居民健康卡技术规范

中华人民共和国卫生部

2011 年 **7** 月 **4** 日

目　录

1 适用范围

本规范适用于所有制作、发行、使用居民健康卡的医疗卫生机构、第三方联合发卡机构、持卡人和生产企业。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。

GB 11643—1999	公民身份号码
GB 11714—1997	全国组织机构代码编制规则
GB 2261.1—2003	人的性别代码
GB 2261.2—2003	婚姻状况代码
GB 3304—1991	中国各民族名称的罗马字母拼写法和代码
GB 4658—1984	文化程度代码
GB/T 2260—2007	中华人民共和国行政区划代码
GB/T 2312—1980	信息交换用汉字编码字符集基本集
GB/T 16649.4—2010	识别卡　带触点的集成电路卡　第 4 部分
GB/T 16649.5—2002	识别卡　带触点的集成电路卡　第 5 部分
GB/T 18347—2001	128 条码
GB/T 6565—2009	职业分类与代码
ICD-9-CM	国际疾病分类 第九版 临床修订
ICD-10	国际疾病与相关健康问题分类代码第十版
ISO/IEC 14443	识别卡　非接触式集成电路卡 接近式卡
ISO/IEC 7810—2003	识别卡　物理特性
ISO/IEC 7811/2—2001	卡识别记录技术第 2 部分
GA 342.1—2001	户口类别代码
WS 363—2011	卫生信息数据元目录
WS 364—2011	卫生信息数据元值域代码
WS 365—2011	城乡居民健康档案基本数据集
JR/T 0025—2010	中国金融集成电路 IC 卡规范
JR/T 0008—2000	银行卡发卡行标识代码及卡号

3 定义和缩略语

3.1 定义

3.1.1 居民健康卡 （Residents Health Card）

居民健康卡是中华人民共和国居民拥有的，在医疗卫生服务活动中用于身份识别，满足健康信息存储，实现跨地区和跨机构就医、数据交换和费用结算的基础载体，是计算机可识别的 CPU 卡。

3.1.2 CPU 卡 （Central Processing Unit Card）

带有中央处理器（CPU）、存储单元以及芯片操作系统的集成电路卡。

3.1.3 芯片 （Chip）

本规范中特指居民健康卡中用于完成数据处理和存储功能的集成电路器件。

3.1.4 芯片操作系统 （COS，Chip Operating System）

CPU 卡芯片中存储和可运行的，以保护应用数据和程序的机密性和完整性，控制 CPU 卡芯片与外界信息交换为目的的嵌入式软件。

3.1.5 加密算法 （Cryptographic Algorithm）

为了隐藏或显现数据信息内容的变换算法。

3.1.6 对称加密算法 （Symmetric Cryptographic Algorithm）

加密密钥可以从解密密钥中推算出来，反过来也成立，在大多数算法中加/解密密钥是相同的。

3.1.7 非对称加密算法 （Asymmetric Cryptographic Algorithm）

加密算法的加密密钥和解密密钥是不一样的，不能由一个密钥推导出另一个密钥。

3.1.8 密钥 （Key）

加密转换中控制操作的符号序列。

3.1.9 对称密钥 （Symmetric Key）

在对称加密算法中使用的密钥。

3.1.10 非对称密钥 （Asymmetric Key）

在非对称加密算法中使用的密钥，包括公钥和私钥。

3.1.11 公钥 （Public Key）

在一个实体使用的非对称密钥对中可以被公众使用的密钥。在数字签名方案中，公钥用于验证。

3.1.12 私钥 （Private Key）

在一个实体使用的非对称密钥对中仅被该实体使用的密钥。在数字签名方案中，私钥用于签名。

3.1.13 数字签名 （Digital Signature）

对数据的一种非对称加密变换。该变换可以使数据接收方确认数据的来源和完整性，保护数据发送方发出和接收方收到的数据不被第三方篡改，也保护数据发送方发出的数据不被接收方篡改。

3.1.14 生物标识 （Biomarker）

人的某种特异性的生物学特征，具有遗传性和终身携带性，如血型。

3.1.15 医学警示 （Medical Alert）

患者在就医、急诊或抢救时需要特别提醒医生注意的信息，包括疾病史、体内装置、药物过敏史、对某些物质的不耐受史等。

3.2 缩略语

以下缩略语和符号表示适用于本规范。

表 3-1 缩略语和符号列表

缩略语	中文名	英文名
‘0’-‘9’ ‘A’-‘F’	十六进制数字	
AID	应用标识符	Application Identifier
an	字母数字型	Alphanumeric
ans	特殊字母数字型	Alphanumeric Special
b	二进制	Binary
CBC	密码块链接	Cipher Block Chaining
CLA	命令报文的类别字节	Class Byte of Command Message
cn	压缩数字	Compressed Numeric
COS	芯片操作系统	Chip Operating System
CPU	中央处理器	Central Processing Unit
CVN	卡安全码	Card Verification Number
DDF	目录定义文件	Directory Definition File
DF	专用文件	Dedicated File
EF	基本文件	Elementary File
FCI	文件控制信息	File Control Information
FID	文件标识符	File Identifier
IC	集成电路	Integrated Circuit
IEC	国际电工委员会	International Electrotechnical Commission
INS	命令报文的指令字节	Instruction Byte of Command Message
ISO	国际标准化组织	International Organization for Standardization
M	必选型	Mandatory
MAC	报文鉴别代码	Message Authentication Code

MF	主控文件	Master File
O	可选型	Optional
PIX	专用应用标识符扩展码	Proprietary Application Identifier Extension
SAM	安全存取模块	Secure Access Module
PVC	聚氯乙烯	Polyvinyl Chloride
RID	已注册的应用提供者标识	Registered Application Provider Identifier
RS232	串行通信接口	
USB	通用串行总线	Universal Serial BUS
xx	任意值	

4 卡号编码规则

居民健康卡的卡号采用公民身份号码（GB 11643—1999）。

5 卡介质

5.1 卡介质选择

居民健康卡采用非接触式高安全型 CPU 卡，符合 ISO/IEC 14443 通讯协议，可写数据存储器容量不少于 32K 字节，为加密非挥发存储器。

5.2 卡体材料

卡体材料使用普通 PVC，推荐使用环保材料。

5.3 制卡要求

居民健康卡制造机构必须符合以下条件：

1．居民健康卡芯片以及卡片制造机构应具有国家 IC 卡注册中心分配的注册标识号和注册证书。

2.居民健康卡制造机构必须取得国家集成电路中心的 ICCR 注册证书和国家 IC 卡生产许可证。

3．居民健康卡芯片操作系统（COS）要通过中国国家信息安全认证中心的 EAL4+强制性安全认证。

4．居民健康卡须经卫生部信息化领导小组办公室指定的相关检测机构进行符合性检测，取得 COS 检测合格证书。居民健康卡 COS 检测规范另行制定。

5．居民健康卡增加金融应用的应符合中国人民银行相关要求。

6 卡面

6.1 卡片外形规格

居民健康卡卡片外形为圆角矩形，外形和尺寸分别见表 6-1 和图 6-1。

表 6-1 卡片尺寸

参数	尺寸	公差
卡片宽度 L	85.60mm	85.47 mm -85.72 mm
卡片高度 W	53.98mm	53.92 mm -54.03 mm
卡片厚度 T	0.81mm	±0.03mm
倒角半径 R	3.18mm	±0.30mm

注：倒角是在圆柱型工件的末端加工出一个具有角度的边。

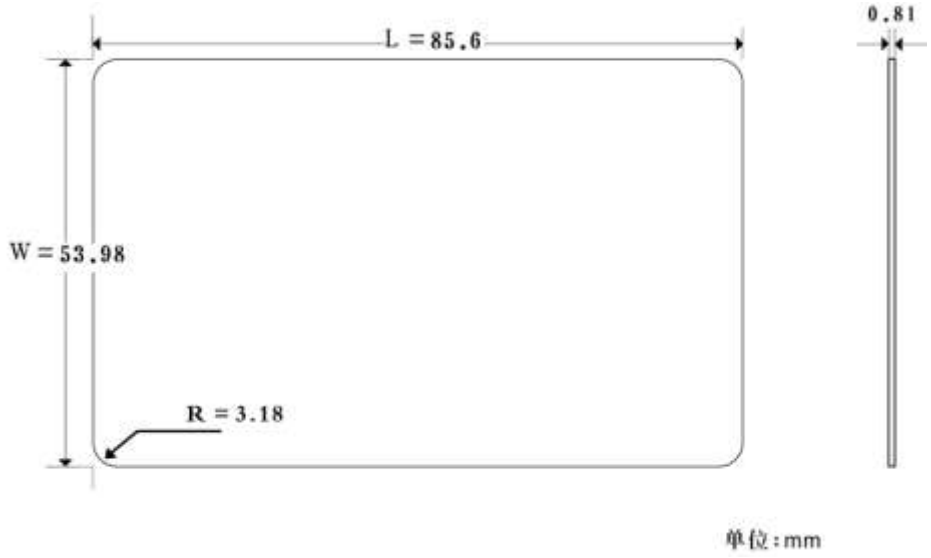


图 6-1 卡片尺寸

6.2 芯片位置

居民健康卡芯片放置位置不能影响卡片使用。

6.3 印刷要求

6.3.1 卡片正面样式

卡片正面应包括以下要素：持卡人照片、持卡人姓名、性别、民族、居民健康卡号、居民健康卡号条形码、发卡机构名称、发卡机构公章。

卡片正面参考布局及参数见图 6-2 和表 6-2。

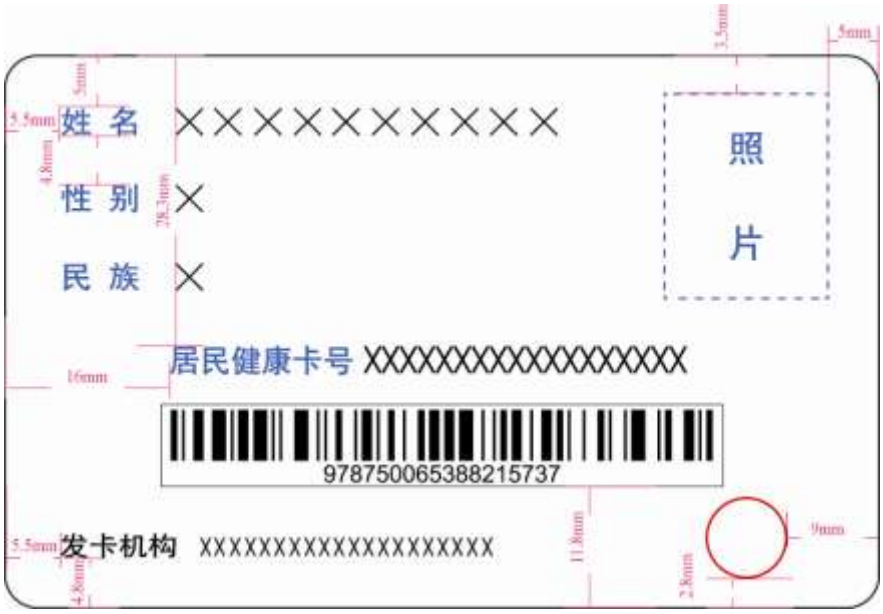


图 6-2 卡片正面布局

表 6-2 卡片正面布局参数

参数	规格及要求	公差
发卡机构标识区		
“发卡机构”字体	黑体 8pt	/
“发卡机构”左边沿到卡的左边沿的距离	5.50mm	±0.30mm
“发卡机构”下边沿到卡的下边沿的距离	4.80mm	±0.30mm
发卡机构公章直径	8.00mm	/
发卡机构公章右边沿到卡的右边沿的距离	9.00mm	±0.30mm
发卡机构公章下边沿到卡的下边沿的距离	2.80mm	±0.30mm
红色公章色值	C0 、 M100 、 Y100、K0	/
持卡人照片信息		
“照片”的宽度	16.00mm	±0.10mm
“照片”的高度	20.00mm	±0.10mm
“照片”右边沿到卡的右边沿的距离	5.00mm	±0.30mm
“照片”上边沿到卡的上边沿的距离	3.50mm	±0.30mm
持卡人个人信息		
“姓名” 、“性别”、“民族”字体	黑体 8.5 pt	/
“姓名”左边沿到卡的左边沿的距离	5.50mm	±0.30mm

“姓名”上边沿到卡的上边沿的距离	5.00mm	±0.30mm
“姓名”、“性别”、“民族”三行的行间距	4.80mm	/
“居民健康卡号”字体	黑体 8.5 pt	/
“居民健康卡号”左边沿到卡的左边沿的距离	16.00mm	±0.30mm
“居民健康卡号”上边沿到卡的上边沿的距离	28.30mm	±0.30mm
蓝色字体色值	C85 、 M60 、 Y0\K0	/
可变信息部分		
“姓名、性别、民族”填写值字体	黑体 8.5 pt	/
“姓名、性别、民族”字色值	K100	/
“居民健康卡号”填写值字体	黑体 8.5 pt	/
“居民健康卡号”字色值	K100	/
条形码代码区		
条形码宽度	55.00mm	/
条形码高度	8.00mm	/
条形码	水平居中	/
条形码下边沿到卡的下边沿的距离	11.80mm	±0.30mm

居民健康卡使用照片基本要求：一寸近期正面免冠彩色头像，不着制式服装，常戴眼镜的居民应配戴眼镜，要求人像清晰、层次丰富，神态自然，无明显畸变，照片背景为白色，无边框。

6.3.2 卡片背面样式

卡片背面应包括以下要素：居民健康卡标识图案、卡名（中华人民共和国居民健康卡）。卡片背面布局及参数见图 6-3 和表 6-3。

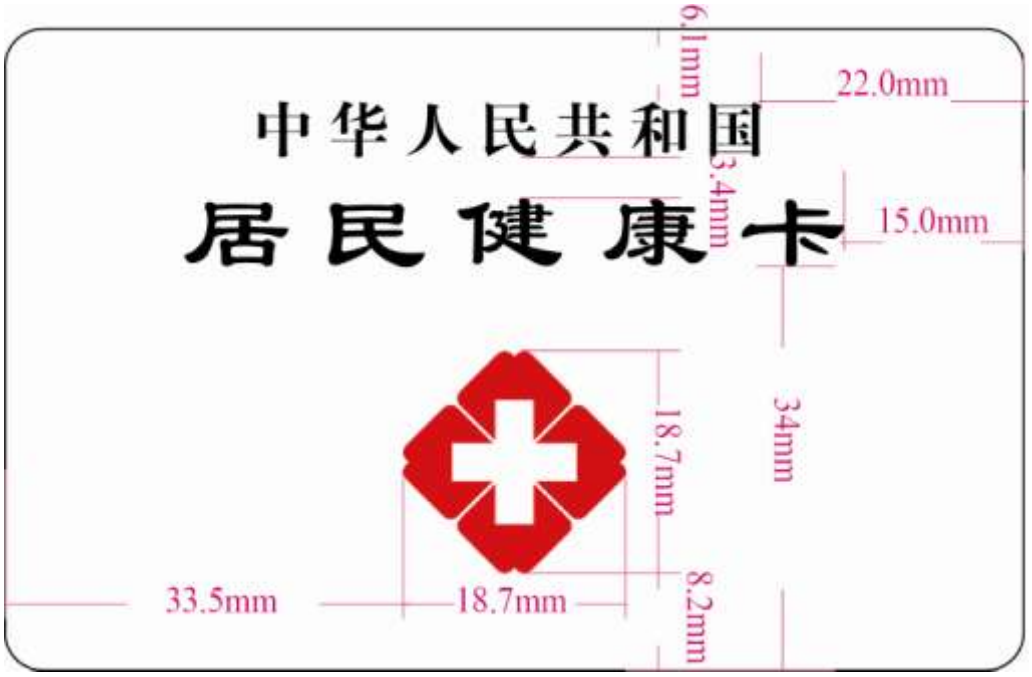


图 6-3 卡片背面布局

表 6-3 卡片背面布局参数

参数	规格及要求	公差
居民健康卡标识图案		
居民健康卡标识图案		
表示图案宽度	18.70mm	/
标识图案高度	18.70mm	/
标识图案左边沿到卡的左边沿的距离	33.50mm	±0.30 mm
标识图案下边沿到卡的下边沿的距离	8.2mm	±0.30 mm
红色部分色号	C0、M100、Y100、K0	/
中华人民共和国居民健康卡		
“中华人民共和国”字样	宋体 15pt 加粗	/
右边沿到卡的右边沿的距离	22.00mm	±0.30 mm
上边沿到卡的上边沿的距离	6.10mm	±0.30 mm
“居民健康卡”字样	隶书 26.5pt	/
右边沿到卡的右边沿的距离	15.00mm	±0.30 mm
下边沿到卡的下边沿的距离	34.00mm	±0.30 mm
两行间距	3.40mm	/

6.3.3 卡面颜色标准及图案

色度差、公差见表 6-4。

表 6-4 卡片颜色标准

	居民健康卡标识图案红	公章红	字体颜色
允许公差Δ E*	<=5.00	<=5.00	<=5.00

注：Δ E*表示色差。

图案（矢量文件）及颜色由卫生部信息化工作领导小组办公室统一提供。

具有金融功能的居民健康卡的卡面规范卫生部将于中国人民银行联合制定，另行发布。

7 终端接口要求

终端应能够对居民健康卡进行操作。

终端可通过 USB 或 RS232 等接口与计算机通信。RS232 通讯速率默认值为 9600bps，8 个数据位，1 个起始位，1 个停止位，无校验位。若通过 USB 接口与计算机交换数据，可采用四种传输方式之一：等时传输方式、中断传输方式、批处理方式、控制传输方式。

终端射频接口应符合 ISO/IEC 14443 通讯协议。

终端应采用醒目的方式标示读卡区域，保证能方便地将卡放置到操作区域。

终端应带有至少一个安全存取模块（SAM）卡座，用以支持居民健康卡应用的安全认证功能。

终端须经卫生部信息化领导小组办公室指定的相关检测机构进行符合性检测，取得终端检测合格证书。

终端技术规范及检测指南将另行制定。

8 卡数据标准

8.1 数据框架

居民健康卡数据分为身份识别数据、卡识别数据、基础健康数据、管理数据四大类，框架见图 8-1。

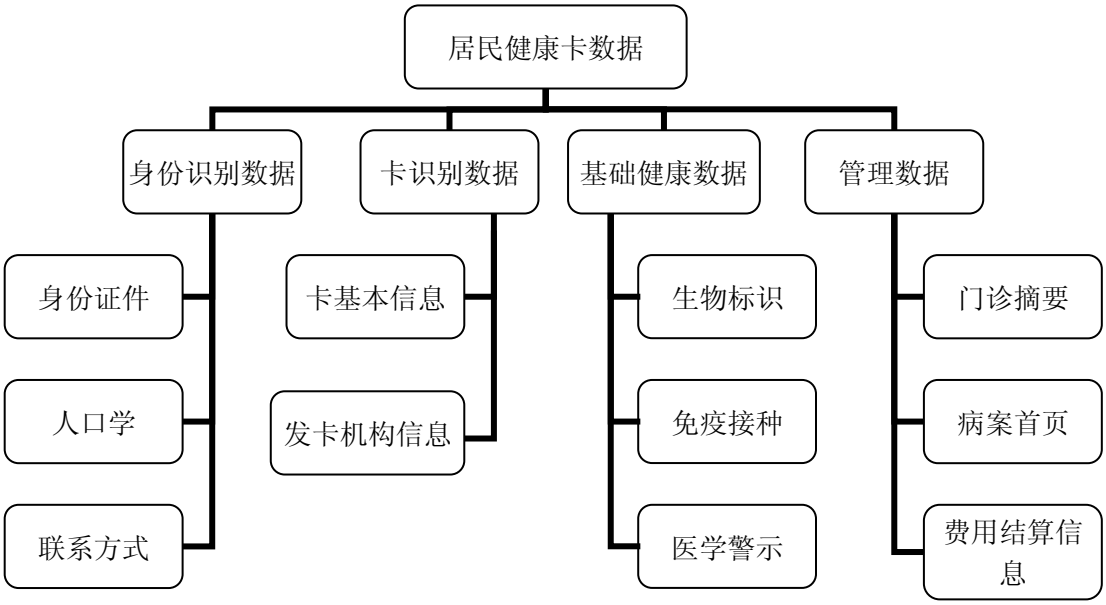


图 8-1 居民健康卡数据框架示意图

8.1.1 身份识别数据

身份识别数据指持卡人的唯一的身份标识，包括身份证件、人口学、联系方式等。

8.1.2 卡识别数据

卡识别数据指与居民健康卡基本数据及发卡机构有关数据，包括卡基本信息、发卡机构信息等。

8.1.3 基础健康数据

基础健康数据指与持卡人急诊、急救相关的静态数据，包括生物标识、免疫接种、医学警示等。

8.1.4 管理数据

管理数据指与持卡人基本诊疗活动有关的动态数据，包括门诊摘要、病案首页、费用结算信息等。其中，费用结算信息填写新农合住院结算费用。

8.2 数据标准

居民健康卡数据标准列表见表 8-1。居民健康卡基础数据采集表见附录 1。

表 8-1　居民健康卡数据标准列表

类别	子类别	数据项名称	隐私保护	表示格式	重复次数	必选项
身份识别数据	身份证件	居民身份证号码	一般	AN..18	1..1	M
		证件类别	限制	N1	0..1	O
		证件号码	限制	AN..18	0..1	O
		健康档案编号	限制	AN..17	1..1	O
		新农合证（卡）号	限制	N18	1..1	O
	人口学信息	姓名	一般	A..30	1..1	M
		出生日期	一般	D8	1..1	M
		性别	一般	N1	1..1	M
		民族代码	一般	N2	1..1	M
		婚姻状况代码	一般	AN1	1..1	M
		文化程度代码	一般	N2	1..1	M
		职业代码	一般	AN..3	1..1	M
		地址类别	一般	N1	1..2	M
		地址-省	一般	A..20	1..2	M
		地址-市	一般	A..20	1..2	M
		地址-县（区）	一般	A..20	1..2	M
		地址-乡镇（街道）	一般	A..20	1..2	M
		地址-村（居委会）	一般	A..20	1..2	M
		医疗费用支付方式	一般	N1	1..3	M
	联系方式	本人电话	一般	N..20	0..2	O
		联系人姓名	一般	A..30	1..3	M
		联系人关系	一般	N2	1..3	M
		联系人电话	一般	N..20	1..3	M

卡识别数据	卡基本信息	卡号	系统管理	AN18	1..1	M
		安全码	系统管理	N3	1..1	M
		芯片序列号	系统管理	AN..10	1..1	M
		卡的类别	系统管理	N1	1..1	M
		规范版本	系统管理	AN..4	1..1	M
	发卡机构信息	发卡机构名称	系统管理	AN..30	1..1	M
		发卡机构代码	系统管理	N22	1..1	M
		发卡时间	系统管理	D8	1..1	M
		卡有效期	系统管理	D8	1..1	M
基础健康数据	生物表示	ABO 血型代码	一般	N1	1..1	M
		RH 血型代码	一般	N1	1..1	M
	免疫接种	免疫接种名称	一般	AN..20	0..10	O
		免疫接种时间	一般	D8	0..10	O
	医学警示	哮喘标志	一般	T/F	1..1	M
		心脏病标志	一般	T/F	1..1	M
		心脑血管病标志	一般	T/F	1..1	M
		癫痫病标志	一般	T/F	1..1	M
		精神病标志	限制	T/F	1..1	M
		凝血紊乱标志	一般	T/F	1..1	M
		糖尿病标志	一般	T/F	1..1	M
		青光眼标志	一般	T/F	1..1	M
		透析标志	一般	T/F	1..1	M
		器官移植标志	一般	T/F	1..1	M
		器官缺失标志	一般	T/F	1..1	M
		可装卸的义肢标志	一般	T/F	1..1	M
		心脏起搏器标志	一般	T/F	1.1	M
		过敏物质名称	一般	AN..20	0..3	O
		过敏反应	一般	AN..100	0..3	O
		其他医学警示名称	一般	AN..40	0..1	O
管理数据	门诊摘要	就诊机构名称	系统管理	AN..70	0..1	O
		就诊机构组织机构代码	系统管理	AN10	0..1	O
		就诊日期时间	系统管理	DT15	0..1	O
		门诊号	系统管理	AN..18	0..1	O

	就医科室名称	系统管理	AN..50	0..1	O
	医疗付款方式	系统管理	N..2	0..1	O
	症状名称	系统管理	A..50	0..5	O
	症状代码	系统管理	AN..5	0..5	O
	诊断日期	系统管理	D8	0..5	O
	门诊诊断名称	系统管理	A..50	0..5	O
	门诊诊断代码	系统管理	AN7	0..5	O
	发病日期时间	系统管理	DT15	0..5	O
	症状持续时间	系统管理	N..3	0..5	O
	检查/检验项目名称	系统管理	AN..80	0..10	O
	检查/检验结果代码	系统管理	N1	0..10	O
	检查/检验定量结果	系统管理	N..10	0..10	O
	检查/检验计量单位	系统管理	A..20	0..10	O
	检查/检验项目代码	系统管理	AN..20	0..10	O
	药物名称	系统管理	AN..50	0..5	O
	药物剂型代码	系统管理	N2	0..5	O
	用药天数	系统管理	N..5	0..5	O
	药物使用频率	系统管理	A..20	0..5	O
	药物使用剂量单位	系统管理	AN..6	0..5	O
	药物使用次剂量	系统管理	N..5,2	0..5	O
	药物使用总剂量	系统管理	N..12,2	0..5	O
	药物使用途径代码	系统管理	N..3	0..5	O
	手术/操作名称	系统管理	AN..80	0..3	O
	手术/操作代码	系统管理	AN..5	0..3	O
	手术/操作日期	系统管理	D8	0..3	O
	门诊费用分类名称	系统管理	A..20	0..10	O
	门诊费用分类代码	系统管理	N2	0..10	O
	门诊费用金额（元/人民币）	系统管理	N..8,2	0..10	O
病案首页	住院机构名称	系统管理	AN..70	0..1	O
	住院机构组织机构代码	系统管理	AN10	0..1	O
	入院日期	系统管理	D8	0..1	O
	出院日期	系统管理	D8	0..1	O

	住院患者住院次数	系统管理	N..3	0..1	O
	病案号	系统管理	AN..18	0..1	O
	住院患者入院科室名称	系统管理	AN..50	0..1	O
	住院患者入院病情	系统管理	N1	0..1	O
	住院患者医院感染名称	系统管理	AN..50	0..1	O
	住院患者损伤和中毒外部原因	系统管理	AN..7	0..1	O
	住院患者血清学检查项目代码	系统管理	N1	0..3	O
	住院患者血清学检查结果代码	系统管理	N1	0..3	O
	疾病诊断名称	系统管理	A..50	0..3	O
	疾病诊断代码	系统管理	AN7	0..3	O
	确诊日期	系统管理	D8	0..3	O
	住院患者诊断符合情况-详细描述	系统管理	A…20	0..3	O
	住院患者诊断符合情况-代码	系统管理	N1	0..3	O
	住院患者疾病诊断类型-详细描述	系统管理	A…20	0..3	O
	住院患者疾病诊断类型-代码	系统管理	N..2	0..3	O
	住院患者治疗结果代码	系统管理	N1	0..3	O
	手术/操作-名称	系统管理	AN..80	0..3	O
	手术/操作-代码	系统管理	AN..5	0..3	O
	手术/操作-日期	系统管理	D8	0..3	O
	麻醉-方法	系统管理	A..50	0..3	O
	麻醉-方法代码	系统管理	N..2	0..3	O
	手术切口愈合等级代码	系统管理	N1	0..3	O
	住院期间输血品种代码	系统管理	N1	0..4	O
	住院期间输血量	系统管理	N..4	0..4	O
	住院患者输血量计量单位	系统管理	A..10	0..4	O
	住院患者抢救次数	系统管理	N..3	0..1	O
	住院患者抢救成功次数	系统管理	N..3	0..1	O
	住院患者出院科室名称	系统管理	AN..50	0..1	O
	住院患者住院天数	系统管理	N..5	0..1	O

	住院患者尸检标志	系统管理	T/F	0..1	O
	住院患者随诊标志	系统管理	T/F	0..1	O
	住院费用-分类	系统管理	A..20	0..20	O
	住院费用-分类代码	系统管理	AN..2	0..20	O
	住院费用-金额（元/人民币）	系统管理	N..10,2	0..20	O
	住院费用-医疗付款方式代码	系统管理	N1	0..1	O
费用结算信息	入院日期	结算费用	D8	0..1	O
	出院日期	结算费用	D8	0..1	O
	病案号	结算费用	AN..18	0..1	O
	住院总费用（元/人民币）	结算费用	N..10,2	0..1	O
	床位费（元/人民币）	结算费用	N..10,2	0..1	O
	住院护理费（元/人民币）	结算费用	N..10,2	0..1	O
	住院西药费（元/人民币）	结算费用	N..10,2	0..1	O
	住院中药费（元/人民币）	结算费用	N..10,2	0..1	O
	住院化验费（元/人民币）	结算费用	N..10,2	0..1	O
	住院诊疗费（元/人民币）	结算费用	N..10,2	0..1	O
	住院手术费（元/人民币）	结算费用	N..10,2	0..1	O
	住院检查费（元/人民币）	结算费用	N..10,2	0..1	O
	其他住院费用（元/人民币）	结算费用	N..10,2	0..1	O

注：表 8-1 中第二列“数据项名称”中的数据项“安全码”为发卡机构在发行居民健康卡时必须提供的卡安全码（CVN）。在换发新卡时必须更改安全码。

表 8-1 中关于居民健康卡数据标准的 6 个数据描述项目分别为：

类别：分身份识别数据、卡识别数据、基础健康数据、管理数据四大类。

子类别：是上述四大类的子分类：身份证件、人口学、联系方式、卡基本信息、发卡机构信息、生物标识、免疫接种、医学警示、门诊摘要、病案首页、费用结算信息。

数据项名称：居民健康卡中记录的数据内容。

隐私保护：保护持卡人的隐私，限定居民健康卡数据内容的使用范围，分 4 个级别，即一般、限制、系统管理、结算费用。

表示格式：“表示格式”中“A”为字母字符，“N”为数字字符，“AN”为字母和

数字混合型字符，“D8”为采用 YYYYMMDD 的日期格式，带“..”的为可变字符，“..”后的数字表示最大字符数，“，”后为小数点位数，“T/F”为布尔型，“T”表示真，“F”表示假。

重复次数：指相同含义数据在居民健康卡中记录的次数，0..1 表示最多记录 1 次，0..2 表示最多记录 2 次，1..1 表示只能记录 1 次，1..2 表示最少记录 1 次、最多记录 2 次，以此类推。

必选项：M 表示该数据在居民健康卡中必须记录，O 表示该数据在居民健康卡中可以没有记录。

8.3 数据格式

居民健康卡数据格式见表 8-2：

表 8-2 居民健康卡数据格式列表

标志	数据项	类型	长度	所属文件	备注
01	卡的类别	ans	01	MF\DDF1\EF05	
02	规范版本	ans	04		
03	发卡机构名称	ans	30		
04	发卡机构代码	cn	11		
05	发卡机构证书	b	180		
06	发卡时间	cn	04		
07	卡有效期	cn	04		
08	卡号	ans	18		
09	安全码	ans	03		
10	芯片序列号	ans	10		
11	姓名	ans	30	MF\DDF1\EF06	
12	性别	b	01		
13	民族代码	cn	01		
14	出生日期	cn	04		
15	居民身份证号码	ans	18		
16	本人电话 1	ans	20		
17	本人电话 2	ans	20		

18	医疗费用支付方式	cn	01		
19	医疗费用支付方式	cn	01		
20	医疗费用支付方式	cn	01		
21	地址类别 1	cn	01	MF\DDF1\DF01\EF05	
22	地址 1	ans	100		
23	地址类别 2	cn	01		
24	地址 2	ans	100		
25	联系人姓名 1	ans	30	MF\DDF1\DF01\EF06	
26	联系人关系 1	cn	01		
27	联系人电话 1	ans	20		
28	联系人姓名 2	ans	30		
29	联系人关系 2	cn	01		
30	联系人电话 2	ans	20		
31	联系人姓名 3	ans	30		
32	联系人关系 3	cn	01		
33	联系人电话 3	ans	20		
34	文化程度代码	cn	01	MF\DDF1\DF01\EF07	
35	婚姻状况代码	cn	01		
36	职业代码	ans	03		
37	证件类别	cn	01	MF\DDF1\DF01\EF08	
38	证件号码	ans	18		
39	健康档案编号	ans	17		
40	新农合证（卡）号	ans	18		
41	ABO 血型代码	b	01	MF\DDF1\DF02\EF05	
42	RH 血型代码	cn	01		
43	哮喘标志	b	01		
44	心脏病标志	b	01		
45	心脑血管病标志	b	01		
46	癫痫病标志	b	01		
47	凝血紊乱标志	b	01		

48	糖尿病标志	b	01		
49	青光眼标志	b	01		
50	透析标志	b	01		
51	器官移植标志	b	01		
52	器官缺失标志	b	01		
53	可装卸的义肢标志	b	01		
54	心脏起搏器标志	b	01		
55	其他医学警示名称	ans	40		
56	精神病标志	b	01	MF\DDF1\DF02\EF06	
	过敏物质名称	ans	20	MF\DDF1\DF02\EF07	循环记录文件（3 条记录）
	过敏反应	ans	100		
	免疫接种名称	ans	20	MF\DDF1\DF02\EF08	循环记录文件（10 条记录）
	免疫接种时间	cn	04		
	住院记录有效标志	b	01	MF\DDF1\DF03\EF05	FF: 记录无效 00: 记录有效 循环记录文件（5 条记录）
	门诊记录有效标志	b	01	MF\DDF1\DF03\EF06	FF: 记录无效 00: 记录有效 循环记录文件（5 条记录）
	住院机构名称	ans	70	MF\DDF1\DF03\E	
	住院机构组织机构代码	ans	10		

	入院日期	cn	04	E01 … MF\DDF 1\DF03\E E05	
	住院患者住院次数	cn	02		
	病案号	ans	18		
	住院患者入院科室名称	ans	50		
	住院患者入院病情	cn	01		
	住院患者医院感染名称	ans	50		
	住院患者损伤和中毒外部原因	ans	07		
	住院患者血清学检查项目代码 1	cn	01		
	住院患者血清学检查结果代码 1	cn	01		
	疾病诊断名称 1	ans	50		
	疾病诊断代码 1	ans	07		
	确诊日期 1	cn	04		
	住院患者诊断符合情况-详细描述 1	ans	20		
	住院患者诊断符合情况-代码 1	cn	01		
	住院患者疾病诊断类型-详细描述 1	ans	20		
	住院患者疾病诊断类型-代码 1	cn	01		
	住院患者治疗结果代码 1	cn	01		
	手术/操作-名称 1	ans	80		
	手术/操作-代码 1	ans	5		
	手术/操作-日期 1	cn	04		
	麻醉-方法 1	ans	50		
	麻醉-方法代码 1	cn	01		
	手术切口愈合等级代码 1	cn	01		
	住院患者血清学检查项目代码 2	cn	01		
	住院患者血清学检查结果代码 2	cn	01		
	疾病诊断名称 2	ans	50		
	疾病诊断代码 2	ans	07		
	确诊日期 2	cn	04		
	住院患者诊断符合情况-详细描述 2	ans	20		
	住院患者诊断符合情况-代码 2	cn	01		

	住院患者疾病诊断类型-详细描述 2	ans	20		
	住院患者疾病诊断类型-代码 2	cn	01		
	住院患者治疗结果代码 2	cn	01		
	手术/操作-名称 2	ans	80		
	手术/操作-代码 2	ans	5		
	手术/操作-日期 2	cn	04		
	麻醉-方法 2	ans	50		
	麻醉-方法代码 2	cn	01		
	手术切口愈合等级代码 2	cn	01		
	住院患者血清学检查项目代码 3	cn	01		
	住院患者血清学检查结果代码 3	cn	01		
	疾病诊断名称 3	ans	50		
	疾病诊断代码 3	ans	07		
	确诊日期 3	cn	04		
	住院患者诊断符合情况-详细描述 3	ans	20		
	住院患者诊断符合情况-代码 3	cn	01		
	住院患者疾病诊断类型-详细描述 3	ans	20		
	住院患者疾病诊断类型-代码 3	cn	01		
	住院患者治疗结果代码 3	cn	01		
	手术/操作-名称 3	ans	80		
	手术/操作-代码 3	ans	5		
	手术/操作-日期 3	cn	04		
	麻醉-方法 3	ans	50		
	麻醉-方法代码 3	cn	01		
	手术切口愈合等级代码 3	cn	01		
	住院期间输血品种代码 1	cn	01		
	住院期间输血量 1	cn	02		
	住院患者输血量计量单位 1	ans	10		
	住院期间输血品种代码 2	cn	01		
	住院期间输血量 2	cn	02		

	住院患者输血量计量单位 2	ans	10		
	住院期间输血品种代码 3	cn	01		
	住院期间输血量 3	cn	02		
	住院患者输血量计量单位 3	ans	10		
	住院期间输血品种代码 4	cn	01		
	住院期间输血量 4	cn	02		
	住院患者输血量计量单位 4	ans	10		
	住院患者抢救次数	cn	02		
	住院患者抢救成功次数	cn	02		
	出院日期	cn	04		
	住院患者出院科室名称	ans	50		
	住院患者住院天数	cn	03		
	住院患者尸检标志	b	01		
	住院患者随诊标志	b	01		
	住院费用-医疗付款方式代码	cn	01		
	住院费用-分类 1	ans	20		
	住院费用-分类代码 1	ans	01		
	住院费用-金额 1	cn	05		
	住院费用-分类 2	ans	20		
	住院费用-分类代码 2	ans	01		
	住院费用-金额 2	cn	05		
	住院费用-分类 3	ans	20		
	住院费用-分类代码 3	ans	01		
	住院费用-金额 3	cn	05		
	住院费用-分类 4	ans	20		
	住院费用-分类代码 4	ans	01		
	住院费用-金额 4	cn	05		
	住院费用-分类 5	ans	20		
	住院费用-分类代码 5	ans	01		
	住院费用-金额 5	cn	05		

	住院费用-分类 6	ans	20		
	住院费用-分类代码 6	ans	01		
	住院费用-金额 6	cn	05		
	住院费用-分类 7	ans	20		
	住院费用-分类代码 7	ans	01		
	住院费用-金额 7	cn	05		
	住院费用-分类 8	ans	20		
	住院费用-分类代码 8	ans	01		
	住院费用-金额 8	cn	05		
	住院费用-分类 9	ans	20		
	住院费用-分类代码 9	ans	01		
	住院费用-金额 9	cn	05		
	住院费用-分类 10	ans	20		
	住院费用-分类代码 10	ans	01		
	住院费用-金额 10	cn	05		
	住院费用-分类 11	ans	20		
	住院费用-分类代码 11	ans	01		
	住院费用-金额 11	cn	05		
	住院费用-分类 12	ans	20		
	住院费用-分类代码 12	ans	01		
	住院费用-金额 12	cn	05		
	住院费用-分类 13	ans	20		
	住院费用-分类代码 13	ans	01		
	住院费用-金额 13	cn	05		
	住院费用-分类 14	ans	20		
	住院费用-分类代码 14	ans	01		
	住院费用-金额 14	cn	05		
	住院费用-分类 15	ans	20		
	住院费用-分类代码 15	ans	01		
	住院费用-金额 15	cn	05		

	住院费用-分类 16	ans	20		
	住院费用-分类代码 16	ans	01		
	住院费用-金额 16	cn	05		
	住院费用-分类 17	ans	20		
	住院费用-分类代码 17	ans	01		
	住院费用-金额 17	cn	05		
	住院费用-分类 18	ans	20		
	住院费用-分类代码 18	ans	01		
	住院费用-金额 18	cn	05		
	住院费用-分类 19	ans	20		
	住院费用-分类代码 19	ans	01		
	住院费用-金额 19	cn	05		
	住院费用-分类 20	ans	20		
	住院费用-分类代码 20	ans	01		
	住院费用-金额 20	cn	05		
	住院总费用	cn	05		
	床位费	cn	05		
	住院护理费	cn	05		
	住院西药费	cn	05		
	住院中药费	cn	05		
	住院化验费	cn	05		
	住院诊疗费	cn	05		
	住院手术费	cn	05		
	住院检查费	cn	05		
	其他住院费用	cn	05		
	交易信息签名	b	32		
	SAM 卡证书	b	190		
	就诊机构名称	ans	70	MF\DDF1\DF03\ED01	
	就诊机构组织机构代码	ans	10		
	就诊日期时间	cn	07		

	门诊号	ans	18	… MF\DDF 1\DF01\E D05	
	就医科室名称	ans	50		
	医疗付款方式	cn	01		
	症状名称 1	ans	50		
	症状代码 1	ans	05		
	诊断日期 1	cn	04		
	门诊诊断名称 1	ans	50		
	门诊诊断代码 1	ans	07		
	发病日期时间 1	cn	07		
	症状持续时间 1	cn	02		
	症状名称 2	ans	50		
	症状代码 2	ans	05		
	诊断日期 2	cn	04		
	门诊诊断名称 2	ans	50		
	门诊诊断代码 2	ans	07		
	发病日期时间 2	cn	07		
	症状持续时间 2	cn	02		
	症状名称 3	ans	50		
	症状代码 3	ans	05		
	诊断日期 3	cn	04		
	门诊诊断名称 3	ans	50		
	门诊诊断代码 3	ans	07		
	发病日期时间 3	cn	07		
	症状持续时间 3	cn	02		
	症状名称 4	ans	50		
	症状代码 4	ans	05		
	诊断日期 4	cn	04		
	门诊诊断名称 4	ans	50		
	门诊诊断代码 4	ans	07		
	发病日期时间 4	cn	07		

	症状持续时间 4	cn	02		
	症状名称 5	ans	50		
	症状代码 5	ans	05		
	诊断日期 5	cn	04		
	门诊诊断名称 5	ans	50		
	门诊诊断代码 5	ans	07		
	发病日期时间 5	cn	07		
	症状持续时间 5	cn	02		
	检查/检验项目名称 1	ans	80		
	检查/检验结果代码 1	cn	01		
	检查/检验定量结果 1	cn	05		
	检查/检验计量单位 1	ans	20		
	检查/检验项目代码 1	ans	20		
	检查/检验项目名称 2	ans	80		
	检查/检验结果代码 2	cn	01		
	检查/检验定量结果 2	cn	05		
	检查/检验计量单位 2	ans	20		
	检查/检验项目代码 2	ans	20		
	检查/检验项目名称 3	ans	80		
	检查/检验结果代码 3	cn	01		
	检查/检验定量结果 3	cn	05		
	检查/检验计量单位 3	ans	20		
	检查/检验项目代码 3	ans	20		
	检查/检验项目名称 4	ans	80		
	检查/检验结果代码 4	cn	01		
	检查/检验定量结果 4	cn	05		
	检查/检验计量单位 4	ans	20		
	检查/检验项目代码 4	ans	20		
	检查/检验项目名称 5	ans	80		
	检查/检验结果代码 5	cn	01		

	检查/检验定量结果 5	cn	05		
	检查/检验计量单位 5	ans	20		
	检查/检验项目代码 5	ans	20		
	检查/检验项目名称 6	ans	80		
	检查/检验结果代码 6	cn	01		
	检查/检验定量结果 6	cn	05		
	检查/检验计量单位 6	ans	20		
	检查/检验项目代码 6	ans	20		
	检查/检验项目名称 7	ans	80		
	检查/检验结果代码 7	cn	01		
	检查/检验定量结果 7	cn	05		
	检查/检验计量单位 7	ans	20		
	检查/检验项目代码 7	ans	20		
	检查/检验项目名称 8	ans	80		
	检查/检验结果代码 8	cn	01		
	检查/检验定量结果 8	cn	05		
	检查/检验计量单位 8	ans	20		
	检查/检验项目代码 8	ans	20		
	检查/检验项目名称 9	ans	80		
	检查/检验结果代码 9	cn	01		
	检查/检验定量结果 9	cn	05		
	检查/检验计量单位 9	ans	20		
	检查/检验项目代码 9	ans	20		
	检查/检验项目名称 10	ans	80		
	检查/检验结果代码 10	cn	01		
	检查/检验定量结果 10	cn	05		
	检查/检验计量单位 10	ans	20		
	检查/检验项目代码 10	ans	20		
	药物名称 1	ans	50		
	药物剂型代码 1	cn	01		

	用药天数 1	cn	03		
	药物使用频率 1	ans	20		
	药物使用剂量单位 1	ans	06		
	药物使用次剂量 1	cn	03		
	药物使用总剂量 1	cn	06		
	药物使用途径代码 1	cn	02		
	药物名称 2	ans	50		
	药物剂型代码 2	cn	01		
	用药天数 2	cn	03		
	药物使用频率 2	ans	20		
	药物使用剂量单位 2	ans	06		
	药物使用次剂量 2	cn	03		
	药物使用总剂量 2	cn	06		
	药物使用途径代码 2	cn	02		
	药物名称 3	ans	50		
	药物剂型代码 3	cn	01		
	用药天数 3	cn	03		
	药物使用频率 3	ans	20		
	药物使用剂量单位 3	ans	06		
	药物使用次剂量 3	cn	03		
	药物使用总剂量 3	cn	06		
	药物使用途径代码 3	cn	02		
	药物名称 4	ans	50		
	药物剂型代码 4	cn	01		
	用药天数 4	cn	03		
	药物使用频率 4	ans	20		
	药物使用剂量单位 4	ans	06		
	药物使用次剂量 4	cn	03		
	药物使用总剂量 4	cn	06		
	药物使用途径代码 4	cn	02		

	药物名称 5	ans	50		
	药物剂型代码 5	cn	01		
	用药天数 5	cn	03		
	药物使用频率 5	ans	20		
	药物使用剂量单位 5	ans	06		
	药物使用次剂量 5	cn	03		
	药物使用总剂量 5	cn	06		
	药物使用途径代码 5	cn	02		
	手术/操作名称 1	ans	80		
	手术/操作代码 1	ans	5		
	手术/操作日期 1	cn	04		
	手术/操作名称 2	ans	80		
	手术/操作代码 2	ans	5		
	手术/操作日期 2	cn	04		
	手术/操作名称 3	ans	80		
	手术/操作代码 3	ans	5		
	手术/操作日期 3	cn	04		
	门诊费用分类名称 1	ans	20		
	门诊费用分类代码 1	cn	01		
	门诊费用金额 1	cn	04		
	门诊费用分类名称 2	ans	20		
	门诊费用分类代码 2	cn	01		
	门诊费用金额 2	cn	04		
	门诊费用分类名称 3	ans	20		
	门诊费用分类代码 3	cn	01		
	门诊费用金额 3	cn	04		
	门诊费用分类名称 4	ans	20		
	门诊费用分类代码 4	cn	01		
	门诊费用金额 4	cn	04		
	门诊费用分类名称 5	ans	20		

	门诊费用分类代码 5	cn	01		
	门诊费用金额 5	cn	04		
	门诊费用分类名称 6	ans	20		
	门诊费用分类代码 6	cn	01		
	门诊费用金额 6	cn	04		
	门诊费用分类名称 7	ans	20		
	门诊费用分类代码 7	cn	01		
	门诊费用金额 7	cn	04		
	门诊费用分类名称 8	ans	20		
	门诊费用分类代码 8	cn	01		
	门诊费用金额 8	cn	04		
	门诊费用分类名称 9	ans	20		
	门诊费用分类代码 9	cn	01		
	门诊费用金额 9	cn	04		
	门诊费用分类名称 10	ans	20		
	门诊费用分类代码 10	cn	01		
	门诊费用金额 10	cn	04		
	交易信息签名	b	32		
	SAM 卡证书	b	190		

注：“类型”项是指一种数据表示类型，其中“b”表示二进制数(Binary)，“cn”表示压缩数字(Compressed Numeric)，“ans”表示特殊字母数字型(Alphanumeric Special)。“长度”项采用的是十进制表示。

当为数据定义的长度超过数据实际长度，而位数没有占满时，补位规则如下：格式 cn 的数据元左对齐，右补 F；格式 ans 的数据元左对齐，右补 0。

9 数据安全

9.1 算法

居民健康卡采用国家密码管理局颁布的对称算法SM1算法，非对称算法SM2算法和杂凑算法SM3算法。

9.1.1 SM1 算法

SM1算法的分组长度为128比特，密钥长度为128比特。

9.1.2 SM2 算法

本规范中SM2算法用于证书的生成和验证、签名数据生成和验证。

本规范使用基于256位Fp（素数域）上的椭圆曲线参数。涉及到的参数包括：

— 一个256位长的大素数p；

— 大整数a和b，定义曲线方程 $y^2=x^3+ax+b \bmod p$；

— 椭圆曲线的阶n，表示满足方程 $y^2=x^3+ax+b \bmod p$ 的点的数量，要求n为素数；

— 一个椭圆曲线上的点 $G=(G_x, G_y)$，满足方程 $G_y^2=G_x^3+aG_x+b \bmod p$，G被称为基点，通过基点可以生成椭圆曲线上的所有点。

SM2密钥对包括私钥 S_K 和公钥 P_K ：

— S_K 是一个小于n-1的正整数，使用随机数产生；

— $P_K=(x, y)$ 是椭圆曲线上的点，即满足方程 $y^2=x^3+ax+b \bmod p$，由于p的长度为32字节，因此 P_K 的长度为64字节。

SM2包含下面三种算法：

— 依赖于私钥 S_K 的签名函数 $Sign(S_K)[M]$，该函数输出两个32字节长度的数字r和s。

— 依赖于公钥 P_K 的验证函数 $Verify(P_K)[M, Sign(S_K)[M]]$，该函数输出True或False，表示验证正确或失败。

— 使用SM3哈希算法H[ ]，将任意长度的报文映射为一个32字节的哈希值。

9.1.3 SM3 算法

SM3 算法对于任意长度的报文输入，产生一个 32 字节的哈希值。

9.2 基本安全要求

9.2.1 共存应用

居民健康卡上每一个应用应该放在一个单独的 DF 中，亦即在应用之间应该设计一道“防火墙”以防止跨过应用进行非法访问。

9.2.2 密钥的独立性

用于一种特定功能（如读取数据）的加密/解密密钥不能被任何其他功能所使用，包括保存在居民健康卡中的密钥和用来产生、派生和传输这些密钥的密钥。

9.3 密钥和个人密码的存放

居民健康卡应该能够保证用于选定的加（解）密算法的非对称私钥或对称加密密钥在没有授权的情况下，不会被泄露出来。

如果使用个人密码，则应保证其在居民健康卡中的安全存放，且在任何情况下都不会被泄露。

9.4 安全报文传送

安全报文传送的目的是保证数据的可靠性、完整性和对发送方的认证。数据完整性和对发送方的认证通过使用 MAC 来实现。数据的可靠性通过对数据域的加密来得到保证。

9.4.1 安全报文传送格式

本规范中定义的安全报文传送格式应符合 GB/T 16649.4 的规定。当 CLA 字节的第二个半字节等于十六进制数字‘4’时，表明对发送方命令数据要采用安全报文传送。

9.4.2 报文完整性和验证

MAC 是使用命令的所有元素（包括命令头）产生的。一条命令的完整性，包括命令数据域（如果存在的话）中的数据元，通过安全报文传送得以保证。

9.4.2.1 MAC 的位置

MAC 是命令数据域中最后一个数据元。

9.4.2.2 MAC 的长度

本规范中，MAC 的长度规定为 4 个字节。

9.4.2.3 MAC 密钥的产生

在安全信息处理过程中用到的 MAC 过程密钥是按照 9.6 章节描述的过程密钥的产生过程产生的。应用维护密钥用于产生 MAC 过程密钥。

9.4.2.4 MAC 的计算

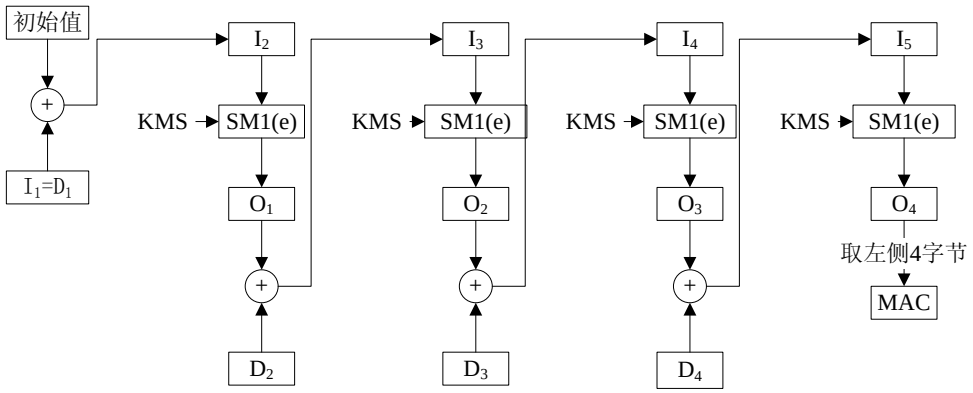
使用 SM1 算法 CBC 分组加密方式产生 MAC，步骤如下：

1) 取 16 字节的十六进制数‘00’作为初始变量。
2) 按照顺序将以下数据连接在一起形成数据块：

   ——（CLA，INS，P1，P2，Lc[1]）

   ——在命令的数据域中（如果存在）包含明文或加密的数据。（例：如果要更改个人密码，加密后的个人密码数据块放在命令数据域中传输）
3) 将该数据块分成 16 字节为单位的数据块，标号为 D1，D2，D3，D4 等。最后的数据块可能是 1-16 个字节。
4) 如果最后的数据块长度是 16 字节的话，则在其后加上十六进制数‘80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00’，转到步骤 5）；如果最后的数据块长度不足 16 字节，则在其后加上十六进制数‘80’，如果达到 16 字节长度，则转入步骤 5）；否则在其后加入十六进制数‘00’直到长度达到 16 字节。
5) 按图 9- 1 所述方法计算 MAC，过程密钥按照 9.6 章节描述的方式产生。
6) 最终得到的是从计算结果左侧取得 4 字节长度的 MAC。

[1] Lc 表示命令数据与后面 4 个字节 MAC 数据的长度。



I = 输入　　D = 数据块

SM1(e) = 数据加密算法（加密模式）　　KMS = MAC 过程密钥

+ = 异或运算　　O = 输出

图 9- 1MAC 计算

9.4.3 **数据可靠性**

为保证命令中明文数据的保密性，系统对数据进行加密。

9.4.3.1 数据加密密钥的计算

在安全报文处理过程中用到的数据加密过程密钥按照 9.6 章节描述的方式产生。应用维护密钥用于产生数据加密过程密钥。

9.4.3.2 被加密数据的结构

当命令中要求的明文数据需要加密时，它先要被格式化为以下形式的数据块：

——明文数据的长度，不包括填充字符（LD）

——明文数据

——填充字符

然后整个数据块使用数据加密技术进行加密。

9.4.3.3 数据加密计算

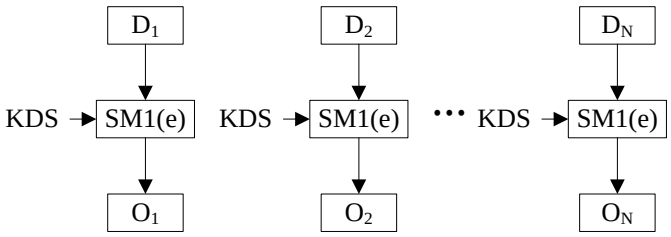
数据加密计算，如图 9-2，步骤如下：

1) 用 LD 表示明文数据的长度，在明文数据前加上 LD 产生新的数据块。
2) 将步骤 1）中生成的数据块分解成 16 字节数据块，标号为 D1，D2，D3，D4 等等。最后一个数据块长度有可能不足 16 字节。
3) 如果最后（或唯一）的数据块长度等于 16 字节，转入步骤 4）；如果不

足 16 字节，在右边添加十六进制数‘80’。如果长度已达 16 字节，转入步骤 4)；否则，在其右边添加十六进制数‘00’，直到长度达到 16 字节。

4) 每一个数据块使用 9.6 章节描述的数据加密过程密钥加密。

5) 计算结束后，所有加密后的数据块依照原顺序连接在一起（O1，O2，等等）。



SM1(e) = 数据加密算法（加密模式） D = 数据块
SM1(d) = 数据加密算法（解密模式） KDS = 数据加密过程密钥
O = 输出

图 9- 2 数据加密

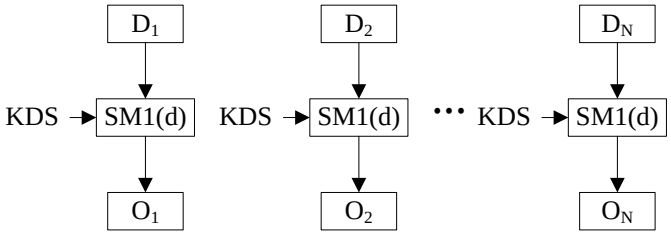
9.4.3.4 数据解密计算

数据解密计算，如图 9-3，步骤如下：

1) 将命令数据域中的数据块分解成 16 字节长的数据块，标号为 D1，D2，D3，D4 等等。每个数据块使用如 9.6 章节所描述的方法产生的数据加密过程密钥进行解密。

2) 计算结束后，所有解密后的数据块依照顺序（O1， O2，等等)链接在一起。数据块由 LD、明文数据、填充字符组成。

3) LD 表示明文数据的长度，用来恢复明文数据。



SM1(e) = 数据加密算法（加密模式） D = 数据块
SM1(d) = 数据加密算法（解密模式） KDS = 数据加密过程密钥
O = 输出

图 9- 3 数据解密

9.5 子密钥分散

如图 9-4，子密钥的分散因子为 8 字节。用指定的分散因子拼接分散因子求反值作为输入数据，做加密计算，产生的 16 字节的结果作为子密钥。

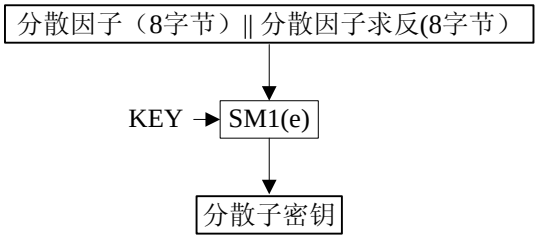


图 9- 4 子密钥计算方法

9.6 过程密钥的产生

如图 9- 5，MAC 和数据加密的过程密钥是用可变数据产生的密钥。

过程密钥产生后只能在某过程中使用一次。

输入数据是 8 字节随机数拼接 8 字节全 ‘00’。

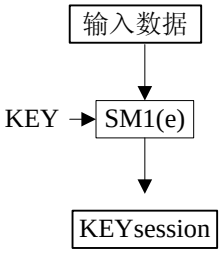


图 9- 5 过程密钥的产生

9.7 操作权限鉴别

操作权限鉴别的目的是验证终端对卡中数据进行读写操作的合法性。

9.7.1 鉴别数据的长度

本规范中，鉴别数据的长度规定为 8 个字节。

9.7.2 操作权限鉴别过程密钥的产生

在操作权限鉴别过程中用到的操作权限鉴别过程密钥是在鉴别过程中用可变数据产生的密钥，按照 9.6 章节中描述的方法产生。

操作权限鉴别加密算法密钥的鉴别密钥用于产生操作权限鉴别过程密钥。

过程密钥产生后只能在鉴别过程中使用一次。

输入数据是鉴别命令引用的可变数据（如随机数）。

9.7.3 鉴别数据的计算

如图 9-6，使用 9.6 章节描述的操作权限鉴别过程密钥对原始数据进行加密，加密结果左右 8 字节异或得到鉴别数据。

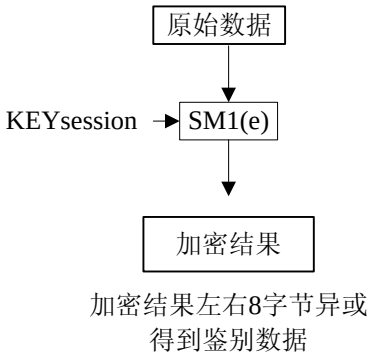


图 9- 6 鉴别数据计算

9.8 数字签名产生与验证

数字签名产生，对任意长数据组成的报文 MSG 签名的步骤如下：

1) 计算报文 MSG 的 32 字节的 HASH 值 h:= H[MSG]；
2) 计算 Sign(S_K)[h]，得到两个 32 字节长度的数字 r 和 s；
3) 数字签名 S 被定义为 64 字节长度的数字 S:=r||s，即数字签名 S 由数字 r 和 s 串联而成。

数字签名验证，对任意长数据组成的报文 MSG 验证签名 S 的步骤如下：

1) 计算报文 MSG 的 32 字节的 HASH 值 h:= H[MSG]；
2) 计算 Verify(P_K)[h, S]，若函数输出 True 表示验证正确，若输出 False，表示验证失败。

9.9 安全规划

卡上数据根据应用安全要求，分为只读数据区、只写数据区、可读写数据区。各使用机构权限分配，根据不同的应用要求配置 SAM 卡来进行数据的安全访问。

SAM 卡内嵌于居民健康卡终端设备中，为系统提供高级别的安全保护。SAM 卡与终端可以视为一体。SAM 卡中存放多组不同版本不同索引的主密钥。所有的主密钥通常必须在终端投入使用之前，被下载到 SAM 卡中。如果在终端使用过程中，主密钥需要修改，必须使用安全报文。该操作的实现必须在特殊的授权情况下完成。为避免伪操作，存放在 SAM 卡中的不同类型的主密钥必须与不同特定的应用操作相结合使用。在终端上进行居民健康卡应用操作时需要使用 SAM 卡进行安全保护。不同机构配发的 SAM 卡中装载的密钥类型依据该机构的所支持的应用类型决定。

居民健康卡 SAM 卡技术规范及检测指南将另行制定。

9.10 密钥机制

9.10.1 对称密钥

对系统使用的对称密钥，用特定的分散因子作为输入数据，做加密计算，产生的结果作为子密钥。系统中密钥的生成机制如图 9- 7 所示。

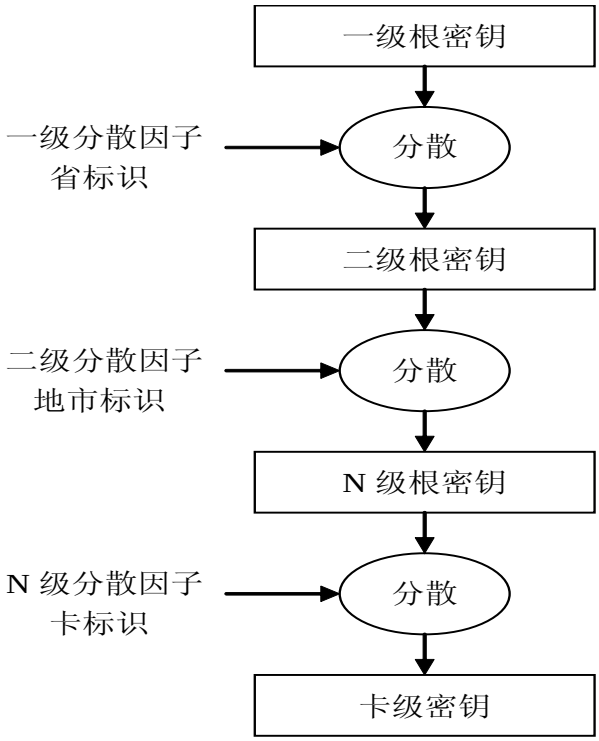


图 9- 7 密钥生成机制

9.10.2 **非对称密钥**

9.10.2.1 居民健康卡二级非对称密钥体系

居民健康卡的非对称密钥体系采用二级架构，如图 9-8 所示。

居民健康卡根密钥管理机构负责签发发卡机构的公钥证书。根密钥管理机构私钥由根密钥管理机构保管并保证其私密性和安全性。

发卡机构负责签发终端 SAM 的公钥证书，发卡机构私钥由发卡机构保管并保证其私密性和安全性。发卡机构的发卡证书，使用居民健康卡根密钥管理机构的根私钥签名生成。

终端 SAM 卡的证书，由发卡机构使用私钥对终端公钥及证书信息进行签名生成。

9.10.2.2 证书密钥使用

证书密钥使用如图 9-9，结算机构终端通过根公钥索引定位根公钥，并用根公钥验证发卡机构的发卡证书并得到发卡机构的公钥值，再使用发卡机构的公钥验证终端 SAM 卡的证书并得到 SAM 卡的公钥，结算机构终端得到 SAM 卡的公钥后，就可以使用该公钥验证卡片中的签名数据。

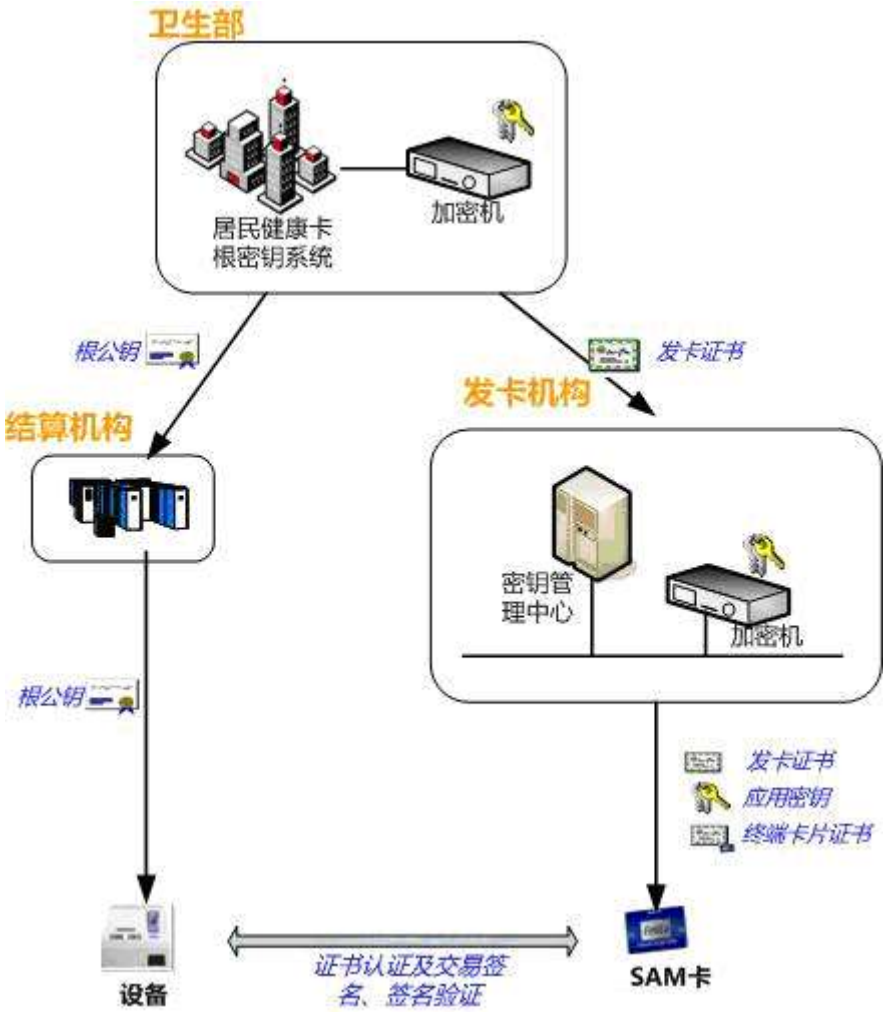


图 9- 8 非对称密钥体系

9.10.2.3 居民健康卡使用的公钥种类

在居民健康卡公钥认证体系中使用了三种公私钥对：根公私钥对、发卡机构公私钥对和终端 SAM 卡公私钥对，其作用如表 9-1。

9.10.2.4 根证书文件

根公钥证书以根证书文件形式进行传递。

1. 根证书的文件命名

根证书文件的命名格式为：00000001.RAA，其中：

— 00000001 为居民健康卡的应用标识号

— R 为根证书的类型标识

— AA 为根公钥的索引，以 0xAA 格式标识

2. 根证书的内容格式

根证书是二进制数据，其格式和内容如表 9-2 所示。

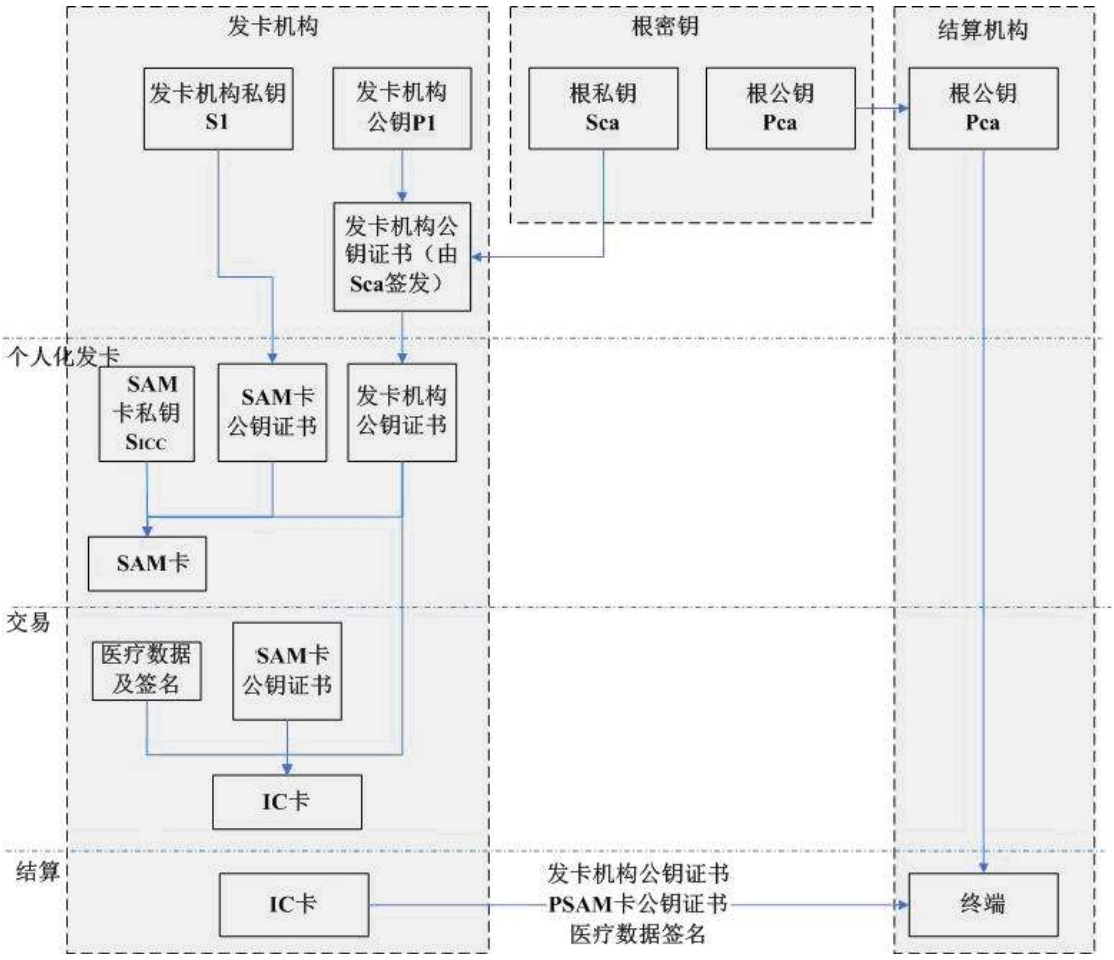


图 9- 9 证书密钥使用

表 9- 1 非对称密钥种类

密钥名称	用途
根公私钥对	用于对发卡机构签发公钥证书
发卡机构公私钥对	用于对 SAM 卡签发公钥证书
SAM 卡公私钥对	用于交易签名和验证

表 9- 2 根证书格式

字段名	长度（字节）	描述
未签名根公钥输出扩展	47+64	详细见表 9-3
自签名的根公钥数据	64	

3. 未签名根公钥输出扩展

未签名根公钥输出扩展是根公钥文件的第一部分，其格式和内容如表 9-3 所

示。

表 9- 3 未签名根公钥输出扩展格式

字段名	长度（字节）	描述	格式
记录头	1	十六进制’20’	b
应用标识号	4	标识一个应用，居民健康卡应用标识为十六进制’00000001’	b
根公钥长度	2	根证书的公钥长度以十六进制表示，当前为’00 40’	b
根公钥算法标识	1	十六进制’02’-SM2	b
哈希算法标识	1	十六进制’03’-SM3	b
应用供应商标识	5	标识卫生部	b
根公钥索引	1	唯一标识根公钥	b
根公钥 1	32	根公钥 1	b
根公钥 2	32	根公钥 2	b
哈希值	32	本表从第 1 到 9 项的连接数据的 SM3 哈希值	b

4. 自签名的根公钥数据

使用根私钥对未签名根公钥输出扩展中的“哈希值”数据进行私钥加密的结果就是自签名的根公钥数据。

9.10.2.5 发卡机构公钥输入文件

发卡机构为获得发卡机构生产型公钥证书或测试型公钥证书，需向根密钥管理机构提交发卡机构公钥证书申请，申请时需要提交发卡机构公钥输入文件。

1. 发卡机构公钥输入文件命名

发卡机构公钥输入文件的命名格式为：WSTTTTTT.INP，其中：

— WS 为卫生部的标识

— TTTTTT 为记录号，唯一标识一个发卡机构的一次申请，由根密钥管理机构统一管理和分发

— INP 为文件类型标识

2. 发卡机构公钥输入文件的内容格式

发卡机构公钥输入文件是二进制数据，其格式和内容如表 9-4 所示。

表 9- 4 发卡机构公钥输入文件格式

字段名	长度（字节）	描述
未签名发卡机构公钥输入扩展	51+64	详细见表 9-5
自签名的发卡机构公钥数据	64	

3. 未签名发卡机构公钥输入扩展

未签名发卡机构公钥输入扩展是文件的第一部分，其格式和内容如表 9-5 所示。

表 9- 5 未签名发卡机构公钥输入扩展格式

字段名	长度（字节）	描述	格式
记录头	1	十六进制’21’	b
应用标识号	4	标识一个应用，居民健康卡应用标识为十六进制’00000001’	b
证书格式	1	十六进制’01’	b
发卡机构标识	4	发卡机构的编号	cn8
证书失效日期	2	月和年（MMYY），在该月最后一天之后证书失效	n4
记录号	3	发卡机构公钥证书申请记录号	n6
公钥算法标识	1	十六进制’02’-SM2	b
哈希算法标识	1	十六进制’03’-SM3	b
发卡机构公钥长度	2	公钥长度以十六进制表示，当前为’00 40’	b
发卡机构公钥 1	32	发卡机构公钥 1	b
发卡机构公钥 2	32	发卡机构公钥 2	b
哈希值	32	本表从第 1 到 11 项的连接数据的 SM3 哈希值	b

4. 自签名的发卡机构公钥数据

使用发卡机构私钥对未签名发卡机构公钥输入扩展中的“哈希值”数据进行私钥加密的结果就是自签名的发卡机构公钥数据。

9.10.2.6 发卡机构公钥输出文件

发卡机构的公钥证书文件。

1. 发卡机构公钥输出文件命名

发卡机构公钥输出文件的命名格式为：AAAAAA.INN，其中：

— AAAAAA 为记录号，唯一标识一个发卡机构的发卡证书，由根密

钥管理机构统一管理和分发，与发卡机构公钥输入文件的记录号一致。

— I 为文件类型标识，表示发卡证书

— NN 为根公钥索引

2. 发卡机构公钥输出文件的内容格式

发卡机构公钥输出文件是二进制数据，其格式和内容如表 9-6 所示。

表 9- 6 发卡机构公钥输出文件格式

字段名	长度（字节）	描述
未签名发卡机构公钥输出扩展	52+64	详细见表 9- 7
签名的发卡机构公钥数据	64	

3. 未签名发卡机构公钥输出扩展

未签名发卡机构公钥输出扩展是文件的第一部分，其格式和内容如表 9-7 所示。

表 9- 7 未签名发卡机构公钥输出扩展格式

字段名	长度（字节）	描述	格式
记录头	1	十六进制’23’	b
应用标识号	4	标识一个应用，居民健康卡应用标识为十六进制’00000001’	b
证书格式	1	十六进制’02’	b
发卡机构标识	4	发卡机构的编号	cn8
证书失效日期	2	月和年（MMYY），在该月最后一天之后证书失效	n4
记录号	3	发卡机构公钥证书申请记录号	n6
公钥算法标识	1	十六进制’02’-SM2	b
哈希算法标识	1	十六进制’03’-SM3	b
发卡机构公钥长度	2	公钥长度以十六进制表示，当前为’00 40’	b
发卡机构公钥 1	32	发卡机构公钥 1	b
发卡机构公钥 2	32	发卡机构公钥 2	b
根公钥索引	1	根密钥系统用来签发发卡机构公钥证书的公钥索引	b
哈希值	32	本表从第 1 到 12 项的连接数据的 SM3 哈希值	b

4. 签名的发卡机构公钥数据

使用根私钥对未签名发卡机构公钥输出扩展中的“哈希值”数据进行私钥加密的结果就是发卡机构公钥数据。

9.10.2.7 终端 SAM 卡证书

终端 SAM 卡的公钥证书格式，该证书不单独形成文件，而是整合在卡片个人化文件中一起下发给个人化系统，由个人化系统写入 SAM 卡。

1. SAM 卡证书格式

SAM 卡证书是二进制数据，其格式和内容如表 9-8 所示。

表 9- 8 SAM 卡证书格式

字段名	长度（字节）	描述
未签名的 SAM 卡公钥输出扩展	62+64	详细见表 9- 9
签名的 SAM 卡公钥数据	64	

2. 未签名的 SAM 卡公钥输出扩展

未签名的 SAM 卡公钥输出扩展，其格式和内容如表 9-9 所示。

表 9- 9 未签名的 SAM 卡公钥输出扩展

字段名	长度（字节）	描述	格式
证书格式	1	十六进制’04’	b
卡号	10	SAM 卡的卡号	cn
证书序列号	3	由发卡机构分配给这张证书的唯一的二进制数	b
证书失效日期	2	月和年（MMYY），在该月最后一天之后证书失效	n4
所属机构代码	10	本终端 SAM 卡所属的医疗机构组织机构代码，不足 10 字节后补十六进制’00’	ans
公钥算法标识	1	十六进制’02’-SM2	b
哈希算法标识	1	十六进制’03’-SM3	b
SAM 卡公钥长度	2	SAM 卡证书公钥长度以十六进制表示，当前为’00 40’	b
SAM 卡公钥 1	32	SAM 卡公钥 1	b
SAM 卡公钥 2	32	SAM 卡公钥 2	b

哈希值	32	本表从第 1 到 10 项的连接数据的 SM3 哈希值	b

3. SAM 卡公钥数据

使用发卡机构私钥对未签名的 SAM 卡公钥输出扩展中的“哈希值”数据进行私钥加密的结果就是 SAM 卡公钥数据。

10 应用

本章主要描述居民健康卡的应用，应用命令集将另行发布。

10.1 文件

本部分定义了居民健康卡在医疗领域的各项专有应用，如图 10-1 所示，DDF1 是居民健康卡应用环境，DDF2 是其他预留应用环境。

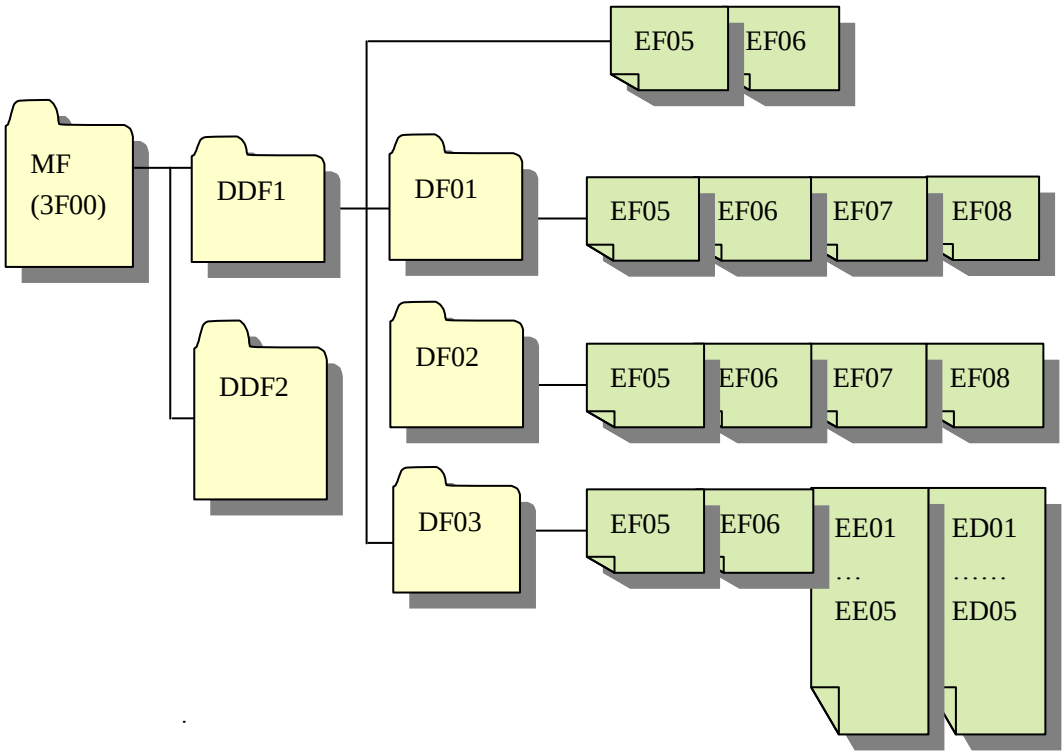


图 10- 1　居民健康卡文件结构示意图

10.1.1 文件结构

居民健康卡应用的文件结构应符合 GB/T 16649.4 及本规范中相关的规定。

居民健康卡应用的各个具体应用项对应的专用文件（DF），与相关的基本数据文件（EF）分别构成一个树状结构的各个分支。每个专用文件（DF）是其下面基本数据文件（EF）的入口点。

10.1.2 专用文件

居民健康卡目录定义文件（DDF1）的下一层是各具体应用所对应的专用文件（DF），各 DF 下应包含一个文件控制信息（FCI）。通过该文件可以对其下的

基本数据文件（EF）进行访问。

10.1.3 数据文件

基本数据文件（EF）包含了一组与应用相关的数据。

居民健康卡应用的基本数据文件（EF）有两种类型：记录文件类型和二进制文件类型。

居民健康卡应用的基本数据文件格式参见本规范第 8 章。

10.1.4 文件选择

居民健康卡应用的各个专用文件，可以用应用标识符（AID）、文件标识符（FID）两种方式来进行选择。

成功选择了居民健康卡应用的专用文件后，该专用文件被设置成当前专用文件，允许使用相关的命令对其进行操作。

10.2 应用标识符

应用标识符（AID）的结构符合 GB/T 16649.5 的规定，它包含两个部分：

1) 一个经过注册的应用提供者标识符（长度为 5 字节），它唯一地标识应用提供者。
2) 一个可选的“专用应用标识符扩展码（PIX）域，由应用提供者定义，最长 11 字节。

居民健康卡应用的各个具体应用的标识符（AID），必须采用由国家 IC 卡注册中心颁发的 RID，并通过 RID 选择该应用。

10.3 应用密钥

10.3.1 密钥配置

所有 SAM 卡安装内部认证密钥，用来进行居民健康卡的鉴别。在需要读取居民健康卡内数据的终端 SAM 卡上安装数据读控密钥，在需要更新居民健康卡内数据的终端 SAM 卡上安装数据写控密钥。居民健康卡密钥配置文件说明见表 10-1。

表 10-1 密钥配置文件列表

数据区	文件标识符	文件类型	读控制	写控制
MF\DDF1	EF05	变长记录	无	写控密钥
	EF06	变长记录	无	写控密钥
MF\DDF1\DF01（身份识别数据区）	EF05	变长记录	无	写控密钥
	EF06	变长记录	无	写控密钥
	EF07	变长记录	无	写控密钥
	EF08	变长记录	读控密钥	写控密钥
MF\DDF1\DF02（基础健康信息）	EF05	变长记录	无	写控密钥
	EF06	变长记录	读控密钥	写控密钥
	EF07	循环记录	无	写控密钥
	EF08	循环记录	无	写控密钥
MF\DDF1\DF03（管理数据）	EF05	定长记录	读控密钥	写控密钥
	EF06	定长记录	读控密钥	写控密钥
	EE01…EE05	二进制	读控密钥	写控密钥
	ED01…ED05	二进制	读控密钥	写控密钥
预留				

注：1、其中，MF\DDF1 区域下的 EF05、EF06 文件，MF\DDF1\DF01 区域下的 EF05、EF06、EF07、EF08 文件，MF\DDF1\DF02 区域下的 EF05、EF06、EF07、EF08 文件，MF\DDF1\DF03 区域下的 EF05、EF06 文件，在进行更新时需要采用密文加 MAC 的安全报文传送格式。

2、读控密钥、写控密钥是用于文件读写控制的鉴别密钥。

10.3.2 密钥用途

居民健康卡上的密钥必须安全存储。表 10-2 描述了存储在居民健康卡上的密钥用途。密钥的生成、分发、传送、管理等将另行制定密钥管理办法。

表 10- 2 密钥用途列表

分类	密钥	用途	密钥对应文件	适用的应用范围
内部认证密钥	IRK	鉴别发卡方的密钥	-	应用提供者
应用维护密钥	STK	发卡方或应用提供	-	发卡方

	STKDF01	方用于产生应用锁定、卡片锁定和更新二进制或记录命令的 MAC	-	身份识别应用
	STKDF02		-	基础健康应用
	STKDF03		-	管理数据应用
卡片或应用锁定控制密钥	BK	发卡方或应用提供方控制锁定卡片或应用操作的密钥	-	发卡方
	LKDF01		-	身份识别应用
	LKDF02		-	基础健康应用
	LKDF03		-	管理数据应用
应用数据更新密钥	UK1MF	发卡方或应用提供方控制应用数据更新操作的鉴别密钥	EF05、EF06	发卡方和持卡人基本信息
	UK1DF01		EF05、EF06、EF07、EF08	身份识别数据信息
	UK1DF02		EF05	医学警示数据信息
	UK2DF02		EF06	特殊信息数据信息
	UK3DF02		EF07、EF08	过敏、免疫基本数据信息
	UK1DF03		EF05、EF06、EE01…EE05 ED01…ED05	管理数据信息
应用数据擦除密钥	UK2DF03	发卡方或应用提供方控制应用数据擦除操作的鉴别密钥	EF05、EF06	管理数据信息
应用数据读取密钥	RK1DF01	发卡方或应用提供方控制部分应用数据读取操作的鉴别密钥	EF08	证件记录信息
	RK1DF02		EF06	特殊信息数据信息
	RK1DF03		EF05、EF06、EE01…EE05 ED01…ED05	管理数据信息

10.4 应用流程

本节描述了居民健康卡应用的应用流程。该流程描述的是持卡人刷卡、卡片与终端相互作用后，所进行的应用处理流程。

所有应用都要求终端必须安装居民健康卡 SAM 卡。终端与 SAM 之间以安全方式进行通信，本规范不定义任何与 SAM 通信相关的命令。

10.4.1 应用预处理流程

图 10-2 给出了居民健康卡应用的所有应用类型共有的预处理流程。

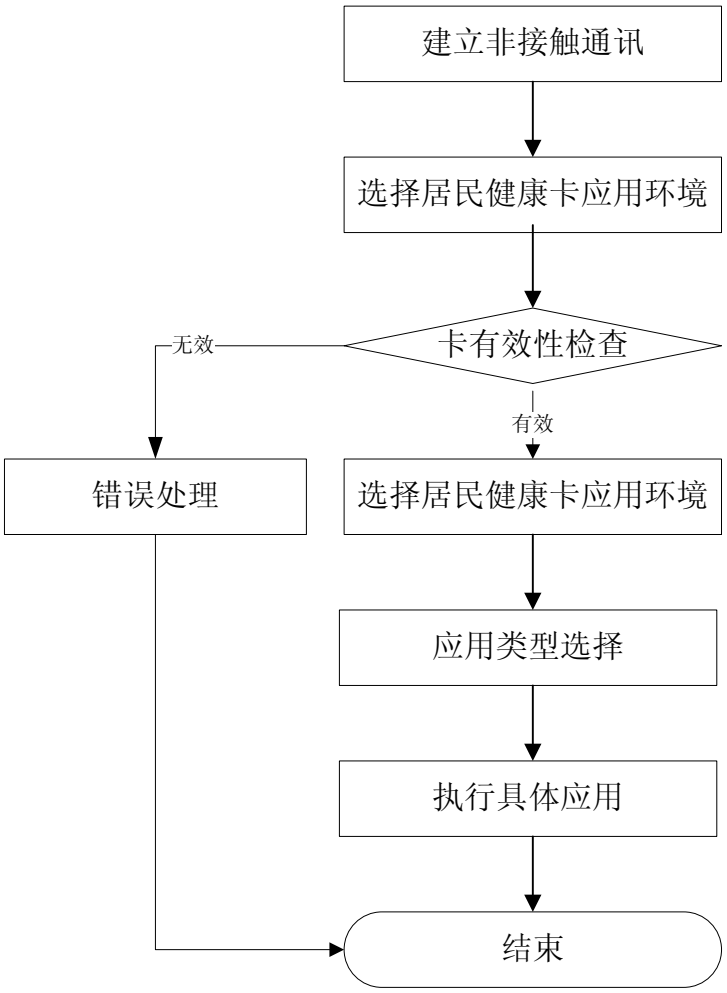


图 10- 2　　应用预处理流程

10.4.1.1 建立非接触通信

终端按照 ISO/IEC 14443 的通信协议方式与进入场内的居民健康卡建立通信。

10.4.1.2 选择居民健康卡应用环境

使用“选择”命令对居民健康卡应用环境进行选择。

10.4.1.3 卡有效性检查及持卡人身份认证

首先使用 IRK（内部认证密钥）对居民健康卡的有效性进行验证，步骤如下：

1) 终端产生 8 字节的随机数，该随机数作为“内部认证”命令的数据域。

2) 终端发送“内部认证”命令，卡计算鉴别数据并回送。

3) 终端收到鉴别数据后，进行比较验证。

如果验证不通过，则按 10.4.1.4 描述进行。

如果验证通过，则用“读记录”命令读取发卡机构数据，终端对所得数据进行检查，步骤如下：

1) 卡是否在有效期内。

2) 卡是否在终端存储的黑名单之列。

3) 终端是否支持发卡机构代码。

4) 终端是否支持从居民健康卡回送的“卡的类别”所代表的卡类型。

5) 终端是否支持从居民健康卡回送的版本。

10.4.1.4 错误处理

终端对应用预处理出错的处理方法不属于本规范的范围。

10.4.1.5 应用选择

成功地选择了某个具体的居民健康卡应用后，居民健康卡回送文件控制信息。终端可以依此建立居民健康卡所支持的应用列表。

10.4.2 **应用操作流程**

10.4.2.1 卡数据读取

通过读应用信息，业务管理部门的操作员可以从居民健康卡中获得持卡人办理具体事务时需要读取的相关信息。

对某一具体的应用信息的读操作仅受终端中的 SAM 卡的控制，操作流程如图 10-3，步骤如下：

1) 判断读信息是否受控。终端应该明确知道对某一具体的应用信息的读取操作是否受控。如果信息读取操作是不受控的，则转入步骤 3)；否则，继续按下述步骤执行。

2) 读操作权限的鉴别。

3) 发出读命令。根据应用数据的存储格式，终端应按读命令来读取所需的应用信息。

4) 返回确认。在成功读取数据后，卡应向终端回送状态码来确认数据读取操作的完成。

5) 判断是否还需继续读取数据。终端在成功读取一条信息后，应根据应用的要求，判断是否还要读取更多的数据。如果需要继续读取数据，则转入步骤 3）继续进行，否则继续后续操作。

6) 提示已读取完毕。终端在确认应用要求的所有数据都已读取完成后，将通过适当的设备向业务管理部门的操作员提示应用完成。

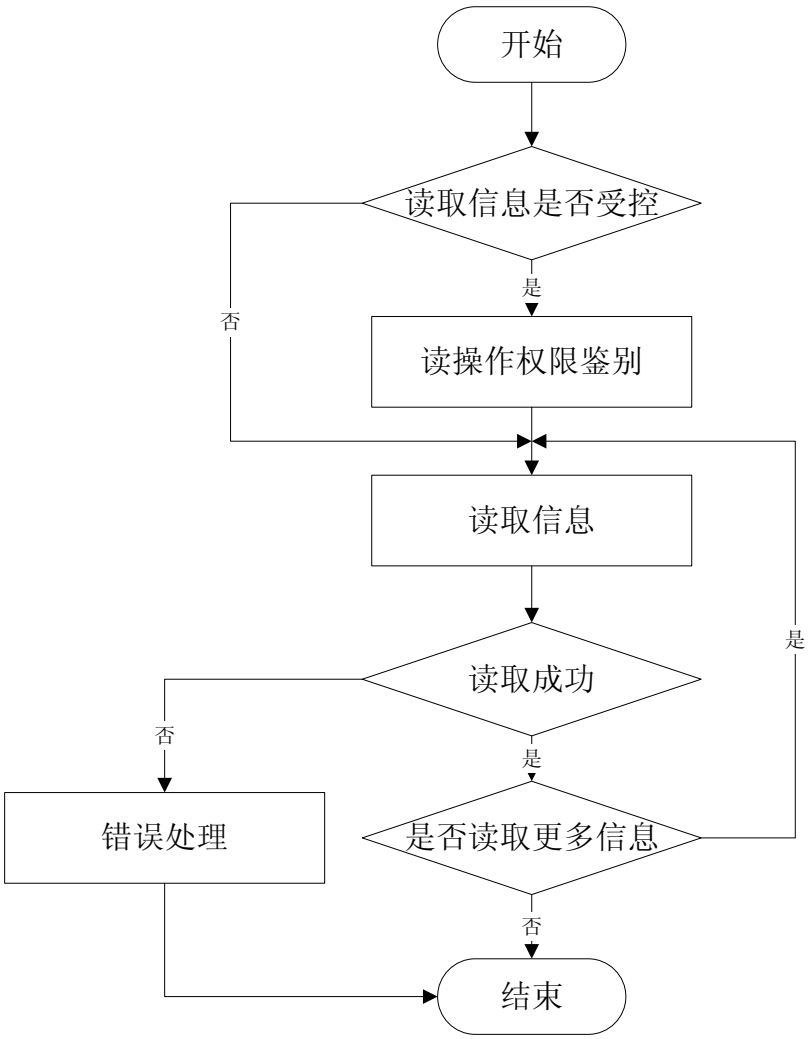


图 10- 3 卡数据读取流程

10.4.2.2 卡数据更新

通过写应用信息，业务管理部门的操作员可以在居民健康卡中记录持卡人办理具体事务时产生的相关信息。

对某一具体的应用信息的更新操作仅受终端中的 SAM 卡的控制，操作流程如图 10-4，步骤如下：

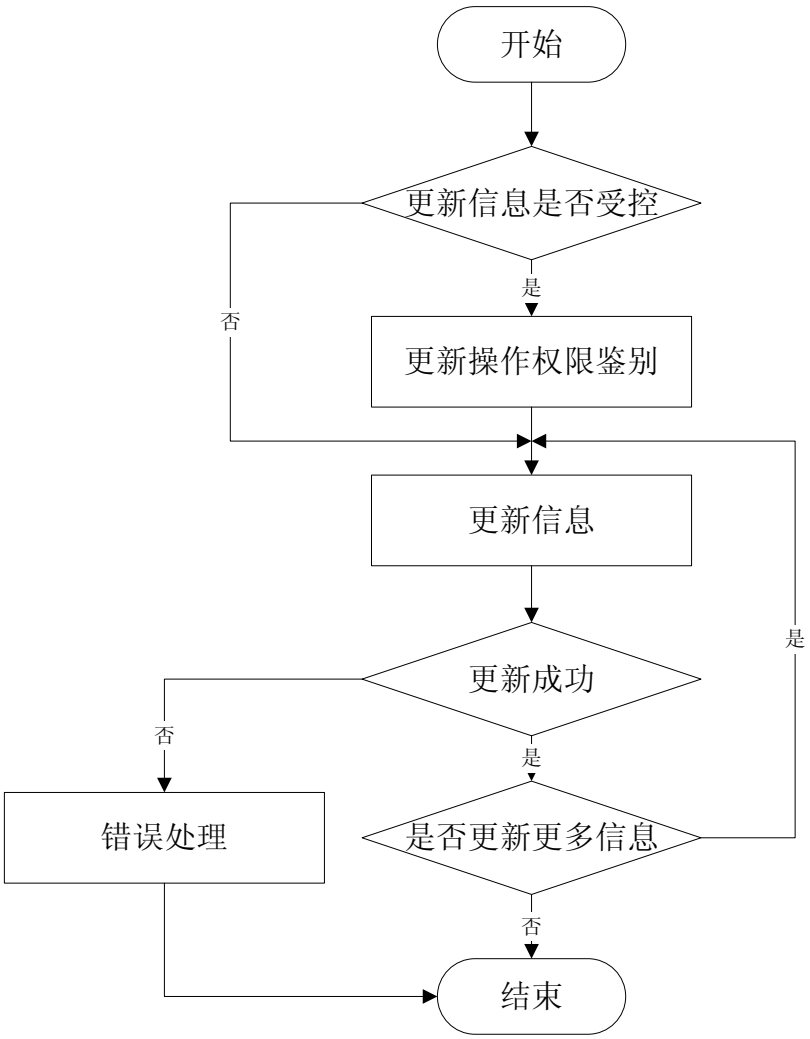


图 10- 4 卡数据更新流程

1) 判断更新信息是否受控。终端应该明确知道对某一具体的应用信息的更新操作是否受控。如果信息更新操作是不受控的，则转入步骤 3）；否则，继续按下述步骤执行。
2) 更新操作权限的鉴别。
3) 发出更新命令。根据应用数据的存储格式，终端应按规范中的描述发出更新命令来更新所需的应用信息。
4) 返回确认。在成功更新数据后，卡应向终端回送状态码来确认数据更新

操作的完成。

5) 判断是否还需继续更新数据。终端在成功更新一条信息后，应根据应用的要求，判断是否还要更新更多的数据。如果需要继续更新数据，则转入步骤 3）继续进行，否则继续后续操作。

6) 提示已更新完毕。终端在确认应用要求的所有数据都已更新完成后，将通过适当的设备向业务管理部门的操作员提示应用完成。

10.4.2.3 门诊信息管理流程

门诊信息记录流程如图 10-5，步骤如下：

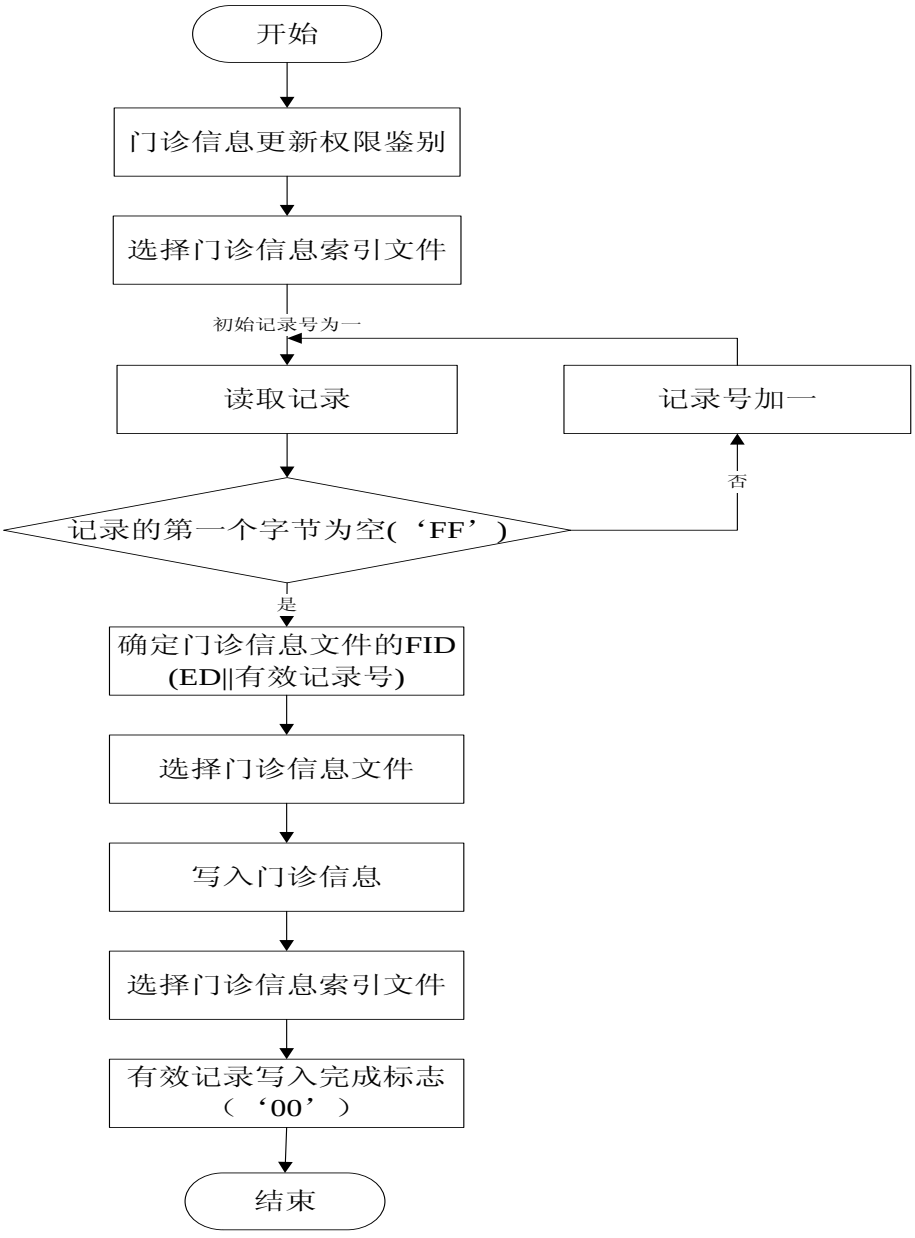


图 10- 5 门诊信息记录流程

1) 获得门诊信息写权限。
2) 选择门诊信息索引文件，从第一条记录开始搜索到第一个值为空（'FF’）的记录，根据这条记录的记录号 RN 确定门诊信息文件的文件标识符 FID（‘ED’+RN）。
3) 选择门诊信息文件，写入本次门诊信息记录。
4) 再次选择门诊信息索引文件，将第 RN 条记录写入完成标识（‘00’）。
5) 流程结束。

门诊信息读出流程如图 10-6，步骤如下：

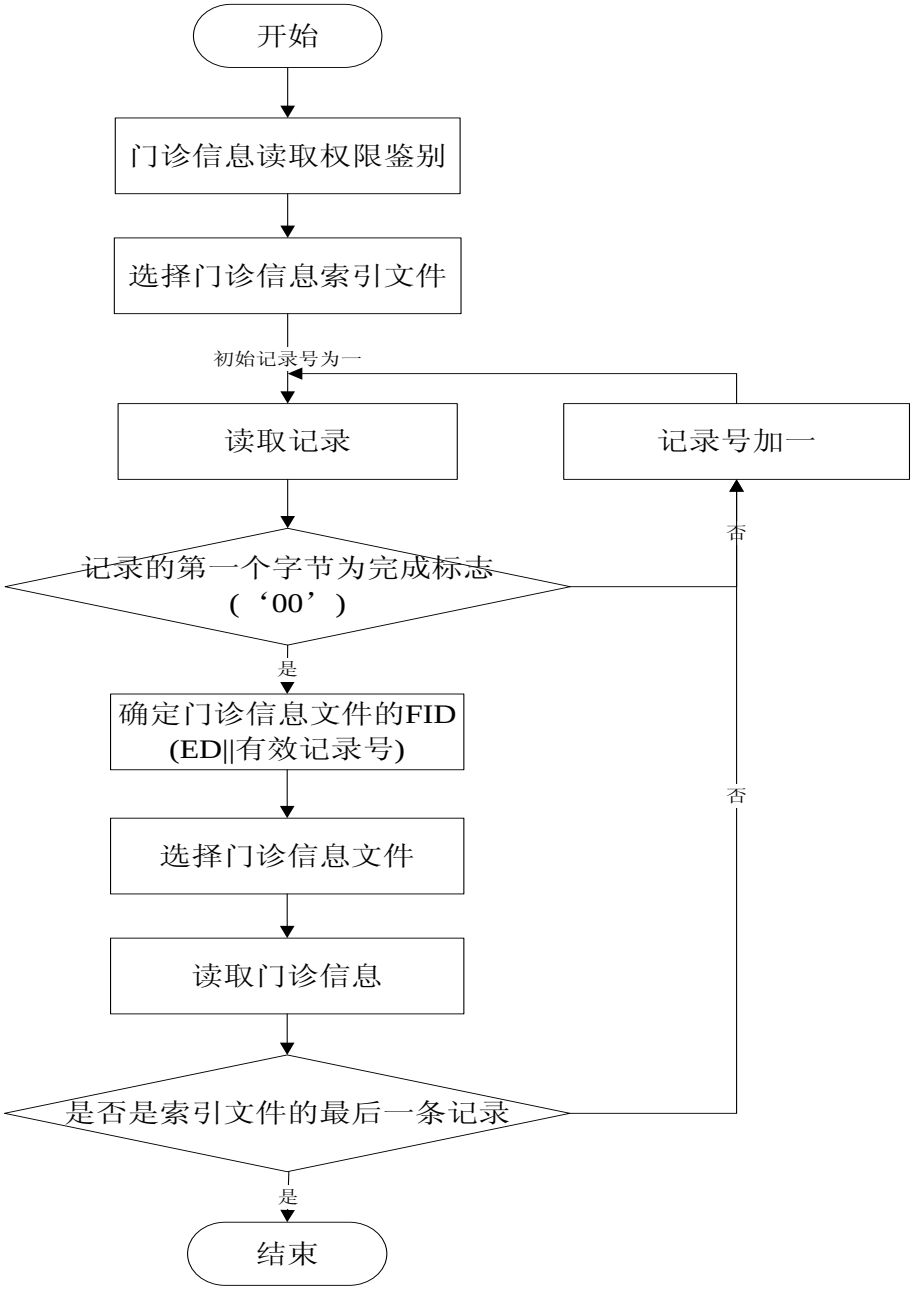


图 10- 6 门诊信息读出流程

1) 获得门诊信息读权限。
2) 选择门诊信息索引文件，从第一条记录开始，如果记录值为‘00’，表示存在有效门诊信息记录，根据该记录号 RN 确定存放门诊信息记录的文件标识符 FID（‘ED’+RN）。
3) 使用 FID 选择门诊信息文件，读出本次门诊信息记录。
4) 记录号递增，从步骤 2）开始重复执行，直到门诊信息索引文件的最后一条记录结束，读取所有门诊信息记录。
5) 流程结束。

门诊信息擦除流程，如图 10-7，步骤如下：

1) 获得门诊信息擦除权限。
2) 选择门诊信息索引文件，擦除门诊记录有效标志，即写入‘FF’。
3) 流程结束。

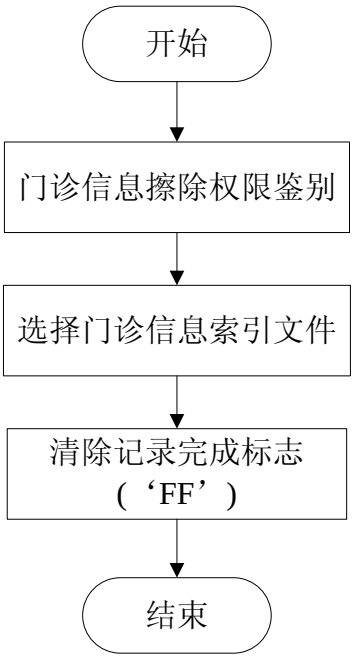


图 10- 7 门诊信息擦除流程

10.4.2.4 住院信息流程

住院信息记录流程，如图 10-8，步骤如下：

1) 获得住院信息写权限。
2) 选择住院信息索引文件，从第一条记录开始搜索到第一个值为空（‘FF’）

的记录，根据这条记录的记录号 RN 确定住院信息文件的文件标识符 FID（‘EE’+RN）。

3) 选择住院信息文件，写入本次住院信息记录。

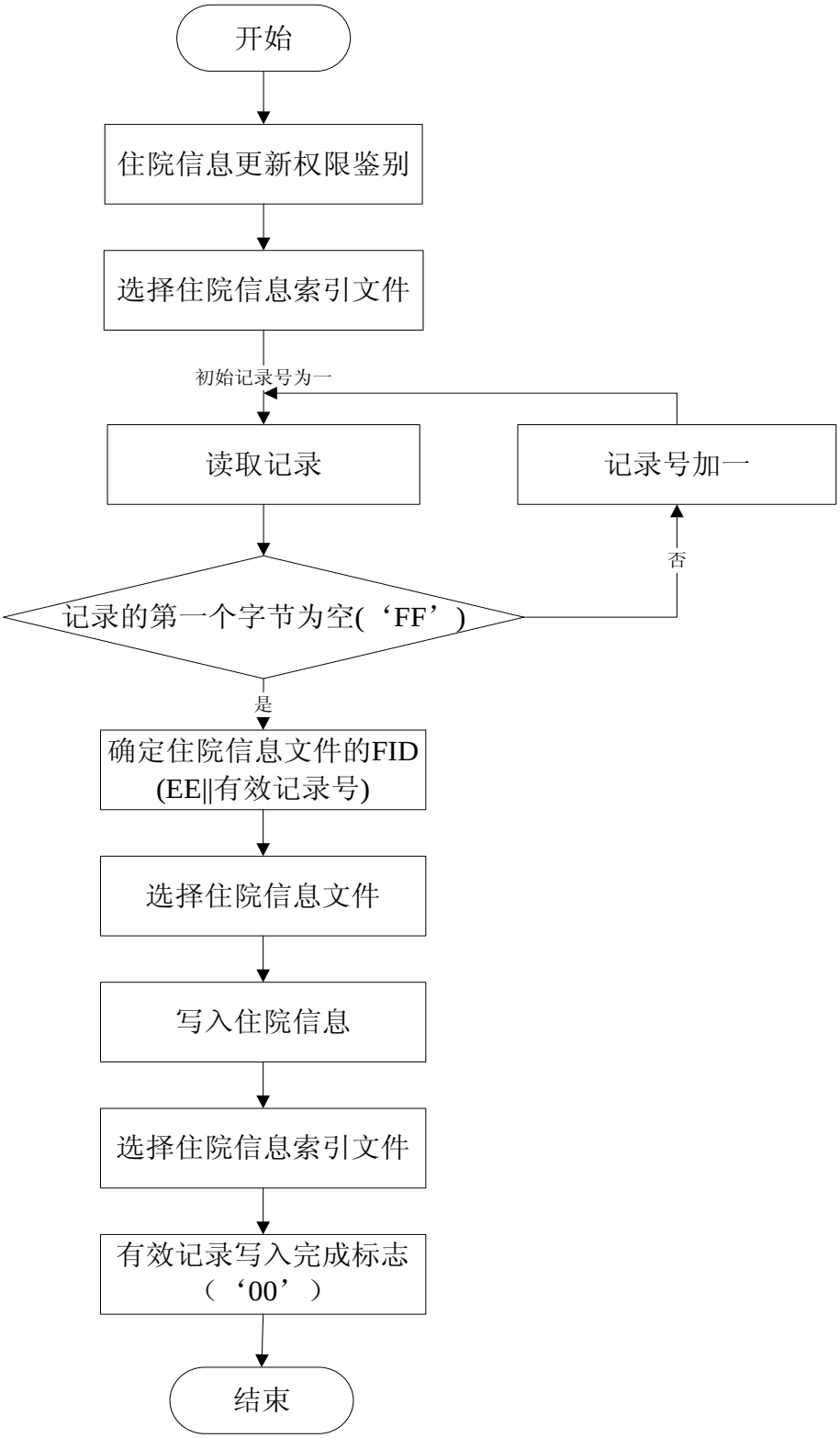


图 10- 8 住院信息记录流程

4) 再次选择住院信息索引文件，将第 RN 条记录写入完成标识（‘00’）。

5) 流程结束。

住院信息读出流程，如图 10-9，步骤如下：

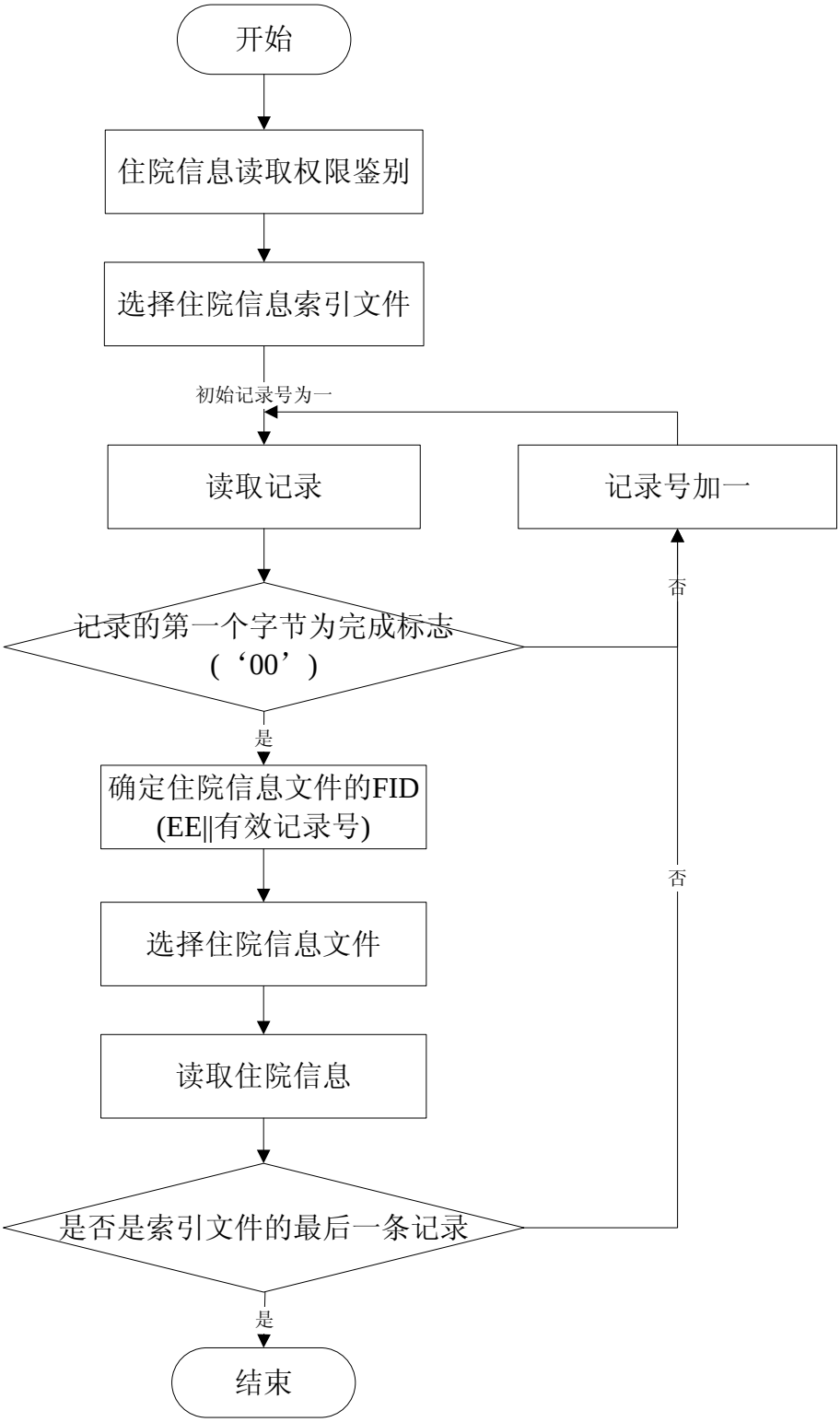


图 10- 9 住院信息读出流程

1) 获得住院信息读权限。
2) 选择住院信息索引文件，从第一条记录开始，如果记录值为‘00’，表示存在有效住院信息记录，根据该记录号 RN 确定存放住院信息记录的文件标识符 FID（‘EE’+RN）。
3) 使用 FID 选择住院信息文件，读出本次住院信息记录
4) 记录号递增，从步骤 2）开始重复执行，直到住院信息索引文件的最后一条记录结束，读取所有住院信息记录。
5) 流程结束。

住院信息擦除流程，如图 10-10，步骤如下：

1) 获得住院信息擦除权限。
2) 选择住院信息索引文件，擦除住院记录有效标志，即写入‘FF’。
3) 流程结束。

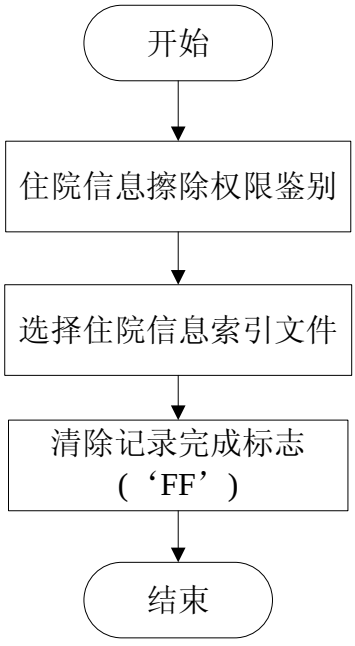


图 10- 10 住院信息擦除流程

附录 居民健康卡基础数据采集表

<table>
<tr><td rowspan="10">身份识别数据</td><td>姓名</td><td colspan="2"></td><td>出生日期</td><td colspan="2">□□□□年□□月□□日</td></tr>
<tr><td>性别</td><td colspan="5">0 未知的性别 1 男 2 女 9 未说明的性别 □</td></tr>
<tr><td>身份标识</td><td colspan="5">居民身份证号码：□□□□□□□□□□□□□□□□□□
其他证件_____ 证件号码：□□□□□□□□□□□□□□□□□□
新农合证（卡）号：□□□□□□□□□□□□□□□□□□
健康档案编号：□□□□□□□□□□□□□□□□□□</td></tr>
<tr><td>民族</td><td colspan="2">1 汉 2 少数民族____ □</td><td>本人电话</td><td colspan="2"></td></tr>
<tr><td>婚姻</td><td colspan="5">1 已婚 2 未婚 3 离婚 4 丧偶 5 未说明的婚姻状况 □</td></tr>
<tr><td>职业</td><td colspan="5">1 国家机关、党群组织、企业、事业单位负责人 2 专业技术人员 3 办事人员和有关人员 4 商业、服务业人员 5 农、林、牧、渔、水利业生产人员 6 生产、运输设备操作人员及有关人员 7 军人 8 不便分类的其他从业人员 □</td></tr>
<tr><td>文化程度</td><td colspan="5">1 文盲及半文盲 2 小学 3 初中 4 高中/技校/中专 5 大学专科及以上 6 不详 □</td></tr>
<tr><td>联系人</td><td colspan="5">1 姓名_____ 与持卡人的关系_____ 电话_____;
2 姓名_____ 与持卡人的关系_____ 电话_____;
3 姓名_____ 与持卡人的关系_____ 电话_____;</td></tr>
<tr><td>户籍地址</td><td colspan="5">_____省_____市_____县（区）_____乡(镇、街道)_____村(居委会)</td></tr>
<tr><td>居住地址</td><td colspan="5">_____省_____市_____县（区）_____乡(镇、街道)_____村(居委会)
(当现居住地址与户籍地址不符合时填写)</td></tr>
<tr><td>医疗费用支付方式</td><td colspan="5">1 城镇职工基本医疗保险 2 城镇居民基本医疗保险 3 新型农村合作医疗
4 贫困救助 5 商业医疗保险 6 全公费 7 全自费 8 其他 □/□/□</td></tr>
<tr><td colspan="7"></td></tr>
<tr><td rowspan="2">基础健康数据</td><td>生物标识</td><td colspan="5">ABO 血型： 1 A 型 2 B 型 3 O 型 4 AB 型 5 不详 □
RH 阴性： 1 否 2 是 3 不详 □</td></tr>
<tr><td>医学警示</td><td colspan="5">1 哮喘 □ 2 心脏病 □ 3 心脑血管病 □ 4 癫痫病 □
5 精神病 □ 6 凝血紊乱 □ 7 糖尿病 □ 8 青光眼 □
9 透析 □ 10 器官移植 □ 11 器官缺失 □ 12 可装卸的义肢 □
13 心脏起搏器□ 99 其他医学警示_____</td></tr>
</table>

		过敏物 1：名称_____ 过敏反应：_____ 过敏物 2：名称_____ 过敏反应：_____ 过敏物 3：名称_____ 过敏反应：_____
	免疫接种	疫苗 1：疫苗名称_____ 接种时间_____ 疫苗 2：疫苗名称_____ 接种时间_____ 疫苗 3：疫苗名称_____ 接种时间_____ 疫苗 4：疫苗名称_____ 接种时间_____ 疫苗 5：疫苗名称_____ 接种时间_____ 疫苗 6：疫苗名称_____ 接种时间_____ 疫苗 7：疫苗名称_____ 接种时间_____ 疫苗 8：疫苗名称_____ 接种时间_____ 疫苗 9：疫苗名称_____ 接种时间_____ 疫苗 10：疫苗名称_____ 接种时间_____

填表说明：

1．性别：按照国标分为未知的性别、男、女及未说明的性别。

2．出生日期：根据居民身份证的出生日期填写。按照年（4 位）、月（2 位）、日（2 位）顺序填写，如 20110612。

3．居民身份证号码：需如实、完整填写。如果不是居民身份证，需填写证件名称及证件号码。

4．新农合卡（证）号：适用于已建卡的参合农民，需完整填写，最多 18 位数字。

5．健康档案编号：适用于已建健康档案者，需完整填写。

6．民族：少数民族应填写全称，如彝族、回族等。

7．联系人：指紧急情况联系人。需至少填写一位联系人的姓名、与持卡人的关系、联系电话。这里要求填写与建卡对象关系紧密的亲友姓名，该联系人应为当遇特殊情况或紧急情况无法与建档对象直接沟通而急需建卡对象亲友提供帮助时，确实可以取得联系并能提供帮助的人。

8．联系人电话：填写确实能够及时、有效取得联系的电话号码。

9．婚姻：

<1>已婚：指在婚者，包括曾离婚或丧偶现已再婚的人。

<2>未婚：指建档之前从未结过婚的人。

<3>离婚：指建档时已与配偶解除婚姻关系，且未再婚的人。

<4>丧偶：指配偶去世未再婚的人

10．职业：

“国家机关、党群组织、企业、事业单位负责人”指在中国共产党中央委员会和地方各级党组织、各级人民代表大会常务委员会、人民政协、人民法院、人民检察院、国家行政机关、各民主党派、工会、共青团、妇联等人民团体，群众自治组织和其他社团组织及其工作机构、企业、事业单位中担任领导职务并具有决策、管理权的人员。

“专业技术人员”指专门从事各种科学研究和专业技术工作的人员。

“商业、服务业人员”指从事商业、餐饮、旅游、娱乐、运输、医疗辅助服务及社会和居民生活等服务工作的人员。

“办事人员和有关人员”指在国家机关、党群组织、企业、事业单位中从事行政业务、行政事务工作的人员和从事安全保卫、消防、邮电等业务人员。

“农、林、牧、渔、水利生产人员”指从事农业、林业、畜牧业及水利生产、管理、产品初加工的人员。

“生产、运输设备操作人员及有关人员”指从事矿产勘查、开采，产品的生产制造、工程施工和运输设备操作的人员及有关人员。

11．户籍地址：需如实填写户籍所在地，准确到村（居委会）。

12．现居住地：当居住地与户籍地址不符时填写，该地址应为建卡人常住或近期居住地址。

13．医疗费用支付方式可填多项。

14．医学警示：符合医学警示情况，在其后“□”打“√”，没有列出的医学警示，如高血压、恶性肿瘤、结核、肝炎及其他法定传染病，需在“_____”处填写医学警示名称。

15．过敏物名称主要指青霉素、磺胺、链霉素等药物名称，如有其他药物或食物等其他物质（如花粉、酒精、油漆等）过敏，请写明过敏物质名称。“过敏反应”描述发生过敏时患者的症状。

16．免疫接种：需详细填写曾接种的疫苗名称以及最后一次接种时间，以计划免疫为主。