ICS03.060
A11

IAC

中 国 保 险 行 业 协 会 标 准

T/IAC XX—2018

健康保险数据安全管理指引

Data Management Guidelines of Health Insurance Security

（征求意见稿）

××××-××-××发布　　××××-××-

中国保险行业协会　　发布

目　　次

前　言

本标准是按照GB/T1.1-2009给出的规则起草的。

本标准由中国保险行业协会提出并归口。

本标准负责起草单位：平安健康、国寿寿险、太保寿险、太平人寿、大地保险、人保寿险、人保健康、阳光人寿、中邮保险、友邦保险、和谐健康、昆仑健康、泰康人寿、太保安联健康险。

本标准主要起草人：里志仁、董元鹏、岳明泽、万文兵、彭恺、吴爱玲、马强、刘跃、熊鑫、王化、孙佳、李登武、吴旭东、戴颖艺、杨晓红、魏俊杰、陈京春、谷雨、陈应文。

健康保险数据安全管理规范

1 范围

本标准针对健康保险数据安全管理的术语定义、数据分类、数据获取、数据存储、数据使用、数据出境、数据销毁、数据安全事件及监督管理进行了明确的指引。

本标准适用于所有开展健康保险业务的保险机构。

2 术语和定义

下列术语和定义适用于本标准。

2.1

健康保险数据 health insurance data

健康保险数据是指机构在开展健康保险业务时，所获取、创造、使用及维护的包括但不限于客户、员工个人信息和专有数据，以下健康保险数据简称“数据”。

2.2

信息主体 information subject

信息主体是指数据信息所描述的对象，包括自然人、法人以及其它组织机构。

2.3

外部机构 external organization

外部机构包括企业、事业单位、社团、政府机关、军队等所有境内境外机构。

2.4

数据出境 data exit

数据出境是指将在中华人民共和国境内运营中收集和产生的数据，提供给位于境外的机构、组织、个人。

2.5

数据脱敏 data desensitization

数据脱敏是指通过对信息数据的技术处理，使其在不借助额外信息的情况下，无法识别或分析出个信息主体或信息主体的行为特征的过程。

2.6

数据安全事件 data security incident

指由于人为原因、软硬件缺陷或故障、自然灾害等，导致数据被窃取、篡改、假冒、破坏，对国家、社会、企业及公众利益造成一定影响及损失的事件。

3.数据分类

健康保险数据应归为如下几类：

3.1 个人数据

个人数据是指在开展健康保险业务过程中收集或产生的与个人有关的信息数据。

3.1.1 个人基本数据

个人基本数据是指与个人直接关联的基本信息数据，包括姓名、性别、出生日期、证件号码、住址、联系方式、个人生物识别信息、个人财产信息。

3.1.2 个人健康数据

个人健康数据是指能够描述个人健康状况的信息数据，包括个人生理信息、疾病症状、诊疗信息、病程信息、护理信息。

3.1.2 个人衍生数据

个人衍生数据是指个人通过一系列活动后产生的信息数据，包括保险交易信息、个人征信信息、通信内容。

3.2 商业数据

指在开展健康保险业务中，反映保险机构的运营管理、策略及价值的信息数据，包括企业的险种信息、理赔方案数据、分销渠道数据、消费市场数据。

3.3 其它信息数据

其它信息数据是指除开个人数据及商业数据之外的所有信息。

4. 数据获取

4.1 数据获取的合规要求

保险机构应通过正规合法的通道获取数据，对保险机构的要求包括：

1) 不得欺诈、诱骗、强迫信息主体提供数据；
2) 不得对信息主体隐晦或欺骗数据收集的原因、用途及使用范围；
3) 不得从非法渠道获取数据；
4) 不得收集与业务功能无关的数据；
5) 在获取数据前必须取得信息主体授权，如果间接获取数据，必须明确数据的来源依法合规以及原信息主体的授权范围是否包括同意转让、共享、公开披露等。
6) 在通过外部机构获取数据时，应明确数据的可使用范围，并对数据合作的产出物的专利约定受益人。
7) 当保险机构停止某产品或者服务时，应立即停止针对此产品或服务的信息收集。

4.2 数据获取的安全要求

1) 在获取数据的过程中，应采用安全可靠的方式进行，对保险机构要求包括：
2) 采取网络形式获取数据信息时，应采取可靠的技术手段确保数据在传输过程的安全性
3) 采取人工形式获取数据信息时，应采取必要的手段确保信息存储介质的安全性。
4) 在与外部机构进行长期的数据合作时，应建立长效安全的传输机制并签定保密协议。
5) 对于能直接接触数据的相关人员应签订完善的保密协议。

4.3 信息主体的权利

信息主体针对数据拥有知情权、反对与限制使用的权利以及纠正与删除的权利。

4.3.1 知情权

信息主体对数据获取的目的以及使用范围拥有知情的权利，保险机构在获取数据时应事先告知信息主体数据获取的目的及使用范围。当信息主体在事后行使知情权时，保险机构应及时告知。但是当信息主体行使知情权时保险机构提供的信息应仅限于信息主体自身相关的信息，不得包含其它信息主体信息。

4.3.2 更正权利

在数据不完整、不正确的情况下，信息主体有权要求保险机构对数据进行更正，保险机构应当及时对数据进行更正。

5. 数据存储

保险机构在数据存储过程中应当遵循“保密、可用、完整”原则。采取必要措施防止文件被非法使用、窃取、篡改和破坏，采取的措施包括但不限于以下方式：

5.1 完善的权限管理策略

5.1.1 保险机构应当针对数据信息进行完善的权限管理，合理授权、分级管理。

5.1.2 保险机构应具备数据访问的权限列表，根据岗位分配权限。

5.1.3 维护人员应当定期检查并清理权限列表。

5.2 完整的数据操作记录

数据操作应当具备完整的操作日志记录，以备审计，日志应包括访问、处理、删除、修改等操作。所有日志应当具备操作用户的自身属性信息及操作信息，以便追踪溯源。

5.2.1 数据操作日志保留期限

数据操作日志的保留时间应不低于 6 个月。

注：如果因硬件或者空间限制需要清理日志，应当由保险机构部门人员、业务人员根据业务及实际需要进行评估后进行日志删除或者迁移工作。

5.3 数据审计

5.3.1 保险机构应当定期针对日志进行审计。审计频率应不低于 6 个月。

5.3.2 审计范围应包括所有日志记录，针对重要的用户行为和重要安全事件进行审计和数据分析。

5.4 数据清理与备份管理

5.4.1 保险机构应当定期检视授权用户的有效性与安全性，对无效的用户、访问异常的用户进行清理。

评估接口的有效性与安全性，清理并整改异常接口。
5.4.2 当保险机构违反法律法规或事先约定，信息主体要求删除信息数据时，应及时删除信息，并立即停止与信息主体约定外的行为。
5.4.3 数据在存储过程中应当定期进行备份。备份应由服务器管理人员发起进行。备份数据存放的物理环境必须预防人为破坏和自然灾害。原信息和备份信息严禁在同一处保存。

5.5 其它安全防护

保险机构可在数据保管过程中采取其它安全防护措施，包括但不限于身份鉴别、访问控制、入侵检测与防御、资源控制等方式。

6 数据使用

数据在传输流转过程中，在未经规定程序批准的情况下，任何单位、个人不得擅自复制、更改和删除数据。保险机构应采取必要的技术手段保证数据在传输流转过程中的保密性、可用性和完整性。

6.1 数据使用范围

保险机构可自主使用所属数据，并严格管控、审核数据使用及外发的合规性。

非该保险机构使用数据必须经过保险机构授权后，才可使用。非保险机构的敏感数据使用必须进行数据脱敏，数据脱敏由保险机构进行处理。

6.2 数据使用脱敏

脱敏处理原则：脱敏后的数据记录必须不可对应至某一信息主体。

脱敏方式包括：全部屏蔽、部分屏蔽、信息提取、信息转化及信息泛化。保险机构必须根据数据分析需求及信息安全规范在保证数据可用性的前提下，对数据进行脱敏处理。

如果因业务需求，不能进行脱敏，且数据外发至境内，涉及到如下任意一条情况，应当经过公司数据管理部门、信息安全及合规多方评估过后方可发送：

a) 含有个人基本信息数据

b) 含有健康信息数据

c) 含有未公开的商业数据

d) 其它可能影响国家、社会及企业利益

6.3 数据传输要求

对于数据在网络的传输应符合国家与行业相关标准要求，采取必要的技术手段，如加密等，以确保数据传输的保密性、完整性和真实性。

7. 数据出境的要求

若涉及数据出境，应参考国家相关法律法规及行业相关标准的要求执行。

8.数据销毁

数据在保险机构不具有可用性后，应当按照相关标准要求进行销毁操作。

9 数据安全事件处置

针对数据安全事件，保险机构应：

a) 制定数据安全事件的应急预案，建立事件的响应机制；
b) 至少一年一次开展数据安全事件应急演练；
c) 发生数据安全事件后，应完整记录事件内容及信息，记录的信息至少应包括事件的时间、人员、地点、涉及的数据及影响人数、涉及的信息系统、对外的影响以、处置措施及改进措施；
d) 采取必要措施，及时控制事态，以免造成进一步的影响；
e) 按照《国家网络安全事件应急预案》的有关规定及时进行上报监管机构。

10 监督管理

保险机构应当在数据生命周期内的各个环节进行管理，数据使用人员应当严格遵守数据使用规范，并对数据负有保密责任与义务。对于因违反数据使用规范造成保险机构及个人损失的，保险机构可要求其承担民事责任，构成犯罪的移交司法机关依法追求其刑事责任。同时信息主体有权追究保险机构相关责任。

参考文献

[1]《General Data Protection Regulation》
[2]个人信息和重要数据出境安全评估办法（征求意见稿）
[3]信息安全技术　个人信息安全规范
[4]国家网络安全事件应急预案
[5]《网络安全法》
[6]保监统信[2016]202号文 《中国保监会关于印发《保险机构信息化风险非现场监管报表》暨启用保险机构信息化风险非现场监管信息系统的通知》