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。

2.8

参与方　participants

数据导出方和数据导入方。

2.9

个人数据　personal data

任何涉及已标识或可标识自然人的信息。

2.10

个人健康数据　personal health data

任何涉及已标识或可标识自然人的健康情况的个人数据。

2.11

主要控制方　primary controller

数据导出方，作为控制方对确保数据主体同意跨国传输其个人健康数据等所有相关事宜负责。

2.12

处理方　processor

代表控制方处理个人数据的自然人、法人、政府机关、机构或其他团体。

2.13

个人数据处理　processing of personal data

处理　processing

对个人数据进行的自动化或非自动化(系列)操作，如采集、记录、组织、存储、改编或改动、检索、咨询、使用、(通过传输)披露、散播、提供、调整或组合、拦截、删除或销毁。

2.14

数据导入方　data importer

获取他国数据导出方数据的自然人、法人、政府机关、机构或其他团体。

2.15

数据导出方　data exporter

向他国数据导入方发送数据的自然人、法人、政府机关、机构或其他团体。

3　缩略语

下列缩略语适用于本标准。

EEA　欧洲经济区(European Economic Area)

EU　欧盟(European Union)

HLSP　高层安全策略(High Level Security Policy)

OECD　经济合作与发展组织(Organisation for Economic Co-operation and Development)

UN　联合国(United Nations)

4　本标准的结构

本标准的结构如下：

——第5章列出了国际文件中反映本主题的一些基本原则，并阐述了数据导入方和导出方、数据控制方和处理方这些主要角色；

——第6章概述了在本标准语境下合法传输个人健康数据的两个主要要求，即“同意”和数据保护的充分性，而本标准的其他部分则以此为基础；

——第7章详细论述了这两个主要的基本要求，确定了判断“充分性”的所有标准，深化了“同意”的概念；

——第 8 章要求数据导入方要有一个现行的高层数据保护策略，并对“高层”在本标准中的含义给出了解释；

——第 9 章针对高层策略给出详细的要求，这将确保充分的数据保护准则得到实施；

——第 10 章对数据导入方策略方面给出了详细要求，其中涉及保障数据处理安全的管理和技术手段；

——第 11 章论述了非电子形式的个人健康数据。

5 基本原则和角色

5.1 基本原则

本标准遵循以下基本原则：

——处理个人健康数据时，参与方应对自然人的有关隐私权的基本权利及自由给予保护；

——对数据主体而言，参与方的责任和义务应明确且透明；

——与确保安全一致，处理与之有关的个人健康数据时，数据主体应能够了解到并被告知该应用现有的安全措施、安全惯例和安全程序及其基本范围；

——应用及其相应的安全措施应当尊重所有相关方的权利和合法利益；

——应用的安全等级、费用、措施、惯例和程序应与该应用的价值和可靠度相当，并与该应用对数据主体潜在危害的范围、可能性及严重性相适应；

——为建立一个前后一致的安全系统，用于应用安全的措施、实践和程序不仅在其相互之间应协调和整合，而且还应与参与方的其他措施、实践和程序协调、整合；

——各参与方应及时协调以防止应用的安全遭到破坏，并能在破坏发生时及时做出反应；

——对与该应用相关的安全措施应定期评估；

——应用的安全性应与数据及信息合法使用和流动相适合。

5.2 角色

5.2.1 数据导出方和数据导入方

跨国的个人健康数据交换，需要数据导出方(2.15，下同)负责从一国发送数据以及数据导入方(2.14，下同)从另一国接收该数据，他们相互之间都有义务。

只有数据导入方符合本标准的相关部分时，数据导出方才能传输数据给数据导入方。

只有数据导出方符合本标准的相关部分时，数据导入方才能参与应用。

5.2.2 控制方和处理方

数据控制方(2.3，下同)有权决定处理的目的和方式，而处理方(2.12，下同)则代表控制方并依照其指示处理数据(见 2.13，下同)。作为应用中的各参与方，应被指明是控制方还是处理方。

6 数据传输合法化

6.1 “充分的”数据保护概念

本标准的基本理念是，要确保跨国传输个人健康数据得到“充分的”数据保护。

“充分的”保护既包括符合数据保护要求的管理和技术安全措施，同时还包含其他的重要事项。

当个人健康数据传输给其他国家时，数据主体有权得到导入方的尊重。数据主体认为其应享有权利的程度和性质，取决于他所定居的国家和文化。如果已知或怀疑数据导入方可能不尊重这些权利，数据主体应被完全告知，以便能够“同意”或不“同意”数据传输。另一方面，数据主体在某些情况下(即使从本标准方面来说数据保护可能不够“充分”)也会同意数据传输，如健康紧急时刻涉及其重大利益时。

数据主体希望个人健康数据在数据传输过程中能够得到保护，并且数据导入方接收数据时要采取“充分的”保障措施。这些保障措施包括管理安全和技术措施，如访问控制、数据完整性、审计追踪、数据准确性等。数据主体希望导入机构应任用能胜任并经过训练的处理个人健康数据的工作人员。他们希

望数据导入方采用了考虑到这些问题的安全策略。

数据主体有权知晓其数据的处理情况，并在必要时可访问这些数据，并有机会提出任何异议。

数据主体享有传输许可权，并享有关于传输的充分的知情权。

最后，数据主体若被数据传输侵害了权利，可以提出申诉，如有必要可由一独立机构对这一投诉进行公正地调查，若数据主体受损则在规定范围内以合理的方式赔偿数据主体。

本标准在提供“充分的”数据保护这一框架下讨论了所有这些问题。详细描述了“充分的”数据保护标准(第7章)和数据导入方应在实践中贯彻的“充分的”保护数据安全的高层安全策略的内容(第8章、第9章和第10章)。

6.2 合法传输的条件

6.2.1 同意

除保护数据主体切身利益所必要的传输之外，个人健康数据不应传输，除非得到数据主体明确的同意。

6.2.2 传输条件

除导入方能够确保充分的保护程度(见第7章)或符合下列条件中任一项外，个人健康数据不应传输给数据导入方：

a) 在知道存在保护措施不充分的情况下，数据主体明确同意进行相关的传输(应注意，尽管6.2.1要求在所有情况下都同意，但此处是要求这种同意应是各参与方都知道不充分的情况下还采用该条件，见7.7)；

b) 有关传输对于履行数据主体和控制方之间的合同或为了响应数据主体在形成合同前提出的请求而采取措施而言是必要的；

c) 有关传输对于控制方和第三方之间达成或执行符合数据主体利益的合同而言是必要的；

d) 有关传输基于重要公众利益考虑是必要的或法律要求的，或是为了证明、提出法律请求或为了就该请求进行辩护而言是必要的或合法的；

e) 为了保护数据主体的切身利益，有关传输是必要的；

f) 由合法注册方实施的传输，该注册方根据法律或法规向公众提供信息，并向一般公众或任何能证明其有合法权益的个人开放查询，前提是在每个特定情形下法律规定的查询条件得到了遵守；

g) 通过使用附录E和附录F所示例的合同条款，控制方提供足够保证的情况。

注：7.4要求在所有情况下“应用中处理的实施应由参与方之间所签订的合同来管理”，但对合同的形式无要求。然而如g)所示，应特别注意，需要确保该合同能涵盖数据保护方面的不足之处，以适用于补救、调查投诉等。附录E和附录F为此给出了示例。

7 个人健康数据传输的充分数据保护准则

7.1 充分数据保护要求

控制方不得传输个人健康数据给数据导入方，除非导入方能提供充分的数据保护。充分性有两大要素：

——内容原则：导入方在处理个人健康数据过程中，数据保护条款和相应责任的充分性；

——程序/执行要求：确保这些条款能在实践中遵循并确保数据主体权利的方式。

7.2 内容原则

内容原则见7.2.1～7.2.6。

7.2.1 目的限制、数据质量和相称原则

在应用的语境下，遵从7.2.7规定的豁免原则，个人健康数据应：

a) 被公正并合法地处理。

b) 特定、明确、有合法目的地传输且进一步处理方式不能与上述目的相冲突。

c) 对传输和/或进一步处理的目的而言是充分、相关且不多余的。

d) 准确，必要时更新。围绕传输或进一步处理目的，采取一切合理步骤，确保不准确或不完整的数据被删除或纠正。

e) 应以识别数据主体的时长不超过数据传输或进一步处理时长的形式保存。参与方可同意个人健康数据存储更长的时间以用于历史、统计或科研用途，前提是不对数据主体产生任何影响，但应告知数据主体相关协定。

7.2.2 透明原则

在应用的语境下，遵从7.2.7规定的豁免原则，应向数据主体提供以下信息：

a) 数据导出方、数据导入方及其代理(如果有的话)的身份；

b) 所传输数据的处理目的；

c) 对与其相关的应用中的任何数据享有的访问权和修正权；

d) 关于任何违背其权利时的责任、赔偿和制裁措施；

e) 数据的保留期限，特别是有关医疗的法律要求和关于数据主体死亡的任何政策的数据；

f) 有可能影响其是否同意该传输的任何因素；

g) 本标准规定的任何其他信息。

7.2.3 访问权、修正权和反对原则

在应用的语境下，遵从7.2.7规定的豁免原则，数据主体应享有以下权利：

a) 无额外延迟，无需费用，并在合理的时间间隔内不受限地获取：

——与其相关的数据是否正被处理的确认信息，至少含有处理的目的、包含的数据类别、接收(被透露)数据的数据导入方或数据导入方的类别信息；

——以可理解的形式，向其传输正在被处理的数据及其来源信息。

b) 有权对相关处理不符合本标准要求的数据进行修正、删除和阻止，特别是因为数据的不完整性或不准确性；

c) 将依据b)对泄漏的数据所作的任何修正、删除或阻止通知给已接收该数据的第三方，除非证明(该权利)不可能或不值得；

d) 由于其特殊情况，有权在任何时候反对处理与其相关的数据，一旦反对意见被证明合理，控制方发起的处理应不再涉及这些数据。

7.2.4 后续传输的限制原则

不允许原始数据传输的导入方进一步传输个人健康数据，除非第二个数据导入方能够提供与6.2及本标准的其他相关要求相一致的充分的数据保护。

7.2.5 安全原则

数据导入方应采取与处理中的风险相应的技术和组织安全措施。

7.2.6 特定情况下的附加原则

直接营销：当参与方以直接营销为目的而期望处理个人数据时，数据主体应有权对此提出反对(应需并无偿)；或有权要求在个人数据第一次被透露给第三方前或在个人数据被用于直销的目的前被告知，并有权被明确赋予权利无偿反对上述泄漏和使用。数据主体应被告知具有以上权力。

数据主体的死亡：数据主体死后个人健康数据的保密处理方式在各国立法中不同，如英国数据保护法案只适用于生者。然而在许多情况下，死者的健康记录可以揭示与其他个体相关的个人健康数据并损及他人。记录可能明确地提及其他个体，如死者的家庭成员。如果某一个体死于可遗传的基因缺陷，他的记录可能揭示有关其后代的问题。

应用中的各参与方应就死亡情形下的处理方法达成明确的协议。该协议可能取决于有关国家及其处理医疗记录的方式，如用于死后医疗记录保存时间长短的法律或条规。不同的所有权也适用于这种

情况，如患者是其记录的合法所有人，则死后此记录就可成为其部分遗产并遵从遗嘱。患者是否许可其个人健康数据被处理和传输给第三方可能取决于其死后这些数据将如何被处理，因此患者应被告知其死后关于处理这些数据的任何安排。

7.2.7 内容豁免原则

各参与方可豁免遵从 7.2.1、7.2.2、7.2.3 a)、b)和 c)原则，当豁免被认为必要并用于保障：

a) 国家安全；

b) 国防；

c) 公共安全；

d) 预防、调查、侦查和指控刑事犯罪或违反职业道德规范的行为；

e) 参与方所在国家重要的经济或金融利益，包括货币、预算和税务问题；

f) 与 c)、d)和 e)项提到的职权行使相关的监督、检查或监管职能；

g) 数据主体和权利的保护以及其他人的自由。

作为同意与否条件的一部分，当各参与方同意任何豁免时，数据主体应被告知，除非这种做法违反数据导出方的法律。

7.3 程序/执行机制

7.3.1 概述

即使“内容原则”是由个人健康数据处理、存储、传输等规则组成，除非切实遵照这些规范执行，否则就不能确保个体权利，如果不能保证其权利，个体应可得到有效的赔偿。

许多国际和各国文件，如经济合作与发展组织[1][2]、欧洲委员会[3][4]和联合国[5]的文件，涉及个体权利要求的本质一致，而其有效性的确保方式不同。

一些国家(如欧盟成员国)通过具有监测和信访职能的数据保护/保密专员或相应部门，以及法律规定的如责任、制裁和补救办法，确保有效性的方式在法律中得以体现。

很多国家和国际的指南和规则，在倡导相似的个体权利的同时，可能：

——不够全面；

——在法律上没有明文规定；

——没有涵盖与健康相关的所有部门，如可能只涉及公共部门。

因此，判断数据导入方是否提供了充分的数据保护要求司法和其他机制予以评估。这种评估应实现以下目标：

——提供遵守规则的良好水平(没有体系可以保证 100%遵守规则，但有一些体系会相对更好)。好的体系的特征通常是能使数据控制方高度意识到其义务和数据主体高度意识到其权利及相应的行使手段。有效的制裁和劝阻性制裁能够在确保尊重规则方面发挥重要的作用，由权威机构、审计机构或独立的数据保护官员进行直接核查的体系同样也发挥重要的作用。

——为单个数据主体行使其权利提供支持和帮助。能确保个体行使其权利时快速、有效并无过高花费。为达到此目的，应有某种机制能允许独立的投诉调查。

——当规则未被遵守时，为受害方提供充分的赔偿。这是一个关键因素，应有能独立判决或仲裁的体系允许支付赔偿并在适当时实施制裁。

7.3.2 确保遵守规则

确保遵守规则的方式是传输数据的控制方要求导入方处理被传输的个人健康数据应有明确的安全策略，这点包括：

——按本标准要求的组织和技术的安全措施以确保充分的数据保护；

——确保政策能得以遵守的措施，包括违规情况下的惩罚或制裁。

第 9 章、第 10 章和第 11 章对此政策的要求有详细说明。

7.3.3 提供赔偿

对于任何不符合本标准规定而蒙受损失的数据主体应能获得适宜的赔偿。

这一点最好由合同方式达成，下面给出了三种示例[8]。

方法一是数据导出方限制数据导入方仅为合同中的附属处理方，没有自主决策权。数据导出方，作为数据控制方，将详细规定该处理方的权限和职责。因此数据导出方对数据传输负全责，对于任何一方造成的损失，都由数据导出方自动承担其国家的法律责任。因此数据主体要求赔偿的权利可不比违规发生在其所在国时少。然而有些情形经常发生，如远程医疗共享电子病历时，导入方不仅仅提供数据处理服务。数据导入方认为合适时自主处理数据是必要的，因此也成为控制方。在这种情况下，要求有进一步的保护措施。

方法二是数据导出方与数据主体单独建立合同，规定数据导出方仍将承担数据导入方行为所造成的任何损失。如该合同在从数据主体获得数据时就建立，并在之后处理传输的问题。

这两种方法都是在数据导出方想追回向数据主体所支付的任何损失赔偿时，由数据导出方追究数据导入方违约的责任。

方法三取决于各国涉及合同的法律体系。有些法律体系允许第三方（非合同方）根据合同条款请求权利。在数据导出方和数据导入方之间有公开成文的合同的情况下，这就能提供令人满意的主体权利。

作为同意传输的一部分，数据主体应被告知其获赔偿权。

7.3.4 对数据主体的支持和帮助

数据主体有权对侵犯其权利的行为投诉，要求客观调查，包括当其投诉得不到解决时，有权要求独立的主管机构调查和/或仲裁。

例如许多国家已经合法成立的机构，有权监督其（如数据保护专员们）是否遵守数据保护法并有权调查投诉。如果某国数据主体能合法促使某数据导入国的这种机构进行调查，那么这就能构成符合独立调查要求的方式。

也可通过合同条款中数据导入方允许数据主体所在国的数据保护专员（或相应的机构）对投诉进行调查（如有必要通过导入方所在国机构）来形成相应的机构机制。

另一种方法是数据主体和数据导出方之间签订合同，一致形成数据主体可以合法援用的调查机制。

数据主体应被告知享有投诉并获得调查的权利。

7.4 合同

应用中处理的实施应由参与方之间所签订的合同来管理，即使数据导入方是唯一的处理方。

从本标准的广义上来看，合同的范围和内容取决于体现数据导入方所需要的数据保护充分性的程度。

数据导入方仅作为处理方时，该合同可能主要致力于将处理方与控制方/导出方捆在一起，确保处理方只遵照控制方的指令行动。当数据导入方是控制方时，其责任范围会更大，因此更加需要在合同中明确导入方对导出方的保证。

7.5 优先法规

国家的一般法或特殊法可能包含（在特殊情况下）数据导入方向另一方（如警方、法院、安全机构）透露数据的要求。这些法律可能凌驾于合同条款之上，因此在某些情况下，数据控制方向数据主体泄露其数据访问已被用于诸如警方调查等事件，此行为可能违法。7.2.7 中阐述了哪些情形下会发生对权利的限制。

数据主体应被告知可能产生的后果，任何这样的法律或国家惯例至少要在 7.2.7 所列出的范围内。如有疑问应明示。如法律允许，一旦发生例外访问应尽快告知数据主体。

7.6 匿名处理

7.6.1 概述

跨国传输个人健康数据的解决方案可以使其非个人化。应在本标准给出的个人数据定义的语境下

实现数据非个人化。

7.6.2 数据非个人化

本标准定义的个人数据是“任何涉及已标识或可标识自然人的信息”。可标识的个人是“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来标识的个人”。

数据非个人化通常被称为匿名处理。然而对匿名处理的理解各不相同。本标准中“匿名处理”是指本标准中“个人数据”定义语境下的数据“非个人化”。“可标识的个人”包括可“间接”由“一个或多个具体因素”标识的个人。显然这些因素不仅仅包括姓名和地址。数据主体可由任何一个或多个因素来标识,如年龄、性别、种族、职业、邮政/邮递编码、收入群体、心理或精神状态、家庭特征等。此外在一些健康应用中,如影像、牙齿记录、放射影像或脑电图扫描,都有详细记录单独或与其他数据(如专业和/或健康组织的特性)一起,使数据可标识到个人,从而作为个人数据。

这些数据元素的组合可能使被视为纯统计意义的数据个人化。邮政/邮递编码提供了在一个小群体中定位个体的有效途径。类似的事情也可通过小概率事件发生,如即使在一个大的地理区域内怀有三胞胎的妇女仍然极少。

数据非个人化要求注重大量的细节。如有足够的资源并能访问其他的相关信息,数据库推理问题在理论上总是可解的。然而,充分的匿名处理通常是通过保留明显的可标识信息,并确保数据导入方不重新标识个体或不透露超出所同意使用目的要求的匿名信息来实现。

相应地,考虑到公共领域中的资源以及其他数据库的引用,有关健康的统计信息通常会泄露个体身份。显然,基于涉及数据所需安全性和敏感性的概念的准则需要用于这些统计(见 5.1 第 5 项)。

任何向数据主体所作出的数据非个人化的保证应明确其身份被泄露的风险,并与实现该保证所需努力的程度相对应。这种资源的范围和花费将因技术进步而随时间变化。

7.7 同意的合法性

见 6.2.1 和 6.2.2 提及的“明确同意”。

“同意”需是“自主给予、具体并知情”(见 6.2.1)。“明确同意”应在了解所有相关情况的基础上,尤其是不予同意时所得到的权利会被削弱的情况。因此数据主体需要了解的不仅仅是个人健康数据跨国传输,也应了解所承担的(风险)。应注意,针对一种用途的同意不代表也同意另外一种。

当寻求数据主体明确同意时,应提供本标准具体指出的信息及其他影响其决定的任何信息。

注:本标准没有具体说明同意是否是隐含的还是明确的,或是否应成文或同等形式。本标准也没明确指出当数据主体因任何原因无法给出实质性的同意时应采取何种措施。这些问题可能在数据导出方所在国的国家级规章中有具体规定或是该国文化或风俗的问题。对于这些方面的考虑是,应在适用于数据主体的任何规章、习俗或文化的氛围下,由数据主体依照其期望给予同意。

8 安全策略

8.1 概述

数据控制方传输个人健康数据到另一国时,需要保证数据导入方已经采取必要的组织和技术方面的安全措施来充分地保护传输的数据,如涵盖保密性、完整性和可用性的一种充分的安全策略。以下章节给出了关于数据传输保护的要求,一般性安全管理的细节参见 ISO 17799(参见附录 C)。

作为控制方的数据导入方,应采取适当的安全策略以达到:

——确保数据控制方和数据导入方之间形成的合同条款(见 7.4)被满足;

——符合本标准第 8 章、第 9 章、第 10 章和第 11 章的规定。

仅作为处理方的数据导入方,应采取适当的安全策略以达到:

——确保其和数据导出控制方之间形成的合同条款(见 7.4)被满足;

——符合本标准第 8 章、第 9 章、第 10 章和第 11 章的规定。

8.2 安全策略的目的

适用于数据导入方的安全策略的目的是：

——向数据控制方导出数据提供保证；

——为数据主体提供保证，即数据导入方将满足本标准的规定。

8.3 安全策略的“层次”

本标准给出了用于数据导入方高层安全策略的指南。8.4.6 给出了“高层”含义的说明。

8.4 高层安全策略的一般性问题

8.4.1 确保安全性的抽象层次

安全性可从四个不同的层次[9]来看，见图 1。本标准关注的是高层策略。该图和以下章条将说明“高层”含义所包含的内容。

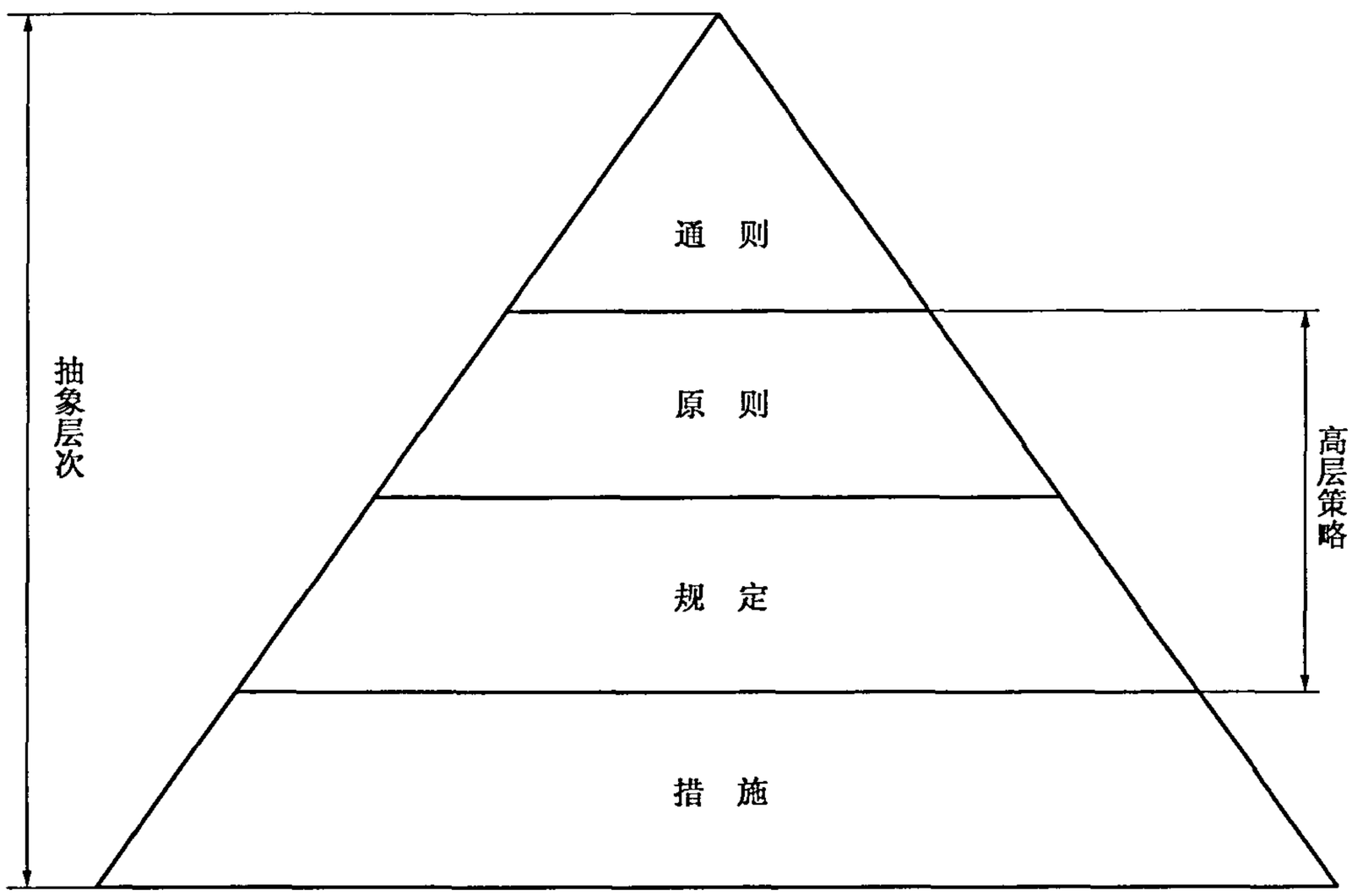

图 1 抽象层次

8.4.2 通则

“通则”源于能体现人权和隐私的社会文化环境。这种权利如何体现，世界各地各不相同。例如 EU 数据保护指令[6]源于西欧的民主文化，特别是 EU 成员国。因此它源于《欧洲保护人权和基本自由公约》[10]所包含的一种情形。后者不是仅适用于 EU 或仅适用于欧洲。世界其他地区可能也有其他高于或等同水平的公约。

其重要性是通过像“优先法规”(见 7.5)一样的事情来证明。以 EU 数据保护指令允许 EU 成员国限制权利和义务的范围为例，此时指令所考虑的情形如：保障国家或公共安全、国防、刑事犯罪的调查、成员国的重大经济或金融利益的需要(见 7.2.7)。其他国家也可有类似的法律条款，可超越任何组织机构的数据保护规则。这里的“优先法规”可能基于不同的人权观念，也可能不同于和/或更广于导出方所在国相关法律。这些问题将在获得传输同意时得到解释，并能在组织安全策略中得到体现。

8.4.3 非通用的原则

当通则需要在特定的国家或地方的行政环境中考虑时就产生了具体“原则”。例如，这些原则是针对特定机构的，但会受到通则的影响，如受到机构所在国家的文化或立法影响。

8.4.4 规定

“规定”源于“原则”，是为了满足特定的原则所要遵循的特定操作步骤。它们指出满足原则应做的

事而不指出具体如何去做。

8.4.5 措施

当“规定”在特定环境中考虑时就产生了“措施”。它详细地规定了遵循规定应做的事。

8.4.6 高层安全策略要素

高层安全策略应包括中间的两个抽象层:原则和规定。

高层安全策略应以“通则”为基础,并在特定的机构中依据特定的“措施”来补充。

本标准关注的是高层安全策略的指南,而措施与组织紧密相关,因此不具体给出“措施”的内容。然而,对应支持规定的措施提出了指导性意见。

9 高层安全策略的内容

9.1 原则一 首要通则

作为首要通则,HLSP 应明确其应用的个人健康数据不是来自导入方所在国时,数据主体的权利应得到与本国相同范围的保障。

9.1.1 规定一 基本权利和自由

应基于对数据主体的首要基本权利和自由的考虑,由数据导入方来决定其期望 HLSP 中应包含来自数据控制方的何种声明。该声明应包含在 HLSP 中。例如,导出方所在国是欧盟成员国时,则参照欧洲人权和自由保护公约[10],以及 EU 数据保护指令[6]。

HLSP 应以保障导出方规定的这些权利为目的。

9.1.2 规定二 质疑信息

如有任何关于基本权利保障的疑问,都应告知数据主体使其在充分知情时作出同意或其他决定。

9.1.3 理论依据

并不是所有的国家都同意人权和自由宣言,因此导入方所在国可能有与数据主体的期望不一致的优先法规或法案。例如,公共权威机构有可能在数据主体不同意时访问病例。一旦被知晓或怀疑,数据主体都有权了解并决定如何处理。

9.1.4 措施建议

数据主体关于权利和自由最高期望的应给出简短声明。如以 EU 数据主体为例,所有工作人员应了解 EU 指令的要旨。

9.2 原则二 主管方支持

该 HLSP 应由组织机构的主管方签署,任何有需要的数据主体或其他合法查询人都能免费获得。

9.2.1 规定一 符合本地实际

在实践中,该 HLSP 应与数据导入方所在机构的一般数据保护策略一致。否则,应明示。

9.2.2 规定二 组织安排

导入方机构应建立一个适当的组织结构来支持 HLSP。

9.2.3 规定三 定期复审 HLSP

应定期对 HLSP 进行复审,间隔时间不得超过两年。

9.2.4 理论依据

主管方不支持的策略不一定能确保得到全体工作人员遵守,也不一定能要求数据主体尊重。与一个机构的总体实际严重脱节的策略和措施更有可能不被遵守。

9.2.5 措施建议

对 HLSP 的签署仅有主管方的签名是不够的,还应有主管方的评价,最好还有其个人意见。

如有高级临床工作人员如医疗主管的附加签署则更好,这可通过“措施”来实现。

9.3 原则三 措施的文档化和复审

HLSP 应由成文的措施来支持以确保遵守“原则”和“规定”,并应定期复审且间隔时间不得超过

一年。

9.3.1 规定一 工作人员信息

合理构建措施以便接收它们的工作人员应用。

9.3.2 理论依据

工作人员需要明确知道要做和不要做的。措施应被调整以适合相关工作人员贯彻执行，如适用于临床工作人员的措施可与管理人员的措施无关。大部分工作人员不需要了解大多数技术安全措施的确切细节。

9.3.3 措施建议

措施以业务守则的形式成文较实用。

9.4 原则四 数据保护安全官员

应单独任命数据保护安全官员以确保 HLSP 得到遵守并有相应的“措施”支撑。

9.4.1 规定一 数据保护安全官员和作为处理方的数据导入方

当数据导入方仅为个人健康信息处理方时，数据安全保护官员应确保数据处理要按照传输数据的控制方的规定来执行，并符合管辖这些规定的合同。

9.4.2 规定二 数据保护安全官员和作为控制方的数据导入方

当数据导入方本身也是控制方时，个人健康数据的处理界限应明确指出，并得到导出数据的主要控制方的认同。数据保护安全官员应确保遵守这些规定。

9.4.3 规定三 数据保护官员的岗位资格

数据保护安全官员应具备保护个人健康数据安全的必要技能和经验以承担其职责，还应有主管方或相应权威人员的授权。

9.4.4 理论依据

处理个人健康数据的导入方机构需自行决定必要的处理目的和方式。例如，在远程医疗/远程会诊中作为导入方的临床专家在与其他专家会诊时要求拥有最大的决断力，以适当的电子或纸质病例的形式保存结果以便其他授权人员访问。这种情况下通常要求该专家或该组织机构充当控制方而不仅仅是处理方。

数据保护安全官员要求来自最高管理层的授权。最好是主管方的授权，但其他方面（如医疗总监）的授权也可能满足要求。

9.4.5 措施建议

数据保护安全官员应有明确的参考条款，其审计和违规调查的授权应在“措施”中予以明确。

9.5 原则五 处理许可

除 7.2.1 所允许的外，如不能确保数据主体恰当同意（见 6.2.1 和 6.2.2a））就不能进行数据处理，且只能按照这种同意来进行该数据处理。

9.5.1 规定一 明确同意传输

（导出数据的控制方）应恰当确保数据主体“明确”同意传输其数据到导入方所在国，并同意其处理健康数据。

9.5.2 规定二 限于同意的目的

个人健康数据的处理应限于获得同意的目的。这些目的应当成文。

9.5.3 规定三 有条件同意

如果任何数据主体是有条件同意，而且这些同意条件被数据导入方所接受，那么这些同意条件应与个体的个人健康数据相关联并有“措施”来确保符合这些条件。

9.5.4 规定四 同意信息的复审

（作为）获取知情同意过程中（的一部分），提供给数据主体的信息应在相关“措施”中予以明确。这些信息应定期复审，且间隔时间不超过一年，以确保信息的正确性和没有其他应当补充的信息。

9.5.5 理论依据

数据主体对于传输他们的个人健康数据必须给出明确的同意，除非传输是在与数据主体生命攸关的情况，如紧急救治(或急诊)。

同意应以知情为前提。因此如同意要想有效，则应向数据主体提供所有的相关信息，且需由数据导入方提供大量的这些信息。为此提供的任何信息都应成文，并保持更新。这些信息应包含以下问题，如：

——允许外界权威机构访问数据的优先法规或习惯做法，如执法机构或公共安全机构、外界临床审查或调查；

——缺少哪些与隐私相关的职业道德准则；

——本标准语境下数据保护不充分时，确保充分数据保护还应采取的措施。

数据导入方不清楚这些问题(如优先法规或习惯做法)时，应使其了解这些问题。

9.5.6 措施建议

如果任何条件都围绕“同意”展开(都以同意为中心)，则这些条件应在相关措施中得以反映。这些措施应确保处理是限于给出同意的目的下(处理是依据给出同意的目的)。

9.6 原则六 对处理知情

应依照本标准以确保数据主体对处理的知情权、数据质量的获保障权、访问其个人数据以及反对处理的权利。

9.6.1 规定一 将经同意的处理文档化

数据主体同意处理个人健康数据的目的应明确成文，不应发生不符合这些目的的处理。

9.6.2 规定二 数据收集和处理的质量

对于数据主体所同意的目的而言，个人健康数据的收集和处理应是充分、相关且不多余的。

9.6.3 规定三 数据处理的准确性

应采取措施以确保个人健康数据的收集和处理准确并在必要时更新。

9.6.4 规定四 数据保存和销毁的策略

应有向数据主体交流数据保存和销毁策略的机构，该策略应与数据主体所同意的目的相符，包括个人健康数据用于处理的时间不应超过在数据主体同意的目的下所需要的时间。

9.6.5 规定五 数据主体对本人数据的访问

对于数据主体对本人数据访问的要求应做出识别和安排，并确保这些访问任何法定时间段得到允许且无需额外费用。

9.6.6 规定六 对处理的反对

数据主体有权反对与其相关的数据处理，如反对合理，对该数据的进一步处理应应数据主体的要求停止。

9.6.7 规定七 修正，删除和阻止

数据主体认为其数据不准确或不完整，或本标准的规定和/或任何数据导入方的保证未被遵守时，数据主体应能要求其个人健康数据被修正、删除或阻止。

对个人数据持有异议且不能得到客观解决时，数据主体对这些数据的看法应被记录下来并与该数据主体的其他个人数据一同处理。

9.6.8 规定八 传输数据标识

所有传输给导入方的个人健康数据都应进行同样的标识。

9.6.9 规定九 数据主体死亡的通告

关于数据主体死亡的通告，应执行 7.2.6 所要求的协议。

9.6.10 规定十 直接营销

未经数据主体明确同意，个人健康数据不得用于直接营销。

9.6.11 规定十一 非个人化数据再次个人化

如果个人健康数据是在其本身为非个人化健康数据(匿名数据,见 7.6)的基础上传输给导入方时,应采取措施,确保其身份没有偶然或故意(有意或无意)因任何处理(包括与其他数据集的关联)而泄漏。适当时应制定应对"小概率"事件的策略。

9.6.12 理论依据

数据主体给出同意的目的应成文,以便提供给任何相关工作人员,并确保不用于其他目的。在医疗保健机构如医院,个人健康数据可能经常被用于国家或地区机构的审计、统计、财务或统计报表,第三方补偿,公共卫生部门疾病监测。这些都不适用于数据传输的目的,除非数据主体另外同意,否则需采取措施以避免(个人健康数据)不知情地被用于这些目的。

不能期望工作人员遵守 HLSP 及支持 HLSP 的"措施",除非他们知道使用中的数据受到特别限制,因而同样需予以标识。

个人健康数据的保留时间不得超过数据主体所同意目的所需时间这一要求可能会引起一些问题。导入国可能要求保留病例至少一段时间。数据导入方可能希望有充分时间保留含有个人健康数据的记录以用于统计、审计并以防法律质疑或投诉。倘若如此,则应获得数据主体对这些目的的同意。

如果数据主体死亡,删除其数据时,除非事先取得另外同意,否则就可能会产生同样的困难。因此需要有明确的数据保管和销毁策略。

数据主体对与其相关的、正被处理的数据的知情权可能会引起困难,除非该数据已经被事先处理。例如,在医院,个人数据可能由许多部门系统和记录保有,除非医院有全面的电子病历系统,否则会导致追踪困难。

同样,如果由于法医学要求保留所有数据供审计和投诉调查,删除数据这一要求可能无法执行。这一点应在数据主体给出同意时予以告知。因此,恰当的方式是除因重要法医学目的而进行受控制的访问外,对数据进行存档并阻止任何的进一步处理。

9.6.13 措施建议

"措施"需含有用于快速处理数据主体访问要求的步骤以及用于数据主体死亡后需遵循的程序步骤。

"非个人化数据"的保障措施取决于风险程度。存在充分的技术处理有关"推理"的小概率问题[9]。

9.7 原则七 提供数据主体信息

应向数据主体告知数据导入方的身份、处理目的;其个人健康数据可能或将被传输的任何其他方;其反对处理的权利;投诉程序;第三方仲裁和调查安排;投诉权及如何投诉;可能影响数据主体同意的任何信息。所提供的这些信息应成文并予以保存。

9.7.1 理论依据

虽然很多这些信息是来自数据导入方,但应由传输数据的控制方负责向数据主体提供这些信息。应特别指出的是,需要向数据主体提供所有可能影响其数据传输同意决定的信息。因此数据导入方有责任全面考虑所有数据主体不希望的、可能会影响其隐私和基本自由的所有情况。

个人健康数据导入方的类别包括除临床医生和健康专业人员以外的其他人员,如财务管理结算人员或数据录入文秘人员等。

9.7.2 措施建议

"措施"应包括所提供信息的定期复审,时间间隔不超过一年。

9.8 禁止未经同意的数据传输

除非是有必要为保护数据主体或其他人的切身利益,且仅当数据主体不能亲自或合法同意时,否则未经传输数据的控制方和数据主体许可,个人健康数据不得从数据导入方传输给另一方。收到这些数据的任何其他方,除仅用于传输目的外,应提供充分的数据保护。

9.8.1 规定一 确保传输安全

应在本标准语境下判断“其他方”所提供的数据保护的充分性。

9.8.2 规定二 用于进一步传输的 HLSP

“其他方”应遵守或执行符合本标准的 HLSP。

9.8.3 规定三 公开注册

对于数据传输给其他方应公开注册和维护。

9.8.4 理论依据

如果个人健康数据再传输给另一方,数据主体会期望所得到的数据保护不被减弱。

可能经常会出现这样的情况,临床医生希望征求另一家机构同行的意见。如果与特定同行/机构的进一步会诊属于常规做法,则此时该“其他”机构应完全遵守其 HLSP。然而,如果该会诊只是偶尔发生,而且参与人员只限于一两个较少的次要专业人员时,虽然也是正式行为,则会诊即可。

任何情况下都要求有数据主体同意。但是并不一定总能预知需要的是什么的“其他”机构的其他医疗专家来参与会诊。在这种情况下,为满足数据主体所同意的处理目的所需,各类人员(如来自其他机构的其他临床医生)应寻求数据主体的同意。但不得滥用,且任何隐私风险应予以说明。

如果“其他方”是,或可能是在非导入方所在国,那么将考虑更多且复杂的因素。一开始为数据导入方所设立的充分数据保护可能无法适用。如数据要从某国家的一个州传输到采用不同数据保护法的另一州时,就是这种情况。

9.8.5 措施建议

如果要传输个人健康数据给另一方,“措施”中应包括需遵循的程序。

9.9 原则九 补救和赔偿

对于任何侵权行为,数据主体有权要求司法的或其他相当的补救,并有权要求赔偿由此造成的任何损害。

9.9.1 规定一 调查投诉

应有向数据主体公开的,独立于数据导入方的投诉调查机制。

9.9.2 规定二 独立仲裁

对未解决的争议,应有向数据主体公开的独立仲裁机制。

9.9.3 理论依据

这些机制是建立充分数据保护的必要部分。这些机制可能较复杂但应成文,并以使数据主体能理解并知道该机制如何及何时可启用的语言和形式提供给数据主体。

这些成文的机制应包括当个人健康数据传输给可导致违反权利的另一方(如在别的机构与别的医疗专家会诊)时应有的暗示或限制。

9.9.4 措施建议

与此原则相关的“措施”通常需要法律介入。

9.10 原则十 安全处理

应保护个人健康数据免遭意外或非法破坏或意外丢失、改动以及未经授权披露或访问以及任何非法处理。

9.10.1 规定一 风险分析

安全措施应与风险评估相适合。

9.10.2 规定二 传输过程加密处理

个人健康数据在数据导出方和数据导入方之间的传输应加密。

9.10.3 规定三 数据完整性证明和源鉴别

个人健康数据在数据导出方和数据导入方之间的传输应服从于保证数据完整性和源鉴别的安全服务。

9.10.4 规定四 访问控制和用户鉴别

个人数据的处理应有有效的访问控制,应对系统用户进行恰当鉴别。

9.10.5 规定五 人身和环境安全

应遵守有效医疗保健的要求采取有效的人身和环境安全措施。

9.10.6 规定六 应用管理

对所传输的个人健康数据进行处理的所有应用都应由具备相应知识和能力的人来管理。

9.10.7 规定七 网络管理

由导入方直接控制的网络和个人健康数据的传输都应由具备相应知识和能力的人来管理。

9.10.8 规定八 病毒监控

应安装有效的病毒监控工具,防止恶意软件对所传输的个人健康数据或相关系统处理数据的完整性造成危害。

9.10.9 规定九 违反安全报告

与被传输的个人健康数据相关的所有工作人员和信息系统用户应学会识别并向数据安全保护官员报告违反信息安全的事件。如有涉及数据主体的数据推理,应明确数据导出方和数据导入方对数据主体各自应承担的责任,相应的处理措施也应予以明确。

9.10.10 规定十 业务连续性计划

如处理系统发生故障,数据导入方应进行相关安排以保障继续完成对个人数据的处理。

9.10.11 规定十一 审计跟踪

对所有被传输的个人健康数据应有可防篡改的审计跟踪。

9.10.12 规定十二 处理特别敏感的数据

个人健康数据特别敏感时应进行严格的风险评估,并严格执行任何必要的特别措施。如个人基因数据以及与性传播疾病有关的数据(见附录 G)。

9.10.13 理论依据和措施建议

涉及安全处理的理论依据和措施建议详见第 10 章。

9.11 原则十一 工作人员和其他承办方的职责

所有工作人员和为数据导入方工作以及参与处理传输个人健康数据的其他承办方应被告知其职责并能履行其职责。

9.11.1 规定一 告知工作人员和其他承办方

参与个人健康信息处理的工作人员和其他承办方应被告知 HLSP 并提供能使其遵守 HLSP 的“措施”。

9.11.2 规定二 指导和培训

参与个人健康数据处理的工作人员和其他承办方应接受与自己职责相对应的指导和/或(亦或)培训。培训材料应定期复审,间隔时间不超过一年。培训应在恰当的间隔时间内重复进行。

9.11.3 规定三 工作人员和承办方的合同义务

工作人员和承办方遵守“措施”以执行 HLSP 的义务应写进雇佣合同或合同条款中。

9.11.4 理论依据

工作人员可能受过关于数据保护的一般指导或培训。但是参与个人健康数据传输的工作人员还应了解任何相关附加或改进的程序。

9.11.5 措施建议

应建立一个可用来充当培训文件的简要说明性文件。

10 “原则十 安全处理”的理论依据和措施建议

10.1 概要

原则十(见 9.10)要求数据导入方保护数据免遭“意外或非法破坏或意外丢失、改动以及未经授权

被披露或访问以及任何非法处理”。

这些要求也适用于网络数据传输的处理。

导入方(如处理个人健康数据的健康机构)可能已经有保护这些数据的措施。然而这些措施应予以复审检查,确保其遵守本标准和传输该数据的控制方的要求。

“措施”应与处理中存在的风险和待保护数据的性质相对应。为确保“措施”能针对相应的风险,应进行正式的风险评估。

由于为“原则”规定对应的详细“措施”(见 8.4.6)不在本标准范围内,因此本章中以下各建议不应被视为是管理和技术“措施”所需的完整或充分说明。

“措施”应满足传输数据的控制方的要求。

10.2 传输到数据导入方过程中的加密和数字签名

考虑到实施的技术和费用,数据导出方和数据导入方之间个人健康数据的电子传输应以能确保完整性和鉴别的方式予以加密和数字签名。

加密算法的强度应与风险相对应,并可能受相关国家法规的限制。有些国家出于执行法律或国家安全的目的可能要求密钥第三方托管或依法获取密钥。对此数据主体应有所了解。

10.3 访问控制和用户鉴别

信息系统中所存个人数据完整性的一种控制方法是对所有的数据输入、编辑、处理以及所有需记录和审计的活动都进行有效签名。依据时间和地点进行物理控制是第一道防线,但还要求身份证明,以避免发生未授权的活动。病程记录签名就是出于类似的原因。

密码是访问控制和用户鉴别最常用的设置,但这是最低级形式的鉴别。采取如 CEN ENV 12551(参见附录 C)中详述的要求可能会使控制更有效,更有效的智能卡和生物识别系统正在逐渐可行,这些也应当给予考虑。数字签名也能用于确保信息不被篡改,并确保发送信息的个体经过鉴别。

10.4 审计跟踪

要保证数据主体的独立调查权,防篡改的审计跟踪将必不可少。需要强有力的“措施”来支持赔偿诉讼或制裁的法律活动。如有可能,宜只有数据安全保护官员才能访问这些审计跟踪。

10.5 物理安全和环境安全

需有物理安全以阻止不需要访问系统的人员访问系统,并确保已采取措施以防止、减轻或恢复如水灾、雷电、电力故障(断电)、抢劫等事件的影响。也需有充分的环境措施以确保系统能在指定的环境条件范围内持续工作。

10.6 应用管理和网络管理

详细的技术支持可由外部机构提供,但是地方管理部门应有权了解所有应用系统的人员以及能够应对基础培训、管理和故障排除的人员。支持措施应包括充分的应用文献和培训材料。这一点适用于应用和网络。网络配置和防火墙管理是系统安全的重要方面。

10.7 恶意软件

恶意软件攻击是对信息系统和网站攻击的最常见的一种形式。和导致拒绝服务一样,这种攻击可以摧毁或损坏机构所持有的个人健康数据。应以每月不少于一次的频率进行控制更新。

10.8 安全漏洞

数据安全保护官员有权访问关于当前安全问题的材料,并了解导入方所在组织机构的一些关键问题。然而除非贯穿整个组织机构的安全漏洞细节被重点报道,否则将没有人完全了解该机构所面临的隐患并着手解决这些隐患。

在培训计划中纳入安全漏洞报告的要求会有益,且报告应以不具威胁性为基础从而鼓励报告,至少其中一些报告将仅采自于操作方的失误。

10.9 业务连续性计划

即使处理设施遭受灾害被毁,机构也有必要能持续开展业务,如患者的诊断和治疗。如有灾难出

现,则需要有明确的能解决问题的灾难评估,需要拟定、测试可供使用的合适计划并记录成文。问题出现后再制定计划会为时已晚。各种系统故障的后果应成为风险分析的一部分。发展业务连续性计划是针对其当前所承担的处理的重要项目。应当定期予以测试和更新。

10.10 处理特别敏感的数据

尽管所有的个人健康数据都敏感,但数据主体会认为有些数据额外敏感,如涉及性传播疾病、人工流产的数据等。患者的诊断和治疗中基因/染色体组信息的日益使用,以及出于警方和安全目的对这些信息的使用,要求特别保护这些数据的安全,避免不当泄漏。欧洲委员会第 R(97)5 号医疗数据保护建议书中包含关于处理个人遗传数据的最新建议。然而这仍是个当前研究活跃的领域。

一旦怀疑个人健康数据有可能对数据主体特别敏感,应就任何可能存在的额外安全预防措施的性质向数据主体咨询并执行经数据主体同意的额外安全措施。附录 G 提出了关于哪些数据可被视作“特别敏感”的意见。

10.11 标准

对于跨国电子传输个人健康数据宜参照 ISO 和 CEN 安全标准。附录 C 列出了可应用的标准。附录 D 列出了其他有用的意见来源。

11 非电子形式的个人健康数据

非电子形式的个人健康数据也应遵守本标准。例如非电子形式的个人健康数据只能在数据导出方和数据导入方之间以能提供应对风险的安全模式传输。这也许会要求安排特别信使。

应指出的是,非电子个人健康数据除了纸质以外,还可采取其他形式,如放射线照片、心电图、标本,这些数据需要同样有效的物理安全。

附 录 A
（资料性附录）
数据保护的主要国际文件

A.1 欧盟数据保护指令

欧盟国家最重要的数据保护文件是“欧盟数据保护指令”[6]。该指令的两个目标是保护自然人的基本权利和自由、促进个人数据在该指令保护下的自由流动。

A.1.1 覆盖范围

指令提及健康数据，但其规定是普遍的，涵盖所有部门和应用，无论是私人的或公共的。适用于手册、纸质文档和电脑记录。个人数据包含任何可直接或间接用于可识别人员的信息。如：通过一个或多个个体的特定因素，如身份证号码，物理特性，居住地的地理标识等。

A.1.2 合法处理的规定

个人数据必须：

——公正和合法地处理；

——对处理目的而言是充分、相关且不多余的；

——准确并保持更新；

——仅在处理目的所需时间内可识别；

——收集时要有具体、明确、合法目的，且不做与这些目的不符的进一步处理。

个人数据可在某种条件下被处理，如：仅当

——数据主体（给出）“明确同意”；

——或数据主体应是合同的当事人；

——或应遵守法律；

——或为了保护数据主体的切身利益；

——或为了执行实现公共利益的任务。

A.1.3 特殊的处理类型

有一些例外，成员国应禁止在处理个人数据时泄露：

——种族或原籍裔系；

——政治见解；

——宗教或哲学信仰；

——工会会员身份；

——有关健康或性生活的数据处理。

本附录最重要的特例是在第8章第3条，其中指出：

“禁令不适用于下述数据处理目的：

——预防医学；

——医疗诊断；

——提供护理或治疗；

——医疗保健服务的管理；

——按照国家主管机关建立的法律或法规，这些数据被承担保密职责的健康专业人士或承担同等保密职责的其他人来处理。”

成员国必须“确定在何种条件下的国家身份证号码或任何普遍适用的其他标识符可以被处理。”

A.1.4 数据主体的权利

收集数据时，应向数据主体至少提供以下信息，包括：

——拥有和控制该数据处理的团体身份；

——处理目的；

——数据接收方，或数据接收方及数据的类别；

——保证处理公正的其他信息。

如被处理的个人数据并非采自数据主体，仍应向数据主体提供该信息。特殊情况例外，如处理是用于统计或具体研究、且若向数据主体提供有关信息则耗费巨大时。

数据主体有权知道他/她的数据是否正在被处理，如果是，是什么数据，用于何种目的。如果该处理不符合指令，数据主体有权要求清除该数据或阻止该处理。在这种情况下已经被提供数据的第三方必须被告知且必须清除和阻止处理，但当这样做耗费巨大时则可例外处理。但是当数据被用于统计和科学研究的时，访问的权利可能会受限，如指令中第 13 章第 2 条中指出：

“受充分的法律保护，尤其当数据不是被用于采取措施或涉及任何特定个体的决定时，在明显不存在泄漏数据主体隐私风险的情况下，成员国可能通过立法措施限制第 12 章规定的访问权。”

A.1.5 安全处理

第 17 章规定了关于安全的义务。第 1 条规定：

“各成员国应规定控制方需执行适当的技术及组织措施，以保护个人数据免遭意外或非法破坏或意外损失、改动、未经授权的披露或访问，特别是涉及通过网络传输数据的处理和所有其他非法形式的处理。

重视技术发展水平和执行成本的同时，这类措施应确保安全级别与处理所带来的风险和待保护数据的特性相适应。”

以数据控制方名义进行数据处理时，处理方应“以书面或同等的形式”提供相同的安全保证。

A.1.6 监督机构

每个成员国应有一个独立的公共监督机构负责监督该指令的执行情况，通过该机构任何人都可提出其权利保护的“要求”。该机构必须具有调查权和有效的干预权。数据控制方应在数据处理前通知该监督机构。在某些情况下通知可由成员国简化或免除，如任命独立的数据保护官员以确保执行该指令并记录处理操作。通知的具体内容至少应含有计划/打算给第三方的任何传输。

A.1.7 补偿和制裁

对于任何违权行为，如果造成伤害，数据主体应可以从数据控制方获得“司法补救”。

A.1.8 传输个人数据给第三国

指令第 25 章要求各成员国不得向第三方国家传输个人信息，除非该国确保充分的保护（级别/水平）。第 2 条规定：

“第三国提供的保护（水平的）充分性应从数据传输操作或系列（数据传输）操作的所处环境予以评估，尤其对有问题的第三国，应从全面和局部两方面大规模地考虑数据的性质、计划处理操作及系列操作的目的和持续时间、数据原发国及最终目的国、法律法规以及与该国相符的专业规则和安全措施。”

如果欧盟委员会认为第三国没有充分的保护措施，可以要求成员国防止传输，并介入与该第三国的协商（第 4 条和第 5 条）。

但是第 26 章允许在特殊的情况下向不确保提供充分保护的第三国传输数据，如：

——数据主体明确同意；

——履行经数据主体同意的合同或数据主体的利益需要；

——保护数据主体切身利益的需要。

A.2 经济合作与发展组织（OECD）

经合组织的成员包括 24 个国家。其在数据保护领域最具权威性的文件是一套指导文件——并非

指令或法规。其中有一般安全指南[2]和跨国数据流动的隐私保护指南[1]。后者包括8个基本原则：

a) 数据收集的限制：对个人数据的收集应加以限制。个人数据应在数据主体知情或同意的情况下，通过恰当的、公平和合法的手段获得。

b) 数据质量：个人数据宜围绕使用目的保证其准确性，完整性和有效性。

c) 目的性规范：收集数据时应告知该个体其个人数据被收集的原因。这些数据随后应只用于此目的或相似的目的。

d) 使用限制：不得泄漏或使用个人数据，除非目的规定原则允许、有个人同意或法律要求。

e) 安全保障：应使用合理的安全防范措施以防止未经授权地访问、使用、破坏、修改或泄漏个人数据。

f) 开放性：涉及个人数据的策略和程序应易于获得。个人数据收集的种类和数据收集负责方的联系信息应随时可得。

g) 个体参与：个体有权确认是否有其他个体或组织持有其个人数据，有权及时、合理地查看这些数据，有权在上述权利遭到拒绝时被给予理由(并予以反驳/争辩)。

h) 责任：数据控制者应负责执行上述原则。

A.3 欧洲委员会

欧洲委员会的成员较欧盟更广泛。欧洲委员会的部长委员会在各类国际公约下形成国际条约和建议书方面具有很明显的实力，尽管不必让公民个人在具体案例中要求其执行相应的法律权力。在数据保护方面，欧洲委员会的建议书为监督机构提供了重要的指导。第108号公约“个人数据自动化处理中的个体保护公约”为欧洲指令提供了基础。它主要涉及自动化处理，但也涉及参与国对非自动化处理应用同一原则，并为法人或个人团体以及已识别的或可识别的个体提供同样的保护。建议书R(97)5“关于医疗数据的保护”建议各签约国政府：

“采取措施确保本建议书中的各原则在其法律和实践中予以体现”和“确保本建议书中的各原则在收集和处理医疗数据涉及的各专业人员间普及”。

它涵盖如下主题：

——合法处理；

——提供信息给患者；

——同意及反对处理的权利；

——主体访问和校正；

——安全；

——个人数据的泄露；

——跨国的数据流动。

其中特别关注遗传数据。

A.4 联合国大会

A.4.1 总则

联合国发布了“个人数据文档规范指南”。该联合国指南根据一些“定位”为成员国提供了执行涉及计算机化个人数据文档有关规范的程序，其精髓见下面的A.4.2和A.4.3。

A.4.2 任何国家立法应提供的最低保障原则

a) 合法性和公正性：信息收集应以公平、合法的方式，其使用目的不得用于与联合国宪章相悖。

b) 隐私：宜保持文档的有效性与准确性。

c) 目的说明：文档的使用与使用目的宜明确并合法，并告知相关人员。任何人未经同意不应泄漏与目的不符的任何信息，数据保留时间应不超过目的所需时间。

d) 利害相关人的访问:利害相关人宜有访问权、修订权、删除权。

e) 非歧视原则:遵守下文 f),不应编辑可能引起歧视的数据,如种族或血统、肤色、性生活、政治观点、宗教、哲学和其他信仰、社团或工会会员。

f) 例外权:只有在保护国家安全、公共秩序、公共健康或道德或保护他人的权利和自由需要时,才可获准不遵守原则 a)至原则 d)。只有在"国际权利和自由法案"范围内才可获准不遵守原则 e)。

g) 安全:应采取恰当的措施保护文档使其免遭丢失、破坏、未授权访问、欺诈性滥用和恶意使用。

h) 监督和制裁:法律应指定负责监督贯彻这些原则的机构。它宜有恰当、独立的权力。任何违反行为都将受到法律或其他制裁并对个体适当赔偿。

i) 跨国流动:如两国之间有相当的安全措施保护隐私,则信息应能在这两国之间自由流动,否则应根据隐私保护的需要对其流动进行限制。

j) 应用领域:这些原则宜首先应用于所有公共和私人计算机文档。经适当调整,这些原则也可任意用于手册类文档。

A.4.3 指南应用于政府间国际组织持有的个人数据文档

这些指南宜应用于政府间国际组织,每个组织都应指定一个主管机构监督其执行。

当文档的目的是保护人权和个体的基本自由时,可(规定)降低或部分不遵守这些原则。

附 录 B
（资料性附录）
一些国家的国家文件性要求和法律条文

B.1 澳大利亚

AS 4400—1995 澳大利亚标准——医疗保健信息系统中的个人隐私保护(AS 4400—1995 Australian Standard-Personal Privacy Protection in Health Care Information Systems)。

澳大利亚隐私修正法案(隐私部分)2000(Australian Privacy Amendment (Private Sector) Act 2000)。

公正处理个人信息的国家法则,隐私委员会办公室,澳大利亚,修订版,1999 年 1 月(National Principles for the Fair Handling of Personal Information, Office of the Privacy Commission, Australia, Revised edition January 1999)。

信息隐私,惯例法规,新南威尔士健康,1996(Information Privacy, Code of Practice, New South Wales Health, 1996)。

B.2 加拿大

COACH 健康信息保护指南(2001)——加拿大(COACH Guidelines for the Protection of Health Information (2001)-Canada)。

加拿大个人信息及电子档案法案 2000(Canadian Personal Information and Electronic Documents Act 2000。)

B.3 欧洲

欧盟成员国(如:奥地利、比利时、丹麦、爱尔兰、芬兰、法国、德国、希腊、意大利、卢森堡、荷兰、葡萄牙、西班牙、瑞典和英国等)遵守“欧盟数据保护指令”[6](EU Data Protection Directive)。非欧盟成员但属于欧洲经济区(EEA)的成员国(如:冰岛、列支敦士登、挪威)则遵守 1999 年 6 月 25 日达成的“83/1999 号欧洲经济区贸易决议”(EEA Treaty Decision 83/1999)。

欧盟委员会有权判别其他国家所提供的数据保护是否达到与“欧盟数据保护指令”相当的水平。获得此认同的国家有匈牙利[13]和瑞士[14]。

遵守“欧盟数据保护指令”也是申请成为欧盟成员的必要条件之一。

B.4 日本

JIS Q 15001:1999,个人信息保护一致计划的要求(JIS Q 15001:1999, Requirements for compliance program on personal information protection),见〈http://privacymark.org/ref/jisq15001.en.html〉。

政府办公法案第 100 条(The Government Officials Act Article 100)中提到:公务员在职期间以及退休后都不得泄露他们知道的私密信息。

地方办公法案第 34 条(The Local Officials Act Article 34)中提到:公务员在职期间以及退休后都不得泄露他们知道的私密信息。

刑法第 134 条(The Criminal Law Article 134)中提到:医生、药剂师、药品商、助产士…,在职期间没有正当理由而泄露私密信息属于违法。

公共保健护士、助产士及护士法(The public health nurse, midwife and nurse law),放射咨询法

(The consulting radiologist law),牙科医师法(The dental technician law),急诊医师法(The emergency medical technician law),五官科医师法(The speech and hearing technician law),都规定了保守私密的义务和打击泄露私密的行为。

管理机构持有并计算机处理相关个人信息保护法(The Administrative Agency holding and computer processing related Personal Information Protection Law)涉及/处理:泄漏管理性文档时保护个人信息的责任。

个人信息保护法(讨论草案)(The Personal Information Protection Law (Draft under discussion))是基于多项原则进行拟定的,这些原则包括:恰当地获取个人信息,确保准确性,采取安全保护措施,向数据所有者共享信息(告知其个人数据的使用、披露、阻止和修正目的)。

远程服务安全隐私要求,NEMA/COCIR/JIRA 安全隐私联合委员会,2001 年 7 月 11 日(Security and Privacy Requirement for Remote Servicing, Joint NEMA/COCIR/JIRA Security and Privacy Committee, July 11, 2001)。

医疗保健信息技术安全隐私检查,NEMA/COCIR/JIRA 安全隐私联合委员会,2001 年 7 月 11 日(Security and Privacy Auditing in Health Care Information Technology, Joint NEMA/COCIR/JIRA Security and Privacy Committee, July 11, 2001)。

B.5 新西兰

健康信息隐私法规 1994,隐私专员,新西兰(Health Information Privacy Code 1994, Privacy Commissioner, New Zealand)。

B.6 英国

BS 7799-1:2000 第 1 部分,信息安全管理试实行法规,英国标准协会,伦敦(BS 7799-1:2000 Part 1, Code of Practice for Information Security Management, British Standards Institution, London)。

BS 7799-1:2000 第 2 部分,信息安全管理系统规定,英国标准协会,伦敦(BS 7799-2:2002 Part 2, Specification for Information Security Management Systems, British Standards Institution, London)。

数据保护法案 1998(Data Protection Act 1998)。

健康记录访问法案 1990(Access to Health Records Act 1990)。

保密普通法(Common Law of Confidentiality)。

保密性:国家医疗服务实行法规——2003,7 (卫生部,英格兰)(Confidentiality: National Health Service (NHS) Code of Practice—July 2003 (Department of Health, England)")。

医疗数据使用和披露——2002,5(Use and Disclosure of Health Data-May 2002 (Office of the Information Commissioner))。

B.7 美国

美国健康保险轻便和责任法案,1996(USA Health Insurance Portability and Accountability Act, 1996)。

医疗保健信息标准目录, ANSI/HISB, 1997, 1 (An Inventory of Healthcare Information Standards, ANSI/HISB, January 1997)。

ASTM E 1762,医疗保健信息电子认证标准指南(ASTM E 1762, Standard Guide for Electronic Authentication of Health Care Information)。

ASTM E 1869-97,含基于计算机的患者记录的健康信息保密、隐私、访问标准指南和数据安全法则(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，健康信息系统使用检查和泄漏日志暂行标准规范(ASTM PS 115-99，Provisional Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems)。

安全海港隐私法则[15]，美国商务部，2000，7，21(Safe Harbor Privacy Principles[15]-US Department of Commerce-July 21，2000)。

附 录 C
（资料性附录）
相关的 ISO 和 CEN 标准

C.1 ISO

ISO/IEC 17799:2000,Information technology—Code of practice for information security management（信息技术 信息安全管理实行法规）。

ISO/IEC TR 13335,Information technology—Guidelines for the management of IT Security(信息技术 IT 安全管理指导)：

——Part 1:Concepts and models for IT Security(第 1 部分:IT 安全概念和模型)；

——Part 2:Managing and planning IT Security (第 2 部分:IT 安全管理及计划)；

——Part 3:Techniques for the management of IT Security(第 3 部分:IT 安全管理技术)。

C.2 CEN

ENV 12924:1997,Medical informatics—Security categorisation and protection for healthcare information systems(医疗信息学 医疗保健信息系统安全分类和保护)。

ENV 12388:1996,Medical informatics—Algorithm for digital signature services in health care(医疗信息学 医疗保健数字签名服务算法)。

ENV 13608:2000,Health informatics—Security for healthcare communications(健康信息学 医疗保健通信安全)：

——Part 1:Concepts and terminology(第 1 部分:概念和术语)；

——Part 2:Secure data objects(第 2 部分:安全数据对象)；

——Part 3:Secure data channels(第 3 部分:安全数据通道)。

ENV 13729:2000, Health informatics—Secure user identification—Strong authentication using microprocessor cards(健康信息学 安全用户识别 (使用)微处理器卡强认证)。

ENV 12251:2000,Health Informatics—Secure user authentication for health care—Management and security of authentication by passwords(健康信息学 安全用户识别 密码认证管理及安全)。

附 录 D
（资料性附录）
本标准中建议的来源

D.1 参考资料

信息系统安全指导，OECD，OECD/GD(92)190 巴黎，1992，11（“Guidelines for the Security of Information Systems”，OECD，OECD/GD(92)190 Paris，November 1992）。

SEISMED 协会，(面向)医疗远程信息处理安全，Barber B 等编，健康技术和信息学，卷 27(vol. 27)，IOS 出版社，阿姆斯特丹，1996，ISBN 90 5199 246 7(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)。

卫生保健数据安全，SEISMED Consortium，IOS 出版社，阿姆斯特丹，1996（“Data Security for Health Care” ed the SEISMED Consortium，in Studies in Health Technology and Informatics，IOS Press，Amsterdam，1996）：

——管理指导 卷 1(Management Guidelines vol. Ⅰ ISBN 90 5199 264 5)；

——技术指导 卷 2(Technical Guidelines vol. Ⅱ ISBN 90 5199 265 3)；

——户用指导 卷 3(User Guidelines vol. Ⅲ ISBN 90 5199 266 1)。

信任健康 1&2，EU DG 13，健康远程通信处理计划第四构架，HC1051 and HC 4023，1996-1999（“TrustHealth 1 and 2，EU DG XIII Fourth Framework Health Telematics Projects，HC1051 and HC 4023，1996-1999”）。

安全隐私标准手册 卫生保健可交付 4 EU MEDSEC 计划，EU DG 3，信息社会 EU DG 3 卫生保健安全隐私，ISIS 计划，1997-1998（“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，安全电子医疗信息通信，EU DG 3，ISIS 计划，1997(SEMRIC，Secure Electronic Medical Information Communication，EU DG III，ISIS programme，1997)。

欧洲隐私标准化提案权，(IPSE)，讨论草案，2001，9(Initiative on Privacy Standardisation in Europe (IPSE)，Discussion Draft，September 2001)。

CRAMM 用户指南，2001，3，29，CCTA 风险分析和管理方法，CRAMM，软件版 4.0，CRAMM 管理人员，理解咨询有限公司，Churchfield House，5 The Quintet，Churchfield Road，Walton on Thames，KT12 2TZ[软件含用户指南](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])。

不安全世界中的健康信息通信，Bakker AR，Barber B，Pellikka RT K & Treacher A 编，生物医学计算关机期刊，卷(43)，pp. 1-152，增刊，1996，10，阿姆斯特丹(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)。

患者数据通信安全通用解决方法，Bakker AR，Barber B，Ishikawa K & Yamamoto K 编，生物医学计算关机期刊，卷(49)，pp. 1-137，增刊，198，10，阿姆斯特丹(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)。

电子患者记录分布安全，Bakker AR，Barber B，Moehr J 编，生物医学计算关机期刊，卷(60)，pp. 1-237，2000(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 所选的网址

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〉

附 录 E
（资料性附录）
“控制方到控制方”合同条款范例

E.1 导言

下面给出适用于“控制方到控制方”之间传输个人健康信息(见 6.2.2 中的 g))时的合同范例。

E.2 来历

这些“控制方到控制方”的标准合同条款最初由欧盟委员会创建,以允许控制方在充分理解欧盟数据保护指令的背景下例证数据保护的“充分性”。

E.3 合同的本质特征

任何合同都应包括以下内容:

——数据导出方和数据导入方的职责;

——数据传输的目的;

——数据主体对按照所陈述的目的进行传输给出了明确的同意;

——数据主体持有一份该合同条款副本的权利;

——数据主体获得赔偿、对投诉的客观调查和仲裁的权利;

——管辖法律;

——到第三方的数据传输;

——为确保充分的数据保护,数据导入方必须满足的要求。

上述内容均应符合本标准的规定。

E.4 合同范例及注意事项

以下合同条款只是一个范例。每一次国际应用时都需要依据应用特点和可能影响本合同的相关国家法律来考虑这些条款。有时候可能有必要去寻求法律建议。

宜注意的是:

——本合同条款宜是可强制执行的,不仅对合同各方的组织机构而言,而且对各数据主体也是如此,尤其是在数据主体会因合同的违背而遭受损害的地方。

——本合同的管辖法律应是传输数据的主要控制方所在国家的法律,目的是使第三方受益人能够实施本合同。在明确有利于数据主体的情况下,此款可以被修改。宜允许数据主体由协会或其他团体来代表。

——为了在根据这些合同条款去行使各自权利时减少数据主体可能遇到的实际困难,数据导出方和数据导入方宜共同承担由于违背了这些条款(包括第三方受益条款)而造成的任何损害,并负起各自的责任。

——数据主体有权采取行动并获得数据导出方和数据导入方或双方由于其任何不符合这些条款规定义务的行为导致的赔偿。如果他们可以证明各自都没有责任,但两方都可免于赔偿。

——连带赔偿责任不适用于第三方受益条款不涉及的规定,也不需要一方赔偿由于另一方非法处理所造成的损害。尽管参与方之间的相互赔偿不做要求的,并可能会被删除,但是为了清晰起见,将此列入条款中,以避免参与方之间单独协商赔偿条款的需要。

——在各参与方和数据主体之间发生的纠纷没有得到和解,并且数据主体援引了第三方受益条款

的情况下，各参与方同意数据主体选择调解或诉讼。数据主体能在多大程度做出有效选择将取决于可靠的和公认的调解和仲裁系统的可用性。通过传输数据的主要控制方所属国家公认的权威机构来调解，如一个国家或地方的数据保护/隐私管理机构或同级机构将是一个好选择，如果可以有这种服务提供的话。

——当出现关于数据主体的数据被干扰时，宜明确数据导出方和数据导入方对于数据主体的责任。

标准合同条款的范例

数据导出机构的名称：_____

地址：_____

电话：_____传真：_____ Email：_____

机构的其他信息：_____

（数据导出方）

以及

数据导入机构的名称：_____

地址：_____

电话：_____传真：_____ Email：_____

机构的其他信息：_____

（数据导入方）

现已达成以下合同条款（简称："条款"），目的是对个人健康数据在数据导出方与数据导入方间传输时（具体见附件1）在个体隐私保护、基本人权和自由方面举出充分的安全保障措施。

条款1

定义

以下定义适用于本合同的各条款：

——控制方：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；

——数据主体：已标识或可标识的自然人，个人数据的主体；

——参与方：数据导出方和数据导入方；

——个人数据：任何涉及已标识或可标识自然人的信息；

——个人健康数据：任何涉及已标识或可标识自然人的健康情况的个人数据；

——个人数据的处理（处理）：对个人数据进行的自动化或非自动化（系列）操作，如采集、记录、组织、存储、改编或改动、检索、咨询、使用、（通过传输）披露、散播、调整或组合、拦截、删除或销毁；

——数据导入方：获取他国数据导出方数据的自然人、法人、政府机关、机构或其他团体；

——技术和组织性安全措施：这些措施旨在保护个人数据免受意外或非法破坏或意外丢失、改动、未经授权披露或访问（特别是处理中涉及到通过网络的数据传输时），并避免一切非法处理形式；

——数据导出方：向他国数据导入方发送数据的自然人、法人、政府机关、机构或其他团体。

条款 2

传输细节

作为条款的基本组成部分，附件 1 详细说明了传输的细节，特别是个人数据的种类，以及它们被传输的目的。

条款 3

第三方受益条款

数据主体能作为第三方受益者主张强制执行本条款，以及条款 4 中 b)、c)和 d)项，条款 5 中 a)、b)、c)、d)、e)、f)和 g)项，条款 6 中 1)和 2)，以及条款 7、9 和 11。各参与方不得反对数据主体由符合他们意愿的协会或团体来代表，只要是国家法律允许的。

条款 4

数据导出方的义务

数据导出方同意并保证：

a) 由其进行的个人健康数据的处理（包括传输本身）已经（直到传输时刻）并将继续根据数据导出方所在国家（且适用范围已经通知该国的有关权威机构）的相关规定执行，并且不会违反该国的相关规定；

b) 在传输前，数据主体已被告知或将被告知该数据会传输给导入国，并且数据主体已经明确地同意；

c) 数据主体获取本合同各项条款副本的要求总是可以被满足；并且

d) 应在合理的时间和范围内回答数据主体关于数据导入方对其个人健康数据处理方面的任何问题。

条款 5

数据导入方的义务

数据导入方同意并保证：

a) 他没有理由相信，适用于他的立法会不允许他完成本合同下他应履行的各项义务，并且当立法发生变更并对本条款提供的担保产生了不利的影响时，他会将本变更通知给数据导出方，而此时，数据导出方有权暂停数据传输和/或终止本合同。

b) 依照附件 2 列出的强制性数据保护要求来处理个人数据。

c) 迅速并适当地处理来自数据导出方或数据主体对有关其如何处理传输中的个人健康数据的所有合理查询。

d) 应数据导出方的要求为审计提交其数据处理的责任，该审计由数据导出方执行，或由独立成员组成的、并拥有所要求的专业资质的检查机构(并由数据导入方来选定)来执行。

e) 将迅速通知数据导出方关于：

   i) 执法机关任何涉及披露个人数据的司法要求，除非法律禁止他进行该等通知，如根据刑法下的禁令，从而维护执法调查的保密性；

   ii) 任何意外或未经授权的访问；

   iii) 直接来自数据主体的任何请求，但并不对数据主体作出回应，除非他已另外获得授权可以对该等请求作出回应。

f) 数据主体获取本合同各项条款副本的要求总是可以被满足，并且指定处理投诉的部门。

g) 遵守附件 3 中列出的数据导出国的数据保护/隐私管理机构的各项要求。

条款 6

责　　任

1) 各参与方同意因条款 3 中的规定被违反而遭受损失的数据主体有权从导致损失方获得赔偿。各参与方同意，在能够证明他们都对违反规定不负有责任时，他们可以免于承担责任。

2) 数据导出方和数据导入方同意他们将为 1)中提到的数据主体遭受的损失共同承担责任。在这种违规行为中，数据主体可对数据导出方或数据导入方或对两者都提起诉讼。

3) 各参与方同意，如果一方被另一方据 1)所述中的违反行为而承担法律责任，后者将承担他应承担的扩展责任，赔偿前者的任何损耗、费用、损害、支出或已造成的损失。

赔偿取决于：

i) 数据导出方及时将索赔要求通知给数据导入方；并且

ii) 数据导入方被提供了与数据导出方在对索赔的进行辩护与和解方面合作的可能性(*)。

条款 7

调解和管辖

a) 各参与方同意，如果数据主体和其他方之间存在没有得到和解的争端，并且数据主体引用了条款 3 中关于第三方受益的条款，他们接受数据主体的如下决定：

1) 将争端提交给一名独立的个人或机构来调解；

2) 将争端提交给数据导出方所在国家的法院来裁决。

b) 各参与方同意，根据数据主体和相关参与方之间协定，能将争端提交给一个仲裁机构。（**）

c) 各参与方同意，a)和 b)条款的适用，不得损害数据主体依据国家或国际法律的其他规定寻求赔偿的实体上的或程序性的权利。

条款 8

与国家权威机构的合作

各参与方同意向任何国家数据保护/私隐管理机构或等同机构交存一份本合同的副本，如果国家法律要求这样做的话。

条款 9

条款的终止

各参与方同意在任何时候、任何情况和任何原因下终止条款后，依然要对与处理所传输数据相关的条款中的义务和/或条件负责。

条款 10

管辖法律

本合同各项条款受数据导出方所在国的国家法律制约，即（***）：

条款 11

合同的变动

各方承诺不更改或修改条款。

数据导出方：

机构图章

名称(全称)：_____

地址：_____

电话：_____传真：_____ Email：_____

使合同具有约束力的其他必要信息(如有的话)：

_____

数据导入方：

机构图章

名称(全称)：_____

地址：_____

电话：_____传真：_____ Email：_____

使合同具有约束力的其他必要信息(如有的话)：

_____

_____

(签字)

(*) 3)是可选的。

(**) 相关参与方是否成立于签署了关于仲裁实施方面的纽约公约的国家中是重要的。

(***)管辖法律通常是数据导出方所在国家的法律，除非一些其他安排明显更有利于数据主体。

附件 1

关于合同条款

本附件作为合同条款的组成部分，且由各参与方完成并签署。
（各参与方可在本附件中填写或指定的任何其他必要的附加信息）。

数据导出方
数据导出方是（请简要说明您与传输有关的活动）：

数据导入方
数据导入方是（请简要说明您与传输有关的活动）：

数据主体
个人健康数据的传输，涉及以下数据主体类型（请具体说明）：

传输目的
传输主要用于下列目的（请详细说明）：

数据的类别
所传输的个人数据具有以下性质（请具体说明，并指出任何可能特别敏感的性质）：

接收方
所传输的个人数据只能披露给以下接收方或以下几类接收方（请具体说明）：

存储限制
所传输的个人数据的存储时间不可超过
（以“月/年”或以其他方式填写，确保数据保存时间不超过传输目的所需时间）：

数据导出方	数据导入方
姓名：_____	姓名：_____
（授权签字）	（授权签字）

附件 2

关于合同条款

条款 5 中 c)提到的强制性数据保护要求

强制性数据保护要求是指 ISO 22857 Health informatics—Guidelines on data protection to facilitate trans-border flows of personal health information 中的强制性要求。在中华人民共和国则对应的是 GB/T 25512—2010《健康信息学　推动个人健康信息跨国流动的数据保护指南》中规定。

附件 3

关于合同条款

在此附件中详细说明数据导出方所在国家的国家/地方数据保护/私隐管理机构或等同机构规定的任何要求，如果有的话。

附 录 F
（资料性附录）
“控制方到处理方”合同条款范例

F.1 导言

下面给出适用于“控制方到处理方”之间传输个人健康信息(见 6.2.2 中的 g))时的合同范例。

在“控制方到控制方”的传输模式中，导入控制方作为控制方，有权决定如何处理个人健康数据及其方式，即使传输数据的主要控制方可能违反确保数据保护的全部充分性应遵循的基本原则。由于导入控制方有这种权利，他必须承担因其特权所采取的任何行为的后果，并对由于其中的缺陷所引起的对数据主体的赔偿负责。

在“控制方到处理方”的传输模式中，导入处理方作为处理方，仅遵守控制方的指令来处理传输的数据。后者因此必须具体说明处理方要做的事情以及必须执行的技术和组织性安全措施。如此则控制方要对其指令和措施的充分性负责，并对由于(已证实的)不充分性引起的对数据主体的赔偿负责。处理方有责任贯彻控制方指定的技术和组织性安全措施，而控制方有责任确保这些措施得以实际执行。

在“控制方到处理方”的传输环境中，数据主体宜仅对控制方并在控制方所在国家的管辖法律下主张其所有权利。由处理方体现出的任何缺陷都将是控制方和处理方之间要解决的问题。然而，如果控制方不复存在，数据主体宜能够就处理方应负责的缺陷向导入处理方行使其权力。

F.2 来历

这些“控制方到处理方”的标准合同条款最初由欧盟委员会创建，以允许处在欧盟成员国的控制方在充分理解欧盟数据保护指令的背景下例证数据保护的“充分性”。

F.3 合同的本质特征

任何合同都应包括以下内容：

——数据传输的控制方和导入处理方的职责；

——数据传输的目的；

——数据主体对按照所陈述的目的进行传输给出了明确的同意；

——数据主体持有一份该合同条款副本的权利；

——数据主体获得赔偿、对投诉的客观调查和仲裁的权利；

——管辖法律；

——导入处理方须确保充分数据保护的技术和组织性安全保护措施。

上述内容均应符合本标准的规定。

F.4 合同范例及注意事项

以下合同条款只是一个范例。每一次国际应用时都需要依据应用特点和可能影响本合同的相关国家法律来考虑这些条款。有时候可能有必要去寻求法律建议。

需要注意的是：

——导入处理方只能代表传输控制方并按照其指示和合同条款中的各项义务来处理传输的数据。特别是数据导入方不应向第三方公开个人健康数据，除非按照传输控制方的指示。输入控制方宜在整个数据处理服务过程中指导导入处理方按照其指令处理数据，并遵守本合同条款中任何适用的数据保护法律和义务。

——本合同条款宜是可强制执行的，不仅对合同各方的组织机构而言，而且对各数据主体也是如此，尤其是在数据主体会因合同的违背而遭受损害的地方。

——本合同的管辖法律应是传输数据的主要控制方所在国家的法律，目的是使第三方受益人能够实施本合同。

——数据主体对不符合本合同条款规定的行为有权采取行动并从传输数据的控制方获得适当的赔偿。特殊情况下，如当传输控制方已消失或已在法律上不复存在或已经破产，由于导入处理方的违规(参照条款3中范例条款规定的责任)，数据主体也宜有权采取行动，并酌情获得导入处理方的赔偿。

——在各参与方和数据主体之间发生的纠纷没有得到和解，并且数据主体援引了第三方受益条款的情况下，各参与方同意数据主体选择调解或诉讼。数据主体能在多大程度做出有效选择将取决于可靠的和公认的调解和仲裁系统的可用性。通过传输数据的主要控制方所属国家公认的权威机构来调解，如一个国家或地方的数据保护/隐私管理机构或同级机构将是一个好选择，如果可以有这种服务提供的话。

——当出现关于数据主体的数据被干扰时，宜明确数据导出方和数据导入方对于数据主体的责任。

标准合同条款的范例

数据导出机构的名称：_____

地址：_____

电话：_____传真：_____ Email：_____

机构的其他必要信息：_____

(数据导出方)

数据导入机构的名称：_____

地址：_____

电话：_____传真：_____ Email：_____

机构的其他必要信息：_____

(数据导入方)

现已达成以下合同条款(简称“条款”)，目的是对个人健康数据在数据导出方与数据导入方间传输时(具体见附件1)在个体隐私保护、基本人权和自由方面举出充分的安全保障措施。

条款1

定　义

以下定义适用于本合同的各条款：

——控制方：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；

——数据主体:已标识或可标识的自然人,个人数据的主体;
——参与方:数据导出方和数据导入方;
——个人数据:任何涉及已标识或可标识自然人的信息;
——个人健康数据:任何涉及已标识或可标识自然人的健康情况的个人数据;
——个人健康数据的处理(处理):对个人数据进行的自动化或非自动化(系列)操作,如采集、记录、组织、存储、改编或改动、检索、咨询、使用、(通过传输)披露、散播、调整或组合、拦截、删除或销毁;
——数据导入方:获取他国数据导出方数据的自然人、法人、政府机关、机构或其他团体;
——技术和组织性安全措施:这些措施旨在保护个人数据免受意外或非法破坏或意外丢失、改动、未经授权披露或访问(特别是处理中涉及到通过网络的数据传输时),并避免一切非法处理形式;
——数据导出方:向他国数据导入方发送数据的自然人、法人、政府机关、机构或其他团体。

条款 2

传输细节

作为条款的基本组成部分,附件 1 详细说明了传输的细节,特别是个人数据的种类,以及它们被传输的目的。

条款 3

第三方受益条款

数据主体能作为第三方受益者向传输控制方主张执行本条款,以及条款 4 中 b)到 h),条款 5 中 a)到 e)和 g)、h),条款 6 中 1)和 2),条款 7,条款 8,条款 9,条款 10 和条款 11。

当传输控制方已经事实上消失或从法律上消失时,数据主体能向导入处理方主张执行本条款,以及条款 5 中 a)到 c)和 g),条款 6 中 1)和 2),条款 7,条款 8,条款 9,条款 10 和条款 11。

各参与方不得反对数据主体由符合他们意愿的协会或团体来代表,只要是国家法律允许的。

条款 4

数据导出方的义务

数据导出方同意并保证:

a) 由其进行的个人健康数据的处理(包括传输本身)已经(直到传输时刻)并将继续根据数据导出方所在国家(且适用范围已经通知该国的有关权威机构)的相关规定执行,并且不会违反该国的相关规定。

b) 他已指示,并将在个人数据服务整个过程中指示数据导入方代表数据导出方来处理所传输的数据,并遵守本合同条款中任何适用的数据保护法律和义务。

c) 数据导入方应提供本合同附件 2 中技术和组织性安全保障措施方面的足够担保。
d) 评定任何可适用的数据保护法的需求后，其安全保护措施可用于保护个人健康数据免受由意外损失、更改、非授权泄露或访问引起的意外或者非法破坏，特别是涉及网络数据传输的处理，使其免受其他非法的处理形式。这些措施可以确保与处理风险和被保护数据本质相对应的安全级别，并考虑到了现行实施现状和成本。
e) 确保遵守安全措施。
f) 数据主体已被告知或将在传输前被告知其数据可以传输给导入国并得到明确的许可。
g) 除附件 2 可用一个安全措施的简要说明代替外，只要数据主体要求就向其提供一份本合同各条款的副本。
h) 应在合理的时间和范围内回答数据主体关于数据导入方对其个人健康数据处理方面的任何问题。

条款 5

数据导入方的义务

数据导入方同意并保证：

a) 仅代表数据导出方处理个人数据并遵守其指示和本合同的条款。如果他无论基于何种原因不能遵守时，都将此及时通知给数据导出方，在这种情况下，数据导出方有权暂停数据传输和/或终止本合同。
b) 他没有理由相信，适用于他的立法会不允许他完成本合同下他应履行的各项义务，并且当立法发生变更并对本条款提供的担保产生了不利的影响时，他会将本变更通知给数据导出方，而此时，数据导出方有权暂停数据传输和/或终止本合同。
c) 在处理所传输的个人数据前，已实施附件 2 规定的技术和组织性安全保障措施细则。
d) 将迅速通知数据导出方关于：
   i) 执法机关任何涉及披露个人数据的司法要求，除非法律禁止他进行该等通知，如根据刑法下的禁令，从而维护执法调查的保密性；
   ii) 任何意外或未经授权的访问；
   iii) 直接来自数据主体的任何请求，但并不对数据主体作出回应，除非他已另外获得授权可以对该等请求作出回应。
e) 迅速并适当地处理数据导出方对有关其如何处理传输中的个人健康数据的所有询查。
f) 应数据导出方的要求为审计提交其数据处理的责任，该审计由数据导出方执行，或由独立成员组成的、并拥有所要求的专业资质的检查机构(并由数据导入方来选定)来执行。
g) 除附件 2 可用一个安全措施的简要说明代替外，只要数据主体要求就向其提供一份本合同各条款的副本，并且指定处理投诉的部门。
h) 遵守附件 3 中列出的数据导出国的数据保护/隐私管理机构的各项要求。

条款 6

责　　任

1) 各参与方同意因条款 3 中的规定被违反而遭受损失的数据主体有权从导致损失方获得赔偿。

2) 如果因为数据导出方事实上消失、或者在法律上不复存在、或者破产，数据主体不能因数据导入方的违规依据 1)中所述采取的行动，或无法依据条款 3 要求数据导出方承担任何义务时，数据导入方同意数据主体可将其作为传输控制方提起索赔。

3) 各参与方同意，如果一方被另一方据 1)所述中的违反行为而承担法律责任，后者将承担他应承担的扩展责任，赔偿前者的任何损耗、费用、损害、支出或已造成的损失。

赔偿取决于：

i) 数据导出方及时将索赔要求通知给数据导入方；并且

ii) 数据导入方被提供了与数据导出方在对索赔的进行辩护与和解方面合作的可能性(*)。

条款 7

调解和管辖

a) 数据导入方同意，如果数据主体针对数据导入方引用了条款 3 中关于第三方受益权和/或按照合同条款向其索赔，数据导入方将接受数据主体的如下决定：

1) 将争端提交给一名独立的个人或机构；

2) 将争端提交给已确定的数据导出方所在的国家法院。

b) 数据导入方同意，根据其与数据主体之间的协定，能将具体争端提交给一个仲裁机构。(**)

c) 各参与方同意，a)和 b)条款的适用，不得损害数据主体依据国家或国际法律的其他规定寻求赔偿的实体上的或程序性的权利。

条款 8

与国家权威机构的合作

各参与方同意向任何国家数据保护/私隐管理机构或等同机构交存一份本合同的副本，如果国家法律要求这样做的话。

条款 9

管辖法律

本合同各项条款受数据导出方所在国的国家法律制约，即(***)：

条款 10

合同的变动

各方承诺不更改或修改条款。

条款 11

个人数据处理终止后的责任

1) 各参与方同意，终止提供数据处理服务时，数据导入方应按照数据导出方的选择，向数据导出方归还所有已传输的个人数据及其副本或销毁所有已传输的个人数据并向数据导出方证实他已这么做了，除非法律不允许数据导入方归还或销毁全部或部分已传输的个人数据。在后一种情况下，数据导入方应确保已传输个人数据的保密性并不再擅自处理已传输的个人数据。

2) 数据导入方保证依据数据导出方的要求，他将提交数据处理工具以用于涉及上段所述某种方式的审计。

数据导出方：

机构图章

名称(全称)：_____

地址：_____

电话：_____传真：_____ Email：_____

使合同具有约束力的其他必要信息(如有的话)：

_____

数据导入方：

机构图章

名称(全称)：_____

地址：_____

电话：_____传真：_____ Email：_____

使合同具有约束力的其他必要信息(如有的话)：

_____

_____

(签字)

(*) 3)是可选的。

(**) 相关参与方是否成立于签署了关于仲裁实施方面的纽约公约的国家中是重要的。

(***)管辖法律通常是数据导出方所在国家的法律，除非一些其他安排明显更有利于数据主体。

附件 1

关于合同条款

本附件作为合同条款的组成部分，且由各参与方完成并签署。
（各参与方可在本附件中填写或指定的任何其他必要的附加信息。）

数据导出方
数据导出方是（请简要说明您与传输有关的活动）：

数据导入方
数据导入方是（请简要说明您与传输有关的活动）：

数据主体
个人健康数据的传输，涉及以下数据主体类型（请具体说明）：

传输目的
传输主要用于下列目的（请详细说明）：

数据的类别
所传输的个人数据具有以下性质（请具体说明，并指出任何可能特别敏感的性质）：

接收方
所传输的个人数据只能披露给以下接收方或以下几类接收方（请具体说明）：

存储限制
所传输的个人数据的存储时间不可超过
（以“月/年”或以其他方式填写，确保数据保存时间不超过传输目的所需时间）：

数据导出方	数据导入方
姓名：_____	姓名：_____
（授权签字）	（授权签字）

附件 2

关于合同条款

条款 5 中 c)提到的强制性数据保护要求

强制性数据保护要求是指 ISO 22857,“*Health informatics—Guidelines on data protection to facilitate trans-border flows of personal health information*”中的强制性要求。在中华人民共和国则对应的是 GB/T 25512—2010《健康信息学　推动个人健康信息跨国流动的数据保护指南》中的规定。

数据导出方在此插入一个保护所传输个人健康数据的必要“措施”的详细说明,这里“措施”的含义由本标准的 9.4.5 给出。

附件 3

关于合同条款

在此附件中详细说明数据导出方所在国家的国家/地方数据保护/私隐管理机构或等同机构规定的任何要求,如果有的话。

附 录 G
（资料性附录）
处理特别敏感的个人健康数据

G.1 导言

所有的个人健康数据在欧洲委员会的《关于医疗数据的保护》建议书和“欧盟数据保护指令”中作为一个尤其敏感的类别被定义。另一方面，大多数数据主体都认为某些种类的个人健康数据更是特别敏感的。许多国家正式在国家级规章或指南中承认，例如关于性传播疾病和人工流产，针对这些特别敏感的个人健康数据可能需要采取特别严格或特殊的预防措施。

G.2 遗传学或基因组学数据

随着个体的遗传特征和各种敏感个体的疾病及其身体或精神上的特征有关的信息的日益增多，新的围绕个人遗传学数据使用权的争论变得越来越敏感。来自遗传学检测的“意外”发现可能会特别敏感并需要特殊保护；在某些情况下如果未经过专门的商议或讨论，这种“意外”发现甚至可能来自其本人。此外，个人遗传学数据所提供的信息还包含了具有相同遗传系谱的其他人的特征信息。这些数据目前已普遍被视为敏感的医疗数据，但详细的遗传检测提供了大量的来源于 DNA 分析的额外数据。

能够把“个人基因组数据”或“个人以 DNA 为基础的数据”定义为“特别敏感”类别的一部分：该类别可扩大到包括所有的“个人遗传学数据”。前者中的大多数数据可能会在专门的实验室发现，并在病程记录中只出现一个摘要，而后者，一些“个人遗传学数据”会出现在大多数病案注释中。

“个人基因组数据”或“个人以 DNA 为基础的数据”的一个问题是，许多非健康机构出于就业、保险、标识和司法的目的有兴趣获得它。确定这种数据的特征的方法是将“个人基因组数据”或“个人以 DNA 为基础的数据”作为“个人遗传学数据”的一个子类，而“个人遗传学数据”又作为“个人医疗数据”的一个子类。这样不管是谁要进行 DNA 分析或此分析是为了何种目的，这都将确保任何个人 DNA 分析包括在“特别敏感”的个人健康数据类别中。这也可以对那些处理这种数据的人员提出法律的或专门的安全保护要求，无论他们是医务人员、DNA 检测实验员、警察和司法机关，还是雇主或保险公司。这类附加的要求将会阻止人们处理这种类型的个人数据，除非事关重要。

在一些数据保护要求的管辖区仅适用于有生命的个体。在这种情况下需要注意，死者试验提供的信息包括了一个遗传系谱中有生命的个体或虽不是但接近该遗传系谱的个体。正常的数据保护措施还必须满足保护有生命个体的要求。

G.3 社会敏感性或传染性疾病

历史上，社会敏感性疾病或传染性疾病一直是疑难问题，这也是个人健康数据被赋予一个特别敏感的地位的主要原因之一。然而，社会联系的电子化使得在更广阔的地理区域上都能访问此类信息，因此尽管系统具有更良好的访问控制机制，“这只有我和医生知道”这种传统保护的观念与以前相比已不再那么有效了。这些数据同样常常会提供第三方信息。

G.4 有关妊娠和分娩的信息

在一些地方，有关人工流产的信息和怀孕及收养的信息一样特别敏感。在许多情况下，个人数据也将涉及另一个体。这种数据需要特殊的保护。

G.5 健康信息的特异性语境

保护个人健康数据的问题之一是其敏感性往往有特异性语境。目前仍有很多，甚至大多数人可能

会对特殊人群的看法存在相当严重的问题。可能仅仅涉及到他们的住址或出席了一个特别的门诊，更不用说需要公开的特殊护理了。这些问题必须由“用户自定义”，因为只有患者自己知道在何种特殊环境下需要对他们的个人健康或遗传学数据进行特定地保护。

G.6 一类“特别敏感”的个人健康数据

因为每一个体根据个体情况，甚至他的民族文化会对特别敏感的数据有不同的理解，很难对“特别敏感”的类别下一个令人满意的定义。本标准也没有因此提供一个定义。然而，大多数人认为下列内容属于这种“特别敏感”的类别：

——来自 DNA 分析的基因组信息和可能所有的个人遗传学数据；

——有关测试结果或阳性结果，尤其是社会敏感的传染性疾病，包括性传播疾病；

——有关妊娠信息，结果或终止怀孕或收养。

此外任何被数据主体视为“特别敏感”的个人健康数据都属于这一类。

G.7 确保“特别敏感”的个人健康数据的安全

考虑特殊的健康数据是否“特别敏感”没有任何意义，除非已超过或适用于其他个人健康数据的安全措施能够得到执行。这些措施可能取决的情况，例如包括伪匿名处理、加密、特殊的手段来限制访问和用户身份鉴别、审计跟踪的特殊监控，对可能参与的工作人员额外的集中培训和因违反规则而采取的特别强有力的制裁措施。

参 考 文 献

[1] OECD "Recommendations of the Council of the OECD Concerning Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data", OECD, 23 September 1980.

[2] OECD "Guidelines for the Security of Information Systems", 1996, OECD Publications, ISBN 96-64-14569-9.

[3] "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108)", Council of Europe, Strasbourg, 28 January 1981.

[4] "Council of Europe Recommendation R(97)5 on the Protection of Medical Data". Council of Europe Publishing, Strasbourg, 12 February 1997.

[5] "Guidelines for the Regulation of Computerised Personal Data Files", United Nations General Assembly, 14 December 1990.

[6] "Directive 95/46/EC of the European Parliament and of the Council of Europe of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data", Official Journal of the European Communities, Number L281/31, 23 November 1995.

[7] Ray Rogers and Joy Reardon, "Barriers to a Global Information Society for Health: Recommendations for International Action, Appendices 7 to 15", Studies in Health Technology and Informatics No. 63, IOS Press, Amsterdam, February 1999.

[8] "Transfers of personal data to third countries: Applying Article 25 and 26 of the EU Data Protection Directive", Working Party on the Protection of Individuals with regard to the Processing of Personal data, Working document DGXV D/5025/98 WP 12, Adopted 24 July 1998.

[9] Data security for healthcare, Vol. 1 Management Guidelines, Vol. 2 Technical Guidelines, Vol. 3 User Guidelines, Edited by the SIESMED Consortium, Studies in Health Technology and Informatics 31, 32, and 33, IOS Press, Amsterdam.

[10] European Convention on the Protection of Human Rights and Fundamental Freedoms, Council of Europe, Strasbourg 1951.

[11] EN 14485, Health Informatics—Guidance for handling personal health data in international applications in the context of the EU data protection directive.

[12] EN 14484, Health Informatics—International transfer of personal health data covered by the EU data protection directive—High level security policy.

[13] "Opinion 6/99 on level of personal data protection in Hungary", working party on the protection of individuals with regard to the processing of personal data, 7 September 1999.

[14] "Opinion 5/99 on level of protection of personal data in Switzerland", working party on the protection of individuals with regard to the processing of personal data, 7 June 1999.

[15] Commission Decision of July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce.

[16] Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, Official Journal of the European Communi-

ties, L181/19, 4. 7. 2001.

[17] Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, Official Journal of the European Communities, L6/52, 10. 1. 2002.

中华人民共和国
国家标准
健康信息学 推动个人健康信息跨国流动的数据保护指南
GB/T 25512—2010/ISO 22857:2004
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3.5 字数 94 千字
2011年4月第一版 2011年4月第一次印刷
*
书号:155066·1-42413

GB/T 25512-2010