国 际 电 信 联 盟

ITU-T

H.812

(11/2017)

国际电信联盟
电信标准化部门

H 系列：视听及多媒体系统

电子医疗多媒体服务和应用 – 个人健康系统

个人互联健康系统的互操作性设计导则：服务接口

ITU-T H.812 建议书

国际电信联盟

ITU-T H 系列建议书

视听及多媒体系统

可视电话系统的特性	H.100-H.199
视听业务的基础设施	
概述	H.200-H.219
传输多路复用和同步	H.220-H.229
系统概况	H.230-H.239
通信规程	H.240-H.259
活动图像编码	H.260-H.279
相关的系统问题	H.280-H.299
视听业务的系统和终端设备	H.300-H.349
视听和多媒体业务的号码簿业务体系结构	H.350-H.359
视听和多媒体业务的服务质量体系结构	H.360-H.369
远程呈现	H.420-H.429
多媒体的补充业务	H.450-H.499
移动性和协作程序	
移动性和协作、定义、协议和程序概述	H.500-H.509
H 系列多媒体系统和业务的移动性	H.510-H.519
移动多媒体协作应用和业务	H.520-H.529
移动多媒体应用和业务的安全性	H.530-H.539
移动多媒体协作应用和业务的安全性	H.540-H.549
车辆网关和智能交通系统（ITS）	
车辆网关的体系结构	H.550-H.559
车辆网络的接口	H.560-H.569
宽带、三网合一和先进的多媒体业务	
在 VDSL 上传送宽带多媒体业务	H.610-H.619
先进的多媒体服务和应用	H.620–H.629
无处不在的传感器网络应用和物联网	H.640–H.649
IPTV 多媒体服务和 IPTV 应用	
一般问题	H.700–H.719
IPTV 终端设备	H.720–H.729
IPTV 中间件	H.730–H.739
IPTV 应用程序事件处理	H.740–H.749
IPTV 元数据	H.750–H.759
IPTV 多媒体应用框架	H.760–H.769
IPTV 业务发现至消费	H.770–H.779
数字标牌	H.780–H.789
电子医疗多媒体服务和应用	
个人健康系统	**H.810–H.819**
个人健康系统的互操作性认证测试(HRN、PAN、LAN 和 WAN)	H.820–H.849
多媒体电子医疗数据交换服务	H.860–H.869

欲了解更详细信息，请查阅 ITU-T 建议书目录。

ITU-T H.812 建议书

个人互联健康系统的互操作性设计导则：
服务接口

摘要

康体佳设计导则（CDG）定义了底层标准和准则的框架，用于确保个人连接健康服务设备和数据之间的互操作性。此外，它亦包含用于进一步澄清底层标准或规范的设计导则（DG），该导则使用的方式为减少相关方案或是在这些标准和规范中加入缺失的特性以增强互操作性。

ITU-T H.812 建议书概述了服务接口（Services-IF）、所有服务接口认证的能力类别（CCC）的公共设计导则以及针对知情同意书使能个人健康网关（PHG）和服务 CCC 的设计导则。

支持以下经认证的能力类别（CCC）的设计导则通过以下独立的导则文件给出定义：

– 有关观测上载能力的ITU-T H.812.1（2017）
– 有关问卷调查表能力的ITU-T H.812.2（2017）
– 有关功能交换能力的ITU-T H.812.3（2017）
– 有关经认证的持续会话能力的ITU-T H.812.4（2017）

ITU-T H.811 建议书是“ITU-T H.810 个人互联健康系统的互操作性设计导则”子系列的组成部分，涵盖如下领域：

– ITU-T H.810 – 个人互联健康系统的互操作性设计导则：概述
– ITU-T H.811 – 个人互联健康系统的互操作性设计导则：个人健康设备接口
– ITU-T H.812 – 个人互联健康系统的互操作性设计导则：服务接口（本设计导则文件）
– ITU-T H.812.1 – 个人互联健康系统的互操作性设计导则：服务接口：观测上载能力
– ITU-T H.812.2 – 个人互联健康系统的互操作性设计导则：服务接口：问卷调查表能力
– ITU-T H.812.3 – 个人互联健康系统的互操作性设计导则：服务接口：功能交换能力
– ITU-T H.812.4 – 个人互联健康系统的互操作性设计导则：服务接口：经认证的持续会话能力
– ITU-T H.813 – 个人互联健康系统的互操作性设计导则：医疗保健信息系统接口

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T H.812	2015-11-29	16	11.1002/1000/12653
2.0	ITU-T H.812	2016-07-14	16	11.1002/1000/12913
3.0	ITU-T H.812	2017-11-29	16	11.1002/1000/13415

关键词

CDG、康体佳设计导则、医疗保健信息系统、个人互联健康系统、个人健康设备、服务。

* 为了获取此建议书，输入网址：http://handle.itu.int/intheaddressfieldofyourwebbrowser，后接建议书的唯一识别码。例如 http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息通信技术（ICT）领域工作的联合国专门机构。国际电联电信标准化部门（ITU-T）是国际电联的一个常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化发布有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，而后由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准 ITU-T 建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，也指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性的条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才认为达到了本建议书的合规性要求。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已声明的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的、有关已声明之知识产权的证据、有效性或适用性不表明任何意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的、有关受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新的信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http：//www.itu.int/ITU-T/ipr/。

目录

页码

页码

表清单

页码

图清单

页码

0 引言

康体佳设计导则（CDG）定义了底层标准和准则框架，用于确保个人互联健康服务设备和数据之间的互操作性。此外，它亦包含进一步澄清底层标准或规范的设计导则，该导则使用的方式为减少相关方案或是在这些标准和规范中加入缺失的特性以增强互操作性。

该设计导则文件还包含其他针对互操作性的设计导则，以进一步澄清或减少底层标准或规范或是在这些标准和规范中加入缺失的特性。

该设计导则文件概述了服务接口（Services-IF）、所有服务接口认证的能力类别（CCC）的公共设计导则以及针对知情同意书使能个人健康网关（PHG）和健康与健身服务 CCC 的设计导则。

支持以下经认证的能力类别（CCC）的设计导则通过以下独立的设计导则文件给出定义：

– [ITU-T H.812.1] – 个人互联健康系统的互操作性设计导则：服务接口：观测上载能力

– [ITU-T H.812.2] – 个人互联健康系统的互操作性设计导则：服务接口：问卷调查表能力

– [ITU-T H.812.3] – 个人互联健康系统的互操作性设计导则：服务接口：功能交换能力

– [ITU-T H.812.4] – 个人互联健康系统的互操作性设计导则：服务接口：经认证的持续会话能力

该设计导则文件是“ITU-T H.810 个人健康系统的互操作性设计导则”子系列的组成部分。更多细节请参见[ITU-T H.810]。

0.1 组织

该设计导则文件按以下方式来组织：

第 0 至 5 条：引言和术语 – 这些条款提供服务接口特定的信息，以帮助理解设计规范的结构。

第 6 条：服务接口概述 - 本概述服务接口 CCC。

第 7 条：用例 – 本条款提供实际的例子。

第 8 条：行为模型 – 本条款概述服务接口常见 CCC 下的交互序列，并概括典型的交互、约束和异常。

第 9 条：实施方案 – 本条款详细介绍了在公共服务接口经认证的能力类别中使用公共有效载荷内容和简单对象访问协议（SOAP）与基于表示状态转移（REST）的传输方法。

0.2 导则发布和版本修订

有关发布和版本修订信息，请参见[ITU-T H.810]第 0.2 条。

0.3 新内容

欲知本设计导则发布的最新内容，请参见[ITU-T H.810]第 0.3 条。

ITU-T H.812 建议书

个人互联健康系统的互操作性设计导则：
服务接口

1 范围

本设计导则文件重点关注以下接口：

– **服务接口（Service-IF）** 个人健康网关（PHG）与服务之间的接口。

该接口在康体佳架构中予以定义，如[ITU-TH.810]第 6 节中所述，如图1-1 所示。

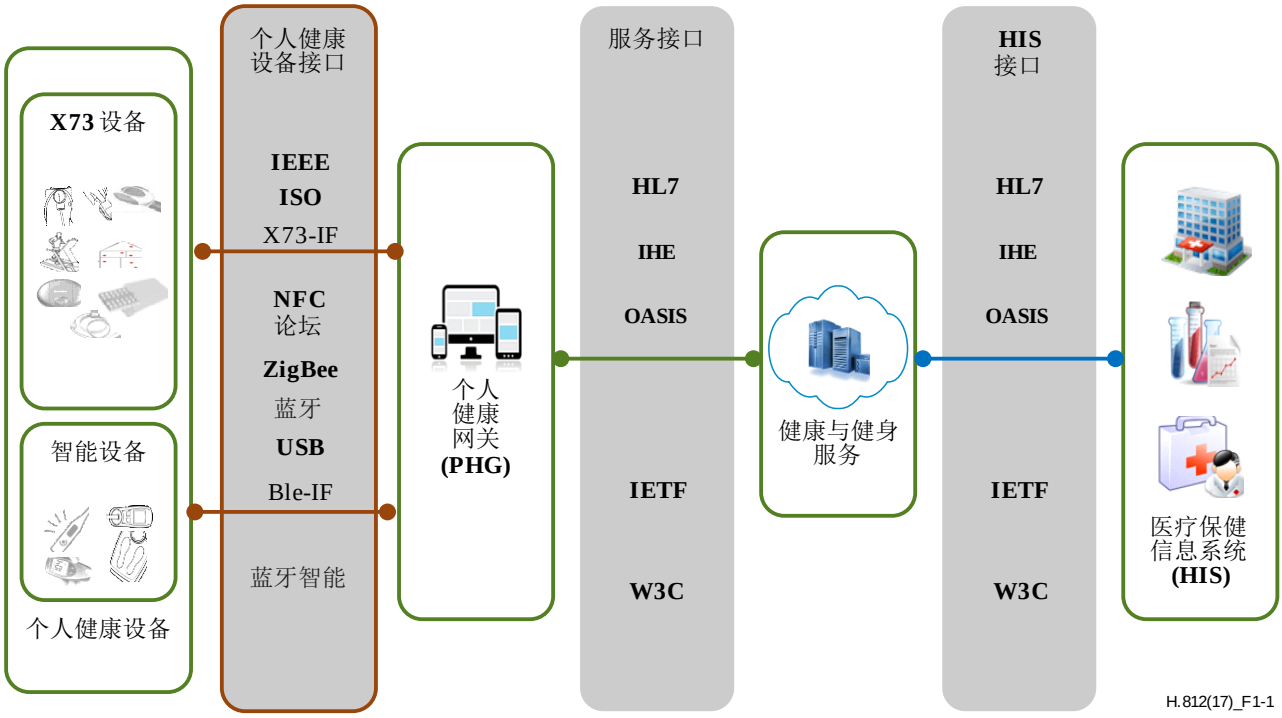

图1-1 – 康体佳架构中的服务接口

有诸多与服务接口相关的、经认证的能力类别（CCC）。本设计导则文档包含适用于若干 CCC 的互操作性设计导则。安全互操作性设计导则就是这样一个例子。此外，本设计导则文档包含知情同意书使能个人健康网关（PHG）和服务接口 CCC 的设计导则。这些 CCC 可以与多个其他服务接口相关的 CCC 相组合，例如观测上载 CCC 或具备问卷调查表能力的 CCC。

2 参考文献

下列 ITU-T 建议书及含有本建议书引用条款的其他参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其他参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其他参考文献的可能性。ITUT-T 建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

[ITU-T H.810] ITU-T H.810建议书（2017年），个人互联健康系统互操作性的设计导则：引言。

其他参考文献请参见[ITU-T H.810]第 2 节。

3 定义

本设计导则文件使用[ITU-T H.810]中定义的术语。

4 缩略语和首字母缩写词

本设计导则文件使用[ITU-T H.810]中定义的缩略语和首字母缩写词。

5 惯例

本设计导则文件遵循[ITU-T H.810]中定义的惯例。

6 架构

在此端到端（E2E）参考架构中，服务接口（Services-IF）将个人健康网关（PHG）连接到健康与健身服务（HFS）。图 6-1 显示了康体佳 E2E 架构中的服务接口，图 6-2 显示了服务接口的一个示例。

服务接口设计导则侧重于在服务接口上实现可互操作的信息交换。为 PHG 和健康与健身服务定义了一组服务接口相关的、经认证的能力类别，以实现诸多不同用例的互操作性，包括上载测量数据、完成问卷调查表和执行命令等。

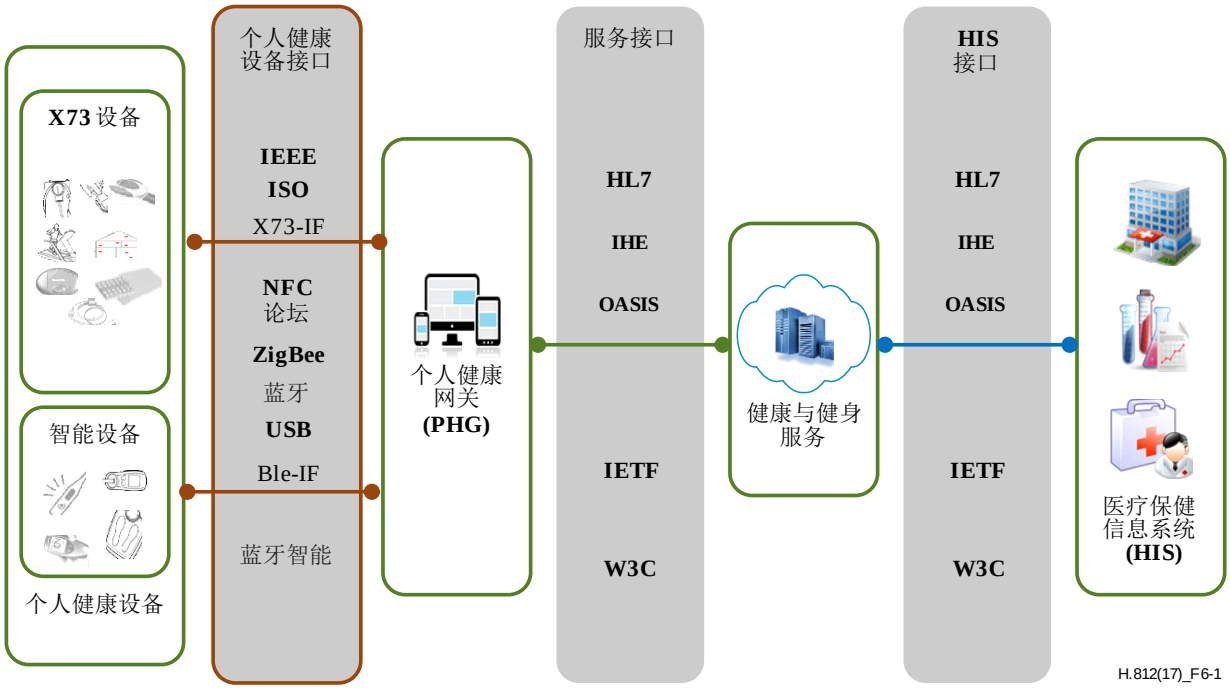

图6-1 – 康体佳E2E架构中的服务接口

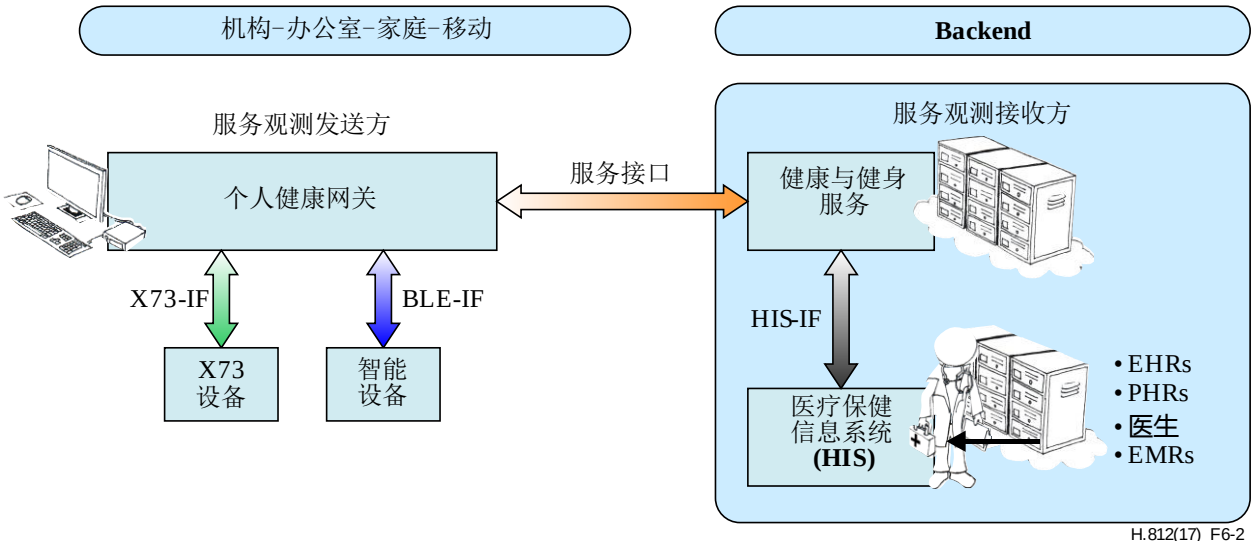

图6-2 – 服务接口实例

除了服务接口之外，端到端参考架构还定义了医疗保健信息系统接口（HIS-IF）。服务接口旨在实现 PHG（通常是个人电脑、笔记本电脑、平板电脑、移动电话或其他类型的嵌入式设备）之间的细粒度信息交换，PHG 是靠近用户/患者的一个设备和一种健康与健身服务（通常为基于后端云的服务），它收集来自这些用户的信息并使之可供进一步使用。相比之下，HIS-IF 被设计成能够在两个后端系统之间进行聚合信息交换，例如疾病管理系统和电子健康记录（EHR）[1]。HIS-IF 在[ITU-T H.813]中定义。

还期望一个 PHG 可以用于家庭或用户携带的应用场合，它对服务接口设计提出了诸多限制。由于在“现场”维护与/或升级这些设备存在难度，因此一个 PHG 应足够强健、独立和简单，以保持成本低廉和对技术操作经验或专业技能的要求最小。因为这个侧重点，故服务接口允许大多数与观测交换相关联的文本元数据存在于 PHG 之外。

另一方面，期望一个健康与健身服务将是一个能力更强的系统，例如一个服务器或个人电脑。因此，服务接口的设计目标是推动健康与健身服务复杂性和可维护性问题的解决，以免在 PHG 上出现这些问题。

服务接口是一个抽象信道，由一个或多个 CCC 对组成，它们将 PHG 应用程序和健康与健身服务应用程序连接起来。每对 CCC 都有一个驻留在健康与健身服务应用程序中的部件和一个驻留在 PHG 应用程序中的部件。康体佳定义了服务接口两侧经认证的能力类别。

该版本的服务接口导则支持以下经认证的功能类别：

– 以两种不同的方式将观测值从PHG上载到健康与健身服务：网络服务（SOAP）和REST（数据）[ITU-T H.812.1]；

[1] 注 - 在端到端架构内，服务和医疗保健信息系统（HIS）接口都可以在靠近用户/患者的某个设备上（个人电脑、笔记本电脑、移动电话等）实现，以便与地理上远离此类设备的实体进行信息交换。本导则对特定硬件上经认证的能力类别的部署没有设置任何限制。

– 以两种不同的方式将知情同意书信息从PHG上载到健康与健身服务：网络服务（SOAP）和REST（数据）[ITU-T H.812]；

– 将待完成的问卷调查表从健康与健身服务下载到PHG，并将已完成的问卷调查表从PHG上载到健康与健身服务[ITU T H.812.2]；

– 通过经认证的持久会话在健康与健身服务与PHG之间交换信息（例如，未经请求的命令）[ITU-T H.812.4]；

– 作为其他用例的推动者，在PHG和健康与健身服务之间交换所支持的、经认证的能力类别信息（能力交换）[ITU-T H.812.3]。

PHG 可以支持一个或多个应用程序，每个应用程序实现一种或多种康体佳经认证的能力类别。图 6-3 描绘了康体佳服务接口，显示了 PHG 应用程序和健康与健身服务应用程序，当中实现了所有可能的服务接口经认证的能力类别。

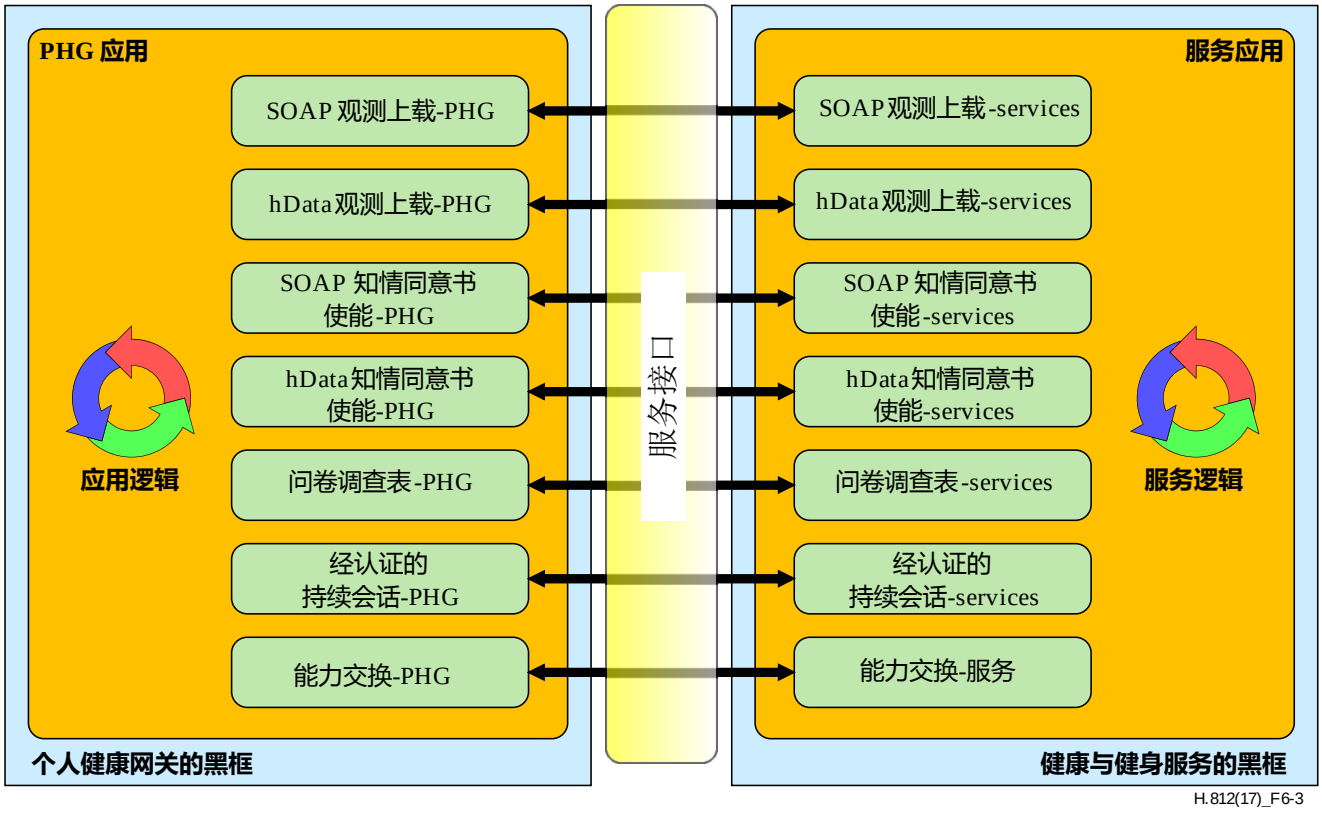

图6-3 – 康体佳服务接口，显示服务接口经认证的能力类别

这些导则旨在详细规定系统行为，以便为特定用例实现可接受的互操作性水平。用例封装在经认证的能力类别（CCC）中。该导则对 CCC 部件的网络接口如何发挥作用做了规范性陈述。对于服务接口，这些部件存在于驻留在 PHG 或健康与健身服务上的应用程序或服务中。

通用平台通常限制应用程序可以相互通信的方式，以确保整个平台的稳定性。应用程序之间这种有限的交互称为沙盒。为了支持沙盒应用程序，该版本的服务接口使用一个参考模型，它将一个应用程序定义为一个或多个 CCC 部件的容器。应用程序容器内的部件之间的交互没有规范性要求，完全取决于应用程序的开发人员。为了通过认证，PHG 上应用程序 CCC 和健康与健身服务上对应 CCC 之间的服务接口交互是可见的，并且有规范性要求。

参考模型允许 PHG 或健康与健身服务中存在多个应用程序，但应用程序与其他应用程序交互，除非通过网络接口。在这些导则中，运行在健康与健身服务上的应用程序通常被称为服务，因为健康与健身服务通常是网络服务平台。健康与健身服务在概念上与 PHG 应用程序相同。

这些导则记录了各机制，通过这些机制，各部件可以通过一个内部应用程序编程接口（API）来相互通信。未来版本的服务接口可以使用这些机制来实现一个应用程序内各部件之间的互操作性。

在图 6-4 中，服务接口参考模型的概念用于描述具有两个与服务应用程序通信的独立应用程序的 PHG。一个 PHG 应用程序支持三个 CCC，另一个支持单个 CCC。对 PHG 和健康与健身服务之间的网络接口提出了规范性要求。应用程序容器内各 CCC 部件之间的交互不是规范性的，显示为由应用程序内部处理协调的红色虚线，这不在这些导则的讨论范围内。

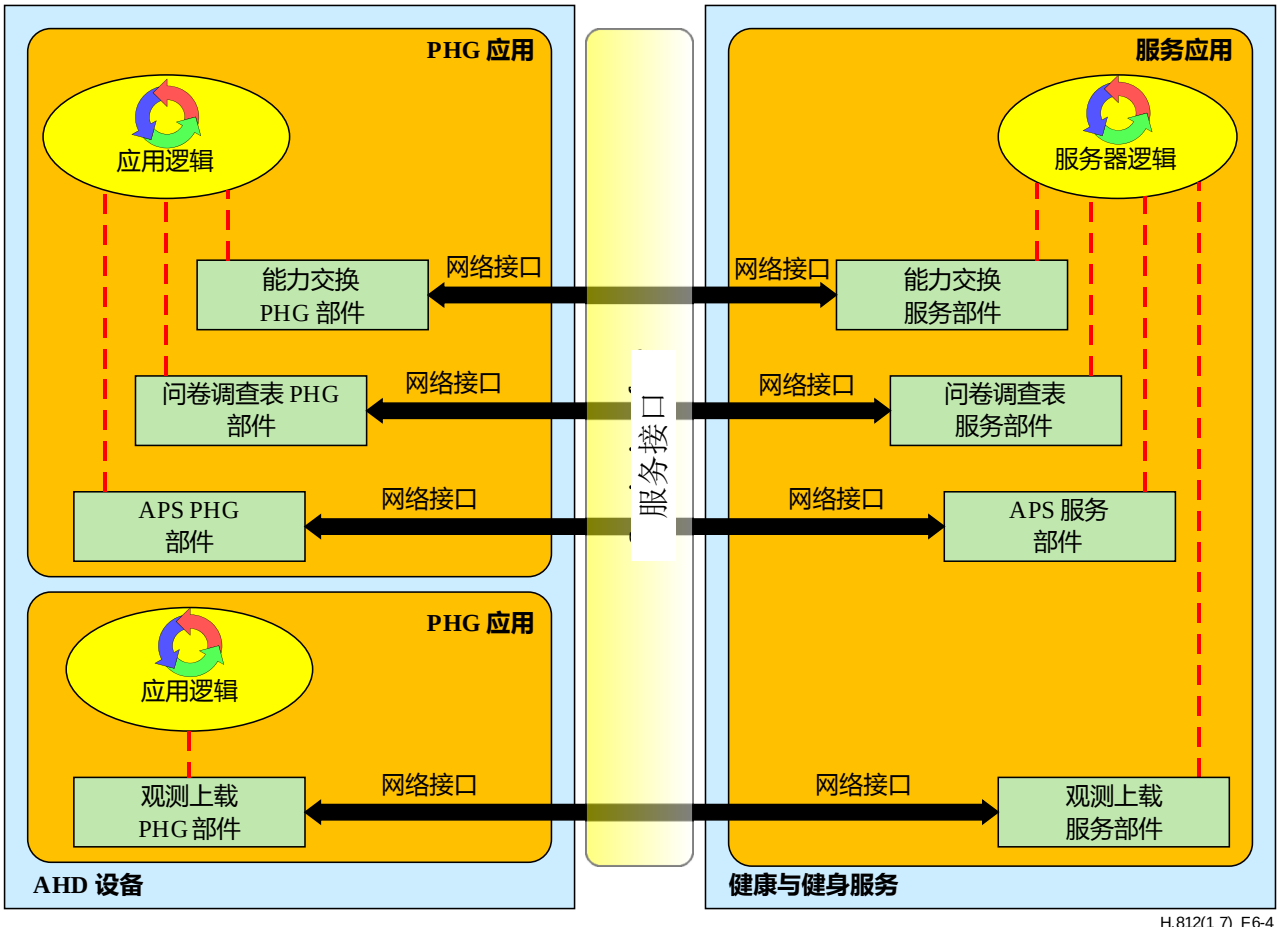

图6-4 – 服务接口参考模型

使用服务接口的通信从 PHG 的能力交换部件开始。该部件向健康与健身服务上的对等部件发送一个请求。该请求要求健康与健身服务指定它支持的、不同的经认证的能力类别。PHG 应用程序用通用语言询问“你能做什么？”，健康与健身服务应用程序根据其支持的 CCC 来回答这个问题。在图 6-4 的情况下，健康与健身服务应用程序将说“我支持能力交换、问卷调查表、SOAP 观测上载和经认证的持久会话（APS）”。当服务应用程序的能力交换部件应答 PHG 应用程序时，它通常会向 PHG 提供附加信息，例如一个 URL，这使得 PHG 应用程序能够进行与特定 CCC 通信的下一步骤。仅支持使用 SOAP 上载观测的 PHG 不需要实施能力交换。如果 PHG 已经了解健康与健身服务的功能，则无需调用能力交换。

7 用例

7.1 知情同意书管理

一个知情同意书指令是一条有关医疗保健客户端私密性策略的记录，它批准或拒绝针对个体可识别健康信息（IIHI）的知情同意书[HL7 CDA IG]。

用户知情同意书要求源自不同的规定，例如健康信息和便利性责任法案（HIPAA）、EU 指令 95/46 等。这些私密性法律定义了并对患者指定了关于采集、访问、使用和透露其健康信息的特殊权利。这些法律要求在患者健康信息可以被访问、使用或共享之前必须要得到其知情同意书。例如，可以要求一个患者在注册某个疾病管理机构（DMO）期间填写一份知情同意书表格。该知情同意书表格得到该患者对一系列预定义策略的认可与/或签名，即规定允许谁访问其 IIHI、出于什么目的以及他们可以如何使用之。本节介绍了在服务接口上获得和传送电子格式的知情同意书策略。数字知情同意书致力于改进患者授权和进行有效处理以符合知情同意书要求。患者知情同意书的示例包括基本的选择加入/选择退出 IIHI、允许紧急优先、功能角色的限制访问（例如，直接医疗保健提供者）、用于特定研究项目的的特定文件等。

在一个基本情形中，一名患者将在注册健康与健身服务应用程序期间或之后定义其知情同意书。他如何准确说明其知情同意书超出了这些导则的讨论范围，但它可能涉及对一个默认策略的选择和调整，使用其 PHG 上的一个用户接口，将之转换为机器可读的知情同意书策略表示。这样的策略通常包含对所涉各方、数据对象和授权或不授权行动的一个参照。接收一个特殊患者知情同意书的健康与健身服务将对其进行存储，并针对接收的患者健康数据执行之。

以下用例侧重于为患者知情权同意书管理确定的需求。

7.1.1 上载知情同意书到服务器

Adam Everyman 注册了一个机构（例如，疾病管理组织（DMO）），该机构远程监控家中的患者，并从安装在 Adam 家中的健康测量设备收集健康信息。在注册时，Adam 填写了个人健康网关（PHG）应用程序上的 eConsent 表格。eConsent 表格包括关于谁将能够访问、使用、更新和透露通过远程患者监测系统收集之不同类型生命体征的选项。在指定这些首选项后，Adam 随后点击其远程医疗中心上的“提交”按钮。远程医疗中心将其首选项汇编成隐私知情同意书指令文件，它基于 HL7 CDA R2 标准，然后从其 PHG 发送到提供远程患者监控服务的 DMO。而后，知情同意书指令管理对 DMO 上患者数据的访问，如果 Adam 的数据发送给第三方，假设允许这样做，即可以包括患者的个人健康记录（PHR）、电子健康记录（EHR）和电子病历（EMR）。然后，Adam 的隐私知情同意书指令将通过患者标识符与数据相关联。

7.1.2 从服务器检索已完成的患者知情同意书

Adam 可能想要更新他的隐私首选项，例如，允许其健身教练访问他的数据，因为根据 DMO 护士的建议他最近注册了一项健身服务。其 PHG 提供一个至其最新版本隐私知情同意书指令文件的链接。Adam 点击链接，然后 PHG 从服务器检索其最新版本的隐私知情同意书指令，并将之呈现给 Adam。

7.1.3 上载经更新的知情同意书到服务器

Adam 审查他的隐私知情同意书首选项，并在其健身教练无法访问他的数据时更新它们。在更新了知情同意书首选项后，他点击其 PHG 上的“提交”按钮，而后将把其首选项汇编成一个隐私知情同意书指令文件，发送给 DMO。DMO 用经过更新的隐私知情同意书指令文件替代旧的知情同意书。

7.2 知情同意书的执行

通过加密执行患者知情同意书，可有效保护患者的隐私。并确保仅有预期的接收者可看到其内容（如观测结果或对问卷调查表的响应）。这防止了可能工作在同一机构中的其他个人看到其内容，例如，管理人员。知情同意书使能健康与健身服务应在对内容解密之前评估知情同意书。为了确定接收者是否能够观看其内容，要对知情同意书进行评估。例如，知情同意书评估处理的结果为“成功-1”或“失败-0”。知情同意书使能健康与健身服务应执行知情同意书文件中所述的知情同意书首选项。

7.2.1 在上载前对知情同意书进行加密

Adam Everyman 注册了 DMO，它在家中远程监控他，并从他家中安装的健康测量设备处收集健康信息。Adam Everyman 还根据 DMO 护士的建议注册了一个健身教练。Adam Everyman 希望其健身教练查看他的活动数据，而不是来自其他测量设备（如血压监测仪（BPM））的数据。Adam 对其 PHG 进行配置，使得现在只有 DMO 机构中的护士才能访问来自 BPM 和活动监视器的数据，而健身教练只能访问来自活动监视器的数据。这通过加密来实现。

7.3 其他 CCC 用例

有关其各自的CCC用例，请参阅以下设计指南中的第6节：

– [ITU-T H.812.1] 观测上载；
– [ITU-T H.812.2] 问卷调查表；
– [ITU-T H.812.3] 能力交换；
– [ITU-T H.812.4] 经认证的持久会话。

8 行为模型

该节包括：

– 服务接口消息交换行为；
– 基于REST的CCC的安全行为；
– 知情同意书的管理和CCC行为的执行。

8.1 公共服务接口消息交换行为

出于对安全性和私密性的考虑以及整个系统的技术可行性，服务接口要求所有连接要从 PHG 发起。如图 8-1 所示。请参阅每个设计导则，了解其消息有效载荷和其他规定。

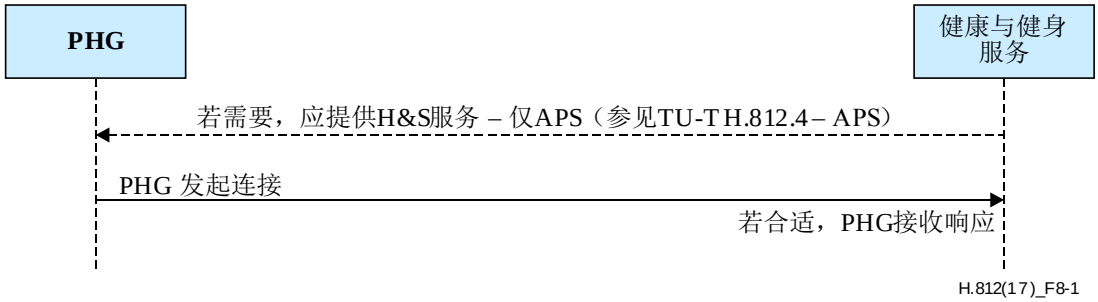

图8-1 – 所有连接要从PHG发起

当点对点内容安全性需要传输级安全性（TLS）时，在 TLS 握手中使用相互证书验证将取决于健康与健身服务的安全策略。

当需要进行验证时：

– 在SOAP情况下，验证是一个SAML 2.0令牌；以及

– 对数据，是一个OAuth 2.0持有者令牌。

在本导则中没有规定 PHG 如何获得这些令牌，因为它取决于各方之间建立的信任关系。健康与健身服务应用程序可以支持一个或多个 WS 信任选项以获取 SAML 2.0 令牌，或者它可以使用一个或多个授权类型（例如，资源所有者密码证书授予类型）来支持 OAuth 2.0 授权框架服务器。如果健康与健身服务同时支持数据和 SOAP 上载，则它可以支持这两种服务。在这些情况中的任何一种情况下，必须进行带外操作，当中 PHG 的用户在健康与健身服务应用程序上建立某种类型的帐户，允许客户端获得这些令牌。健康与健身服务令牌服务生成这些为接收方定制的令牌，它可以在接收内容时进行验证。另一方面，健康与健身服务可以要求从 PHG 与之建立信任关系的第三方授权服务（例如 CA）获得这些令牌。在这种情况下，健康与健身服务允许第三方授权服务对客户端进行验证。然后，健康与健身服务可以选择接受来自该第三方服务的任何令牌，或者它可以另外选择将任何接收到的令牌传递给第三方授权服务以在接受之前进行确认。信任关系详细信息由健康与健身服务的安全策略确定。

8.2 基于 REST 的 CCC 实施的公共安全模型

图 8-2 提供了基于 HTTP 上的数据（REST）的、经授权的 RESTful 事务处理的交互图。使用 OAuth 2.0 授权框架、使用资源所有者密码证书作为授权授予类型来实现授权。当资源所有者（患者）与客户端（例如，在应用程序托管设备上运行的可信应用程序）之间存在高度信任时，通常使用资源所有者密码证书。在未来版本的设计指南中，可能需要基于用例的其他证书类型，当中第三方应用程序（较少特权）可用于访问患者数据。资源所有者证书用于单个请求，并进行交换以访问令牌。然后，访问令牌用于在某个资源上执行 RESTful 事务处理。使用[IETF RFC 4346]，在安全会话中执行与授权和资源服务器的所有交互。

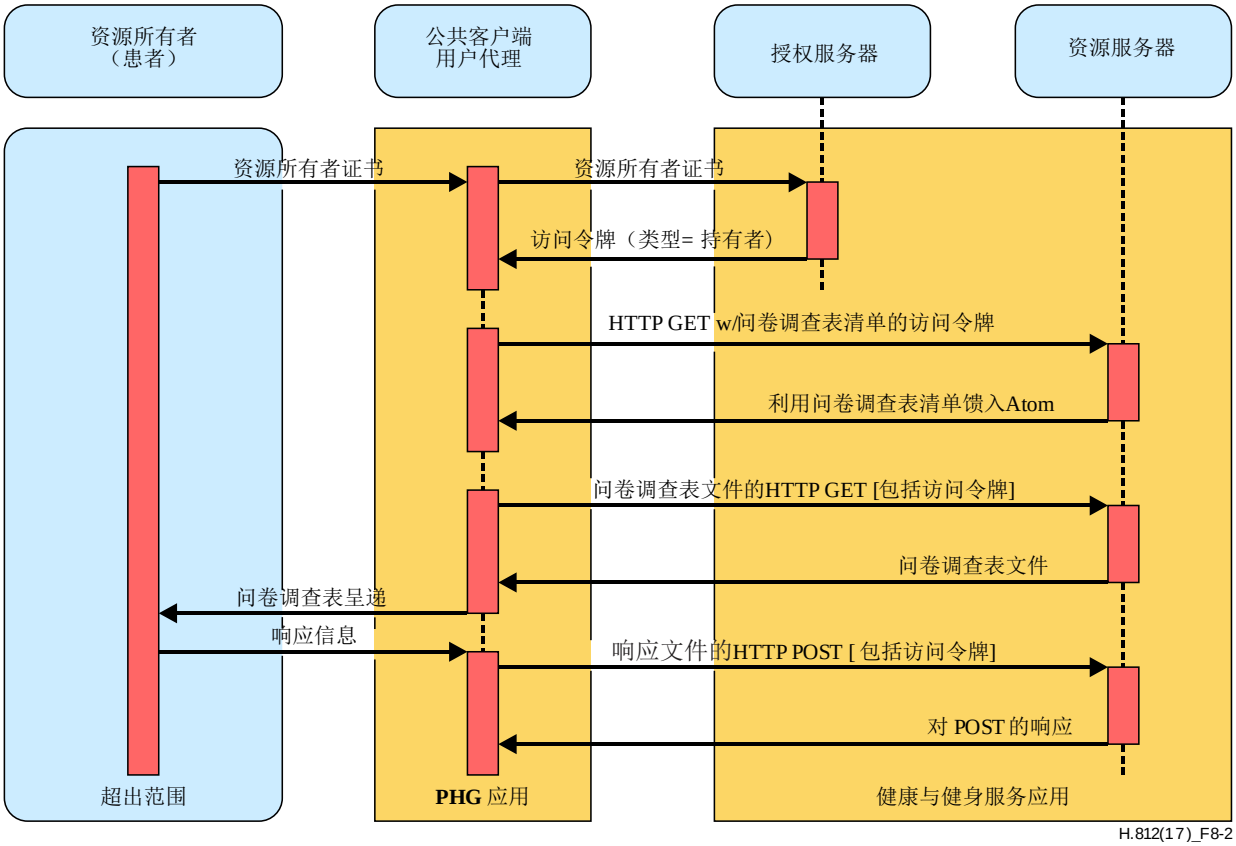

图8-2 – 经授权的RESTful CCC行为的安全行为

（以问卷调查表用例为例）

有关 REST CCC 安全导则，请参见表 B.1 和表 B.2。

8.3 知情同意书管理行为模型

为知情同意书的管理服务规定了以下交换机制：

– 在服务器上创建一个新的知情同意书文件。
– 从服务器检索已规定的知情同意书文件。
– 将经更新的知情同意书文件上载到服务器。

图 8-3 显示了与该内容文件中描述的知情同意书管理用例相关的事务处理。

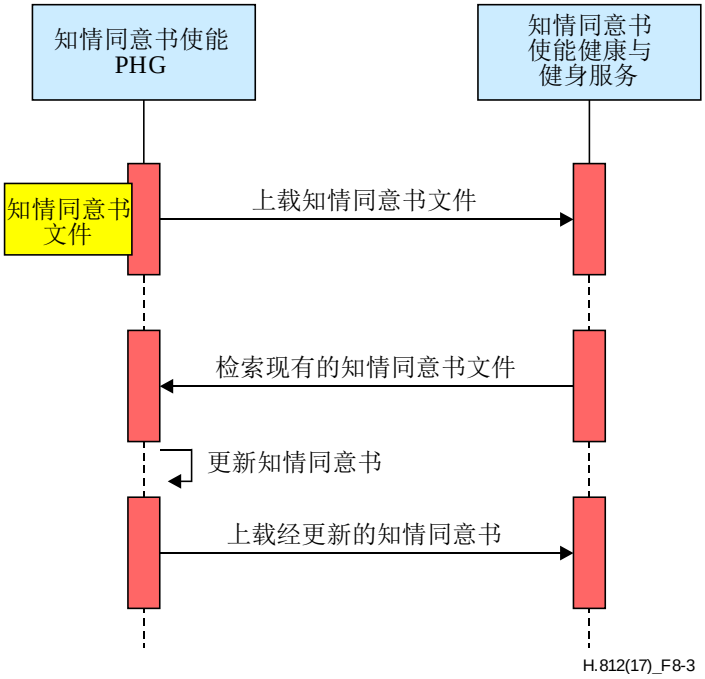

图8-3 – 与知情同意书管理有关的、PHG和健康与健身服务之间的事务处理

有关知情同意书管理导则，请参见表 C.1 和表 C.2。

8.4 知情同意书执行行为模型

为知情同意书的执行规定了以下功能：

– 对要上载的知情同意书进行加密

图 8-4 示出了同意执行功能。

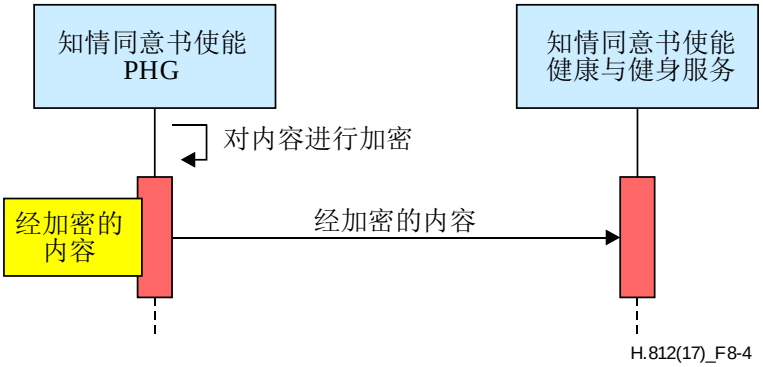

图8-4 – 在服务接口上执行知情同意书

有关知情同意书导则，请参见表 C.3 和表 C.4。

9 实施

9.1 知情同意书的表示

根据 CDA 版本 2.0 的 HL7 实施指南：[HL7 CDA IG]中的知情同意书指令，表示知情同意书首选项。

可以在上述标准的提交包中找到知情同意书文件的示例文件。

9.2 传输协议

9.2.1 使用 HTTP 上的数据的传输协议

在这种情况下，HTTP 上的数据用作为跨服务接口交换知情同意书文件的传输协议，并支持第 7.1 节和第 7.2 节中提到的所有用例。有关 PHG 和健康与健身服务之间使用 HTTP 协议上的数据的详细要求，请参阅附件 A、表 C.1、表 C.2、表 C.3 和表 C.4。

9.2.2 使用 IHE XDR 的传输协议

在这种情况下，[IHE ITI TFS XDR]用作为跨服务接口交换知情同意书文件的传输协议，并仅支持将知情同意书上载到服务器用例。知情同意书文件通过患者标识符链接到健康信息（PCD-01 消息）。以这种方式，知情同意书被关联到健康信息，并因此控制其使用。

9.3 执行知情同意书

9.3.1 使用 XML 加密来执行知情同意书

对于使用[IHE ITI TFS XDR]的传输协议，通过加密，XML 加密标准[W3C XMLENC]促成知情同意书的执行。XML 加密标准促成在知情同意书使能健康与健身服务上为特定的接收者（例如，医生或护士）对 PCD-01 事务处理的有效载荷进行加密。

使用 XML 加密标准，通过加密，来促成知情同意书的执行。

9.3.2 使用 IHE DEN 执行知情同意书

在使用 HTTP 上的数据的传输协议的情况下，通过使用 IHE DEN 配置文件[IHE ITI DEN]来促成知情同意书的执行。

附件 A

规范性导则概述

（本附录是本建议书不可分割的组成部分）

表 A.1 列出了服务经认证的能力类别。

表A.1 – 经认证的能力类别

经认证的能力类名称	经认证的能力类别	经标识的能力类别
SOAP观测上载 - PHG	是	是
SOAP观测上载 - 健康与健身服务	是	是
数据观测上载 - PHG	是	是
数据观测上载 - 健康与健身服务	是	是
SOAP知情同意书使能 - PHG	是	是
SOAP知情同意书使能 - 健康与健身服务	是	是
数据知情同意书使能 - PHG	是	是
数据知情同意书使能 - 健康与健身服务	是	是
问卷调查表 - PHG	是	是
问卷调查表 - 健康与健身服务	是	是
能力交换 - PHG	是	是
能力交换 - 健康与健身服务	是	是
经认证的持续会话 - PHG	是	*
经认证的持续会话 - 健康与健身服务	是	*[2]

适用于每个设备认证分类的导则在表 A.2 中列出。

表A.2 – 经认证的设备类别的导则

经认证的能力类别	相关导则
SOAP观测上载 - PHG	请参见[ITU-T H.812.1]和[ITU-T H.812]表A.3、表B.3
SOAP观测上载 - 健康与健身服务	请参见[ITU-T H.812.1]和[ITU-T H.812]表A.3、表B.3
数据观测上载 - PHG	请参见[ITU-T H.812.1]和[ITU T H.812]表A.3、表B.1

[2] * 这些单元格有意置空。

表A.2 – 经认证的设备类别的导则

经认证的能力类别	相关导则
数据观测上载 - 健康与健身服务	请参见[ITU-T H.812.1]和[ITU T H.812]表A.3、表B.2
SOAP知情同意书使能 - PHG	请参见[ITU-T H.812.1]和[ITU-T H.812]表A.3、表B.3、表C.5、表C.7
SOAP知情同意书使能 - 健康与健身服务	请参见[ITU-T H.812.1]和[ITU-T H.812]表A.3、表B.3、表C.6、表C.8
数据知情同意书使能 - PHG	请参见[ITU-T H.812] 表A.3、表C.1、表C.3、表B.1
数据知情同意书使能 - 健康与健身服务	请参见[ITU-T H.812]表A.3、表C.2、表C.4、表B.2
问卷调查表- PHG	请参见[ITU-T H.812.2]表A.1和[ITU-T H.812]表A.3、表B.1
问卷调查表- 健康与健身服务	请参见[ITU-T H.812.2]表A.2和[ITU-T H.812]表A.3、表B.2
能力交换 - PHG	请参见[ITU-T H.812.3]表A.2和[ITU-T H.812]表A.3、表B.1
能力交换 - 健康与健身服务	请参见[ITU-T H.812.3]表A.1和[ITU-T H.812]表A.3、表B.2
经认证的持续会话 - PHG	请参见[ITU-T H.812.4]表A.1、表A.2、表A.3、表A.5和[ITU T H.812]表A.3、表B.1
经认证的持续会话 - 健康与健身服务	请参见[ITU-T H.812.4]表A.1、表A.4、表A.6和[ITU T H.812]表A.3、表B.2

表A.3 – 对所有CCC的共同要求

名称	描述	注释
CapX-HFS-Universality	所有的健康与健身服务都**须**支持能力交换，除了基于SOAP的观测上传或知情同意书使能 - 健康与健身服务CCC。	健康与健身服务仅执行基于SOAP的观测上传或知情同意书使能 – 健康与健身服务CCC，不需要支持能力交换 – 健康与健身服务CCC。
HFS-Transport_Connection_Initiation	所有的健康与健身服务连接都**须**从健康与健身服务PHG应用程序启动，**不得**从健康与健身服务启动。	

附件B

服务接口CCC的一般安全性导则

（本附录是本建议书不可分割的组成部分）

表B.1 – 使用REST的PHG安全导则

名称	描述	注释
PHG-Grant_Type	PHG可以使用资源所有者密码证书作为授权类型，如OAuth v2.0 [IETF RFC 6749]第1.3.3节中所定义。	PHG可以使用其他手段从授权服务器处获取授权令牌。
PHG-authorization_request	PHG可以根据OAuth v2.0 [IETF RFC 6749]第4.3节和第4.3.2节从授权服务器处获取授权令牌。	有关授权请求的有线格式，请参见附录III中的示例。 关于响应，请参见导则健康与健身服务 - authorization_request_response。
PHG-bearer_token	当请求访问关于健康与健身服务[IETF RFC 6750]的受保护资源时，PHG**须**根据[IETF RFC 6750]使用“持有者”令牌。	请参见相关导则健康与健身服务 - authorization_request_response。
PHG-Token_Transmit	当发送[IETF RFC 6750]第2.1节中定义的持有者令牌时，PHG**须**使用授权请求报头字段方法。	
PHG-Confidentiality	PHG至少**须**使用TLS协议v1.1与授权服务器和健康与健身服务[IETF RFC 4346]进行安全的点对点通信。	
PHG-Cipher	PHG**须**使用TLS_RSA_WITH_AES_128_CBC_SHA的加密密码套件。	

表B.2 – 使用REST的健康与健身服务导则

名称	描述	注释
HFS-authorization_request_response	根据OAuth v2.0 [IETF RFC 6749]第4.3.3节，实施授权服务器的健康与健身服务**须**在验证访问令牌请求之后返回“持有者”类型的授权令牌。	请参见指南PHG-authorization_request以获取请求格式。 授权可以是一个单独的实体，不需要成为健康与健身服务的一部分。
HFS-refresh_token	实施授权服务器的健康与健身服务**须**返回刷新令牌。	
HFS-Token_Evaluation	健康与健身服务**须**在授予对健康与健身服务记录的访问权限之前，对授权令牌及其范围进行评估。	

表B.3 – 一般安全性导则

名称	描述	注释
HFS-Security_Transport	健康与健身服务应用程序和PHG应用程序至少**须**支持来自WS-I BSP v1.0的TLS协议v1.1 [IETF RFC 4346]，以进行安全通信。	当启用加密时，本导则与IHE ATNA概要一致。 为了相互认证，康体佳导则依靠TLS v1.0 [IETF RFC 2246]中的导则。
HFS-Security_Transport_Cipher	健康与健身服务应用程序和PHG应用程序**须**支持[IETF RFC 3268]中规定的AES密码。	IHE ATNA要求选择采用以下密码套件： TLS_RSA_WITH_AES_128_CBC_SHA 为了安全，HIS导则应采用以下密码套件： TLS_RSA_WITH_AES_128_CBC_SHA 允许采用其他密码套件，但是将需要在PHG和健康与健身服务之间做好协商。
HFS-Confidentiality	健康与健身服务**须**使用TLS协议v1.1与授权服务器和具有问卷调查表能力的健康与健身服务[IETF RFC 4346]进行安全的点对点通信。	
HFS-Cipher	健康与健身服务**须**支持TLS_RSA_WITH_AES_128_CBC_SHA加密密码套件。	

附件 C

知情同意书管理的规范性导则

（本附录是本建议书不可分割的组成部分）

表C.1 – 用于知情同意书使能PHG的、使用REST的知情同意书管理导则

名称	描述	注释
PHG-Consent_Enabled	知情同意书使能PHG**须**符合HL7 CDA R2知情同意书指令标准，以便呈现患者的知情同意书首选项[HL7 CDA 1G]。	
PHG-Consent_Enabled_ Transport_Standards	知情同意书使能PHG**须**符合以下传输标准： HL7第3版规范：数据记录格式，第1版[HL7 hRF] RLUS的OMG数据REST绑定[OMG/数据绑定] OMG检索、定位和更新服务（RLUS）规范1.0.1 [OMG /数据RLUS]	
PHG-Post_Consent	知情同意书使能PHG**须**使用带有以下URL的HTTP POST来发布对健康与健身服务的知情同意书： *baseURL/continua/consent*	请参见第7.1节中的用例。 对于通过REST传输进行的检索、定位和更新服务（RLUS）数据，这是通过在此URL处使用隐私知情同意书文件在请求正文中执行不带查询参数的HTTP POST请求来执行的。
Consent_Enabled-PHG-Observation_Association	知情同意书使能PHG进行传送的知情同意书文件**须**包含和健康与健身服务观测测量消息相同的患者标识符。	这将知情同意书文件和健康与健身服务观测测量消息相关联。
Consent_Enabled-PHG-Observation-Association_ Value	知情同意书文件报头中的“患者ID”字段**须**被设置为PID-3值。 子字段CX-1和CX-4**须**存在，而子字段CX-5**不得**存在。	
Consent_Enabled-PHG-Questionnaire Response_Confidentiality	知情同意书使能PHG**须**在问卷调查表响应文件报头中将保密编码设置为“R”值。	

表C.1 – 用于知情同意书使能PHG的、使用REST的知情同意书管理导则

名称	描述	注释
Consent_Enabled-PHG-Questionnaire Response_Association_Value	为了将问卷调查表响应文件与患者知情同意书文件相关联，知情同意书使能PHG须采用如表IV.3中所定义的保密编码系统的转换要素。	请参见表IV.1，表IV.2和表IV.4
Retrieving_Consent	知情同意书使能PHG须采用HTTP GET和以下URL来获取健康与健身服务的知情同意书： *baseURL/continua/consent* 知情同意书使能PHG须采用HTTP GET和ATOM馈入条目的链接要素的值，来从健康与健身服务中检索实际的知情同意书文件，并验证它是有效的HL7 CDA R2知情同意书指令文件[HL7 CDA IG]。	请参见第7.1节中的用例。 对于通过REST传输的RLUS数据，这是通过在表示患者知情同意书数据部分路径的URL处执行不带查询参数的HTTP GET请求来执行的，它将返回ATOM馈入条目。 有关Atom馈入条目要素的更多信息，请参见表I.1。

表C.2 – 用于知情同意书使能健康与健身服务的、使用REST的知情同意书管理导则

名称	描述	注释
Consent_Enabled-Health-&-Fitness-Service	知情同意书使能健康与健身服务须能接收HL7 CDA R2知情同意书指令知情同意书文件[HL7 CDA IG]。	
Health-&-Fitness Service-Consent_Enabled_Transport_Standards	知情同意书使能PHG须符合以下传输标准： HL7第3版规范：数据记录格式，第1版[HL7 hRF]； RLUS的OMG数据REST绑定[OMG/数据绑定]； OMG检索、定位和更新服务（RLUS）规范1.0.1 [OMG/数据RLUS]。	

表C.2 – 用于知情同意书使能健康与健身服务的、使用REST的知情同意书管理导则

名称	描述	注释
HFS-Consent_Root	知情同意书使能健康与健身服务**须**在root.xml文件中包含以下问卷调查表内容要素： 1. 概况 a. id="consent" b. reference="http://handle.itu.int/11.1002/3000/hData/Consent/2017/01/H.812.pdf" 2. 章节 a. path="consent" b. profileID= "consent" c. resourceTypeId="consent" 3. 资源类型 a. resourceTypeId="consent" b. reference="http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=63" c. representation d. mediaType="application/xml2	注：为1.b引用提供的URL仅为示例。
HFS-Consent_Validate	知情同意书使能健康与健身服务**须**验证知情同意书文件是否为有效的HL7 CDA R2知情同意书指令文件，如果是有效文件，则将HTTP 200作为一个响应予以发送。	
HFS-Post_Consent-Response	知情同意书使能健康与健身服务**须**在从知情同意书使能PHG处接收POST消息后创建一条知情同意书文件记录，并将HTTP 201作为一个响应予以发送。	请参见上面的PHG-Post_Consent。
PHG-Delete_Consent_Response	知情同意书使能健康与健身服务**不得**支持删除现有知情同意书文件记录，并**须**在知情同意书URL上返回HTTP 405 Method Not Allowed作为对HTTP DELETE请求的响应。	

表C.3 – 用于知情同意书使能PHG的、使用数据的知情同意书执行导则

名称	描述	注释
Consent_Enabled-PHG-Content-Encryption_Actor	知情同意书使能PHG**须**按照IHE文件加密（DEN）概要对内容进行加密[IHE ITI DEN]。	此处的内容可以是PCD-01事务处理或问卷调查表响应文件的载荷。
Consent_Enabled-PHG-Questionnaire-Response_MIMEtype_	知情同意书使能PHG**须**将MIME类型设置为“application / xml”，以防加密内容为问卷调查表响应。	目的是要指明加密载荷的类型。
Consent_Enabled-PHG-Observation - Upload_MIMEtype_	知情同意书使能PHG**须**将MIME类型设置为“application/txt”，以防加密内容为观测上载。	目的是指明加密载荷的类型。

表C.3 – 用于知情同意书使能PHG的、使用数据的知情同意书执行导则

名称	描述	注释
Consent_Enabled-PHG-Content-Encryption_Algorithm	知情同意书使能PHG须将AES-128 CBC用于内容的加密。	所用算法通过CMS中的ContentEncryptionAlgorithmIdentifier来确定（加密消息句法），它通过IHE DEN来做进一步配置。
Consent_Enabled-PHG-Encryption-Recipient_Binding_PKI	知情同意书使能PHG须使用来自IHE DEN概要的、基于PKI的密钥管理方法[IHE ITI DEN]。	基于PKI的内容密钥管理方法将KeyTransRecipientInfo用作CMS RecipientInfoType。这针对的是公共密钥或接收者的x.509 v3证书。

表C.4 – 用于知情同意书使能健康与健身服务的、使用数据的知情同意书执行导则

名称	描述	注释
HFS-Device_HTTP_Ack	知情同意书使能健康与健身服务须在成功接收加密内容后将HTTP 202作为一个响应予以发送。	
Consent_Enabled-HFS-Content-Decryption_Actor_XDR	知情同意书使能健康与健身服务须按照IHE DEN概要对加密内容进行解密[IHE ITI DEN]。	
Consent_EnabledKey_Management	知情同意书使能健康与健身服务须使用基于PKI的密钥管理方法，如IHE DEN概要所规定的那样[IHE ITI DEN]。	
Consent_Enabled-HFS-Decryption-Algorithm	知情同意书使能健康与健身服务须将AES-128 CBC解密算法用于载荷的解密。	所用算法通过CMS中的ContentEncryptionAlgorithmIdentifier来确定（加密消息句法）。
Consent_Enabled-HFS-Consent_Enforcement_	知情同意书使能健康与健身服务须执行知情同意书文件中所述的知情同意书首选项。	例如，防止将内容进一步泄露给未授权的实体。

表C.5 – 用于知情同意书使能PHG的、使用SOAP的知情同意书管理导则

名称	描述	注释
Services-Observation-PHG-Consent	知情同意书使能服务观测PHG须遵循[HL7 CDA IG]知情同意书指令来在一个知情同意书文件中呈现患者的知情同意书。	
Services-Observation-PHG-Consent-Transport	知情同意书使能服务观测PHG须实施IHE XDR的文件源角色，使用ITI 41提供和注册文件集-b事务处理来发送一个知情同意书文件。	
Services-Observation-PHG-Consent-Frequency	知情同意书使能服务观测PHG须至少向观测健康与健身服务发送一次知情同意书文件。	例如，知情同意书文件将首先在与该服务注册期间予以发送。 建议在连接的寿命期间至少向观测健康与健身服务发送一次知情同意书文件。还支持诸如更新知情同意书首选项的应用情况。 经更新的知情同意书文件是通过知情同意书使能观测健康与健身服务对现有知情同意书文件的替换。
HFS-Observation_ Measurement_ Consent_Document_ Association	由知情同意书使能服务观测PHG传送的知情同意书文件须包含与服务观测测量消息相同的患者标识符。	这将把知情同意书文件和健康与健身服务观测测量消息关联起来。
HFS-Observation_ Measurement_Consent_ Document_Association_Value	知情同意书文件报头中的“Patient ID”字段须被设置为PID-3值。 子字段CX-1和CX-4须存在，而子字段CX-5不得存在。	

表C.6 – 用于知情同意书使能健康与健身服务的、使用SOAP的知情同意书管理导则

名称	描述	注释
Observation-Health-&-Fitness-Service-Consent	知情同意书使能观测健康与健身服务须能接收[HL7 CDA IG]知情同意书指令知情同意书文件。	
Observation-HFS-Consent_Transport	知情同意书使能观测健康与健身服务须实施IHE XDR的文件接收者角色，以便使用ITI 41提供和注册文件集-b事务处理来接收一个知情同意书文件。	如果如知情同意书文件的XDS元数据所指示接收到一个新版本，WAN观察接收器替换现有的知情同意书文件

表C.7 – 用于知情同意书使能PHG的、使用SOAP的知情同意书执行导则

名称	描述	注释
HFS-PHG-Content_ Encryption_Actor	知情同意书使能健康与健身服务观测PHG须按照在 XML加密规范[W3C XMLENC]第4.1节中所定义的加密处理规则对PCD-01事务处理的载荷（[ITU-T H.812.1]附件D）进行加密。	
HFS-PHG-Content_ Encryption_MIMEtype	知情同意书使能健康与健身服务观测PHG须将MIME类型设置为 "application/hl7-v2+xml"。	目的是指明被加密载荷的类型。
HFS-Services-PHG-Content_ Encryption_Algorithm	知情同意书使能健康与健身服务观测PHG须将AES-128 CBC用作来自XML加密规范的载荷加密算法。	AES-128 CBC算法是通过使用以下标识符来确定的：http：//www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC]
HFS-PHG-Encryption_ Recipient_Binding_PKI	为了内容密钥传输，知情同意书使能健康与健身服务观测PHG须支持来自XML加密规范的RSA版本1.5。	基于RSA v1.5的密钥传输是通过使用以下标识符[W3C XMLENC] 来确定的：http：//www.w3.org/2001/04/xmlenc#rsa-1_5 关于RSA v1.5的详细信息，请查阅[b-RFC 2437]。 基于RSA v1.5的密钥传输也被用于用在HRN-IF上的CMS （加密消息句法）标准中。更多信息，请查阅[b-RFC 3370]及用于HRN-IF的知情同意书执行导则。

表C.7 – 用于知情同意书使能PHG的、使用SOAP的知情同意书执行导则

名称	描述	注释
HFS-PHG-Encryption_Recipient_Binding_Symmetric	对内容密钥传输，知情同意书使能健康与健身服务观测PHG**应**使用来自XML加密规范的AES-128 对称密钥卷绕算法。 在基于口令的加密的情况下，知情同意书使能健康与健身服务观测PHG**可以**将PBKDF2用作来自[IETF RFC 3211]的密钥推算算法。	用于AES-128对称密钥卷绕的标识符是：http：//www.w3.org/2001/04/xmlenc#kw-aes128 [W3C XMLENC]。用在卷绕中的密钥被称为KEK，它可以从一个口令或一个长期共享的秘密密钥中得出。
HFS-PHG-Integrity_Payload_PCD-01_Create	知情同意书使能健康与健身服务观测PHG**须**根据XML加密规范使用SHA256（第5.7.2节）来计算加密载荷的摘要。	SHA256算法是通过使用以下URL来确定的：http：//www.w3.org/2001/04/xmlenc#sha256 [W3C XMLENC]。
HFS-Encrypted_Payload_PCD-01_transaction	知情同意书使能健康与健身服务观测PHG**须**将加密的载荷卷绕到以下单元中： <CommunicateEncPCDData xmlns= "urn:ihe:continua:enc:pcd:dec:2012">	在未加密载荷的情况下，内容被卷绕到以下单元中： <Communicate PCDData xmlns= "urn:ihe:pcd:dec:2010"> 参见图II.1中的示例。
HFS-Encrypted_Payload_PCD-01_Transaction_Header	在加密载荷的情况下，SOAP报头**须**包含： urn:ihe:continua:enc:pcd:dec:2012:CommunicateEncPCDData" instead of "urn:ihe: pcd:dec:2010: CommunicatePCDData	普通PCD-01事务处理包含： urn:ihe: pcd:dec:2010:CommunicatePCDData。 参见在图II.1、图II.2和图II.3中的示例。

表C.8 – 用于知情同意书使能健康与健身服务的、使用SOAP的知情同意书执行导则

名称	描述	注释
HFS-HTTP-Ack	知情同意书使能观测健康与健身服务**须**在成功接收加密消息后发送带有状态码等于202的SOAP HTTP响应。 知情同意书使能观测健康与健身服务**不应**发送PCD-01应用级别的确认。	原因是观测健康与健身服务不可以拥有解密密钥，因为该内容可以为了健康与健身服务上的一个特定接收者而被加密。
HFS-Payload-PCD-01-Verify-Integrity	知情同意书使能观测健康与健身服务**须**验证加密载荷的消息摘要。	

表C.8 – 用于知情同意书使能健康与健身服务的、使用SOAP的知情同意书执行导则

名称	描述	注释
HFS-Payload-PCD-01-Verify-Integrity-Algorithm	知情同意书使能观测健康与健身服务**须**支持SHA256算法。	
HFS-Content-Decryption-Actor	知情同意书使能观测健康与健身服务**须**按照观察接收器 **须**符合在XML加密规范[W3C XMLENC]第4.2节中规定的解密规则。	
HFS-Key-Transport-RSA	知情同意书使能观测健康与健身服务**须**支持来自XML加密规范[W3C XMLENC]的RSA版本1.5。	
HFS-Key-Transport-Symmetric	知情同意书使能观测健康与健身服务**须**支持来自XML加密规范[W3C XMLENC]的AES-128对称密钥卷绕算法。 知情同意书使能观测健康与健身服务**须**支持PBKDF2作为来自[IETF RFC 3211]的密钥推算算法。	用于AES-128对称密钥卷绕的标识符是：http：//www.w3.org/2001/04/xmlenc#kw-aes128 [W3C XMLENC]。用在卷绕中的密钥被称为KEK，它可以从一个口令或一个长期共享的秘密密钥中得出。
HFS-Content-Decryption-Algorithm	知情同意书使能观测健康与健身服务**须**使用来自XML加密规范[W3C XMLENC]的AES-128 CBC解密算法。	AES-128 CBC算法是通过使用以下标识符来确定的：http：//www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC]。

附录 I

用于知情同意书管理的 ATOM 馈入要素

（本附录非本建议书不可分割的组成部分）

以下条目要素的 ATOM 馈入子要素具有用于知情同意书文件的特定用法。

表I.1 – 用于知情同意书管理的ATOM馈入要素

要素	用法
作者	人员构件，指明谁在提供知情同意书文件中的信息，即谁填写了知情同意书。
标题	患者知情同意书文件的标题（例如，Adam的知情同意书授权）。
链接	参考Adam的知情同意书指令文件，该文件**须**是一个有效的HL7 CDAR2知情同意书指令IG文件。 链接应是相对的，隐私许可文件**须**在数据记录的知情同意书部分中。
发布的	发布的要素**须**设置将隐私许可文档发布到服务器的日期和时间。

I.1 root.xml 中的知情同意书信息

```
<profile>
   <id>consent</id>

<reference><http://handle.itu.int/11.1002/3000/hData/Consent/2017/01/H.812.pdf></reference>
</profile>
<section>
  <path>consent</path>
  <profileID>consentId</profileID>
  <resourceTypeID>consent</resourceTypeID>
</section>
<resourceType>
  <resourceTypeID>consent</resourceTypeID>
  <reference>
    http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=63
  </reference>
  <representation>
     <mediaType>application/xml</mediaType>
  </representation>
</resourceType>
```

附录 II

使用 SOAP 的知情同意书管理示例

（本附录非本建议书不可分割的组成部分）

```
<html version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
   <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing" >
      <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
soapenv:mustUnderstand="true" >
      <wsa:To
soapenv:mustUnderstand="true">
https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Service>/wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand="true">
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand="true">urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand="true">urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicatePCDData xmls="urn:ihe:pcd:dec:2010">
            MSH|^~\&|AT4_PHG^123456789ABCDEF^EUI-
            64|||20120409103145+0000||ORU^R01^ORU_R01|MSGID2848518|P|2.6|||NE|AL|||||IHE PCD ORU-
            R012006^HL7^2.16.840.1.113883.9.n.m^HL7 PID|||789567^^^Imaginary
            Hospital^PI||Doe^John^Joseph^^^^L
            OBR|1|POTest^AT4_PHG^1234567890ABCDEF^EUI-64|POTest^AT4_PHG*1234567890ABCDEF^EUI-
            64|182777000^monitoring of patient^SNOMED-CT|||20100903124015+0000
            OBX|1|CWE|68220^MDC_TIME_SYNC_PROTOCOL^MDC|0.0.0.1|532224^MDC_Time_SYNC_NONE^MDC||||||
            R
            OBX|2|CWE|68220^MDC_REG_CERT_DATA_AUTH_BODY^MDC|0.0.0.2|1^auth-body-康体佳(2)||||||R
            OBX|3|ST|588800^MDC_REG_CERT_DATA_康体佳_VERSION^MDC|0.0.0.3|1.5||||||R
            OBX|4||528388^MDC_DEV_SPEC_PROFILE_PULS_OXIM^MDC|1||||||X||||||1234567890ABCDEF^EUI-64
            OBX|5|ST|531696^MDC_ID_MODEL_NUMBER^MDC|PulseOx v1.5||||||R
            OBX|6|ST|531970^MDC_ID_MANUFACTURER^MDC|1.0.0.2|AT4 Wireless||||||R
            OBX|7|DTM|67975|^MDC_ATTR_TIME_ABS^MDC|1.0.0.3|20100903124015+0000||||||R2010090312401
            5+0000
            OBX|8|CWE|68218^MDC_CERT_DATA_AUTH_BODY^MDC|1.0.0.4|1^auth-body-康体佳(2)||||||R
            OBX|9|ST|588800^MDC_REG_CERT_DATA_康体佳_VERSION^MDC|1.0.0.5||||||R
            OBX|10|NA|588801^MDC_REG_CERT_DATA_康体佳_CERT_DEV_LIST^MDC|1.0.0.6|16388||||||R
            OBX|11|CWE|588802^MDC_REG_CERT_DATA_康体佳_REG_STATUS^MDC|1.0.0.7|0^unregulated-
            device(0)||||||R
            OBX|12|NM|150456^MDC_DIM_PERCENT^MDC|||||R|||20100903124015+0000
            OBX|13|NM|149520^MDC_PULS_OXIM_RATE^MDC|1.0.0.9|71|264864^MDC_DIM_BEAT_PER_MIN^MDC||||
            |R|||20100903124015+0000
         </soapenv:Body>
      </soapenv:Envelop>
```

图II.1 – 具有未加密有效负载的PCD-01事务处理

```
<html version=”1.0” encoding=”UTF-8” ?>
<soapenv:Envelope xmlns:soapenv=”http://www.w3.org/2003/05/soap-envelope”>
   <soapenv:Header xmlns:wsa=”http://www.w3.org/2005/08/addressing” >
      <wsse:Security xmlns:wsse=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd”
   soapenv:mustUnderstand=”true”>
<wsa:To
soapenv:mustUnderstand=”true”
>https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Services/DeviceObservationC
onsumer_Service</wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand=”true”>
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand=”true”>urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand=”true”>urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicateEncPCDData xmlns=”urn:ihe:康体佳 cenc:pcd:dec:2012”>
<EncryptedData xmlns=http://www.w3.org/2001/04/xmlenc#    MimeType=”applicationhl7-v2+xml”>
      <EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc/>
      <KeyInfo xmlns+”http://www.w3.org/2000/09/xmldsig#”>
            <EncryptedKey xmlns=http://www.w3.org/2001/04/xmlenc#”>
<Encryption Method Algorithm=http://www.w3.org/2001/04/xmlenc#rsa-1_5/>
                     <KeyInfo xmlns=http://www.w3.org/2000/09/xmldsig#>
                        <KeyName>John Smith</KeyName>
                     </KeyInfo>
                     <CipherData>
                        <CipherValue>Encrypted Key…</CipherValue>
                     </CipherData>
                  </EncryptedKey>
            </KeyInfo>
            <CipherData>
                     <CipherValu>Enc.OBX Message goes here…</CipherValue>
            </CipherData>
            </EncrptedData>
         </CommunicateEncPCDData>
      </soapenv:Body>
   </soapenv:Envelop>
```

图II.2 – 加密PCD-01事务处理 – 基于公钥

在图 II.2 中显示的 PCD-01 事务处理，使用 XML 加密标准，具有加密有效载荷。内容密钥利用收件方的公钥进行加密。

```
<html version=”1.0” encoding=”UTF-8” ?>
<soapenv:Envelope xmlns:soapenv=”http://www.w3.org/2003/05/soap-envelope”>
   <soapenv:Header xmlns:wsa=”http://www.w3.org/2005/08/addressing” >
      <wsse:Security xmlns:wsse=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd”
   soapenv:mustUnderstand=”true”>
<wsa:To
soapenv:mustUnderstand=”true”
>https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Services/DeviceObservationC
onsumer_Service</wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand=”true”>
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand=”true”>urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand=”true”>urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicateEncPCDData xmlns=”urn:ihe:康体佳 cenc:pcd:dec:2012”>
<EncryptedData xmlns=http://www.w3.org/2001/04/xmlenc#    MimeType=”applicationhl7-v2+xml”>
      <EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc/>
      <KeyInfo xmlns+”http://www.w3.org/2000/09/xmldsig#”>
            <EncryptedKey xmlns=http://www.w3.org/2001/04/xmlenc#”>
<Encryption Method Algorithm=http://www.w3.org/2001/04/xmlenc #rsa-1_5/>
                     <KeyInfo xmlns=http://www.w3.org/2000/09/xmldsig#>
                        <KeyName>John Smith</KeyName>
                     </KeyInfo>
                     <CipherData>
                        <CipherValue>Encrypted Key…</CipherValue>
                     </CipherData>
                  </EncryptedKey>
            </KeyInfo>
            <CipherData>
                     <CipherValu>Enc.OBX Message goes here…</CipherValue>
            </CipherData>
            </EncrptedData>
         </CommunicateEncPCDData>
      </soapenv:Body>
   </soapenv:Envelop>
```

图II.3 – 加密PCD-01事务处理 – 基于对称密钥

在图 II.3 中显示的 PCD-01 事务处理，使用 XML 加密标准，具有加密有效载荷。在这个例子中，假定内容密钥对发送方和接收方都是已知的并为只读。

附录 III

OAuth 示例

（本附录非本建议书不可分割的组成部分）

例1：

– 请求访问令牌

为了获得访问令牌，具有问卷调查表能力的 PHG 向授权服务器发出以下 HTTP POST 请求。

```
POST http://localhost:3000/oauth2/token HTTP/1.1
User-Agent: Fiddler
Host: localhost:3000
Authorization: Basic
MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl
Content-Type: application/x-www-form-urlencoded
Content-Length: 59

grant_type=password&username=john@example.com&password=test
```

其中：

– http://localhost:3000/oauth2/token是到达授权服务器的URL，必须为具有问卷调查表能力的PHG所知。

– 授权：基本 MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl

– 这是一个基本的HTTP授权报头，由具有问卷调查表能力的PHG使用其特定的标识符和密码字、通过将它们编码为Base64哈希字符串Base64（“120094574673767: b54dc82476af2814e620b86776c42c0e”）=

– “MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl”来生成。

– grant_type指明授权码。在该授权编码中是用户名和密码。

– 访问令牌响应

授权服务器验证访问令牌请求，如果得到授权，它将生成一个”持有者”类型的访问令牌和一个可选的刷新令牌。

```
HTTP/1.1 200 OK
Content-Length: 141
Content-Type: application/json
X-Ua-Compatible: IE=Edge
X-Runtime: 0.273027
Server: WEBrick/1.3.1 (Ruby/1.9.3/2013-02-22)
Date: Wed, 03 Apr 2013 08:54:57 GMT
Connection: Keep-Alive

{"access_token":"f779da766bfd1b9164b0fd6d280d52f1","refresh_token":"789f3daf81
a302e0636325114113e4b4","token_type":"bearer","expires_in":899}
```

其中：

– “f779da766bfd1b9164b0fd6d280d52f1”是PHG在访问服务器上的资源时将使用的访问令牌。
– “789f3daf81a302e0636325114113e4b4”是刷新令牌，可用于获取新令牌。
– 上例中的令牌类型为”持有者”。
– 令牌的生命周期为899秒。
– 使用”持有者”类型的访问令牌请求资源。

例2：

在下面的示例中，PHG 使用一个”持有者”令牌，以请求受保护的资源，例如，问卷调查表。

```
GET http://localhost:3000/hdata/root.xml HTTP/1.1
User-Agent: Fiddler
Host: localhost:3000
Authorization: Bearer f779da766bfd1b9164b0fd6d280d52f1
```

附录 IV

知情同意书使能 PHG 问卷调查表响应关联

（本附录非本建议书不可分割的组成部分）

表IV.1 – 保密编码系统的要素

名称	值	注解
编码	"R"	
编码系统	2.16.840.1.113883.5.25	
编码系统名称	"保密"	
显示名称	"限制"	

表IV.2 – 康体佳知情同意书指令编码系统的要素

名称	值	注解
编码	该值须与[HL7 CDA IG]中定义的相同	
编码系统	2.16.840.1.113883.3.1817.1.2.1	
编码系统名称	"康体佳知情同意书指令"	
显示名称	知情同意书文件的ID	

表IV.3 – 从保密编码系统转换到康体佳知情同意书指令编码系统

名称	值	注解
编码	"R"	
编码系统	2.16.840.1.113883.5.25	
编码系统名称	"保密"	
显示名称	"限制"	
转换	编码="<知情同意书文件的ID>" 编码系统=2.16.840.1.113883.3.1817.1.2.1 编码系统名称="康体佳知情同意书指令" 显示名称= 知情同意书文件的ID	"<> " 知情同意书文件的ID 的占位符。 康体佳知情同意书指令编码系统的要素咨询表IV.2。

表IV.4 – 个人互联健康联盟的OID分布

OID	描述	注解
2.16.840.1.113883.3.1817	组织OID：个人互联健康联盟	
2.16.840.1.113883.3.1817.1	康体佳E2E架构V1.0的根OID	
2.16.840.1.113883.3.1817.1.2	E2E 安全和隐私的根OID	
2.16.840.1.113883.3.1817.1.3	个人健康设备接口的根OID	
2.16.840.1.113883.3.1817.1.4	ZigBee个人健康设备接口的根OID	
2.16.840.1.113883.3.1817.1.5	NFC个人健康设备接口的根OID	
2.16.840.1.113883.3.1817.1.6	服务接口的根OID	
2.16.840.1.113883.3.1817.1.7	医疗保健信息系统的根OID	
2.16.840.1.113883.3.1817.1.2.1	E2E安全和的隐私：康体佳知情同意书指令编码系统的根OID	

参考书目

包含更多背景信息的非规范性参考文献和出版物清单，请参见[ITU-T H.810]。

ITU-T 系列建议书

A 系列	ITU-T 工作的组织
D 系列	资费和会计原则以及国际电信/ ICT 经济和政策问题
E 系列	综合网络运行、电话业务、业务运行和人为因素
F 系列	非话电信业务
G 系列	传输系统和媒质、数字系统和网络
H 系列	**视听及多媒体系统**
I 系列	综合业务数字网
J 系列	有线网络和电视、声音节目及其他多媒体信号的传输
K 系列	干扰的防护
L 系列	环境与信息通信技术、气候变化、电子废物、能源效率；电缆和外部设备其他组件的建造、安装和保护
M 系列	电信管理，包括 TMN 和网络维护
N 系列	维护：国际声音节目和电视传输电路
O 系列	测量设备的技术规范
P 系列	电话传输质量、电话设施及本地线路网络
Q 系列	交换和信令及相关的测量和测试
R 系列	电报传输
S 系列	电报业务终端设备
T 系列	远程信息处理业务的终端设备
U 系列	电报交换
V 系列	电话网上的数据通信
X 系列	数据网、开放系统通信和安全性
Y 系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z 系列	用于电信系统的语言和一般软件问题

瑞士印刷
2018年，日内瓦