ICS 35.240.80
L 09

# 中华人民共和国国家标准

GB/T 25512—2010/ISO 22857:2004

# 健康信息学　推动个人健康信息跨国流动的数据保护指南

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

(ISO 22857:2004,IDT)

2010-12-01 发布　　2011-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

# 前　言

本标准等同采用 ISO 22857:2004《健康信息学　推动个人健康信息跨国流动的数据保护指南》(英文版)。

本标准与 ISO 22857:2004 相比做了下列编辑性修改:

——由于 ISO 22857:2004 中没有规范性引用文件但仅设立了该章,所以在本标准中删除了对应的“规范性引用文件”一章。ISO 22857:2004 中第 3 章至第 12 章,在本标准中其章条号对应改为第 2 章至第 11 章,其他各处对章条号的引用均按此相应调整。

——ISO 22857:2004“引言”中最后三段,在本标准中以“注”的形式给出。

——删除了 ISO 22857:2004 第 1 章“范围”中“无需协调现有的国家标准、法规或条例”和“本标准仅作为指南,并不提供明确的法律建议。具体应用时,还需参考适用于该应用的具体法律建议。”的内容,并对该章的语序进行了适当修改,以符合我国的表述惯例。

——ISO 22857:2004 第 1 章“范围”中最后一段,在本标准中以“注”的形式给出。

——删除了 ISO 22857:2004 第 3 章“术语和定义”中第 1 段和第 1 段下面的注解,增加了引导语。

——删除了 ISO 22857:2004 第 3 章 3.1 中“除非意思明显不同”、3.2 中“除非明确指出”、3.6 中“除非另有说明”的内容。

——在“5.1　基本原则”中添加了引导语“本标准遵循以下基本原则:”。

本标准的附录 A、附录 B、附录 C、附录 D、附录 E、附录 F 和附录 G 为资料性附录。

本标准由中国标准化研究院提出并归口。

本标准起草单位:中国标准化研究院。

本部分主要起草人:陈煌、石丽娟、董连续、杨雪峰、周继梅、李宪、郭默宁、黄锋、焦建军。

# 引　言

在健康语境中，有许多个体的信息需要采集、储存和处理以实现多种目标用途，主要包括：

——直接提供医疗看护，如病历；

——管理性流程，如预约；

——临床研究；

——统计。

所需的数据取决于使用目的。在涉及个体标识的语境中，数据可能用于：

——允许对个体进行简易而唯一的标识，如姓名、地址、年龄、性别、身份证号等的各种组合；

——确认两个数据集属于同一个体而不需对个体本身进行标识，如相关记录的链接和/或纵向统计；

——统计目的，但要避免最终能标识出任何个体。

在所有这些情形下，个体的相关数据现在和将来都在不断增加，而且会跨国传输，或者被特意提供给该数据采集地或存储地之外的其他国家访问。数据可能采集于一个国家，存储于另一国家，又由第三个国家管理，同时提供给许多其他国家甚至是全世界访问。关键要求是：

——所有这些处理过程应在一个模式下进行，并与其目标一致同时应得到原始数据采集方的同意；

——尤其是，所有个人健康数据都宜在这些目的和同意的范围内披露给适当的个体和组织。

国际上与健康相关的应用可能需要跨国传输个人健康数据。主要体现在远程医疗，或以电子方式（如电子邮件）发送数据，或作为数据文件添加到国际数据库中。其次还体现在通过互联网等手段查阅他国的数据库。这可能看起来是一种被动的应用，但这种查阅的行为涉及数据披露，可看作是一种“处理”。此外，还需要下载，这会将数据自动保存在电脑缓存中直到被“清空”，这也是一种处理并且涉及了特定的安全隐患。

很多类组织都可能涉及从他国接收个人健康数据，例如：

——医疗机构，如医院；

——进行研究活动的制药公司；

——远程跨国维护医疗保健系统的承包商；

——拥有教学资料库（如：带诊断和病历注释的放射影像）的组织；

——拥有一系列不同国家患者医疗记录的公司；

——开展与健康相关的国际电子商务（如电子药房）的组织。

所有涉及个人健康数据的应用都可能对个体隐私构成潜在威胁。这种威胁及其程度将取决于：

——数据被保护的程度，以防止在存储和传输中的非授权访问；

——有权访问数据的人数；

——个人健康数据的性质；

——访问数据时识别出个体的难易程度；

——未经授权而实现访问的难易程度。

无论在何地采集、存储、处理或发布（包括在互联网上发布）健康数据，对隐私的潜在威胁都要加以评估并采取充分的保护措施。通常有必要进行风险分析以确定所需的安全措施等级。

除了国际标准化组织（ISO）、国际电工委员会（IEC）、欧洲标准化委员会（CEN）和欧洲电工标准化委员会（CENELEC）外，还有四个主要的跨国机构共同协商出台了关于跨国流动中数据保护和安全的权威性国际文件。

——经济合作与发展组织(OECD);

——欧洲委员会(Council of Europe);

——联合国(UN);

——欧盟(EU)。

这些机构的主要文件有:

——OECD《隐私保护和个人数据跨国流动指南》[1];

——OECD《信息系统安全指南》[2];

——欧洲委员会 No.108 公约《个人数据自动化处理中的个体保护公约》[3];

——欧洲委员会第 R(97)5 号建议书《关于医疗数据的保护》[4];

——UN《计算机化个人数据文件规则指南》[5];

——EU《涉及个人数据处理及其自由流动的数据保护指令》[6]。

附录 A 提供了这些文档重点方面的概要。

各国对于个人健康数据保护的手段和程度不同[7]。一些国家有全国性的隐私法案,另一些国家也许只有州级或者同等级别的法规。很多国家可能存在各种从业原则或类似的规范和/或"医疗"法,要求医学专业人士保护患者隐私,但却没有相关的立法。

尽管世界上不同地方的隐私立法都可能会提及个人健康数据,但通常除了可能关系到政府机构和/或医学研究外都没有特定的针对健康的立法。

附录 B 包含了主要的各国国家标准或其他文件要求和不同国家间关于数据保护的法律原则的纲要。

事实上个人健康数据极为敏感,出于保护目的,因此在各国国内和国际上存在大量现行的关于各种行政和技术性"安全措施"的指南和标准(见附录 C 和附录 D)。

# 健康信息学　推动个人健康信息跨国流动的数据保护指南

## 1　范围

本标准给出了推动个人健康数据跨国传输的数据保护要求。

本标准仅适用于个人健康数据的国际交换。国内团体制定和实施数据保护原则可参照使用。

本标准既给出了适用于国际传输的数据保护原则，也给出了为确保与这些原则保持一致各组织应采纳的安全策略。

本标准将优先考虑在许多国家间已达成的多边协议（如 EU 数据保护指令）。

本标准旨在促进个人健康数据传输的国际应用。并致力于提供一些方法以确保数据主体（如患者）相关的健康数据在发送给他国及在他国处理时都能得到充分的保护。

注：各国对隐私和数据保护的要求不断变化，而且更新相对较快。本标准总体上包含了更为严格的国际和各国国内要求，尽管这些要求只是其中的一小部分。有些国家可能有一些更为严格和特定的要求，这有待核查。

## 2　术语和定义

下列术语和定义适用于本标准。

2.1

**应用　the application**

使用本标准的国际应用。

2.2

**委员会　Commission**

指欧盟委员会（European Commission）。

2.3

**控制方　controller**

自然人或法人、政府机关、机构或其他团体，能单独或共同决定处理个人数据的用途和方法。

2.4

**数据主体　data subject**

已标识或可标识的自然人，即个人数据的主体。

2.5

**数据主体的同意　data subject's consent**

体现数据主体意愿的各种特定的、知情的表示，这种表示显示数据主体同意对其个人数据进行处理。

2.6

**欧盟指令　EU directive**

欧盟数据保护指令[6]。

2.7

**可标识的个人　identifiable person**

可以被直接或间接标识的个人，尤其是通过其身份证号或关于其物理、生理、精神、经济、文化或社会身份等一个或多个特定因素标识的个人。