

ICS 35.240.80

CCS L 09



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 25512-2010

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

健康信息学 推动个人健康信息跨国流动的数据保护指南

(English Translation)

Issued on: December 1, 2010

Implemented on: May 1, 2011

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People's Republic of China**

Table of Contents

Preface

Introduction

1 Scope

2 Terms and definitions

3 Abbreviations

Foreword

This standard is equivalent to ISO 22857.:2004 "Health Information Science to promote personal health information transnational flow of data protection guide" (English Version).

This standard has been modified in accordance with ISO 22857.:2004 as follows.

- Since ISO 22857.:2004 does not have a normative reference document but only the chapter is established, the corresponding "Normative reference document" chapter. ISO 22857.:2004, chapter 3 to chapter 12, in this standard, the chapter number corresponding to the change for the purposes of Chapters 2 to 11, references to the chapter numbers are adjusted accordingly.
- ISO 22857.:2004 The last three paragraphs of the "Introduction" are given in the form of "note" in this standard.
- Removal of ISO 22857.:2004 Chapter 1, "Scope", "No harmonization of existing national standards, regulations or regulations" and " Only as a guide, does not provide clear legal advice. For specific applications, refer also to the specific law that applies to the application Meeting. "The content of the chapter and the order of the appropriate changes to meet the formulation of our practice.
- ISO 22857.:2004 Chapter 1 The last paragraph of the "scope" is given in the form of "note" in this standard.
- The following notes have been removed from the first and the first paragraphs of ISO 22857.:2004, Chapter 3, "Terms and Definitions", with the addition of the guide language.
- removed in ISO 22857.:2004 Chapter 3 3.1 "unless the meaning is significantly different", 3.2 "unless explicitly stated", 3.6 "Unless otherwise stated".
- Added the lead in "5.1 Basic Principles". "This standard follows the following basic principles."

Appendix A, Appendix B, Appendix C, Appendix D, Appendix E, Appendix F and Appendix

G of this standard are informative.

This standard is proposed and centralized by China Standardization Research Institute.

The drafting of this standard unit. China Institute of Standardization.

This part of the main drafters. Chen Huang, Shi Lijuan, Dong continuous, Yang Xuefeng, Zhou Jimei, Li Xian, Guo Xiaoning, Huang Feng, Jiao Jianjun.

Introduction

In a healthy context, there are many individual information that need to be collected, stored, and processed to achieve a variety of target uses, including.

- provide medical care directly, such as medical records;
- management process, such as booking;
- clinical research;
- statistics.

The required data depends on the purpose of use. In the context of individual identities, the data may be used to.

- allow the individual to carry out simple and unique identification, such as name, address, age, gender, ID number and other combinations;
- confirm that the two data sets belong to the same individual without the need to identify the individual itself, such as links and/or vertical statistics;
- for statistical purposes, but to avoid eventually identifying any individual.

In all these cases, the relevant data of the individual are now and in the future are increasing, and will be transnational transmission, or be specially provided Access to other countries other than the data collection or storage location. The data may be collected in one country, stored in another country, and by the third National management, while providing access to many other countries and even the world. The key requirements are.

- all of these processes should be carried out in one mode and consistent with their objectives, with the consent of the original data collection party;
- In particular, all personal health data should be disclosed to appropriate individuals and organizations within these and agreed terms.

Internationally health-related applications may require transnational transmission of personal health data. Mainly reflected in telemedicine, or electronically (Such as e-mail) to send data, or as a data file to the international database. Followed by reflected in the Internet and other means through access the database of other countries. This may seem like a passive application, but the behavior of such access involves data disclosure that can

be seen as a " in addition, the need to download, which will automatically save the data in the computer cache until it is "empty", which is a deal and involved Specific security risks.

Many organizations may involve receiving personal health data from other countries, such as.

- medical institutions, such as hospitals;
- pharmaceutical companies conducting research activities;
- contractors for long-range transnational maintenance of health care systems;
- organizations that have a teaching database (eg radiographic images with diagnostic and medical records);

A company with a series of medical records of patients in different countries;

- organizations that conduct health-related international e-commerce (eg e-pharmacy).

All applications involving personal health data may pose a potential threat to individual privacy. This threat and its extent will depend on.

- the degree to which data is protected to prevent unauthorized access in storage and transport;

The number of persons who have access to the data;

The nature of personal health data;

- Identify the difficulty of the individual when accessing the data;
- the ease of access to unauthorized access.

Regardless of where to collect, store, process or publish (including published on the Internet) health data, potential threats to privacy Evaluate and take adequate protection measures. It is often necessary to conduct a risk analysis to determine the required level of safety.

In addition to the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the European Committee for Standardization (CEN) and the European Electrotechnical Standardization in addition to the Committee (CENELEC), there are four major multinational bodies that have jointly consulted on the protection and security of data in transnational flows Authoritative international documents.

- Organization for Economic Co-operation and Development (OECD);

The European Council (Council ofEurope);

- United Nations (UN);

- EU (EU).

The main documents of these bodies are.

OECD Guidelines for Transboundary Movement of Privacy and Personal Data [1];

--- OECD "Information Systems Security Guide" [2];

- European Commission Convention No. 108 Convention on Individual Protection in Personal Data Automated Processing [3];

- European Commission Regulation R (97) 5 on "Protection of Medical Data" [4];

--- UN "Computerized Personal Data File Rules Guide" [5];

--- EU "Data Protection Directive concerning Personal Data Processing and Its Free Flow" [6].

Appendix A provides a summary of the key aspects of these documents.

Countries for personal health data protection means and the degree of different [7]. Some countries have national privacy bills, others also There are only state or equivalent regulations. Many countries may have various practitioners principles or similar norms and/or "medical" laws that require Medical professionals protect the patient's privacy, but there is no relevant legislation.

Although privacy legislation in different parts of the world may refer to personal health data, it may often be relevant to government agencies and /or medical research are not specific to health legislation.

Appendix B contains the main national standards or other document requirements and the legal principles of data protection between different countries

Outline.

In fact, personal health data is extremely sensitive, for the purpose of protection, so there are a large number of domestic and international, Administrative and technical "safety measures" (see Appendix C and Appendix D).

Health information science promotes personal health information across countries Mobile data protection guide

1 Scope

This standard gives data protection requirements that promote transnational transmission of personal health data.

This standard applies only to international exchange of personal health data. Domestic groups to develop and implement data protection principles can refer to the use.

This standard not only provides the principle of data protection applicable to international transmission, but also gives that, in order to ensure consistency with these principles,