

These controller-to-controller standard contract clauses were created by the EU Commission to allow a controller to adduce “adequacy” of data protection in the full context of the EU Data Protection Directive [16].

E.3 Essential features of a contract

Any contract shall cover the following

— the responsibilities of data exporter and data importer;

— the purposes for which the data is transferred;

— that data subjects have given unambiguous consent to the transfer for the stated purposes;

— data subject’s rights to have a copy of the contractual clauses;

— data subject’s rights to redress and objective investigation of complaints and mediation;

— the governing law;

— transfer of data to third parties;

— requirements which the data importer must meet to ensure adequate data protection.

The above shall be consistent with the clauses of this International Standard.

E.4 Exemplar contract: notes

The contract clauses below are an example only. Each international application will need to consider them in the light of the application and any national legal aspects which might bear on the contract. Legal advice may be required.

It should be noted that:

— The contractual clauses should be enforceable not only by the organisations which are parties to the contract, but also by the data subjects, in particular, where the data subjects suffer damage as a consequence of a breach of the contract.

— The governing law of the contract should be the law of the country in which the primary controller transferring the data is established, with the intention that this will enable a third-party beneficiary to enforce the contract. This arrangement may be altered if clearly to the benefit of the data subjects. Data subjects should be allowed to be represented by associations or other bodies of they so wish.

— To reduce practical difficulties which data subjects could experience when trying to enforce their rights under these contract clauses, the data exporter and the data importer should be jointly and severally liable for damages resulting from any violation of those provisions which are covered by the third-party beneficiary clause.

— The data subject is entitled to take action and receive compensation from the data exporter and data importer or from both for any acts incompatible with the obligations contained in these clauses. However both parties may be exempted from that liability if they prove that neither of them was responsible.

— Joint and several liability does not extend to those provisions not covered by the third-party beneficiary clause and does not need to leave one party paying for the damage resulting from the unlawful processing of the other party. Although mutual indemnification between the parties is not a requirement and may therefore be deleted, it is included in the clauses for the sake of clarification and to avoid the need for the parties to negotiate indemnification clauses individually.

— In the event of a dispute between the parties and the data subject which is not amicably resolved and where the data subject invokes the third-party beneficiary clause, the parties agree to provide the data subject with the choice between mediation or litigation. The extent to which the data subject will have an effective choice will depend on the availability of reliable and recognised systems of mediation and arbitration. Mediation through a recognised authority in the country of the primary controller transferring the data such as a national or State Data Protection/Privacy Commissioner or equivalent would be a good option if such a service can be provided.

— The responsibilities of the data exporter and the data importer towards a data subject in the event of interference with data concerning the data subject should be made clear.

EXAMPLE STANDARD CONTRACTUAL CLAUSES

Name of the data exporting organisation: _____

_____

Address: _____

Tel: _____ Fax: _____ Email: _____

Other information needed to identify the organisation: _____

(the data exporter)

and

Name of the data importing organisation: _____

Address: _____

Tel: _____ Fax: _____ Email: _____

Other information needed to identify the organisation: _____

(the data importer)

have agreed on the following contractual clauses ('the clauses') in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal health data specified in Appendix 1.

Clause 1

Definitions

The following definitions apply for the purposes of the Clauses

— **controller:** the 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;

— **data subject:** the identified or identifiable natural person, which is the subject of personal data;

— **participants:** data exporters and data importers;

— **personal data:** any information relating to an identified or identifiable natural person;

— **personal health data:** any personal data relevant to the health of an identified or identifiable natural person;

— **processing of personal health data (processing):** any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

— **data importer:** a natural or legal person, public authority, agency or any other body located in one country which receives data from a data exporter in another country;

— **technical and organisational security measures:** those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where processing involves transmission of data over a network, and against all unlawful forms of processing;

— **data exporter:** a natural or legal person, public authority, agency or any other body located in one country which sends data to a data importer in another country.

Clause 2

Details of the transfer

The details of the transfer and in particular the categories of personal data and the purposes for which they are transferred are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

The data subjects can enforce this Clause, Clauses 4 (b), (c) and (d), Clauses 5 (a), (b), (c), (e), (f) and (g), Clauses 6 (1) and (2), and Clauses 7, 9 and 11 as third-party beneficiaries. The parties do not object to the data subjects being represented by an association or other bodies of they so wish and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants

a) that the processing, including the transfer itself, of the personal health data by him has been and, up to the moment of the transfer, will continue to be carried out in accordance with the relevant provisions of the country in which the data exporter is established (and where applicable has been notified to the relevant authorities of that country) and does not violate the relevant provisions of that country;

b) that the data subject has been informed or will be informed before the transfer that this data could be transmitted to the importing country and has unambiguously consented;

c) to make available to the data subjects upon request a copy of the Clauses; and

d) to respond in a reasonable time and to the extent reasonably possible to any enquiries from the data subject concerning the processing of his personal health data by the data importer.

Clause 5

Obligations of the data importer

The data importer agrees and warrants

a) that he has no reason to believe that the legislation applicable to him prevents him from fulfilling his obligations under the contract and that, in the event of a change in that legislation which is likely to have substantial adverse effect on the guarantees provided by the Clauses, he will notify the change to the data exporter in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b) to process the personal data in accordance with the mandatory data protection requirements set out in Appendix 2;

c) to deal promptly and properly with all reasonable enquiries from the data exporter or the data subject relating to his processing of the personal health data subject to the transfer;

d) at the request of the data exporter to submit its data processing liabilities for audit which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications, selected by the data exporter;

e) that he will promptly notify the data exporter about

    i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

ii) any accidental or unauthorised access, and

iii) any request received directly from the data subjects without responding to that request, unless he has been otherwise authorised to do so;

f) to make available to the data subject upon request a copy of the Clauses and indicate the office which handles complaints;

g) to comply with any requirements laid down by the Data Protection/Privacy Commissioner in the data exporter's country as indicated in Appendix 3.

Clause 6

Liability

1) The parties agree that a data subject who has suffered damage as a result of any violation of the provisions referred to in Clause 3 is entitled to receive compensation from the parties for the damage suffered. The parties agree that they may be exempted from this liability only if they prove that neither of them is responsible for the violation of those provisions.

2) The data exporter and the data importer agree that they will be jointly and severally liable for damage to the data subject resulting from any violation referred to in paragraph 1. In the event of such a violation, the data subject may bring action before a court against either the data exporter or the data importer or both.

3) The parties agree that if one party is held liable for a violation referred to in paragraph 1 by the other party, the latter will to the extent to which it is liable, indemnify the first party for any costs, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon

i) the data exporter promptly notifying the data importer of a claim; and

ii) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim (*).

Clause 7

Mediation and jurisdiction

a) The parties agree that if there is a dispute between a data subject and either party which is not amicably resolved and the data subject invokes the third party beneficiary provision in Clause 3, they accept the decision of the data subject

1) to refer the dispute to meditation by an independent person or authority;

2) to refer to the dispute to the courts in the country in which the data exporter is established.

b) The parties agree that by agreement between a data subject and the relevant party a dispute can be referred to an arbitration body. (**)

c) The parties agree that paragraphs a) and b) apply without prejudice to the data subject's substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with national authorities

The parties agree to deposit a copy of this contract with any national Data Protection/Privacy Commissioner or equivalent if such a deposit is required under national law.

Clause 9

Termination of the Clauses

The parties agree that the termination of the Clauses at any time, in any circumstances and for whatever reason does not exempt them from the obligations and/or conditions under the Clauses as regards the processing of the data transferred.

Clause 10

Governing Law

The Clauses shall be governed by the law of the country in which the Data exporter is established, namely (***):

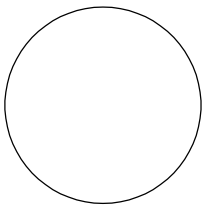
_____

Clause 11

Variation of the contract

The parties undertake not to vary or modify the terms of the clauses.

On behalf of the data exporter:



(stamp of organisation)

Name (written out in full): _____

Address: _____

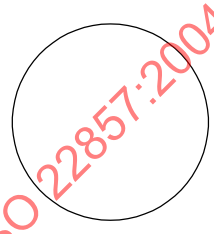
Tel: _____ Fax: _____ Email: _____

Other information necessary in order for the contract to be binding (if any): _____

_____

and

On behalf of the data importer:



(stamp of organisation)

Name of the data importer's organisation: _____

Address: _____

Tel: _____ Fax: _____ Email: _____

Other information necessary in order for the contract to be binding (if any): _____

_____

_____
(Signature)

(*) Paragraph 3 is optional.

(**) Whether the relevant party is established in a country which has ratified the New York convention on enforcement of arbitration awards could be significant.

(***) The governing law will usually be that of the country in which the data exporter is established unless some other arrangement is clearly more beneficial to data subjects.

Appendix 1

to the contractual clauses

This Appendix forms part of the clauses and must be completed and signed by the parties.

(Participants may complete or specify any additional necessary information to be contained in this Appendix).

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

_____

_____

_____

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):

_____

_____

_____

Data Subjects

The personal health data transferred concerns the following types of data subject (please specify):

_____

_____

_____

Purposes of the transfer

The transfer is necessary for the following purposes (please specify):

_____

Categories of data

The personal data is transferred is of the following nature
(specify and indicate any which may be particularly sensitive):

_____

_____

_____

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients (please specify):

_____

_____

_____

Storage limit

The personal data transferred may be stored for no more than
(specify in months/years or in other terms which ensure data is kept no longer than necessary for the purposes):

_____	_____
Data exporter	Data importer
Name: _____	Name: _____
_____	_____
(Authorised signature)	(Authorised signature)

Appendix 2

to the contractual clauses

Mandatory data protection requirements referred to in Clause 5 c)

The mandatory data protection requirements are those mandatory requirements of ISO 22857, *Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health information.*

Appendix 3

to the contractual clauses

Detail here any requirements, if any, laid down by the national/state Data Protection/Privacy Commissioner or equivalent in the country in which the data exporter is established.

Annex F
(informative)

Exemplar contract clauses: Controller to Processor

F.1 Introduction

Given below is an example of a contract suitable for controller to processor transfers (see 7.2.2 g)).

In a controller to controller transfer the importing controller, as a controller, has authority to determine how to process personal health data and the means for so doing albeit the primary controller transferring the data will lay down the essential principles to be followed to ensure overall adequacy of data protection. Since the importing controller has such authority he must take responsibility for any actions he takes as a consequence of that authority and for any redress sought by the data subject as a result of any deficiencies.

In a controller to processor transfer, the importing processor, as a processor, is constrained to process the transferred data only as instructed by the controller. The latter must therefore specify in detail what the processor is to do and the technical and organisational security measures he must implement. Thus the controller takes responsibility for the adequacy of those instructions and measures and thus for any redress sought by a data subject if they prove inadequate. Whereas the processor has an obligation to implement the technical and organisational measures which the controller specifies, the controller has the obligation to ensure that compliance with such measures actually occurs.

In the circumstances of a controller to processor transfer, the data subject should be able to enforce all his rights against the controller only and in the context of the governing law of the country in which the controller is established. Any deficiencies exhibited by the processor will be a matter to be dealt with between the controller and the processor. However should the controller cease to exist, the data subject should be able to exercise his rights against the importing processor for deficiencies for which the processor is responsible.

F.2 Attribution

These controller to processor standard contract clauses were created by the EU Commission to allow a controller in an EU Member State to adduce “adequacy” of data protection in the full context of the EU Data Protection Directive [17].

F.3 Essential features of a contract

Any contract shall cover the following

— the responsibilities of transferring controller and importing processor;

— the purposes for which the data are transferred;

— that data subjects have given unambiguous consent to the transfer for the stated purposes;

— data subject’s rights to have a copy of the contractual clauses;

— data subject’s rights to redress and objective investigation of complaints and mediation;

— the governing law;

— technical and organisational security measures which the importing processor must meet to ensure adequate data protection.

The above shall be consistent with the clauses of this International Standard.

F.4 Exemplar contract: notes

The contract clauses below are an example only. Each international application will need to consider them in the light of the application and any national legal aspects which might bear on the contract. Legal advice may be required.

It should be noted that

— The importing processor should process the transferred data only on behalf of the transferring controller and in accordance with his instructions and the obligations contained in the contractual clauses. In particular the data importer should not disclose the personal health data to a third party unless in accordance with conditions laid down by the transferring controller. The transferring controller should instruct the importing processor throughout the duration of the data processing services to process the data in accordance with his instructions, any applicable data protection laws and obligations contained in the contractual clauses.

— The contractual clauses should be enforceable not only by the organisations which are parties to the contract, but also by the data subjects, in particular, where the data subjects suffer damage as a consequence of a breach of the contract.

— The governing law of the contract should be the law of the country in which the primary controller transferring the data is established, with the intention that this will enable a third-party beneficiary to enforce the contract.

— The data subject is entitled to take action and where appropriate receive compensation from the controller transferring the data for any acts incompatible with the obligations contained in these clauses. Exceptionally the data subject should also be entitled to take action and, where appropriate, receive compensation from the importing processor in those cases arising out of a breach by the importing processor of any of his obligations referred to in Clause 3 of the exemplar clauses, where the transferring controller has factually disappeared or has ceased to exist in law or has become insolvent.

— In the event of a dispute between the parties and the data subject which is not amicably resolved and where the data subject invokes the third-party beneficiary clause, the parties agree to provide the data subject with the choice between mediation or litigation. The extent to which the data subject will have an effective choice will depend on the availability of reliable and recognised systems of mediation and arbitration. Mediation through a recognised authority in the country of the primary controller transferring the data such as a national or State Data Protection/Privacy Commissioner or equivalent would be a good option if such a service can be provided.

— The responsibilities of the data exporter and the data importer towards a data subject in the event of interference with data concerning the data subject should be made clear.

EXAMPLE STANDARD CONTRACTUAL CLAUSES

Name of the data exporting organisation: _____

_____