ICS 35.240.80
CCS L 67

中华人民共和国国家标准

GB/T 21715.2—202X/ISO 21549-2:2014
代替GB/T 21715.2—2008

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 21549-2:2014，IDT）

（征求意见稿）

202X－XX－XX 发布　　202X－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 21715《健康信息学　患者健康卡数据》的第2部分。GB/T 21715已经发布了以下部分：

——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：用药数据；
——第 8 部分：链接。

本文件代替GB/T 21715.2—2008《健康信息学　患者健康卡数据　第2部分：通用对象》，与GB/T 21715.2—2008相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了“健康数据卡”的定义（见 3.9，2008 年版的 3.9）；
b) 删除了“主行业标识符”、“主记录标识符”（见 2008 版的 3.10、3.11）；
c) 删除了“EN”、“ICC”、“IEC”、“ISO”、“MII”（见 2008 年版的第 4 章）；
d) 更改了“UTC”的表述（见第 4 章，2008 年版的第 4 章）；
e) 更改了“患者健康卡数据的总体结构图”（见第 5 章，2008 年版的第五章）；
f) 更改了“内部链接”中“概述”的内容（见 6.2.1，2008 年版的 6.2.1）；
g) 删除了“‘Links’数据对象”（见 2008 年版的 6.2.2）；
h) 删除了“‘ RecPersPointer’数据对象”（见 2008 年版的 6.2.4）；
i) 更改了“‘CodingSchemesUsed’数据对象”的内容（见 6.3.2，2008 年版的 6.3.2）；
j) 更改了“‘CodedData’数据对象”的内容（见 6.3.3，2008 年版的 6.3.3）；
k) 更改了“附加属性”的内容（见 6.4，2008 年版的 6.4）；
l) 更改了“‘AccessoryAttribute’的结构”图（见图 4，2008 年版的图 5）；
m) 更改了“‘AccessoryAttribute’的说明”表（见表 4，见 2008 年版的表 6）；
n) 增加了“‘PersonCode’的单个实体”表、“‘SecurityService’的单个实体”表、“‘SecurityLevels’的单个实体”表、“‘CompressMethodData’的单个实体”表、“‘SecAttData’的单个实体”表（见表 5、表 6、表 7、表 8、表 9）；
o) 增加了“‘SecurityService’的结构”图（见图 5）；
p) 删除了“‘PatientHealthcardSecurity’的结构”图（见 2008 年版的图 6）；
q) 增加了“‘PatientHealthcardSecurityData’的结构”图（见图 6）；
r) 更改了“‘PatientHealthcardSecurity’的说明”表（见表 10，见 2008 年版的表 7）；
s) 增加了“‘DevClassAuthenticateData’的单个实体”表、“‘HcpAuthenticateData’的单个实体”表、“‘PatCardHolderVer’的单个实体”表、“‘PatSignatureFunctionData’的单个实体”表、“‘PatEncryptionData’的单个实体”表、“‘KeyTable’的单个实体”表、“‘AlgorithmTable’的单个实体”表（见表 11、表 12、表 13、表 14、表 15、表 16、表 17）；
t) 修改了附录 A（见附录 A，2008 年版的附录 A）。

本文件等同采用ISO 21549-2:2014《健康信息学　患者健康卡数据　第2部分：通用对象》。

本文件做了下列最小限度的编辑性改动：

本文件的附录A为规范性附录。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国标准化研究院提出并归口。

本文件起草单位：中国标准化研究院、中国人民解放军总医院、北京航空航天大学、上海中医药大学、深圳市卫生健康发展研究和数据管理中心、福建省中科标准科技有限责任公司、浙江大学、浙江师范大学、北京信息科技大学、厦门市众科佰联标准化服务有限公司、福建理工大学。

本文件主要起草人：

本文件及其所代替文件的历次版本发布情况为：

——2008 年首次发布为 GB/T 21715.2—2008；

——本次为第一次修订。

引　言

本文件为有限的临床数据提供了数据结构和定义，供患者持有的医疗保健数据卡使用。

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，临床数据，处方和链接是可选的。

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；

——医疗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，每类数据都应包含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～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

本文件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，或被它们所引用。但并不规定或给出用于存储在设备中的强制性特定数据集。

本文件适用于记录或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文件的范围（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文件要求的数据做准备）。

因此，下列内容不属于本文件的范围：

——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

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 16649（所有部分）　识别卡　集成电路卡

ISO 21090　健康信息学　信息交换用协调数据类型（Health informatics—Harmonized data types for information interchange）

3　术语和定义

下列术语和定义适用于本文件。

3.1

国家　country

标识原始发行该设备的国家代码。

注：不必与设备持有者的国籍相同。本文件中设备是指卡本身。

3.2

数据完整性 data integrity

表明数据没有遭受以非授权方式所作的篡改或破坏的性质。

[来源：GB/T 9387.2—1995，3.3.21]

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。

注：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

证实一个实体就是所声称的实体。

[来源：GB/T 15843.1—2017，3.14]

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访问的过程。

注：这并不涉及从设备中对数据进行物理删除，而是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。

注：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 16649的机器可读卡。

3.10

记录 record

所采集数据的集合。

3.11

被记录人 record person

与一条可标识记录对应的个人。

注：该记录包含与该人相关的数据。

3.12

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文件。

ASN.1：抽象语法记法1（Abstract Syntax Notation，Version1）

HCP：保健受益人（Healthcare Person）

UML：统一建模语言（Unified Modelling Language）

UTC：协调世界时间（Universal Time Coordinated）

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

本文件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类框图见图1。

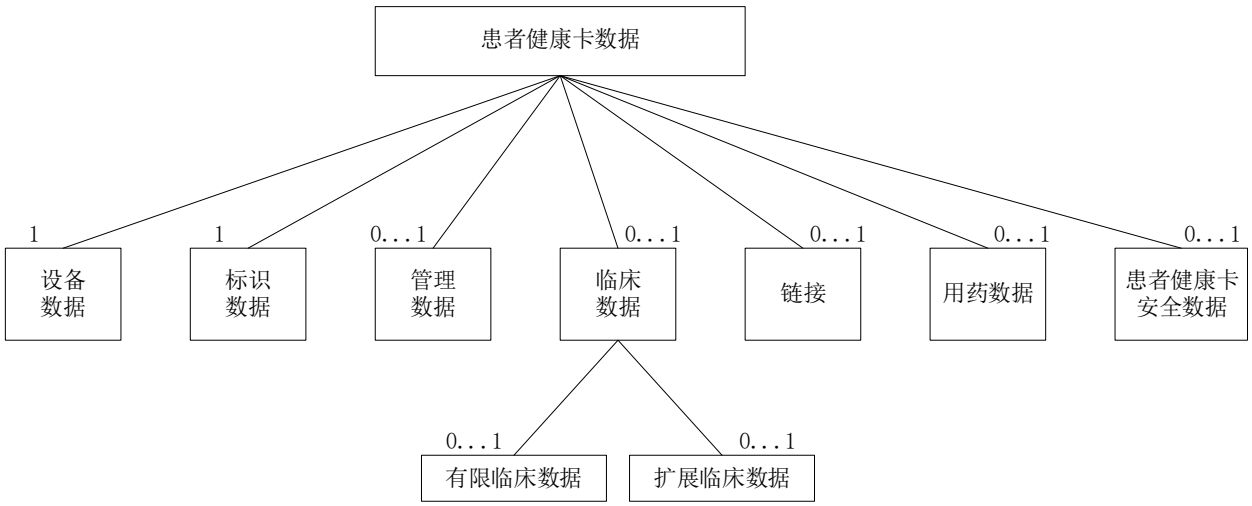

图1 患者健康卡数据的总体结构

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

注1：本文件只适用于包含健康数据的患者健康卡。本文件没有定义包含财务和医疗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，本文件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

本文件已定义了一系列普遍有用的数据类型，这些定义本身没有内在的值，但本文件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

本文件的数据模型中，很多对象主要用作其他对象的引用。在许多情况下，构造对象包含一个RefPointer的通用指针,该指针是允许引用任何对象(包括只能作为构造对象的一部分被引用的子对象）的标记序列，使用应用程序特定的标记和大量上下文特定的标签进行足够深入的引用。

6.2.2 “RefPointer”和“RefTag”数据对象

在文件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。

“RefTag”是本文件中定义的对象的具体标记。每一个“RefTag”都以不断增加的深度指定了上下文特定的标签，“RefPointer”的单个实体见表1。

表1 “RefPointer”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	RefTag	引用标记	整数	1..*	—	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

6.3 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。本文件的总原则是：不强制要求使用特定的编码方案（本文件有特别规定除外）。例如，GB/T 2659.1—2022对国家代码的使用。

当本文件规定了某个特定的编码方案时，不再允许使用其他编码方案。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，且与本文件的其他部分无关。

6.3.2 “CodingSchemesUsed”数据对象

根据ISO 21090的编码方案应由唯一标识符引用，该标识符允许对标准代码系统和其他本地代码系统进行模糊引用。如ISO或HL7已将唯一标识符分配给编码方案，则应使用这些标识符。其他实现应使用适当的ISO对象标识符（OID）或UUID来构建全局唯一的本地编码方案标识符。

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）、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comment表示，长度在1个～20个字符长度的八位组字符串）三部分组成。“CodingScheme”的结构见图2，“CodingScheme”的单个实体见表2。

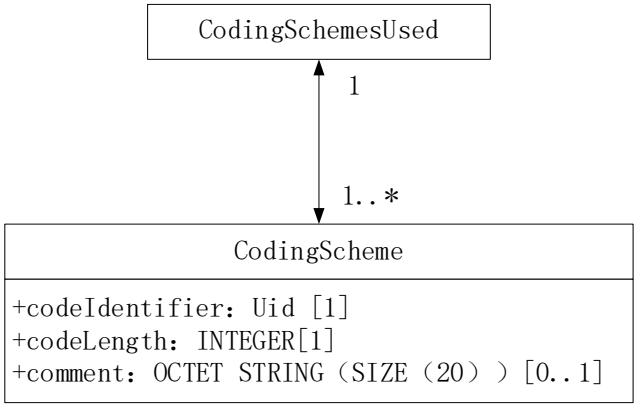

图2 “CodingScheme”的结构

表2 “CodingScheme”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	codeIdentifier	编码标识符	字符串	1	C1..64	标识所引用的特定编码方案
2	codeLength	代码长度	整数	1	—	标识代码的长度
3	comment	自由文本的文字说明	字符串	0..1	C1..20	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。

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，则本文件内含此编码方案。

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。

“CodedData”的结构见图3，“CodedData”的单个实体见表3。

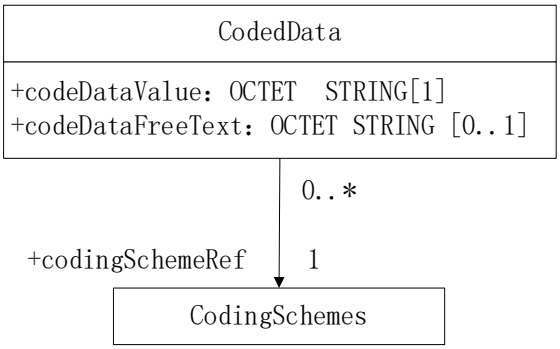

图3 “CodedData”的结构

表3 “CodedData”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	codingSchemeRef	编码方案引用	引用指针	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。如果CodingSchemeRef=0，则使用以下代码集：A=管理数据自由文本，C=临床数据自由文本
2	CodeDataValue	代码数据值	字符串	1		此字符串包含编码数据的值。
3	CodeDataFreeText	代码数据自由文本	字符串	0..1		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，包括：

——date1（日期1）：数据通过接口传送到数据卡的时间/日期；

——date2（日期2）：消息始发方获得数据的时间/日期；

——place1（位置1）：消息发送方的标识符/定位符，并与“Person1”（个人1）关联；

——place2（位置 2）：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，它们所提供的信息被添加到一个系统中，成为“消息”中的数据；

——securitylevel（安全级别）：应按照附录 A 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）：应按照附录 A 中的 ASN，1 定义进行构建，并应包含一个 RefPointer（引用指针），指向某张压缩方法表中定义的压缩方法；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；

——object security attributes（对象安全属性）。

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。

尽管上述属性是非强制性的，宜尽可能使用全部属性。如果系统/媒介允许，宜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， date2， place1， place2， personid3， 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“AccessoryAtiribute”可以和任何其他数据对象相关联。

“AccessoryAtiribute”的结构见图4，“AccessoryAtiribute”的单个实体见表4。

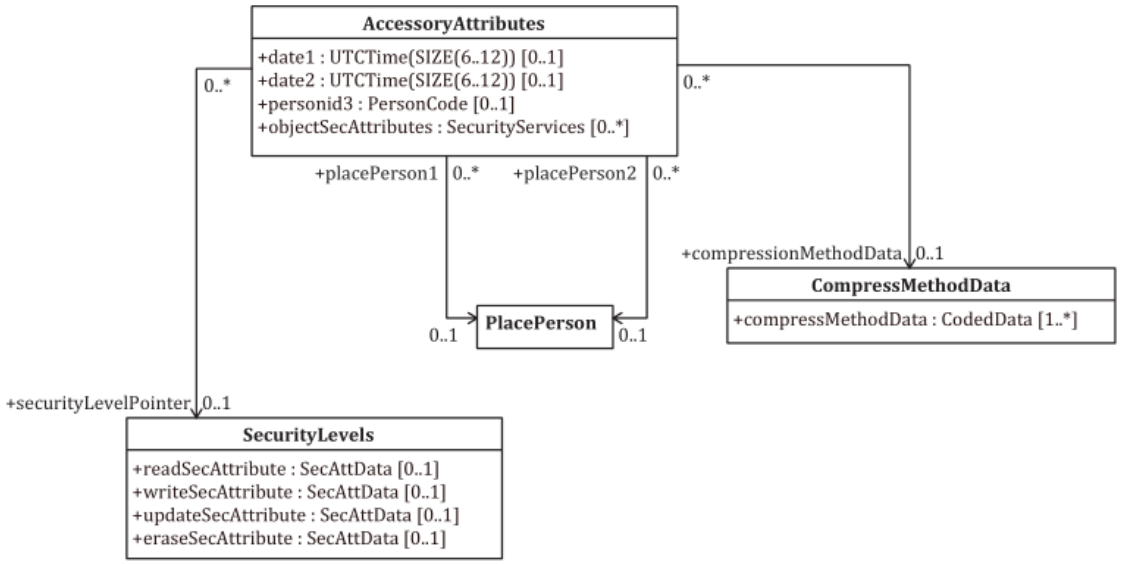

图4 “AccessoryAttribute”的结构

表4 “AccessoryAttribute”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	date1	日期1	UTC时间	0..1		
2	date2	日期2	UTC时间	0..1		

序号	对象	名称	数据类型	可出现频次	长度	说明
3	personid3	个人标识3	人员代码	0..1		
4	objectSecAttributes	对象安全属性	安全服务	0..*	—	
5	securityLevelPointer	安全级别指针	引用指针	0..1	—	是一个指向“securityLevels”对象的引用指针
6	placePerson1	位置个人1	引用指针	0..1	—	是一个指向“PlacePerson”对象的引用指针
7	placePerson2	位置个人2	引用指针	0..1	—	是一个指向“PlacePerson”对象的引用指针
8	compressionMethodData	压缩方法数据	引用指针	0..1		是一个指向“CompressionMethodData”对象的引用指针

“PersonCode”的单个实体见表5。

表5 “PersonCode”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	personCode	个人代码	引用指针	1		
2	personText	个人文本	字符串	0..1		

“SecurityService”的结构见图5，“SecurityService”的单个实体见表6。

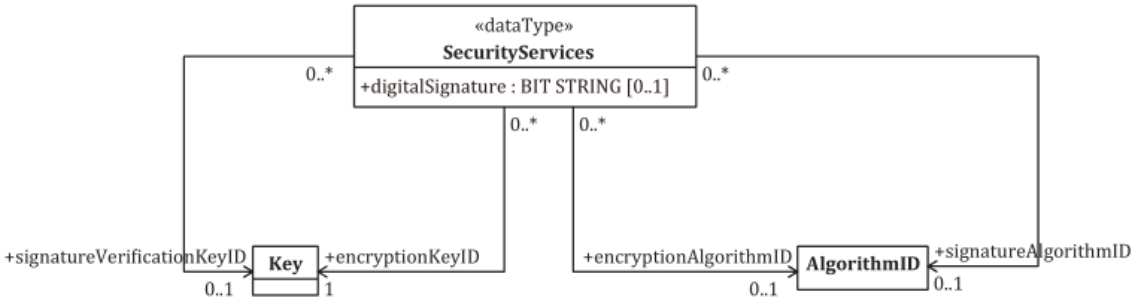

图5 “SecurityService”的结构

表6 “SecurityService”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	digitalSignature	数字签名	字符串	0..1		该属性包含数字签名的可计算的位串
2	signatureAlgorithmID	签名算法标识	引用指针	0..1		关于签名算法表中某行的引用指针
3	signatureVerificationKeyID	签名鉴别密钥标识	引用指针	0..1		关于签名鉴别密钥ID表中某行的引用指针
4	encryptionAlgorithmID	加密算法标识	引用指针	0..1		关于EncryptionAlgorithmID（加密算法ID）表中某行的引用指针
5	encryptionKeyID	加密密钥标识	引用指针	0..1		关于密钥表中某行的引用指针

“SecurityLevels”的单个实体见表7。

表7 “SecurityLevels”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	readSecAttribute	可读安全属性	安全属性数据	0..1		该属性设置读取对象的规则。

序号	对象	名称	数据类型	可出现频次	长度	说明
2	writeSecAttribute	可写安全属性	安全属性数据	0..1		该属性设置向对象写入数据的规则
3	updateSecAttribute	可更新安全属性	安全属性数据	0..1		该属性设置用于更新对象数据的规则
4	eraseSecAttribute	可删除安全属性	安全属性数据	0..1		该属性设置用于擦除对象数据的规则

“CompressMethodData”的单个实体见表8。

表8 “CompressMethodData”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	compressMethodData	压缩方法数据	编码数据	1..*		包含所用压缩方法学的代码型数据值的表示

“SecAttData”的单个实体见表8。

表9 “SecAttData”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	always		布尔	1		如虚假功能受到一个或多个底层参数的保护并受其控制，则True=始终可用
2	extAuth		布尔	1		true=需要外部认证
3	holdAg		布尔	1		true=需要数据卡持有人同意
4	origAg		布尔	1		true=只能由数据元素的发起者完成

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文件的范围内。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 特定数据卡的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 患者设备安全相关数据

患者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“PatCardHoldcrVcr”（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。这些功能由大重分离的子对象提供。与HCP和及其责任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 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“PatientHealth-cardSccurity”（患者健康卡安全性）决定和控制。“PatientHealthcardSecurityData”的结构见图6，“PatientHealthcardSecurity”的单个实体见表10。

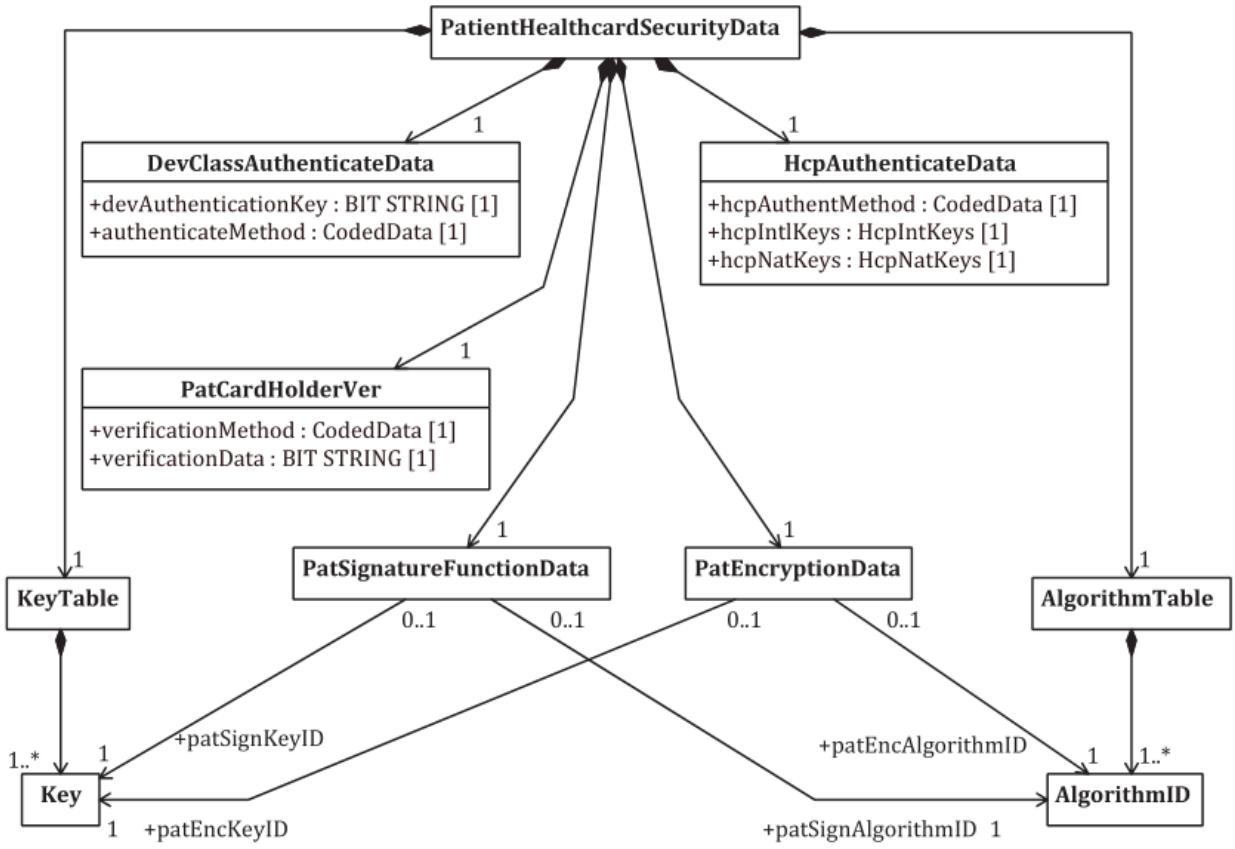

图6 “PatientHealthcardSecurityData”的结构

表10 “PatientHealthcardSecurity”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	DevClassAuthenticateData	设备类鉴别数据	类	1	N/A	
2	HcpAuthenticateData	HCP鉴别数据	类	1	N/A	
3	PatCardHolderVer	数据卡持有者鉴别	类	1	N/A	
4	PatSignatureFunctData	患者签名功能数据	类	1	N/A	
5	PatEncryptionData	患者加密数据	类	1	N/A	
6	KeyTable	关键字表	类	1		
7	AlgorithmTable	算法表	类	1		

“DevClassAuthenticateData”的单个实体见表11。

表11 “DevClassAuthenticateData”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	devAuthenticationKey	设备签别密钥	位串	1	—	包含设备鉴别密钥
2	authenticateMethod	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

“HcpAuthenticateData”的单个实体见表12。

表12 “HcpAuthenticateData”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	HcpAuthentMethod	HCP鉴别方法	代码型数据	1	—	对用于鉴别HCP的签别方法学进行规定的代码型数据
2	HcpIntKeys	HCP国际访问密钥	类	1	N/A	包含一套国际访问密钥
3	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

“PatCardHolderVer”的单个实体见表13。

表13 “PatCardHolderVer”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	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
2	VerificationData	验证数据	位串	1	—	

“PatSignatureFunctionData”的单个实体见表14。

表14 “PatSignatureFunctionData”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	PatSignAlgorithmID	患者签名算法标识	位串	1	—	包含签名算法的OID（对象标识）
2	PatSignKeyID	患者签名密钥标识	位串	1	—	包含签名密钥的 ID

“PatEncryptionData”的单个实体见表15。

表15 “PatEncryptionData”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	PatEncAlgorithmID	患者加密算法标识	位串	1	—	包含加密算法的OID（对象标识）
2	PatEncKeyID	患者加密密钥标识	位串	1	—	包含加密密钥的ID

“KeyTable”的单个实体见表16。

表16 “KeyTable”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	Key	密钥	字符串	1..*		

“AlgorithmTable”的单个实体见表17。

表17 “AlgorithmTable”的单个实体

序号	对象	名称	数据类型	可出现频次	长度	说明
1	Algorithm	算法	字符串	1..*		

附 录 A
（规范性）
ASN.1 数据定义

```
CommonDataTypes DEFINITIONS ::= BEGIN
EXPORTS AccessoryAttributes, CodingSchemesUsed, CodedData, RefPointer
PatientHealthCardSecurityData;
--RefPointer data obiect
RefPointer ::= SEQUENCE OF RefTag
RefTag ::= INTEGER  --This object can hold the ASN.1-tag of another object
--CodingSchemesUsed and CodingScheme data objects
CodingSchemesUsed ::= SEQUENCE OF CodingScheme
CodingScheme ::= SEQUENCE
{
   CodeIdentifier  [0] OCTET STRING （SIZE（64））, --Size is changed from 6 to 64 to
                                                    --allow OIDs here
   codeLength      [1] INTEGER
   comment         [2] OCTET STRING（SIZE（1..20））OPTIONAL
}
--CodedData data obiect
CodedData ::= SET
{
   codingSchemeRef  [0] RefPointer, --CodingSchemeRef is a RefPointer pointing at a
                    --value that identifies a particular coding scheme
                    --within the obiect coding schemes used.
                    --If CodingSchemeRef=0, then the coding scheme
                    --is implicit in this International Standard
   codeDatavalue    [1] OCTET STRING,
   codeDataFreeText [2] OCTET STRING OPTIONAL
}
--AccessoryAttributes data object

AccessoryAttributes ::= SET
{
   date1               [0] UTCTime    OPTIONAL,
   placePerson1        [1] RefPointer OPTIONAL, --This is a pointer to a person/place
                                        --identifier
                                        --stored elsewhere
   placePerson2        [2] RefPointer OPTIONAL, --This is a pointer to a person/place
                                        --identifier
                                        --stored elsewhere
   personid3           [3] PersonCode OPTINAL,
```

```
   securityLevelPointer [4] SecurityLevels OPTIONAL, --Points to Securitylevels
                                                     --table
   compressionMethod    [5] CompressMethodData OPTIONAL,--Points to CompressMethodData
   objectSecAttributes  [6] SET OF Securityservices OPTIONAL
}
PersonCode ::= SET
    {
      personCode [0] RefPointer, --This is a pointer to a person identifier
                                 --stored elsewhere
      personText [1] OCTET STRING (SIZE (0..30) )
    }
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
{
   always    [0] BOOLEAN, --True = Always available, if false
                          --functionality is protected
                          --and is controlled by one or more of
                          --the underlying parameters.
   extAuth   [1] BOOLEAN, --True = Requires external authentication.
   holdAg    [2] BOOLEAN, --True = Requires data-card holder agreement.
   origAg    [3] BOOLEAN  --True = Can only be done by originator
                          --of data element.
}
CompressMethodData ::= SET OF CodedData
--Patient Healthcard Security data set
PatientHealthCardSecurityData ::= SET
```

```
{
   patCardHolderVer          [0] PatCardHolderVer,
   devClassAuthenticateData [1] DevClassAuthenticateData,
   patEncryptionData         [2] PatEncryptionData,
   patSignatureFunctData     [3] PatSignatureFunctData,
   hcpAuthenticateData       [4] HcpAuthenticateData,
   keyTable                  [5] KeyTable,
   algorithmTable            [6] AlgorithmTable
}
PatCardHolderVer :: = SET
{
   verifcationMethod  [0] CodedData,
   verifcationData    [1] BIT STRING
}
DevClassAuthenticateData ::= SET
{
   authenticationMethod  [0] CodedData,
   devAuthenticationKey  [1] BIT STRING
}
PatEncryptionData ::= SET
{
   patEncAlgorithmID [0] RefPointer, --This points to a line in the algorithm table.
   patEncKeyID       [1] RefPointer  --This points to a line in the key table.
}
PatSignatureFunctData ::= SET
{
   patSignAlgorithmID [0] RefPointer, --This points to a line in the algorithm table.
   patSignKeyID       [1] RefPointer  --This points to a line in the key table.
}
HcpAuthenticateData ::= SET
{
   hcpAuthentMethod [0] CodedData,
   hcpIntKeys       [1] HcpIntKeys,
   hcpNatKeys       [2] HcpNatKeys
}
HcpIntKeys ::= SEQUENCE
{
   hcpIntKey [0] BIT STRING
}
HcpNatKeys ::= SEQUENCE
{
   hcpNatKey [0] BIT STRING
}
```

```
AlgorithmTable ::= SEQUENCE OF AlgorithmID
AlgorithmID ::= OCTET STRING
KeyTable ::= SEQUENCE OF Key
Key ::= OCTET STRING
HcpKeyID ::= OCTET STRING （SIZE（1））
END
```

参 考 文 献

[1] GB/T 2659.1—2022 世界各国和地区及其行政区划名称代码 第1部分：国家和地区代码

[2] GB/T 4880.1—2005 语种名称代码 第1部分：2字母代码

[3] GB/T 4880.2—2000 语种名称代码 第2部分：3字母代码

[4] GB/T 7408.1—2023 日期和时间 信息交换表示法 第1部分：基本原则

[5] 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

[6] GB/T 12406—2022 表示货币的代码

[7] GB/T 14916—2022 识别卡 物理特性

[8] GB/T 15843.1—2017 信息技术 安全技术 实体鉴别 第1部分：总则

[9] GB/T 16262.1—2006 信息技术 抽象语法记法一（ASN.1） 第1部分：基本记法规范

[10] GB/T 16264.8—2005 信息技术 开放系统互连 目录 第8部分：公钥和属性证书框架

[11] 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

[12] GB/T 38999—2020 健康信息学 健康卡 通用特性

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

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

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

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

[17] CCITT Numbering plan for the international telephone service