ICS 03.060
A11

Q

中国人民人寿保险股份有限公司企业标准

Q/PICCLIFE 002-2022

电子保单服务 信息安全规范

2022-08-25 发布　　2022-08-26 实施

中国人民人寿保险股份有限公司　发布

目　　次

前　　言

本标准按照GB/T1.1-2020给出的规则起草。

本标准由中国人民人寿保险股份有限公司提出并归口管理。

本标准起草单位：运营管理部。

本标准为第三次修订。

本标准执行遵循新标准替代旧标准原则，新标准执行的同时，原标准《个人电子保单信息安全规范》（Q_PICCLIFE 002-2021）自动失效。

电子保单服务 信息安全规范

1 范围

本标准规定了中国人民人寿保险股份有限公司个人保险电子保单服务的信息安全规范。包括电子保单、保单生成通知、回执、归档、查询查验、下载场景的服务安全规范。

本标准适用于个人客户通过我公司人保e通APP（销售人员登录使用的销售终端），以及通过与我公司合作银行的电子投保端（网银、手机银行、自助终端等）电子投保，经我公司承保并出具的个人人身保险电子保险合同（以下简称“电子保单”）服务信息安全规范。

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 22080-2016 信息安全管理体系要求

GB/T 36687-2018 保险术语

GB/T 22239-2019 信息安全技术 网络安全等级保护技术要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 35273-2020 信息安全技术 个人信息安全规范

GM/T 0070-2019 电子保单密码应用技术要求

JR/T 0033-2015 保险基础数据元目录

JR/T 0161-2018 保险电子签名技术应用规范

JR/T 0174-2019 电子保单业务规范

3 术语和定义

GB/T 36687-2018中界定的以及下列的术语和定义适用于本文件。

3.1 版式电文

指以固定格式的电子文件呈现，无论在何种设备上阅读、打印或印刷时，版面呈现结果均保持一致，以用户阅读为目的的固化数字纸张。

3.2 结构化数据

通过关系型数据库进行存储和管理，以二维表结构来逻辑表达和实现，严格遵循数据格式与长度规范，以计算机操作为目的的解释性文件。

3.3 电子保单

指通过保险人的可靠电子签名签发，用于证明保险合同关系，与纸质保险单具备同等法律效力的版式电文。

3.4 可靠电子签名

指对于所签署确认的数字电文，可认证签名人身份、可证明签名动作不可替代及签名结果不可篡改。

3.5 电子投保单

指投保人向保险人申请订立保险合同时提交的具有可靠电子签名的电子要约版式文件。

3.6 电子投保

指投保人通过电子化方式完成投保询价、签署并提交投保要约、确认保险条款的行为。

3.7 电子保单发送

指保险人以一种或多种形式将电子保单发送给投保人或被保险人的行为。

3.8 电子保单签收

指具有保单签收权的用户使用保险人告知并提供的电子保单方式获取电子保单合同的行为。

3.9 电子保单查验

指具有保单信息获知权的用户通过规范的查验渠道获知结构化数据形式的基本保单信息的行为。

3.10 电子保单下载

指具有保单获取权的用户通过规范的下载渠道获取电子保单的行为。

3.11 人脸识别

指基于人的脸部特征信息进行身份识别的一种生物识别技术。用摄像机或摄像头采集含有人脸的图像或视频流，并自动在图像中检测和跟踪人脸，进而对检测到的人脸进行脸部识别的一系列相关技术。

3.12 活体人脸

指利用活体检测技术判断提交的人脸生物特征是否由现场有生命的个体生成，并进行身份识别的技术。

4 电子保单服务安全要求

包括电子保单制单、保单生成通知、回执、查验、归档、下载场景的服务规范。

4.1 电子保单制单安全要求

电子保单生成前提包括以下内容：

a) 完成客户信息的录入；
b) 保险公司承保及客户确认承保信息；
c) 确认客户完成保险费的缴纳（保险合同另有约定或监管另有规定的除外）。

保单承保之后，电子保单生成系统开始制作电子保单，并满足以下条件：

a) 应根据客户的投保资料以及适配的模版自动生成电子保单，并在电子保单的公司签章位置进行电子签章操作。

b) 电子保单应具备通过可靠电子签名证明其是公司签发的有效保单，且具备可判定电子保单文件是否被篡改的功能。
c) 电子保单所含业务要素原则上应与相对应的纸质保单保持一致，且应保证所签发电子保单信息与签发时的核心系统信息一致。

4.2 电子保单生成通知发送安全要求

电子保单生成之后，应向投保人发送电子保单生成通知，并满足以下条件：
a) 电子保单生成通知发送至投保人，可通过短信或者邮件的形式。
b) 短信或邮件内容为提示客户电子保单已经生成，包含保单号、关系人、险种、电子保单下载方式等基本信息。

4.3 电子保单下载安全要求

电子保单下载要求如下：
a) 投保人需在登录手机客户端或网站的情况下查询电子保单。
b) 投保人只有在实名认证登录手机客户端的情况下，可下载电子保单。
c) 对保险责任终止后5年内的电子保单需提供在线下载服务；
d) 电子保单下载需使用https等安全传输通道，避免电子保单信息泄漏以及电子保单被篡改。

电子保单下载渠道可以选择：
a) 公司官方微信公众号；
b) 公司官方网站；
c) 公司官方APP；
d) 其他渠道

4.4 电子保单回执安全要求

电子保单回执需满足如下要求：
a) 投保人需在手机客户端或网站的情况下在线签收回执。
b) 投保人在线签收回执时，需确保已经收到纸质或者电子保单,并在登录手机客户端或网站时验证客户身份。
c) 投保人在线签收回执时，须在回执页手写签名，回执签收系统需采集签名者的手写签名信息等数据，形成回执签收行为证据链，并将证据链、签名者信息、电子回执单的杂凑值向CA请求数字证书，CA完成签名者身份核验，颁发数字证书。同时回执签收系统利用数字证书私钥完成电子回执单的数字签名。
d) 投保人进行线上签收时，核心系统自动接收客户签收信息进行回执核销，核销成功后记录回执日期、核销日期，并将电子回执单（含签名）影像应存储到核心系统对应的影像类型下。
e) 电子保单线上签收和纸质保单签收具有同等效力。

主要电子回执渠道可选择以下：
a) 公司官方微信公众号；
b) 公司官方网站；
c) 公司官方APP；
d) 其他渠道。

4.5 电子保单归档安全要求

在涉及电子保单归档的业务场景中，应遵循如下要求：

a) 应将电子保单归档至电子保单存储系统，并保证在存储有效期内集中可查。
b) 应保障电子文件和电子档案的信息安全。妥善保管电子保单及电子保险单证（电子投保单、电子保单等档案），建立安全、稳定的网络信息系统，确保归档的电子文件能够及时被查询调取；
c) 所有归档电子保单，保险期限在一年以上的，存储有效期为自保险合同终止之日起不少于10年，一年期及以下短期电子保单的存储有效期为自保险合同终止之日起不少于5年。

4.6 电子保单查验安全要求

电子保单查询查验要求如下：

a) 客户需在登录客户端或网站的情况下查询查验电子保单。
b) 电子保单的查询查验权限需限定为投保人。
c) 页面展示内容包含保单号信息、保险关系人基本信息、保险标的基本信息、保险责任基本信息。
d) 在查询界面展示页，涉及客户敏感信息的，如：银行账户、证件号、手机号等时应屏蔽关键字段，并用*代替。
e) 应确保查询查验时的数据安全。

查询查验渠道可以选择：

a) 公司官方微信公众号；
b) 公司官方网站；
c) 公司官方APP；
d) 其他渠道

5 电子保单信息安全规范

5.1 数据信息安全

5.1.1 防伪技术

电子保单应具备通过可靠电子签名证明其是保险公司签发的有效保单文件，且具备可判定保单文件是否被篡改的功能，不需再含有原纸质保单所要求的防伪印刷图案。

5.1.2 系统管理

应针对电子保单业务现状，按照GB/T 22080和JR/T 0033-2015的要求，制定信息安全管理方针和策略，采用风险管理的方法拟定信息安全管理计划，选择相应的安全机制，制定信息安全解决方案，集成先进的安全技术，形成可靠的安全系统。

电子保单的信息安全管理，应符合保险业务运作的实际情况，具有可操作性、可检查性。

电子保单文件在不同信息系统之间进行传输时，可采用以下方式之一：

a) 公网方式，应选用经国家密码主管部门批准的算法进行加密处理，予以保证安全性；
b) 局域网或采用专线方式（VPN），在保障足够安全性的前提下，可以不对交互报文和文件进行加密处理。

5.1.3 存储规范

电子保单文件应按照《电子签名法》和JR/T 0161-2018要求形成可证明签名人身份、签名过程不可替代、签名结果不可篡改的数字文件进行存储，并满足以下要求：

a） 电子保单的存储须可支持实时在线检索与下载；

b） 电子保单存储时间，应从电子保单签发日起，并根据《保险法》规定来设置不同保险期限的电子保单文件存储时间；

c） 存储的方式应保障足够的安全性和持久性，以防止数据丢失或被盗；

d） 应充分考虑到数据的容灾、备份与恢复。

5.1.4 网络安全等级保护

应按照《中华人民共和国计算机信息系统安全保护条例》《信息安全等级保护管理办法》《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）《信息安全技术 网络安全等级保护技术要求》（GB/T 22239-2019）等法律法规和技术标准要求，坚持科学定级、有效保护的原则，建立电子保单数据网络安全等级保护解决方案。

电子保单信息安全应包括信息的保密性、真实性、完整性及安全通信、边界防护、访问控制、入侵防范、安全审计、安全管理方面，避免内部信息受到来自内部、外部、自然等多方面因素的威胁。

电子保单发生信息丢失时，如为自然灾害、意外事故、人为错误等安全隐患造成部分或大量的信息丢失，公司应充分考虑但不限于以下信息安全保护措施：

a）数据备份：应将系统中的电子保单数据与文件复制到计算机硬盘或可移动媒体上，如磁盘、磁带、光盘等，当数据丢失或发生系统灾难时可将备份的数据恢复到系统硬盘或数据库中，以便有效地保护电子保单数据和文件；

b）数据恢复：可将备份的电子保单和文件恢复到系统硬盘或数据中；

c）容灾：在发生自然灾害等造成电子保单数据和文件丢失时，应采用有效的异地容灾方案，可在短时间内实现系统与数据的恢复，保障电子保单服务的及时正常提供。

5.2 人员信息安全

5.2.1 身份认证

公司应采用身份认证技术验证客户身份，身份认证技术可包括但不限于静态密码、动态密码、数字证书、人脸识别等技术。

公司如进行身份认证，应提供在线个人身份实名认证服务，线上实名认证途径应包括但不限于以下方式：

a）手机号三要素（身份证号、手机号、姓名）在三大运营商的一致性核对；

b）银行卡三要素（银行卡号、身份证号、姓名）在银联的一致性核对；

c）活体人脸、身份证号、姓名三要素在公安部身份证中心的一致性核对；

d）其他方式。

5.2.2 客户信息保密

公司应按照《中华人民共和国个人信息保护法》《网络安全法》要求，对外提供涉及保险客户个人信息的保险单证及相关承保理赔信息时，应能确认信息索取人的真实身份。

公司应建立健全相关客户信息保密制度，配套搭建相关技术安全体系，对提供保险服务过程中收集的投保人、被保险人、受益人及其依法委托的代办人的个人信息严格管理，防止客户信息泄露。

客户信息应实现保密性、完整性和可用性的安全目标：

a） 保密性，应阻止非授权的主体阅读敏感信息，即未认证的客户不能够获取信息，防止信息被泄露；
b） 完整性，应防止信息被未经授权的篡改；
c） 可用性，应具备认证客户在需要信息时能及时得到服务的能力。