



中华人民共和国国家标准

GB/T 38961—2020

个人健康信息码 参考模型

Personal health information code—Reference model

2020-04-29 发布

2020-04-29 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	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 健康码的组成	3
4.1 健康码的结构	3
4.2 授权记录	3
4.3 编码和后续处理	4
5 码制和展现形式	4
5.1 健康码的终端应用	4
5.2 健康码应急管理	5
6 健康码应用系统参考模型	6
6.1 系统组成	6
6.2 健康码使用流程	7
6.3 健康码互认	7
7 健康码应用要求	8
7.1 一般要求	8
7.2 身份认证要求	8
7.3 应用对接要求	8
7.4 信息保护要求	9
7.5 安全要求	9
附录 A (规范性附录) 代码集	10
附录 B (资料性附录) 全国一体化在线政务服务平台防疫健康信息服务系统方案	11
附录 C (资料性附录) 健康码应用场景	14
参考文献	15

前 言

本标准是《个人健康信息码》系列标准之一，该系列标准的结构和名称如下：

- GB/T 38961—2020 个人健康信息码 参考模型；
- GB/T 38962—2020 个人健康信息码 数据格式；
- GB/T 38963—2020 个人健康信息码 应用接口。

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由国务院办公厅电子政务办公室提出。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)归口。

本标准起草单位：国务院办公厅电子政务办公室、中国电子技术标准化研究院、公安部第一研究所、浙江省大数据发展管理局、广东省政务服务数据管理局、南京市政务服务管理办公室、上海市大数据中心、河北省政务服务中心、河南省大数据管理局、贵州省人民政府办公厅、衢州市营商环境建设办公室、浙江省标准化研究院、杭州市数据资源管理局、合肥市数据资源局、中国科学院软件研究所、福建正孚软件有限公司、北京中盾安信科技发展有限公司、深圳市腾讯计算机系统有限公司、支付宝(中国)网络技术有限公司、北京百度网讯科技有限公司、大汉软件股份有限公司、中国电子科技集团有限公司、阿里巴巴(中国)有限公司、腾讯云计算(北京)有限责任公司、电科云(北京)科技有限公司。

本标准主要起草人：卢向东、尹智刚、王齐春、李恒训、赵波、孙文龙、陈亚军、于锐、杨林、周平、于浩、杨庄媛、陈治佳、孙富安、姜舟、徐云、李景曦、王赞萃、李松渊、钱学文、马晓鹄、张晓东、温赫、张红振、林文昊、姜淑娟、李宁、孙茂阳、齐同军、黄颖纯、聂楚江、国伟、赵立、江万鑫、杨强、王剑冰、黄伟耀、罗朝亮、杨鹏、陈磊、陈昊、金震宇、房迎、李昊龙、林冠辰、仲里、王舒墨、侯海实、陈丽平、王永霞、滕一帆、王鹏达、焦秀珍。



引 言

在预防、控制和消除突发公共卫生事件(例如新型冠状病毒感染的肺炎 COVID-19)危害的过程中,需要采集、存储和处理个人健康信息,以实现多种管理用途,主要包括:

- 快速获取个人健康的相关信息;
- 统计某种流行病或疾病的相关信息;
- 管理不同地域之间的人员流动;
- 互认健康信息业务等级。

2020年2月以来,在COVID-19疫情防控和复工复产过程中,全国一体化在线政务服务平台(简称“一体化平台”)提供的防疫健康信息码、部分省(区、市)建设使用的“健康码”,作为个人健康信息码的一种重要形式,成为快速采集、存储和处理个人健康信息的一种有效方式。个人健康信息码在实际应用过程中,存在码制组成不统一、数据格式不一致、缺乏数据共享和互认机制等问题,制约了人员、货物跨地区流动。因此,从当前的实践情况和长远的应用需求来看,需要实现个人健康信息码的标准一致。除突发公共卫生事件的应急处置外,个人健康信息码在个人医疗、健康养老或其他重大公众活动管理过程中同样适用。

本标准中规定的具体事项,法律法规(如《中华人民共和国网络安全法》《中华人民共和国传染病防治法》)另有规定的,需遵照其规定执行。



个人健康信息码 参考模型

1 范围

本标准规定了个人健康信息码的组成结构、码制和展现形式、应用系统参考模型和应用要求。

本标准适用于个人健康信息码相关应用系统的设计、开发和系统集成。其他有关个人健康信息授权发布、查询利用的应用系统可参照执行。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 2260 中华人民共和国行政区划代码
- GB/T 2659 世界各国和地区名称代码
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 27766—2011 二维条码 网格矩阵码
- GB/T 33560—2017 信息安全技术 密码应用标识规范
- GB/T 35273—2020 信息安全技术 个人信息安全规范
- GB/T 35274—2017 信息安全技术 大数据服务安全能力要求
- GB/T 38962—2020 个人健康信息码 数据格式

3 术语和定义

下列术语和定义适用于本文件。

3.1

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

- 注1: 个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通讯通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。
- 注2: 个人信息控制者通过个人信息或其他信息加工处理后形成的信息,例如,用户画像或特征标签,能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的,属于个人信息。

[GB/T 35273—2020, 定义 3.1]

3.2

个人健康信息 personal health information

涉及已标识或可标识自然人健康情况的个人信息。

3.3

个人信息主体 personal information subject

个人信息所标识或者关联的自然人,即个人数据的主体。

注: 改写 GB/T 35273—2020, 定义 3.3。

3.4

个人信息控制者 personal information controller

有能力决定个人信息处理目的、方式等的组织或个人。

[GB/T 35273—2020, 定义 3.4]

3.5

明示同意 explicit consent

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明,或者自主作出肯定性动作,对其个人信息进行特定处理作出明确授权的行为。

[GB/T 35273—2020, 定义 3.6]

3.6

授权同意 consent

个人信息主体对其个人信息进行特定处理作出明确授权的行为。

[GB/T 35273—2020, 定义 3.7]

3.7

居民身份网络可信凭证 cyber trusted identity; CTID

网证

用于在网络空间中证明居民个人身份的电子文件,与居民身份证件具有一一对应关系。

3.8

居民身份网络标识 cyber identifier

由居民身份网络认证服务系统派发给网证应用系统,用于标识居民个人身份的代码。

注 1: 同一网证应用系统中,居民身份网络标识与居民真实身份一一对应。

注 2: 同一居民在不同网证应用系统的居民身份网络标识不同。

3.9

个人健康信息码 personal health information code; PHI-code

健康码

与居民身份网络可信凭证绑定,表达用户授权他人或组织临时访问特定个人健康信息的一串数字或字母的序列。通常使用二维条码作为其存储媒体。

3.10

健康码服务 PHI-code service

对通过身份验证的用户提供生产、分发和验证包含特定应用授权信息的健康码或其对应的二维条码的服务。

3.11

健康码应用 PHI-code application

提供或识别使用健康码的应用软件。

示例:“××省健康码”“××市健康码”。

3.12

个人健康信息服务 personal health information service

在用户授权的前提下,提供个人自愿申报或相关组织合法拥有的个人健康信息的服务。

3.13

健康码应用系统 PHI-code application system

支持个人健康信息的采集、查询和使用的软硬件系统的统称,一般由健康码服务、健康码应用和个人健康信息服务组成。

3.14

个人健康信息目录 personal health information list

经过清洗、加工后形成的综合反映个人健康状态的概要结果,一般提供给上级部门汇集和使用。

4 健康码的组成

4.1 健康码的结构

健康码由数字和/或字母组成,其结构见图1。



图1 健康码的结构

健康码由A、B、S三段构成。其中：

- A段是用户身份标识,需经实名实人认证后取得,代表个人信息主体的身份。可使用网证数据,网证可用于实现跨系统身份互通互认,其数据前两个字节为16位大端序无符号整数,代表A段内容的长度。
- B段是业务数据,代表码的类型、制码平台标识、码的截止时间和信息主体授权记录摘要,其中:
 - 第1部分是长度及版本,前两个字节是16位大端序无符号整数,表示B段内容的长度,后两个字节表示版本号;
 - 第2部分是码类型声明,4位字母或数字,本标准中固定为“JKM1”;
 - 第3段是各类健康码服务在互认机制中注册时分配的标识,6位数字,宜使用GB/T 2260中规定的行政区划代码;
 - 第4段是该健康码的截止时间(UTC时间);
 - 第5段是信息主体授权记录的摘要,摘要时应使用符合国家密码管理要求的算法,见GB/T 33560—2017中标识为“1.2.156.10197.1.401”的算法。
- S段是针对A+B内容的数字签名值。签名时应使用符合国家密码管理要求的算法,见GB/T 33560—2017中标识为“1.2.156.10197.1.501”的算法。

健康码B段的第2部分、第3部分(码类型及平台标识)用来提示健康码的处理者准确识别和路由到生成该码的健康码服务,是建立健康码互通互认的基础。码的截止时间可用来快速识别已过期的授权。

4.2 授权记录

授权记录应完整表达个人信息主体对其个人信息及处理方式的授权情况,主要要素包括授权主体信息、授权有效期限、被授权主体信息、个人信息控制者信息、被授权操作的个人信息类别或索引等,其要素见表1。

表 1 个人信息授权记录的要素

要素名称	短名	约束	说明
授权主体	SQZT	必选	发出授权的个人,应是具有完全民事行为能力的主体。需提供充分和必要的相关信息,如姓名、证件类型和号码、国籍等
有效期限	YXQX	必选	包括发出授权的时间以及该授权有效期限的起止时间
被授权主体	BSQZT	可选	被授权的访问或操作个人信息的个人或组织,需提供充分和必要的标识信息。对于个人来说,需提供姓名、证件类型和号码、国籍等;对于组织来说,需提供组织机构名称、证件类型和号码等
个人信息控制者	XXKZZ	可选	存储和管理个人信息的各种应用系统及其分类信息。在特定场景下,可有默认设定
被授权的信息类别	XXLB	可选	根据应用目标确定,如个人信息的类别或组别等。在特定场景下,可有默认设定
被授权的信息索引	XXSY	可选	查询信息所需的索引信息,如个人信息主体信息、信息的标识等。其中个人信息主体可默认为授权主体
被授权的操作权限	CZQX	可选	获得信息后可对该信息执行何种操作,如只读、保留查询凭证、下载、转储等。默认为只读

对于用于通行的健康码,被授权访问的信息(其数据格式应符合 GB/T 38962—2020)和被授权对象(未明确指定,但一般是各通行卡口的检查人员)均已明确,因此仅需记录授权主体的概要信息。授权情况的明文由个人健康信息主体的姓名、身份证件号码、身份证件类型等组成,并按“B1|B2|B3|B4·B5”的形式拼接:

- a) B1 为个人健康信息主体的姓名;
- b) B2 为个人健康信息主体的身份证件号码;
- c) B3 为个人健康信息主体的身份证件类型的代码,其取值见附录 A;
- d) B4 为个人健康信息主体的国家或地区代号,应采用 GB/T 2659 中规定的“三字母代码”;
- e) B5 为个人健康信息主体的授权时间,应按 YYYYMMDDHHMMSS 的格式组织。

4.3 编码和后续处理

健康码生成后可在健康码服务或健康码应用中按相应码制编码成二维码图像。可在二维码图像中嵌入数字水印或增加溯源标识等,增强条码的使用安全性。

5 码制和展现形式

5.1 健康码的终端应用

将健康码编码为条码图像时应使用 GB/T 27766—2011 规定的二维条码码制,以及其他有关国家标准规定的主流二维条码码制。

健康码宜采用图 2 所示的展现形式。

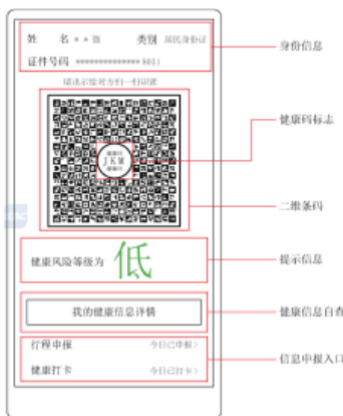


图2 健康码在移动终端中的展示示例

在展现健康码二维码的同时,应同时提供信息业务等级文字或符号提示。宜同时提供脱敏的身份信息、个人健康信息自查和个人健康信息申报等入口。一般在二维码展示界面中还应提供操作提示和切换操作入口。

其中:

- 脱敏的身份信息应提供核对个人登录情况所需的必要信息;
- 出示二维码时,健康码应用应在二维码中心处添加统一健康码标志,并可根据信息业务等级改变条码色块和边框的颜色;
- 除以二维码色块、框线等形式标识信息业务等级外,还应以明显的文字或符号进行提示;
- 用户可自行查看本人申报的健康信息和被授权访问的情况,从而了解本人的健康信息业务等级;
- 信息申报入口提供用户自行申报或为家人等申报健康信息(如体温、相关症状等)和行程信息的功能;
- 统一健康码标志应清晰鲜明,其覆盖二维码图像的面积比例应在10%以下。

健康码应设定有效期,在健康码应用中点击二维码图像可手动刷新。

5.2 健康码应急管理

信息主体查询本人健康信息时,可根据查询所得的信息结合不同场景的应用需要赋予二维码不同的颜色,以便快速标识健康信息业务等级,提升检查和通行效率。二维码的不同颜色标识示例见图3。在特殊情况下可增加其他颜色。



图 3 二维条码的不同涂色示例

除二维条码涂色以外,健康信息业务等级的标识还应配合容易识别的文字或符号提示信息使用。

6 健康码应用系统参考模型

6.1 系统组成

健康码服务不应直接参与个人健康信息的处理,其与具体的个人健康信息服务应在逻辑上做显著区分。健康码应用系统参考模型见图4,参考模型中给出了健康码服务与各类个人健康信息服务的集成关系。

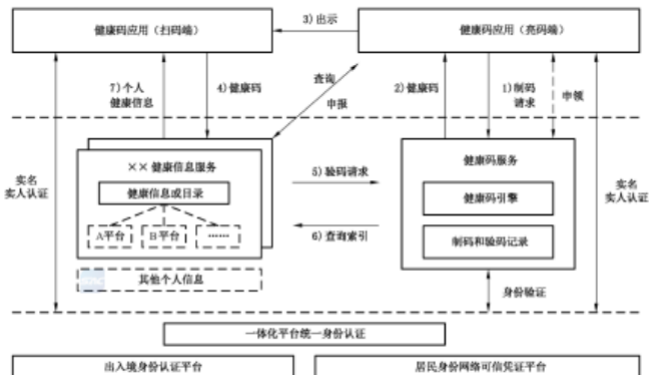


图 4 健康码应用系统参考模型

在图 4 中,各组成部分的功能和协作关系如下:

- 健康码服务主要提供制码、验码功能,还可为应用端提供个人授权使用情况查询;
- 健康码服务主要的功能模块是健康码引擎,用以生成和验证健康码;制码和验证的记录应保留一段时间以供查询;
- 个人健康信息服务系统是个人信息的控制者,应根据个人信息主体(健康码应用的用户)的身份凭证或授权来响应个人健康信息查询请求;
- 个人健康信息服务可采用分级管理模式,采用分级管理时,对外的信息服务由顶层健康信息目

录库统一提供,各子级平台负责本区域人员的健康信息更新和质量保障;

- e) 个人健康信息服务可与其他个人信息控制者建立联系,采用接口调用等方式在个人信息主体授权下查询其他信息并作为本服务的数据来源或参考值;
- f) 健康码的申领、出示、验证等应通过健康码应用完成;
- g) 健康码的使用应先行可信的用户身份认证,身份认证的范围应能覆盖可能使用个人健康信息服务的各人群,包括大陆居民、港澳台人士、华侨和外籍人员等。

防疫健康信息服务系统示例参见附录 B。

6.2 健康码使用流程

健康码应用系统应按 6.1 中规定的参考模型,在系统内明确各部分功能构成和协作关系,整体上通过健康码服务和个人健康信息服务的相互协作完成对外信息服务。

健康码的出示应以用户实名真人认证为前提,健康码服务对接的个人健康信息服务及其对应的应用程序应先取得身份认证后的凭证数据,再以其为主要参数向健康码服务申请制码。

健康码应用的扫码请求应以用户实名真人认证为前提,以扫码用户身份凭证数据和健康码为参数发起健康信息查询请求。

个人健康信息服务响应健康信息查询应以健康码验证为前提,健康码应用应以健康码为参数提交个人健康信息查询请求,个人健康信息服务应根据健康码服务对健康码的验证情况响应该请求。

健康码的使用流程如下:

- a) 健康码应用亮码端的用户在移动终端上完成实名真人认证,申领健康码;
- b) 用户通过健康码应用亮码端向健康码服务申请制码;
- c) 健康码服务向应用亮码端返回健康码或其二维码图像文件流;
- d) 健康码应用亮码端对返回的健康码进行编码或对二维码图像进行加工处理后向扫码端出示;
- e) 健康码应用扫码端解码获得健康码,并以扫码端身份认证凭证和健康码为参数向个人健康信息服务发起查询请求;
- f) 个人健康信息服务接收到查询请求后,将健康码发送到健康码服务进行验证;
- g) 健康码服务根据验证结果向个人健康信息服务返回信息查询索引或其他信息;
- h) 个人健康信息服务检索得到健康信息并返回给健康码应用扫码端,由其用户根据其应用目标确定返回信息的使用方式。

根据应用场景的需求,健康码所代表的个人信息主体授权可被设定为仅可使用一次。已验证并返回结果的健康码应记录验证的请求方及时间。

6.3 健康码互认

各健康码应用系统按图 5 所示的机制采取汇集健康信息目录的方式实现互信互认。

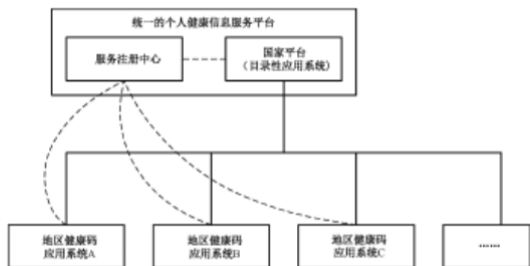


图5 健康码应用系统的目录汇集和互认

各地区建设的健康码应用系统应对接实名实人认证系统,在编码组成、码制和展现形式方面应符合本标准或与本标准兼容,并应获得第三方机构相应的技术检测报告。

经过改造和技术验证的健康码应用系统在统一的个人健康信息服务平台注册并取得平台标识、证书和密钥对等信息。各应用系统中制成的健康码应包含此平台标识,码的利用方根据此标识路由到生成该码的健康码服务进行验证。

各健康码应用系统中的健康信息目录可汇聚到统一的健康信息服务平台。

各健康码应用系统可对外提供信息服务并对数据质量负责,同时应提供数据异议处理服务。

统一的个人健康信息服务平台可对外提供基于健康信息目录的信息服务并提供统一异议处理入口。

7 健康码应用要求

7.1 一般要求

健康码应用以服务业务为原则,在不同的场景中,可在本标准的基础上灵活采用适合实际要求的界面和交互方式。

常见的健康码应用场景参见附录C。

7.2 身份认证要求

健康码出示前应先进行用户实名实人认证,相关认证应至少提供一种生物特征识别功能。

7.3 应用对接要求

健康码服务主要是为各应用提供用户授权行为存证,服务于各类个人健康信息应用。健康码服务与具体应用对接的步骤如下:

- 个人健康信息服务应进行改造,在响应以健康码为参数的信息请求之前,应先进行健康码的验证;
- 应用亮码端应进行改造,支持开通相关健康码功能;
- 应用亮码端应对接健康码服务,支持用户认证后查询本人健康信息和在线请求健康码;
- 应用扫码端应进行改造,应能扫描、解码得到二维码图像中的健康码;
- 应用扫码端应规范与个人健康信息服务的对接方式,以身份凭证和健康码作为必要参数。

基于健康信息的其他业务管理由各应用根据实际需求确定。一般来说,个人健康信息服务还应提供大数据分析、健康风险提示等其他信息服务。

7.4 信息保护要求

健康码的有效时间一般设置为 5 min,制码 5 min 后未产生验码请求的,该码即行无效,再对此码进行验码请求时,应提示“健康码已过期”。

健康码在应用端应被妥善保护,采用符合国家密码管理要求的算法进行加密保存,其使用宜配合用户的口令确认。

个人健康信息服务和健康码服务应动态监控相关应用的请求行为,出现异常情况时可在提示后切断相关服务和响应。

7.5 安全要求

个人健康信息服务及其应用应达到 GB/T 22239—2019 等级保护第三级的要求。

个人健康信息的采集、加工和利用应符合 GB/T 35273—2020 的规定。

个人健康信息服务及其应用采集数据时,应获取用户的明示同意或授权同意,并承诺对相关隐私内容进行保密。

健康码服务运营方和个人健康信息控制者应遵循 GB/T 35274—2017 建立数据安全保护制度,实施必要的数据安全技术措施。

个人健康信息控制者应定期备份数据,提升容灾备份能力。



附 录 A
(规范性附录)
代 码 集

本标准中的自然人是指大陆居民、港澳居民、台湾居民、华侨和取得永久居留身份证的外籍人员,其身份证件类型代码见表 A.1。

表 A.1 自然人身份证件类型代码

序号	证件类型	证件类型代码
1	居民身份证	111
2	港澳居民居住证	551
3	台湾居民居住证	552
4	普通护照	400
5	港澳居民来往内地通行证	516
6	台湾居民来往大陆通行证	511
7	外国人永久居留身份证	516
8	其他自然人有效证件	999

附录 B (资料性附录)

全国一体化在线政务服务平台防疫健康信息服务系统方案

B.1 系统概况

全国一体化在线政务服务平台(简称“一体化平台”)是国家电子政务领域的重要基础设施,提供统一身份认证、统一电子证照、统一数据交换等公共支撑服务。在2020年COVID-19疫情防控和复工复产过程中,国务院办公厅依托一体化平台数据共享服务受理系统,汇集各地区的个人健康信息目录,由国务院有关部门提供防疫相关信息服务和接口进行数据比对分析,通过各类应用软件连接个人和相关组织,提供防疫健康信息服务,取得了积极成效。

B.2 信息服务框架

一体化平台防疫健康信息服务系统整体框架见图 B.1。

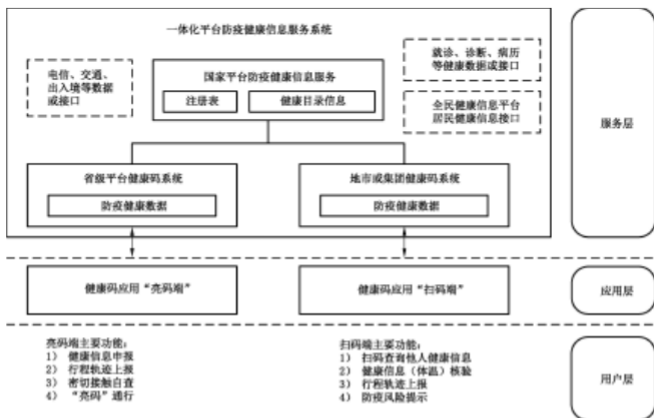


图 B.1 一体化平台防疫健康信息服务系统框架图

防疫健康信息服务系统由服务层(数据层)、应用层和用户层组成。

防疫健康信息服务的用户分为个人和单位两类,应用软件为两类用户提供不同的使用方式。

应用软件可以是国家平台移动端及各地方部门政务服务平台移动端等多种形态。

防疫健康信息依据的数据源包括但不限于:

- a) 确诊、疑似等病情病例数据;
- b) 密切接触者数据;

- c) 医学检测数据(核酸、抗体等检测数据);
- d) 发热门诊数据;
- e) 个人移动通信终端停留超过系统规定的一定时长的漫游地区风险等级信息(依据相关部门公布的地区风险等级信息进行对应);
- f) 交通出行信息;
- g) 出入境数据;
- h) 海关检验检疫数据;
- i) 疫情社区及重点活动场所数据;
- j) 通过全民健康信息平台相关接口调取的健康档案信息;
- k) 社区调查形成的家庭、居住、旅行入住等数据;
- l) 各核查点上报的测温 and 场所出入记录数据;
- m) 用户自行申报的个人或家庭健康数据;
- n) 其他防疫有关的数据。

B.3 服务调用流程

B.3.1 健康信息申报

用户通过应用软件填报个人或家庭成员防疫健康信息后,使用“用户防疫健康信息申报”接口将相关数据推送到一体化平台国家节点。

在防疫控制期内,防疫健康信息应按日申报。

B.3.2 二维码制码

用户在应用软件进行实名认证后,可请求生成“防疫健康信息码”的二维码,并在需要时出示此二维码,作为个人防疫健康信息证明。其主要流程包括:

- a) 用户进行亮码操作时,应用软件通过“二维码调用申请”接口发起业务请求,再调用防疫健康信息服务的“二维码赋码”接口;
- b) “二维码赋码”接口根据参数返回相应的二维码给应用软件。

B.3.3 健康信息查询

在获得用户亮码授权后,通过应用软件查询用户的防疫健康信息:

- a) 扫码端将“二维码验码”接口返回的加密用户信息作为参数,调用防疫健康信息服务的“用户防疫健康信息查询”接口;
- b) 接口调用成功,则默认返回近期(如 14 天)的用户防疫健康申报信息和其他防疫方面的信息。

B.4 应用模式

基于防疫健康信息码的具体防疫业务管理由各地区负责,一体化平台国家节点防疫健康信息码服务主要为地方政务服务平台服务,为各地区提供大数据分析比对结果,为健康码验证和跨地区信息查询提供路由等。

各地区可在一体化平台国家节点返回的个人防疫健康信息基础上,结合本地区数据资源开发健康码应用,在本地区平台上直接面向企业和个人服务。

在国家卫生健康主管部门指导意见的基础上,各地区自行确定防疫风险等级;各地区可自行决定如何使用风险等级信息,如用于企事业单位复工复产、社区网格化管理、辖区内通行等。

各地区负责所辖地的防疫健康信息码服务的投诉处理。

B.5 对接模式

已建设防疫健康信息码的地区,可按本标准与一体化平台国家节点注册对接。各地区应用软件应能识别由一体化平台国家节点生成的二维码,实现基于国家平台健康码的互信互认。一体化平台提供跨地区的防疫健康信息查询服务。各地区可在此基础上,结合本地区防疫健康信息数据,进行风险等级划分和评定。

尚未建设防疫健康信息码的地区,可利用一体化平台国家节点防疫健康信息码,结合本地区数据资源和防疫与复工复产要求进行风险等级划分和评定,作为本地区防疫健康信息码使用。



附 录 C
(资料性附录)
健康码应用场景

C.1 健康码防疫应用场景

健康码应用系统的用户通过移动通信终端或专用终端填报一次个人健康信息后可申请开通“健康码”，申报信息经个人健康信息服务后台校正后生成健康码，用户可凭借健康码进出多种公众场所，如社区、办公场所、交通卡口、交通客运站等，实现不同场景下的快速核验需求。具体可在以下场景下使用：

——村(社区)：

针对村(社区)等居住出行场景，通过亮码、扫码，作为出入居住地的电子凭证。

——交通卡口：

针对城市交通卡口的车辆核查，通过亮码、扫码，作为进入城市的申报电子凭证。

——公共交通：

长途汽车客运站、码头、机场、火车站等使用大规模运输工具但有固定且封闭的客运站，乘客仍以单人出入站台闸口为特点的单人通行场景，出租车、网约车场景等。

——公共场所：

工厂、高校、医院、商场、市场、酒店、公园、景区等人群密集场所，有固定且封闭的出入口，以单人出入为特点的通行场景。

老人、儿童、孤寡老人等可由家人或社区代为填报健康信息，申请开通“健康码”。

老人、儿童等不持有移动通信终端或专用终端时，可通过健康码应用打印有较长有效期的纸质健康证明作为“亮码”通行凭证。

C.2 健康码其他应用场景

健康码应用系统参考模型可用于疫情防控以外的多种个人健康信息应用场景，赋予不同的推广名称，例如：健康码服务与个人健康档案网络服务对接后，健康码可作为“病案码”，出示给医疗、养老等机构扫码端查询留存本人档案使用。

健康码应用系统参考模型用于其他个人健康信息应用场景时，应与对应的个人健康信息控制者及业务主管部门协调一致，按本标准建立技术认证和注册管理机制，保障个人健康信息的安全、高效、有序应用。

参 考 文 献

- [1] GB/T 25512 健康信息学 推动个人健康信息跨国流动的数据保护指南
 - [2] GB/T 32905 信息安全技术 SM3 密码杂凑算法
 - [3] GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法
 - [4] GA/T 1721 居民身份网络认证 通用术语
 - [5] GA/T 1722 居民身份网络认证 整体技术框架
 - [6] GA/T 1723.2 居民身份网络认证 认证服务 第2部分:服务接口要求
 - [7] GA/T 2000.156 公安信息代码 第156部分:常用证件代码
 - [8] 现役军人和人民武装警察居民身份证申领发放办法(中华人民共和国国务院中华人民共和国中央军事委员会令 第510号)
 - [9] 国务院办公厅关于印发《港澳台居民居住证申领发放办法》的通知(国办发〔2018〕81号)
 - [10] 关于依托全国一体化政务服务平台加快推进“健康码”跨地区互通互认的通知(国办电政函〔2020〕24号)
-