ICS 35.240.80
L 67

中华人民共和国国家标准

GB/T 21715.2—2008/ISO 21549-2:2004

健康信息学　患者健康卡数据 第2部分:通用对象

Health informatics—Patient healthcard data—Part 2: Common objects

(ISO 21549-2:2004, IDT)

2008-04-11 发布　　2008-09-01 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

GB/T 21715《健康信息学　患者健康卡数据》分为8个部分：

——第1部分：总体结构；

——第2部分：通用对象；

——第3部分：有限临床数据；

——第4部分：扩展临床数据；

——第5部分：标识数据；

——第6部分：管理数据；

——第7部分：电子处方(用药数据)；

——第8部分：链接。

将来还可能增加新的部分。

本部分为GB/T 21715中的第2部分。

本部分等同采用ISO 21549-2:2004《健康信息学　健康卡数据　第2部分：通用对象》。

本部分与ISO 21549-2:2004的主要差别为对适用范围进行了略微补充。

本部分的附录A为规范性附录。

本部分由中国标准化研究院提出。

本部分由中国标准化研究院归口。

本部分起草单位：中国标准化研究院、解放军总医院。

本部分主要起草人：陈煌、任冠华、董连续、徐成华、刘碧松。

引　言

随着人口流动的增加，社区医疗和家庭保健需求日益增多，对高质量流动治疗服务需求也不断增长，便携式信息系统和存储器也随之得以迅速发展并投入使用。这些设备可实现从身份识别到患者便携式监控系统等一系列功能。

这些设备的功能是携带可识别的个人信息，并与其他系统之间进行传递；因此，在工作期间，它们可能与许多功能和性能有很大差异的不同技术系统一起共享信息。

保健管理越来越依靠类似自动化的识别系统。例如，患者可通过使用便携式可读计算机设备，对处方进行自动处理，并实现在不同地点之间的数据交换。医疗保险公司和保健提供方越来越多地涉及跨区域治疗中。在这种情况下，理赔可能需要在很多不同的保健系统之间自动交换数据。

可远程访问数据库及其支撑系统的出现带动了“保健受益人”识别设备的发展和使用，这些设备能执行安全功能并且能经由网络向远程系统传送数字签名。

随着使用日常保健服务中数据卡的日益增多，有必要对数据格式进行标准化以实现数据交换。

数据卡携带的与人相关的数据可分成3种主要类型：标识数据、管理数据和临床数据。需要特别指出的是，实际使用的健康数据卡必须包含设备本身的标识数据及其携带数据所涉及的个人标识数据，管理数据和临床数据是可选的。

设备数据包括：

——设备本身的标识数据；

——设备功能和性能的标识数据。

标识数据可包括：

——设备持有者的唯一标识或者该设备所携带数据相关的人的唯一标识。

管理数据可包括：

——个人相关的补充数据；

——保健资金的标识，表明其是有支付的还是自付的，以及它们的关系，即保险公司、保险合同和保险单或者保险费的类型；

——保健服务所必需的其他数据（不同于临床数据）。

临床数据可包括：

——提供健康信息和健康事件信息的数据项；

——保健提供者对它们的评价和标注；

——已计划的、要求的或者已经执行的临床行为。

因为数据卡本质上是给明确的查询提供具体的答复，同时有必要通过消除冗余来优化使用存储空间，所以在定义健康数据卡数据结构时使用了高层次的对象建模技术（OMT）。

上述四类数据有许多共同特征。例如，每类数据都必须包含：ID号、名称、日期。某些信息可能同时兼有临床和管理的用途。因此，不在基本数据元的基础上使用类结构而简单罗列健康数据卡携带的数据项是不能满足要求的。这些基本数据元可以通过它们的特性（例如它们的格式）来定义，并且通过它们可以构造复合数据对象。若干这样的对象可以共享某些属性。

本部分通过使用UML、纯文本和ASN.1描述和定义了患者持有的健康数据卡所使用或引用的通用数据对象。这些数据对象用于各种类型的健康数据卡，并且用来构建符合GB/T 21715.3—2008～GB/T 21715.8定义的复合数据对象。

健康信息学　患者健康卡数据
第2部分:通用对象

1　范围

本部分为通用对象的结构和内容构建了一个通用框架。这些结构和内容用于构建患者健康卡中其他数据对象的数据,或者被它们所引用。但并不规定或者给出用于存储在设备中强制性特定数据集。

本部分适用于记录或者传送患者健康卡的数据,这些数据可存放于符合GB/T 14916中ID-1卡物理尺寸规定的卡中。

下列服务的详细功能和机制不属于本部分的范围(即使它的结构允许使用其他地方规定的合适数据对象):

——自由文本数据的编码;

——可由数据卡用户按照具体应用所规定的安全功能和相关服务,例如,保密性保护,数据完整性保护,以及与这些功能相关的个人和设备的鉴别;

——依赖于某些数据卡类型的访问控制服务,例如微处理器卡;

——初始化和发布过程(表明个人数据卡工作周期的开始,并且使数据卡为后续通信中给它传递符合本部分要求的数据做准备)。

因此,下列内容不属于本部分的范围:

——用于特定类型数据卡的实际功能的物理或者逻辑解决方案;

——如何处理在两个系统接口间的消息;

——数据卡外部的数据所使用的格式,以及在数据卡或其他地方用以清晰表达这类数据的方式。

2　规范性引用文件

下列文件中的条款通过GB/T 21715的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 2659—2000　世界各国和地区名称代码(eqv ISO 3166-1:1997)

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分:安全体系结构(idt ISO 7498-2:1989)

GB/T 14916　识别卡　物理特性(GB/T 14916—2006,ISO/IEC 7810:2003,IDT)

GB/T 15843.1—1999　信息技术　安全技术　实体鉴别　第1部分:概述(idt ISO/IEC 9798-1:1997)

ENV 1068:1993,Medical informatics—Healthcare information interchange—Registration of coding schemes

3　术语和定义

下列术语和定义适用于本部分。

3.1

国家　country

标识原始发行该设备国家的代码。

注:不必与设备持有者的国籍相同。本标准中设备是指卡本身。

3.2

数据完整性 data integrity

这一性质表明数据没有遭受以非授权方式所作的篡改或破坏。

[GB/T 9387.2—1995]

3.3

数据对象 data object

自然分组并且可标识为一个完整实体的数据集合。

3.4

数据子对象 data sub-object

数据对象的组成部分,且本身可被标识为一个单独的实体。

3.5

设备持有者 device holder

持有数据卡的个人。该卡中包含了标识此人为主的相关记录。

3.6

实体鉴别 entity authentication

证实某个实体是其声称的实体。

[GB/T 15843.1—1999]

3.7

删除 erasure

在一个给定的时间点之后,永久取消对一个数据实体的访问或者永久拒绝所有参与方对该数据实体的访问的过程。

注:这并不意味着从设备中对数据进行物理删除,而可以通过只改变安全性来永久拒绝所有参与方对数据实体的访问。

3.8

健康卡持有者 healthcard holder

持有健康数据卡的个人,该卡中包含了标识此人为主的相关记录。

3.9

健康数据卡 healthcare data card

用于健康领域且符合 GB/T 14916 的机器可读卡。

3.10

主行业标识符 major industry identifier;MII

标识准备使用数据卡的部门/行业的代码。

注:保健行业的 MII 指定为 80。

3.11

主记录标识符 major record identifier

链接到对应数据卡中和提供保健服务的系统中某一被记录人的主要记录的标识符。

3.12

记录 record

所采集数据的集合。

3.13

被记录人 record person

与一条可标识记录对应的个人,该记录包含与该人相关的数据。

3.14

安全性 security

保密性、完整性和可用性的组合。

4 缩略语

下列缩略语适用于本部分。

ASN.1	抽象语法记法 1 Abstract syntax notation, version 1
EN	欧洲标准 European Standard
HCP	保健受益人 healthcare person
ICC	集成电路卡 integrated-circuit card
IEC	国际电工委员会 International Electrotechnical Commission
ISO	国际标准化组织 International Organization for Standardization
MII	主行业标识符 major industry identifier
UML	统一建模语言 unified modelling language
UTC	协调世界时间 coordinated universal time

5 健康数据卡的基本数据对象模型——患者健康卡数据对象结构

本标准设计了一组能灵活地存储临床数据、并允许增加特定应用的基本数据对象。通过有效利用存储空间的方式，实现已存储数据的通用附加特性。

基本数据对象由基于面向对象模型的类结构组成，该模型的 UML 类框图如图 1 所示。

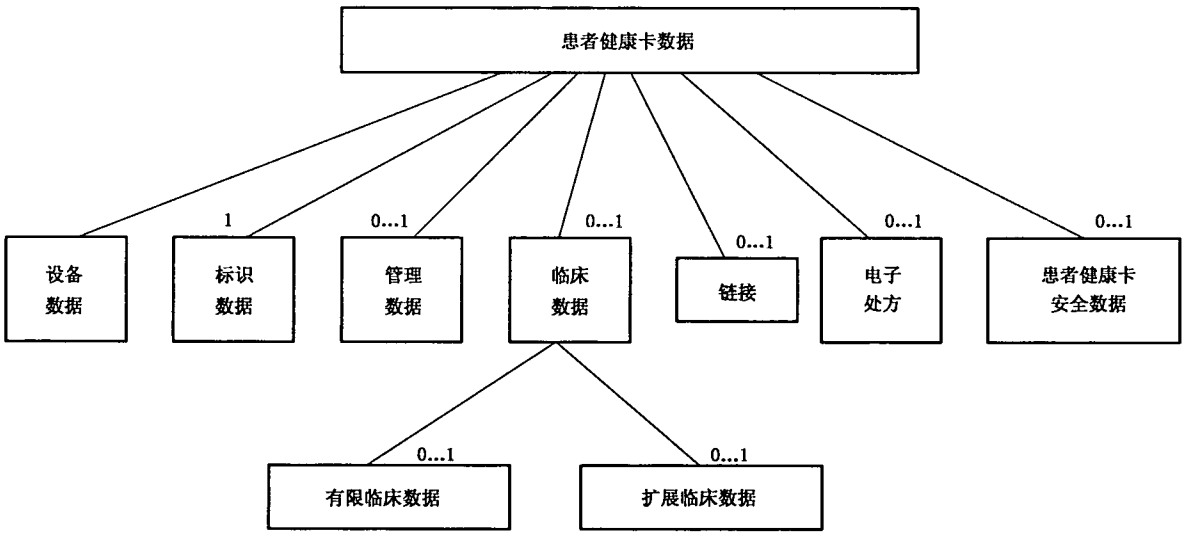

图 1 患者健康卡数据的总体结构

该面向对象的结构的内容在下面描述，也可能需要用到本部分没有定义的其他数据对象。

注 1：本部分只适用于包含健康数据的患者健康卡。本标准没有定义包含财务和保健赔偿数据的数据对象。

注 2：在保持特定语境标记时有可能需要获取数据对象并重新组合它们，在保持互操作性时也可能需要定义新的对象。

除具有用简单的构筑模块建立起复杂的聚合数据对象的能力外，本标准还允许在某些对象之间建立起关联，以便使信息可以共享。例如，该特征主要使一套附加属性可以用来为若干个所存储的信息对象提供服务。

6 供引用的基本数据对象

6.1 概述

本标准已定义了一系列普遍有用的数据类型，虽然这些定义本身没有内在的值，但是本标准可以用其来定义其他对象。可以与其他有关的信息对象相关联的情况下对这些对象进行相应操作来“附加值”。

6.2 内部链接

6.2.1 概述

本部分的数据模型中，很多对象主要用作其他对象的引用。例如，数据对象 RecordPerson(被记录人)其定义是与设备中记录的某人相关的基本标识信息。因为这是按顺序包含关于所有被记录人信息的聚合对象的一部分，所以指针可以是一个简单的一维整数。这种类型的指针称为 RecPersPointer(被记录指针)，并且被广泛地用于指向与特定信息对象相关的被记录人。

注：该内部链接的 RecPersPointer 尤其适用于患者健康卡中包含有不止一个可标识个人相关的记录的情况。

在其他情况下，已构建的对象包含一个更通用的指针：RefPointer(引用指针)，它是一个允许引用任一对象的标记序列。此处，任一对象可包括只能引用为已构建对象的一部分的子对象，而为了达到引用的目的可以通过使用一个具体应用标记和足够数量、层次深度的特定语境标记来实现。

指向某一保健受益人姓名的 RefPointer 可以包含带有合适标记(这里用他们的符号名称来表示)的下列信息：

保健受益人	[7]第 7 号保健受益人	[1]保健受益人姓名
应用标记	第一层语境	第二层语境

还有第三种可能性：允许在所有对象中使用链接对象来彼此建立链接。这是一个链接关联的有序列表。列表中的全部入口是其他对象的一个顺序列表，每一个其他对象都用 RefPointer 来定义。

例如：2 号链接可以链接 4 个对象：

1

2 RefPointer1 RefPointer2 RefPointer3 RefPointer4

3

该链接过程具体到在包含临床数据的数据卡中时，可以表示为：

诊断	RefPointer1
药物处方	RefPointer2
药物记录	RefPointer3
药物配发	RefPointer4

每个 ClinDat(临床数据)对象的 ClinRefPointer(临床引用指针)都可以指向这个链接表入口。

注：虽然“links(链接)”对象本身是开放可用的，但可限制访问已链接的对象。

下面要描述的引用对象可以与其他已定义的信息对象相关联。这种关联不是一种聚合。引用对象不是信息对象的一部分而是独立存在的，并且可以被若干对象引用。本部分使用这一概念是为了对被记录人、保健提供者和相关的附加属性进行引用(指向)。这些链接为数据赋值并且可以被用来提供具体的语境。

6.2.2 “Links”数据对象

“Links”(链接)数据对象用于生成在患者健康卡中的任何其他已定义数据对象之间的内部引用或链接。它是一个由子对象“Link”(单个链接)构成的序列。“链接”数据对象由对其他对象的引用序列组

成，其中对其他对象的引用是以“RefPointer”对象的形式来表示的。“LinkagePointer”(连接指针)对象指向“Link”数据对象。图 2 给出了“Links”数据对象的具体结构，表 1 给出了“Links”中单个实体的说明。

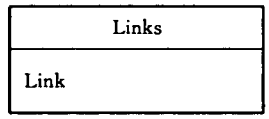

图 2 “Links”的结构

表 1 “Links”中单个实体的说明

对象	名称	数据类型	可出现频次	链接	说明
Link	链接	整数	1...M	—	是对其他对象的引用序列

6.2.3 “RefPointer”和“RefTag”数据对象

在本部分中，一般的引用指针定义为指向被引用的对象或子对象的有序标记列表。数据对象“RefPointer”(引用指针)应由整数型“RefTags”(引用标记)的序列组成。“RefTags”是一个符合本部分定义的对象的具体标记。表 2 给出了对“RefPointer”具体语境标记的详细说明。

表 2 “RefPointer”的说明

对象	名称	数据类型	可出现频次	长度	说明
RefPointer	引用指针	整数	1...M	—	是对其他对象的引用序列。该引用是另一个数据对象的 ASN. 1 标记

6.2.4 “RecPersPointer”数据对象

“RecPersPointer”(被记录人指针)数据对象用于引用某个存储在“RecordPerson”数据对象中的被记录人，且为整数型。表 3 给出了“RecPersPointer”的具体说明。

注：RecordPerson 对象在 GB/T 21715.5 中定义。

表 3 “RecPersPointer”的说明

对象	名称	数据类型	可出现频次	长度	说明
RecPersPointer	被记录人指针	整数	1	—	“RecPersPointer”(被记录人指针)用于引用某个存储在“RecordPerson”(被记录人)数据对象中的被记录人

6.3 代码型数据

6.3.1 概述

代码值的含义是由其对应的编码方案来决定的。本部分的总原则是：除非在本部分里做了特别的规定，否则不强制要求使用特定的编码方案。例如，GB/T 2659—2000 对国家代码的使用。

当本部分规定了某个特定的编码方案时，不再允许使用其他的任何编码方案。然而，对于任一未按上述形式引用的编码方案，将来都可对其进行调整，且与本标准的其他部分无关。

6.3.2 “CodingSchemesUsed”数据对象

在本部分中未规定的编码方案可以按照 ENV 1068:1993 中规定的编码方案的注册程序进行注册，并可以按照所注册的所有相关条件对其进行解释。ENV 1068:1993 规定了编码方案的注册程序，以及分配保健编码方案标志符(HCD)的程序。从而有可能引用已在国际上注册的编码方案和引用未在国际上注册但按照 ENV 1068:1993 条款 5 规定注册的编码方案。然而，当一个设备需要在开放环境中使用时，如果引用这些国际上未注册的专用编码方案则有可能会造成混乱。

来自未注册的编码方案(或者超出了特定应用范围的注册方案)的代码值是无法被理解的,除非信息的接收方与信息的发送方之间达成了使用其他的或非注册的编码方案的协定。

数据对象"CodingSchemesUsed"(所使用的编码方案)应由一个有序的子对象"CodingScheme"(编码方案)序列组成。其中,子对象"CodingScheme"应由编码标识符(用 CodeIdentifier 表示,6 个字符的八位位组串)、代码长度(用 CodeLength 表示,整数型)和可选的自由文本格式的文字说明(用 FreeTextComment 表示,1～20 个字符长度的八位位组串)三部分组成。"CodingSchemesUsed"的结构见图 3,表 4 给出了"CodingSchemesUsed" 中单个实体的规范。

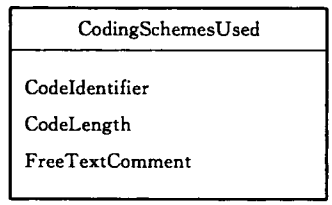

图 3 "CodingSchemesUsed"的结构

表 4 "CodingSchemesUsed"的说明

对象及其属性	名称	数据类型	可出现频次	长度	说明
CodingSchemesUsed	所使用的编码方案	类	1	N/A	
CodeIdentifier	编码标识符	字符串	1	6	标识所引用的特定编码方案
CodeLength	代码长度	整数	1	—	标识代码的长度
FreeTextComment	自由文本的文字说明	字符串	0...1	—	该可选的自由文本元素允许对编码方案文本进行限制

6.3.3 "CodedData"数据对象

"CodedData"(代码型数据)数据对象应包含对所用编码方案的引用和代码数据值,还可包含可选的自由文本,并且由相应的数据子对象"CodingSchemeRef"(编码方案引用)、"CodeDataValue"(代码数据值)和可选的"CodeDataFreeText"(代码数据自由文本)来表示。图 4 给出了数据对象 CodedData 的结构。

对象"CodingSchemeRef"是一个 RefPointer,该指针指向一个标识了在所用的对象编码方案中某个特定编码方案的值。如果 CodingSchemeRef=0,则本标准内含此编码方案。

已定义的数据类型"CodeDataValue"用来指明一个特定编码方案中的实际代码值。如果"CodeDataValue"的长度是一个八位位组,则随后的 CodeDataValue 为:

——"A"(表示关于管理的自由文本入口);

——"C"(表示关于临床的自由文本入口)。

在其他情况下,如果八位位组的长度大于 1,则 CodeDataValue 表示实际的代码值。表 5 给出了"CodedData"数据对象中单个实体的说明。

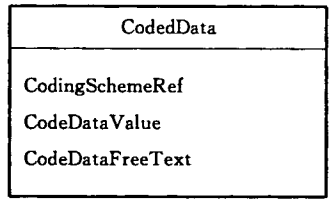

图 4 "CodedData"的结构

表 5 “CodedData”的说明

对象及其属性	名称	数据类型	可出现频次	长度	说明
CodedData	代码型数据	类	1	N/A	
CodingSchemeRef	编码方案引用	整数	1	—	是一个引用指针，该指针指向一个标识了在所用的对象编码方案中某个特定编码方案值
CodeDataValue	代码数据值	字符串	1	—	此字符串包含编码数据的值。如果它的长度为 1 个八位长的字符并且值为 A 或 C，那么 A 代表管理性数据的自由文本，C 代表临床数据的自由文本
CodeDataFreeText	代码数据自由文本	字符串	0...1	80	可选的元素，该自由文本允许对编码方案文本进行限制

6.4 附加属性

数据对象“AccessoryAttribute”(附加属性)应由一组有序的数据组成，这组数据对于记录有关对信息发送方和信息到达接收方的方式的审计跟踪是至关重要的。它应由以下内容组成：

——Date1(日期 1)，表示数据通过接口传送到数据卡的时间/日期；

——Date2(日期 2)，表示消息始发方获得数据的时间/日期；

——Place1(位置 1)，表示消息发送方的标识符/定位符，并且与“Person1”(个人 1)关联；

——Place2(位置 2)，表示数据原始作者的标识符/定位器；

——Personid3(个体标识 3)，人/设备/系统的代码或表示，它们所提供的信息已被加入到一个系统中；

——Securitylevel(安全级别)，应按照 A.6 中的 ASN.1 定义进行构建，并应表示与附加属性相关的数据对象中所包含的数据进行读、写、更新、删除等操作的权限；

——CompressionMethodData(压缩方法数据)，应按照 A.6 中的定义进行构建，并应包含一个 RefPointer(引用指针)，指向某张压缩方法学表中某个已定义的压缩方法学；它表示用于与这些附加属性相关的数据对象中包含的数据的方法学；

——ObjectSecurityAttribute(对象安全属性)。

“AccessoryAttribute”(附加属性)数据对象应由下列可选数据对象组成：

——“日期”(Date)类型数据对象：“Date1”(日期 1)和“Date2”(日期 2)；

——“RefPointer”类型数据：“Place/Person1”(位置/个人 1)和“Place/Person2”(位置/个人 2)；

——“Personid3”：由“RefPointer”类型的“PersonCode”(个人代码)和长度不超过 30 个字符的自由“PersonText”(个体文本)组成；

——“ObjectSecAttribute”(对象安全属性)：由一组“SecurityService”(安全服务)组成。

每个“SecurityService”数据对象应包含一组数字签名以及签名与加密的算法和密钥。图 5 给出了 AccessoryAttribute 的结构，AccessoryAttribute 的说明见表 6。

尽管上述属性是非强制性的，但建议尽可能使用全部属性。如果系统/媒介允许，建议每次传递所有这些属性(“个人标识 3”可能例外)。下面列出了这些属性按照规则应遵循的组合优先级：

{Date1,Place1,Place2,SecurityLevels,CompressionMethodData,ObjSecAttributes}

{Date1,Place1,Place2,SecurityLevels,CompressionMethodData,ObjSecAttributes}

{Date1,Place2,SecurityLevels,CompressionMethodData,ObjSecAttributes}

{Date1,SecurityLevels,CompressionMethodData,ObjSecAttributes}

{SecurityLevels,CompressionMethodData,ObjSecAttributes}

{ObjSecAttributes}

注：数据对象“AccessoryAttribute”可以和任何其他数据对象相关联。

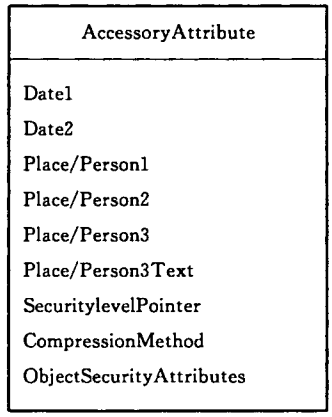

图 5 “AccessoryAttribute”的结构

表 6 “AccessoryAttribute”的说明

对象及其属性	名称	数据类型	可出现频次	长度	说明
AccessoryAttribute	附加属性	类	1	N/A	
Date1	日期 1	UTC 时间	1	8	是一个指向用于标识所用对象编码方案中某个特定编码方案的值的 RefPointer
Date2	日期 2	UTC 时间	0...1	8	
Place/Person 1	位置/个人 1	整数	1	—	
Place/Person 2	位置/个人 2	整数	0...1	—	
Place/Person 3	位置/个人 3	整数	0...1	—	
Place/Person 3Text	位置/个人 3 文本	字符串	0...1	—	
SecurityLevelPointer	安全级别指针	整数	0...1	—	
CompressionMethod	压缩方法	整数	0...1	—	
ObjectSecurityAttribute	对象安全属性	类	0...1	—	由多个“SecurityService”组成
SecurityService	安全服务	类	0...M	—	
SignatureAlgorithmID	签名算法标识	整数	0...1	—	关于签名算法表中某行的引用指针
SignatureVerificationKeyID	签名鉴别密钥标识	整数	0...1	—	关于签名鉴别密钥 ID 表中某行的引用指针
DigitalSignature	数字签名	位串	0...1	—	该属性包含数字签名的可计算的位串
EncryptionAlgorithmID	加密算法标识	整数	0...1	—	关于 EncryptionAlgorithmID(加密算法 ID)表中某行的引用指针
EncryptionKeyID	加密密钥标识	整数	0...1	—	关于密钥表中某行的引用指针
SecurityLevel	安全级别	类		—	布尔型序列

表 6（续）

对象及其属性	名称	数据类型	可出现频次	长度	说明
ReadSecAttribute	可读安全属性	布尔	0...1	—	如果为真，则该对象可读
WriteSecAttribute	可写安全属性	布尔	0...1	—	如果为真，则该对象可被写入数据
UpdateSecAttribute	可更新安全属性	布尔	0...1	—	如果为真，则该对象可更新
EraseSecAttribute	可删除安全属性	布尔	0...1	—	如果为真，则该对象应被应用程序解释为已删除
CompressMethodData	压缩方法数据	代码型数据	0...M	—	包含所用压缩方法学的代码型数据值的表示

7 设备和数据安全属性

7.1 概述

用于健康领域的数据卡中存储的数据对个人来说可能非常敏感。因此，本部分以数据对象形式提供了一系列安全属性，要求这些安全属性能提供所需的安全功能。实际数据内容（值）和使用这些数据元素的机制不在本标准的范围内。需强调的是，如果数据卡中没有实施合适的安全功能和安全机制，则安全属性将不能满足特定的安全需求。

“访问”权限由与各离散数据项相关的特定个体来决定。该权限由应用程序开发者定义，并且由自动化系统（如健康数据卡）来控制。这种权限可以在应用层定义，因而提供了应用和所在国家的一致性。

数据对象“SecurityService”用来存储实现这些安全功能和机制所需的数据。这些数据能附加在单个数据元上，从而当数据对象在不同形式的数据卡间传送时，能够保持源作者的安全需求。因此，这种机制能够保证数据在从主动媒介传向被动媒介，然后再返回主动媒介的过程中重建出原始的安全需求。这种能力还允许准确复制数据卡，例如失败后的重建。

7.2 与具体数据卡安全服务相关的数据对象

7.2.1 概述

所有的安全服务对象是传送与数据卡载有并且传输的患者数据有关的安全性所需要的，应根据以下定义进行构建。

7.2.2 与设备安全性相关的数据

保健受益人持有的数据卡可能需要以下的安全服务：

——设备鉴别；

——数据卡持有者鉴别；

——对访问数据卡中数据的 HCP 的鉴别。

这些安全服务由以下对象提供：

——数据卡持有者验证，及其相关的数据对象“PatCardHolderVer”（数据卡持有者验证）；

——数据卡鉴别，及其相关的数据对象“DevClassAuthenticateData”（设备类鉴别数据）；

——用于访问控制的经过数据卡鉴别的 HCP 类别，及其相关的数据对象“HcpAuthenticateData”（HCP 鉴别数据）。

7.2.3 与 HCP 持有数据卡有关的数据

与 HCP 持有数据卡有关的数据对象应提供标识、访问控制和签名功能。这些功能由大量分离的子对象提供。与 HCP 和对其负责的机构相关的标识信息由数据对象“HcpData”（HCP 数据）提供，它由其内部具有固定顺序排列的三部分数据组成，即：保健受益人标识数据、保健地点位置数据和附加属性（可选）。

7.2.4 与患者健康卡安全性相关的数据

健康卡需要安全服务来控制对其包含的医疗数据的访问。这些服务受数据对象“PatientHealthcardSecurity”(患者健康卡安全性)决定和控制。“患者健康卡安全性”的结构和说明见图6和表7。

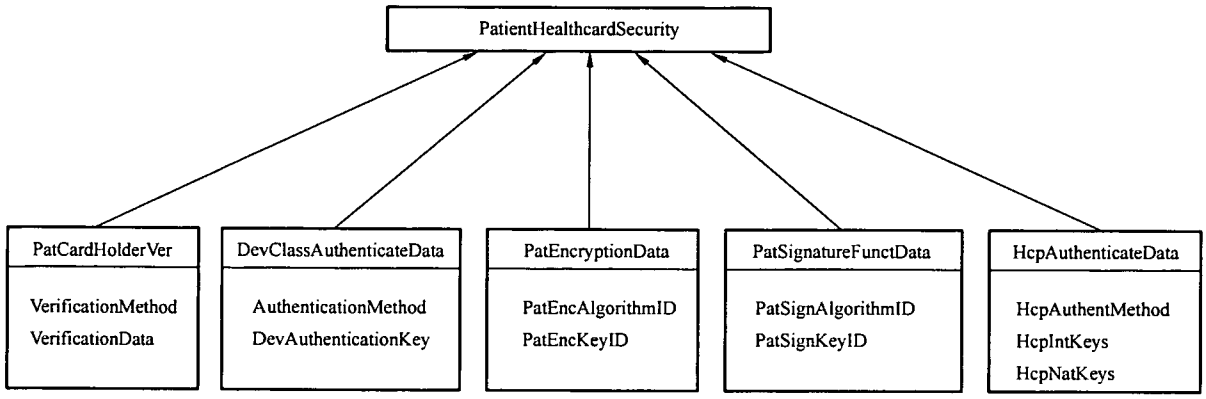

图6 “PatientHealthcardSecurity”的结构

表7 “PatientHealthcardSecurity”的说明

对象及其属性	名称	数据类型	可出现频次	长度	说明
PatientHealthcardSecurity	患者健康卡安全性	类	1	N/A	
PatCardHolderVer	数据卡持有者鉴别	类	1	N/A	
VerificationMethod	验证方法	代码型数据	1	—	包含用来标识方法学的代码型数据，该方法学与VerificationData对象中的数据配合使用来验证被记录人的身份是否正确
VerificationData	验证数据	位串	1	—	
DevClassAuthenticateData	设备类鉴别数据	类	1	N/A	
AuthenticationMethod	鉴别方法	代码型数据	1	—	对用于鉴别数据卡的方法学进行规定的代码型数据
DevAuthenticationKey	设备鉴别密钥	位串	1	—	包含设备鉴别密钥
PatEncryptionData	患者加密数据	类	1	N/A	
PatEncAlgorithmID	患者加密算法标识	位串	1	—	包含加密算法的OID(对象标识)
PatEncKeyID	患者加密密钥标识	位串	1	—	包含加密密钥的ID
PatSignatureFunctData	患者签名功能数据	类	1	N/A	
PatSignAlgorithmID	患者签名算法标识	位串	1	—	包含签名算法的OID(对象标识)
PatSignKeyID	患者签名密钥标识	位串	1	—	包含签名密钥的ID
HcpAuthenticateData	HCP鉴别数据	类	1	N/A	
HcpAuthentMethod	HCP鉴别方法	代码型数据	1	—	对用于鉴别HCP的鉴别方法学进行规定的代码型数据

表 7（续）

对象及其属性	名称	数据类型	可出现频次	长度	说明
HcpIntKeys	HCP 国际访问密钥	类		N/A	包含一套国际访问密钥
HcpIntKey	HCP 国际访问密钥	位串	1...8	—	包含一个国际访问密钥的位串
HcpNatKeys	HCP 国家访问密钥	类		N/A	包含一套国家访问密钥 注：国家访问密钥仅限于患者健康卡发行国使用。
HcpNatKey	HCP 国家访问密钥	位串	1...8	—	包含一个国家访问密钥的位串

附 录 A
（规范性附录）
ASN.1 数据定义

A.1 “Link”数据对象

```
Links ::= SEQUENCE OF Link
-- This is a sequence of references to other objects
Link ::= SEQUENCE OF LinkagePointer
LinkagePointer ::= INTEGER
```

A.2 “ReferencePointer”和“ReferenceTag”数据对象

```
RefPointer ::= SEQUENCE OF RefTag
RefTag ::= INTEGER
-- This object can hold the ASN.1-tag of another object
```

A.3 “RecordPersonPointer”数据对象

```
RecPersPointer ::= INTEGER
```

A.4 “CodingSchemesUsed”数据对象

```
CodingSchemesUsed ::= SEQUENCE OF CodingScheme
CodingScheme ::= SEQUENCE
{
CodeIdentifier [0] OCTET STRING (SIZE (6)),
CodeLength [1] INTEGER,
Comment [2] OCTET STRING (SIZE(1...20)) OPTIONAL
}
```

A.5 “CodedData”数据对象

```
CodedData ::= SET
{
CodingSchemeRef [0] RefPointer,
CodeDataValue [1] OCTET STRING,
CodeDataFreeText [2] OCTET STRING OPTIONAL
}
-- CodingSchemeRef is a RefPointer pointing at a
-- value that identifies a particular coding scheme
-- within the object coding schemes used.
-- If CodingSchemeRef = 0, then the coding scheme
-- is implicit in this International Standard.
-- If the length of the CodeDataValue
-- is one OCTET and the
```

```
-- CodeDataValues are defined as A or C, then
-- "A" = Administrative free text entry and
-- "C" = Clinical free text entry.
```

A.6 “AccessoryAttributes”数据对象

```
AccessoryAttributes ::= SET
{
Date1 [0] UTC TIME (SIZE (6...12)) OPTIONAL,
Place/Person1 [2] RefPointer OPTIONAL,
Place/Person2 [3] RefPointer OPTIONAL,
Personid3 [4] SET OPTIONAL
{
PersonCode [0] RefPointer,
PersonText [1] OCTET STRING (SIZE(0...30))
},
SecurityLevelPointer [5] SecurityLevels OPTIONAL,
-- Points to SecurityLevels table.
CompressionMethod [6] CompressMethodData OPTIONAL,
-- Points to CompressMethodData.
ObjectSecAttributes [7] SET OF SecurityServices OPTIONAL
{
SecurityServices ::= SEQUENCE
{
SignatureAlgorithmID [0] RefPointer OPTIONAL,
-- This points to the algorithm table.
SignatureVerificationKeyId [1] RefPointer OPTIONAL,
-- This points to the signature verification key.
DigitalSignature [2] BIT STRING,
EncryptionAlgorithmID [3] RefPointer,
-- This points to the algorithm table.
EncryptionKeyId [4] RefPointer
-- This points to the encryption key.
}
}
}
SecurityLevels ::= SEQUENCE
{
ReadSecAttribute [0] SecAttData OPTIONAL
WriteSecAttribute [1] SecAttData OPTIONAL
UpdateSecAttribute [2] SecAttData OPTIONAL
EraseSecAttribute [3] SecAttData OPTIONAL
}
SecAttData ::= Sequence of Boolean
```

```
{
Always [0],
-- True = Always available, if false functionality is protected
and is controlled by one or more of the underlying
parameters.
ExtAuth [1],
-- True = Requires external authentication.
HoldAg [2],
-- True = Requires data-card holder agreement.
OrigAg [3]
-- True = Can only be done by originator of data element.
}
CompressMethodData ::= Set of CodedData
```

A.7 “PatientHealthcardSecurity” 数据集

```
PatientHealthcardSecurity ::= SET
{
PatCardHolderVer [0] SEQUENCE,
{
VerificationMethod [0] CodedData,
VerificationData [1] BIT STRING
}
DevClassAuthenticateData [1] SEQUENCE,
{
AuthenticationMethod [0] CodedData,
DevAuthenticationKey [1] BIT STRING
}
PatEncryptionData [2] SEQUENCE,
{
PatEncAlgorithmID [0] RefPointer,
-- This points to the algorithm table.
PatEncKeyID [1] RefPointer -- This points to the key table.
}
PatSignatureFunctData [3] SEQUENCE,
{
PatSignAlgorithmID [0] RefPointer,
-- This points to the algorithm table.
PatSignKeyID [1] RefPointer -- This points to the key table.
}
HcpAuthenticateData [4] SEQUENCE
{
HcpAuthentMethod [0] CodedData,
HcpIntKeys [1] SEQUENCE,
```

```
{
HcpIntKey [0] BIT STRING,
}
HcpNatKeys [2] SEQUENCE
{
HcpNatKey [0] BIT STRING
}
}
}
HcpKeyID ::= OCTET
AlgorithmTable ::= Sequence of AlgorithmID
AlgorithmID ::= String
KeyTable ::= Sequence of Key
Key ::= String
```

参 考 文 献

[1] GB/T 4880.2—2000 语种名称代码 第2部分：3字母代码 (eqv ISO 639-2:1998)

[2] GB/T 7408—2005 数据元和交换格式 信息交换 日期和时间表示法(ISO 8601:2000, IDT)

[3] GB/T 18794.2—2002 信息技术 开放系统互连 开放系统安全框架 第2部分：鉴别框架 (ISO/IEC 10181-2:1996,IDT)

[4] EN 1387:1996 Machine readable cards—Health care applications—Cards: General characteristics(will be replaced by ISO 20301)

[5] ISO 639-1:2002 Codes for the representation of names of languages—Part 1: Alpha-2 code

[6] ISO 4217:2001 Codes for the representation of currencies and funds

[7] ISO/IEC 5218:2004 Information technology—Codes for the representation of human sexes

[8] ISO 6093:1985 Information processing—Representation of numerical values in character strings for information interchange

[9] ISO/IEC 6523-1:1998 Information technology—Structure for the identification of organizations and organization parts—Part 1: Identification of organization identification schemes

[10] ISO/IEC 8824-1:2002 Information technology—Abstract Syntax Notation One (ASN.1): Specification of basic notation

[11] ISO 8859-1:1998 Information technology—8-bit single-byte coded graphic character sets—Part 1: Latin alphabet No. 1

[12] ISO 8908:1993 Banking and related financial services—Vocabulary and data elements (Withdrawn 2001-01)

[13] ISO/IEC 9594-8:2001 Information technology—Open Systems Interconnection—The Directory: Public-key and attribute certificate frameworks

[14] CCITT Numbering plan for the international telephone service

中 华 人 民 共 和 国
国 家 标 准
健康信息学 患者健康卡数据
第2部分:通用对象
GB/T 21715.2—2008/ISO 21549-2:2004
*
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 1.5 字数 34 千字
2008年7月第一版 2008年7月第一次印刷
*
书号:155066·1-32093 定价 20.00 元

GB/T 21715.2—2008/ISO 21549-2:2004

GB/T 21715.2-2008