ICS 35.020
CCS L 80

T/BJTN

团　　体　　标　　准

T/BJTN XXX—2025

健身数据安全分级指南

Guidelines for security grading of fitness data

（征求意见稿）

2025－XX－XX 发布　　2025－XX－XX 实施

北京体能训练协会　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由北京理工大学提出。

本文件由北京体能训练协会归口。

本文件起草单位：北京理工大学……

本文件主要起草人：……

健身数据安全分级指南

1 范围

本文件规定了健身数据安全分级的定级原则、目标和范围、数据安全等级、数据安全定级、核心数据识别、数据分级保护。

本文件适用于相关机构开展健身数据安全分级工作，并为第三方评估机构等单位开展数据安全检查与评估工作提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 5271.1 信息技术 词汇 第1部分：基本术语

GB/T 5271.31 信息技术 词汇 第31部分：人工智能 机器学习

GB/T 12200.1 汉语信息处理词汇 01部分：基本术语

GB/T 35273 信息安全技术 个人信息安全规范

YD/T 3082 移动智能终端个人信息保护规范

YD/T 4538 互联网医疗健康移动应用软件（APP）个人信息保护技术要求

YD/T 6221 移动应用软件个人信息保护要求和评估方法

3 术语和定义

GB/T 5271.1、GB/T 5271.31、GB/T 12200.1界定的以及下列术语和定义适用于本文件。

3.1

泛化 generalization

通过合并或扩展数据值的范围，使得单个数据点变得不那么具体和可识别。

注：这种方法可以在保留数据整体趋势和统计特性的同时，降低敏感信息的暴露风险。

3.2

部分屏蔽 partial masking

对敏感数据的某些部分进行遮掩或替换，通常保留一部分原始数据以保持一定的可读性和可用性，同时防止完全暴露敏感信息。

注：这种方式常用于处理如信用卡号、身份证号、电话号码等具有固定格式的数据。

3.3

匿名化 anonymization

通过去除或改变标识符，使得数据集中不再包含可以直接或间接识别特定个体的信息。

注：经过匿名化处理的数据应确保即使结合其他可用信息，也无法重新识别出原始数据的所有者。

3.4

假名化 pseudonymization

一种较轻度的匿名化形式，用假名或其他标识符代替直接标识符，使得数据在不访问额外信息的情况下无法直接关联到具体个人。

注：假名化并不完全消除重新识别的风险，但它显著降低了这一可能性，并且在某些情况下允许数据所有者在必要时恢复原始信息。

3.5

汇聚融合　convergence

对数据进行集中、清洗、转换、重组、关联分析、多方计算等处理的过程。

4　定级原则、目标和范围

4.1　定级原则

4.1.1　合法合规性

满足国家法律法规及行业主管部门有关规定。

4.1.2　可执行性

健身数据定级规则不过于复杂，确保健身数据定级工作的可行性。

4.1.3　时效性

健身数据安全级别具有一定的有效期限，相关健身数据所有方宜按级别变更策略对健身数据级别进行及时调整。

4.1.4　自主性

结合健身数据所有方自身数据管理需要（如计算需要、业务需要、风险接受程度等）与用户需求，在本文件的框架下自主确定健身数据安全级别。

4.1.5　差异性

根据本机构数据的类型、敏感程度等差异，划分不同的健身数据安全层级，并将健身数据分散至不同的级别中，不宜将所有健身数据集中划分到其中若干个级别中。

4.1.6　客观性

健身数据定级规则是客观且可校验的，即通过健身数据自身的属性和定级规则即可判定其级别，并且健身数据的定级是可复核和检查的。

4.2　定级目标

健身数据安全定级旨在对健身数据进行全面梳理并确立适当的数据安全分级，是对健身数据实施有效数据分级管理的必要前提和基础。健身数据分级管理是建立统一、完善的数据生命周期安全保护框架的基础工作，能够为相关健身机构和应用程序制定有针对性的数据安全管控措施提供支撑。

4.3　定级范围

在健身领域的数据收集范围中，未经电子化的健身数据应依据相关档案文件的管理规范执行；涉及个人隐私或敏感信息的健身数据，应遵守国家有关法律法规的规定。法律禁止收集和使用的相关数据不在本文件的具体规定范围内。其中，安全定级工作所涉及的健身数据包括但不限于以下几类：

a) 在提供健身产品或服务的过程中直接或间接采集的数据，包括：
   1) 通过健身房前台以纸质协议形式签署或收集，并经过信息处理后在计算机系统中流转或保存的数据；
   2) 通过移动应用程序、网站等信息系统签约或收集的电子信息；
   3) 健身者在使用健身设备时自动记录的运动数据，如跑步距离、消耗卡路里等。
b) 健身服务机构信息系统内生成和存储的数据，包括但不限于：
   1) 训练计划数据、会员信息、预约记录、消费记录、医生教练反馈等业务数据；
   2) 相关健身机构在日常管理和运营过程中采集、产生的数据，如员工考勤、财务报表、客户满意度调查、设施维护记录等经营管理数据。
c) 健身服务机构内部办公网络与办公设备（终端）中产生、交换、归档的电子数据，如机构内部的日常事务处理信息、政策与规章制度文档、业务终端临时存储的训练或管理数据、内部沟通的电子邮件等；
d) 健身服务机构原纸质文件经过扫描或其他电子化手段形成的电子数据，如会员注册表单、健康评估报告、训练进度记录等；
e) 授权体检机构出具的数据，如包含用户个人信息与体检指标的体检报告，用户体检次数、体检单位等；
f) 健身应用程序或机构提供的其他服务信息，如紧急情况报警，健身场馆推荐，医生、教练信息，问诊信息等；
g) 其他由服务机构收集的适宜进行分级管理的健身数据，如用户通过社交媒体分享的训练成果、在线论坛中的交流讨论等公开渠道获取的数据。这些数据虽然可能不是直接与健身相关，但在某些情况下也可能需要纳入安全管理和个人信息保护的范畴。

5 数据安全等级

根据健身数据安全性遭受破坏后的影响对象和影响程度，将健身数据安全级别从高到低划分为5级、4级、3级、2级、1级。健身数据安全性遭受破坏后的影响对象和影响程度按6.1、6.2判定。各级别的特征如下：

a) 5 级健身数据：
   1) 为核心数据，通常用于国家相关管理机构或相关央国企、事业单位，如卫健委、医保局中的数据，国家安全机关中的数据，涉密档案中的健身数据等。一般仅对特定国家机关工作人员公开，且仅为必须知悉的对象访问或使用，如使用需征得相关部门授权，且严格遵循相关法律与规章制度；
   2) 数据安全性遭到破坏后，会对公共健康安全、社会秩序造成严重影响。
b) 4 级健身数据：
   1) 为重要数据，通常用于大型或特大型健身服务机构的重要业务，如健康监测数据、个人健康记录等，一般仅对特定工作人员公开，且仅为必须知悉的对象访问或使用；
   2) 个人健康信息中的敏感信息：如详细的病历记录、遗传信息、财产信息、账户信息等；
   3) 数据安全性遭到破坏后，可能对社会秩序造成影响，或对个人隐私或企业合法权益造成严重影响，但不影响公共健康安全。
c) 3 级健身数据：
   1) 为重要数据，用于健身服务机构的关键或重要业务，如会员管理系统的数据，一般仅对特定人员公开，且仅为必须知悉的对象访问或使用；

2) 个人健康信息中的较敏感信息与个人信息：如非常规体检结果、手机号、身份证号、家庭住址等；
3) 数据安全性遭到破坏后，可能对社会秩序造成轻微影响，或对个人隐私或企业合法权益造成一般影响，但不影响公共健康安全。

d) 2级健身数据：
1) 为一般数据，用于健身服务机构的一般业务，如内部管理数据、会员基本信息等，通常仅对内部员工公开，不宜广泛传播；
2) 个人健康信息中的普通信息：如身高、体重、年龄、血压等；
3) 数据安全性遭到破坏后，可能对个人隐私或企业合法权益造成轻微影响，但不影响公共健康安全和社会秩序。

e) 1级健身数据：
1) 为公开数据，一般可被公开或被公众获知、使用的数据，如健身俱乐部或健身场馆的营业时间和地址、健康医生的可预约时间、公开的健身知识等；
2) 个人健身信息主体主动公开的信息：如个人在健身手机软件或其他社交媒体上分享的健身心得、运动照片等；
3) 数据安全性遭到破坏后，可能对个人隐私或企业合法权益不造成影响，或仅造成微弱影响，但不影响公共健康安全和社会秩序。

6 数据安全定级

6.1 定级要素

6.1.1 概述

安全性（保密性、完整性、可用性）是信息安全风险评估中的重要参考属性。健身数据安全性遭到破坏后可能造成的影响（如可能造成的危害、损失或潜在风险等），是确定健身数据安全级别的重要判断依据，主要考虑影响对象与影响程度两个要素。

6.1.2 影响对象

影响对象指当该领域的机构数据安全性受到破坏后，可能受到影响的方面，这些方面包括公共健康安全、个人健身权益、个人隐私以及企业的合法权益等。影响对象的确定主要考虑以下内容：

a) 影响对象为公共健康安全的情况：当健身数据的安全性遭到破坏后，可能对公共卫生政策制定、疾病预防控制、紧急医疗救援、体育设施的安全使用等方面产生不利影响，进而威胁到整个社会的健身水平和公共安全；
b) 影响对象为个人健身权益的情况：当健身数据的安全性遭到破坏后，可能对个人的健身记录、运动习惯、营养摄入等信息的准确性和完整性造成损害，从而影响个人的健康管理决策和个人健身权益；
c) 影响对象为个人隐私的情况：当健身数据的安全性遭到破坏后，可能泄露个人的身体状况、疾病史、运动偏好等敏感信息，导致个人隐私受到侵犯；
d) 影响对象为企业合法权益的情况：当健身数据的安全性遭到破坏后，可能对提供健身服务或健身管理服务的企业造成负面影响，如客户信任度下降、品牌形象受损、商业秘密泄露等，进而影响企业的正常运营和发展。

6.1.3 影响程度

影响程度指当健身数据安全性遭到破坏后所产生的影响大小，从高到低划分为严重损害、一般损害、轻微损害和无损害。影响程度的划分可参见表1，作为评估健身数据安全性破坏后影响程度的依据。确定影响程度时，应综合考虑数据类型、数据特征与数据量等因素，并结合健身服务的特点来判断数据安全性受损后的实际影响。例如：

a) 健身数据安全性遭到破坏后，个人健康信息（如疾病史、体检报告等）产生的影响程度通常要高于非敏感基本信息（如身高、体重等）；

b) 健身数据安全性遭到破坏后，用于身份验证的信息（如登录密码、生物识别数据等）产生的影响程度通常要高于个人的基本生活信息（如饮食偏好、运动频率等）；

c) 在健康监测数据中，对于需要即时反馈的数据（如心率监测、血压变化等），其安全性遭到破坏产生的影响程度通常要高于那些不需要即时处理的数据（如定期的身体质量指数 BMI 记录等）。

表1 影响程度说明

影响程度	说 明
严重损害	a）可能导致危及公共健康安全的重大事件，如泄露大量用户的健康信息，可能引发社会恐慌，或对公共卫生政策的制定和执行造成重大障碍，损害国家和社会的整体健康利益； b）可能导致严重危害社会秩序和公共利益的情况，如因健身数据大规模泄露而引发的大范围公众不满或投诉，甚至导致对健身场所、健康服务机构的信任危机，影响社会稳定和谐； c）可能导致健身服务机构受到监管机构的严厉处罚，或因为健身数据泄露事件导致关键业务流程中断，如在线预约系统故障、会员资料管理混乱等，严重影响机构的正常运营和服务质量； d）可能导致重大的个人健康信息安全风险，如未经同意公开个人健康状况、疾病史等敏感信息，严重侵犯个人隐私权，给个人带来心理压力和社会歧视等问题，危害个人的合法权益
一般损害	a）可能导致危害社会秩序和公共利益的事件，如引发区域性集体投诉或诉讼事件，或者因大规模用户健康信息泄露而导致健康市场的秩序混乱，影响公众对健康服务的信任； b）可能导致健身服务机构受到监管部门的处罚，或者因为健身数据安全事件影响某些业务的正常运作，如线上健身咨询、预约服务中断等，降低服务质量，损害用户体验； c）可能导致一定规模的个人健身信息泄露或滥用等安全风险，对个人隐私权和健康权益造成一定影响，如导致个人健康状况被不当利用，增加个人面临的社会和心理压力
轻微损害	a）可能导致个别投诉或诉讼事件，使健身服务机构的经济利益和声誉受到轻微损害； b）可能导致健身服务机构的部分服务或业务暂时中断，如在线预约、健身咨询服务等，影响用户体验和服务满意度； c）可能导致超出个人客户授权范围的数据加工、处理或使用情况，对个人的隐私权和健身权益造成部分或潜在的影响，如未经授权的健身数据共享或分析可能引发个人的不安和不信任
无损害	对企业合法权益和个人隐私等不造成影响，或仅造成个别微弱影响，且不会影响公共健康安全、社会秩序、健身市场秩序或健身服务机构各项业务的正常开展

6.2 要素识别

6.2.1 安全影响评估

6.2.1.1 总则

安全影响评估应综合考虑健身数据类型、健身数据内容、健身数据规模、健身数据来源、机构职能和业务特点等因素，以评估健身数据安全性（保密性、完整性、可用性）遭受破坏后可能造成的影响。评估过程中，应根据实际情况识别各项安全性在影响评定中的优先级，分别进行保密性、完整性和可用性评估，并综合考虑三方面的评估结果，形成最终的安全影响评估。

6.2.1.2 保密性评估

保密性评估评价健身数据遭受未经授权披露的影响，以及机构继续使用这些数据可能产生的影响。评估内容包括但不限于：

a) 健身数据未经授权披露，可能对公共健康安全、社会秩序、个人隐私及企业合法权益造成的损害，以及损害的严重程度；
b) 健身数据被非授权对象获取或利用，可能对公共健康安全、社会秩序、个人隐私及企业合法权益造成的损害，以及损害的严重程度；
c) 健身数据被非授权对象用于非法目的，如窃密、篡改、销毁或拒绝服务攻击，可能对公共健康安全、社会秩序、个人隐私及企业合法权益造成的损害，以及损害的严重程度；
d) 健身数据的未经授权披露或传播是否违反国家法律法规、行业主管部门的规定或机构内部管理制度。

6.2.1.3 完整性评估

完整性评估评价健身数据遭受未经授权修改或损毁的影响，以及机构继续使用这些数据可能产生的影响。评估内容包括但不限于：

a) 健身数据未经授权修改或损毁，可能对公共健康安全、社会秩序、个人隐私及企业合法权益造成的损害，以及损害的严重程度；
b) 健身数据未经授权修改或损毁，可能对其他组织或个人造成的损害，以及损害的严重程度；
c) 健身数据未经授权修改或损毁，可能对企业或机构的职能履行、公信力造成的损害，以及损害的严重程度；
d) 健身数据未经授权修改或损毁是否违反国家法律法规、行业主管部门的规定或机构内部管理制度。

6.2.1.4 可用性评估

可用性评估评价健身数据及其经组合/融合后形成的各类数据出现访问或使用中断的影响，以及机构无法正常使用这些数据可能产生的影响。评估内容包括但不限于：

a) 健身数据的访问或使用中断，可能对公共健康安全、社会秩序、个人隐私及企业合法权益造成的损害，以及损害的严重程度；
b) 健身数据的访问或使用中断，可能对企业或机构的职能履行、公信力造成的损害，以及损害的严重程度；
c) 健身数据的访问或使用中断，可能对其他组织或个人造成的损害，以及损害的严重程度；
d) 健身数据的访问或使用中断是否违反国家法律法规、行业主管部门的规定或机构内部管理制度。

6.2.2 定级要素识别

通过综合考虑保密性、完整性和可用性的影响评估结果，识别健身数据安全定级关键要素，即作为最终健身数据安全级别评定时所使用的主要影响对象及影响程度，并根据6.3定级规则进行健身数据安全级别的评定。定级要素识别宜至少满足：

a) 因不同健身数据在安全性（保密性、完整性、可用性）方面有不同侧重，以所侧重的安全性评估结果，作为相应健身数据安全定级的主要依据；
b) 健身数据的保密性、完整性和可用性要求基本一致的，重点以保密性评估所确定的定级要素为主要定级依据。

6.3 定级规则

6.3.1 健身领域，数据安全级别划分的通用规则包括但不限于：
a) 重要数据的安全等级不应低于本文件所述的 5 级；
b) 个人健身信息相关数据按 GB/T 35273、YD/T 3082、YD/T 4538、YD/T 6221 及相关健身数据个人信息保护的要求进行定级，并在数据安全定级过程中从高考虑；
c) 对于数据体量大，涉及的用户多、涉及用户数据量大、涉及多行业及多机构用户的情况，影响程度宜从高确定。

6.3.2 数据安全级别划定规则参见表 2，数据定级规则参见附录 A。

表2 健身数据安全定级规则参考表

最低安全级别参考	定级要素	
	影响对象	影响程度
5	国家安全	严重损害/一般损害/轻微损害
	公众权益	严重损害
4	公众权益	一般损害
	个人隐私	严重损害
	企业合法权益	严重损害
3	公众权益	轻微损害
	个人隐私	一般损害
	企业合法权益	一般损害
2	个人隐私	轻微损害
	企业合法权益	轻微损害
1	国家安全	无损害
	公众权益	无损害
	个人隐私	无损害
	企业合法权益	无损害

6.4 定级过程

6.4.1 组织保障

6.4.1.1 健身数据分级工作的领导组织及其负责人：
a) 职责：主要负责统筹和规划健身数据安全分级工作，确保各项工作有序开展；
b) 任务：制定健身数据安全分级的整体策略，审批重要决策，监督实施进度。

6.4.1.2 健身数据分级工作的管理部门（或组织）及其负责人：
a) 职责：主要负责健身数据分级相关工作的组织、协调、管理和审核等；
b) 任务：制定具体的分级标准和流程，组织相关部门进行数据分类，审核分级结果，确保分级工作的准确性和一致性。

6.4.1.3 信息科技部门及其负责人在健身数据安全分级工作中的角色：

a) 职责：主要负责落实健身数据安全分级的相关要求，并主导技术层面的实施工作；
b) 任务：开发和维护健身数据分类系统，确保健身数据存储和传输的安全性，提供技术支持和培训，协助解决技术问题。

6.4.1.4 业务部门（和/或数据属主管部门）及其负责人在健身数据安全分级工作中的角色：

a) 职责：主要负责落实健身数据安全分级的相关要求，并协同开展健身数据安全分级实施工作；
b) 任务：提供健身数据的具体信息，参与健身数据分类的评审和确认，确保分类结果符合业务需求。

6.4.1.5 其他相关部门在健身数据安全分级工作中的角色、职责及负责人：

a) 职责：根据各自的专业领域和职能，支持健身数据分级工作的顺利进行；
b) 任务：提供必要的支持和资源，参与健身数据分类的讨论和评审，确保跨部门协作的有效性。

6.4.2 制度保障

建立健身数据分级工作的相关制度，明确并落实相关工作要求，包括但不限于：

a) 分级的目标和原则；
b) 分级工作涉及的角色、部门及相关职责；
c) 分级的方法和具体要求；
d) 分级的日常管理流程和操作规程，以及分级结果的确定、评审、批准、发布和变更机制；
e) 分级管理相关绩效考核和评价机制；
f) 分级结果的发布、备案和管理的相关规定；
g) 分级清单审核与修订的原则和周期。

6.4.3 定级流程

健身数据定级流程基本步骤如下：

a) 健身数据资产梳理：对健身数据进行盘点、梳理与分类，形成统一的健身数据资产清单，并进行健身数据安全定级合规性相关准备工作；
b) 健身数据安全定级准备：
   1) 明确健身数据定级的颗粒度（如库文件、表、字段等）；
   2) 识别健身数据安全定级关键要素。
c) 健身数据安全级别判定：
   1) 按 6.3 定级规则，结合国家及行业有关法律法规、部门规章，对健身数据安全等级进行初步判定；
   2) 综合考虑数据规模、数据时效性、数据形态（如是否经汇总、加工、统计、脱敏或匿名化处理等）等因素，对健身数据安全级别进行复核，调整形成数据安全级别评定结果及定级清单。
d) 健身数据安全级别审核：审核健身数据安全级别评定过程和结果，必要时重复 c）及其后工作，直至安全级别的划定与数据安全保护目标一致；
e) 健身数据安全级别批准：由健身数据安全管理最高决策组织对健身数据安全分级结果进行审议批准。

6.4.4 级别变更

健身数据安全定级完成后，出现下列情形之一时，健身相关机构宜对相关健身数据的安全级别进行变更，健身数据安全级别变化示例参见附录B，并按照6.4.3定级流程实施：

a) 健身数据内容发生变化，导致原有健身数据的安全级别不适用变化后的健身数据；
b) 健身数据内容未发生变化，但因数据时效性、数据规模、数据使用场景、数据加工处理方式等发生变化，导致原定的健身数据安全级别不再适用；
c) 因健身数据汇聚融合，导致原有健身数据安全级别不再适用汇聚融合后的健身数据；
d) 因国家或行业主管部门要求，导致原定的健身数据安全级别不再适用；
e) 需要对健身数据安全级别进行变更的其他情形。

7 核心数据识别

健身服务机构在识别和认定核心健身数据时，应遵守国家及行业主管部门的相关规定。核心数据的性质和内容参见附录C，这些描述旨在帮助服务机构更好地理解和识别核心数据。核心数据的安全级别不宜低于本文件中确定的5级。

8 数据分级保护

8.1 保护原则

8.1.1 分级分类

对所有健身数据进行详细的隐私影响评估，以确定其敏感性和潜在的风险。根据评估结果将健身数据分为不同的隐私等级：公开、内部使用、敏感、高度敏感等。

8.1.2 保护强度与隐私程度成比例

隐私保护方案的选择应与健身数据的隐私等级成正比，即越敏感的健身数据应采取越严格的保护措施。确保所采取的安全措施不会过度限制健身数据的合法使用。

8.1.3 动态调整

健身数据的价值和风险会随时间变化，应对健身数据的隐私等级定期审查，并相应地调整保护策略。当发生健身数据泄露或其他安全事件时，应及时重新评估受影响健身数据的隐私等级并加强保护措施。

8.1.4 技术与管理结合

结合使用技术和管理手段保障健身数据安全，如加密、访问控制、审计跟踪等技术措施，以及制定内部政策、培训员工等管理措施。对于高隐私级别的健身数据，可能需要额外的技术保护措施，如多重身份验证、数据屏蔽、匿名化或假名化处理。

8.1.5 透明度与用户同意

在收集、存储、处理个人数据前，应向用户提供清晰的信息说明，并获取其明确同意。用户有权知晓他们的数据被如何处理，以及他们可以行使哪些权利（如访问权、删除权）。

8.1.6 合规性

所有的隐私保护措施应遵守适用的法律法规，包括但不限于《网络安全法》、《数据安全法》、《中华人民共和国个人信息保护法》、行业标准及其他相关法规，并定期进行合规性检查。

8.1.7 持续改进

8.1.7.1 应建立用于收集关于健身数据保护实践的意见和建议的反馈机制，并不断优化保护流程。

8.1.7.2 应关注国内外数据保护领域的最新发展和技术进步，适时更新组织的健身数据保护策略。

8.2 保护需求

健身数据各级别的隐私保护需求如下：

a) 5 级数据：
   1) 访问限制：仅限特定国家机关工作人员访问，且应经过相关部门授权，确保只有在必要情况下，经批准的人员才能接触这些数据；
   2) 保护程度：提供最高等级的保护措施，防止未经授权的访问、使用或泄露。任何操作都应遵循相关规定。不应在非涉密环境中处理或保留原始数据，所有中间数据应立即销毁；
   3) 数据收集：仅相关国家机关及授权工作人员进行收集与存储；
   4) 数据传输：仅在保密环境下进行传输；
   5) 数据公开：包括密文在内的所有衍生结果仅能在不涉密的情况下对外透露；
   6) 隐私与可用性平衡：在不影响公共健康安全和社会秩序的前提下，最大限度地保护个人隐私，在内部处理过程中宜减少对敏感信息的直接暴露。
b) 4 级数据：
   1) 访问限制：仅对特定工作人员公开，且仅为必须知悉的对象访问或使用，只允许最少数量的人接触健身数据；
   2) 保护程度：提供高级别的保护措施，确保健身数据的安全性和完整性不受威胁。不应在数据源之外保留原始数据，所有处理过的中间数据应立即销毁；
   3) 数据收集：仅国家授权的企业与机构进行收集与存储，且应征得用户同意；
   4) 数据传输：仅在加密或脱敏环境下进行传输；
   5) 数据公开：包括密文在内的所有可复原的数据处理结果不应对外公开，但可公开哈希、差分等不可复原的结果；
   6) 隐私与可用性平衡：在不影响业务运作的前提下，最大限度地保护个人隐私，内部处理过程中宜减少对敏感信息的直接暴露。
c) 3 级数据：
   1) 访问限制：仅对需要知悉的特定人员开放，实施严格的权限管理和审核机制；
   2) 保护程度：提供适度的保护措施，确保健身数据不会被不当访问或滥用，对于非必要的敏感信息，宜减少其可见性和传播范围；
   3) 数据收集：仅在征得用户同意的情况下进行收集与存储；
   4) 数据传输：仅在加密或脱敏环境下进行传输；
   5) 数据公开：不应公开数据明文，包括无法定位到个人的健身数据，但可公开数据密文以及具有一定信息损失的，无法复原的，经匿名、泛化后的数据明文；
   6) 隐私与可用性平衡：确保健身数据在保护隐私的同时仍然可以用于合法目的，如健身研究和服务改进。避免不必要的信息暴露，同时支持合理的数据分析。
d) 2 级数据：
   1) 访问限制：通常仅对内部相关人员公开，不宜广泛传播，确保相关人员了解并遵守相关的保密规定；
   2) 保护程度：提供基本级别的保护措施，确保健身数据在内部流转时的安全性。对于外部发布或共享，应事先获得适当的审批与用户同意；
   3) 数据收集：仅在征得用户同意的情况下进行收集与存储；
   4) 数据传输：可在公开环境中进行传输，但用户信息与表头等内容应保密；

5) 数据公开：不应公开全量健身数据与用户信息，但可公开处理后无法精确定位到用户的原始数据，或具有一定信息损失的，无法复原的，经匿名、泛化后的用户信息；
6) 隐私与可用性平衡：在不侵犯用户权益与个人隐私，不会泄露用户信息，且征得用户同意的情况下保证健身数据的可用性。

e) 1 级数据：
1) 访问限制：可被全体公众获知和使用；
2) 保护程度：由于这些健身数据已经公开或由主体主动分享，因此不需要特别的技术保护，但仍需确保公开的健身数据准确无误；
3) 数据收集：所有公开健身数据可直接收集与存储；
4) 数据传输：可在公开环境中进行传输；
5) 数据公开：所有健身数据均可直接公开，但一次性发布大量信息或将信息向境外传输，应提前获得相关部门或机构的许可，并确保过程符合相关规定。未经用户同意，不应以广告等形式主动增加部分健身的曝光程度。公开内容不包括健身数据分析结果；
6) 隐私与可用性平衡：宜保障健身数据可用性，无须考虑隐私性要求。但对于用户主动公开的信息，应提供清晰的选择加入/退出选项，让用户能自主决定其信息的可见程度。确保公开健身数据不包含敏感个人信息。

8.3 保护方法

健身数据保护方法参见附录D。

附 录 A
（资料性）
数据定级规则

典型健身数据的定级规则如表A.1所示。实际应用过程中，各健身服务机构应根据其所管辖健身数据的类型、特性、规模以及机构特性等因素，综合考虑本机构健身数据安全管理的总体目标和安全策略要求，按照一定的颗粒度对健身数据资产进行合理的梳理、归类和细分，最终确定健身数据的安全级别划分清单。此外，健身服务机构所承载的重要数据的安全级别不宜低于本文件确定的5级。重要数据的识别、认定及保护工作应依据国家及行业主管部门的有关规定执行。

表A.1 健身数据安全定级参考

数据内容	数据主体	内容举例	最低安全级别参考
涉密数据	个人	所有涉及国家秘密的内容，依照《中华人民共和国保守国家秘密法》执行	5
	机构		5
	其他		5
敏感数据	个人	指纹、虹膜、人脸识别等身份验证信息，各类密码及短信验证码，个人征信信息、犯罪记录、患病史、住院记录、医嘱等生病医治过程中产生的相关记录数据，账单、消费记录、纳税信息等财产及收入信息，准确的定位信息	4
	机构	数据存储位置与方式、系统维护情况与安全报告、系统管理员信息、密码与验证信息、系统架构等涉及数据安全的内容	4
	其他	不涉及国家秘密，但是不适宜公开的健身调研、统计、计算结果，涉及个人敏感信息的模型训练结果与参数	4
重要数据	个人	与疾病相关的敏感体检指标，明显异于常人的身高、体重、血型等体检数据，饮食习惯、生活习惯及心理状况，身份证及其他证件号码、电子邮件、家庭住址、电话号码、社交媒体账号、学号、联系人及社交关系，涉及非公开个人信息的文本	3
	机构	员工编号、员工联系方式、家庭住址等员工精确信息，不公开的内部财务数据、运营策略等	3
	其他	涉及个人信息的比赛数据，不适宜播出的直播片段	3
隐私数据	个人	健身爱好者、健身达人等分类标签，身高、体重、身体质量指数BMI、血压、肺活量等非敏感体检指标，性别、民族、国籍、籍贯、婚姻状况等基本信息，毕业学校、政治面貌、工作单位及职务等身份信息，非公开的睡眠时间、运动时长、跑步距离、心跳、脉搏等健身健康信息，健身记录	2
	机构	未确定的场所营业开放日期，健身设备库存，医生、教练等在岗与休假情况，未到公示或已超公示时间的相关信息，员工工资、机构规模等不能精确定位，但是不适宜公开的信息	2
	其他	非公开的、不涉及个人信息的比赛数据，未播出的直播片段	2
公开数据	个人	在公开平台分享的健身心得及发表的评论，上传的视频、音频等健身知识，账户昵称及发言时所在的省份，在网络上选择公开的所有包括性别、年龄等个人信息，其他依据法律需要公开或公示的内容	1
	机构	健身场所运营时间、地址等需要公开的信息，场所预订情况，相关咨询热线，法定代表人姓名、名称、统一社会信用代码、经营许可证、行业分类等单位基础概况数据	1

表A.1 健身数据安全定级参考（续）

数据内容	数据主体	内容举例	最低安全级别参考
公开数据	其他	可公开查询的健身知识，公开的健身课程视频、音频、网址、介绍信息等，公开的健身比赛相关信息，相关法律、政策、规定及统计、计算的结果、报告，手机软件隐私条款与用户协议等需要公开的内容	1

附 录 B
（资料性）
健身数据安全级别变化示例

B.1 导致数据发生升降级的主要技术手段有数据脱敏、删除关键字段、汇聚融合等。

B.2 脱敏后产生的数据，其安全级别通常低于脱敏前的数据。

B.3 经过不同的数据汇聚融合处理手段所产生的健身数据，其安全级别可能上升，也可能下降。

B.4 因数据脱敏或汇聚融合导致健身数据安全级别发生变更的示例，如表 B.1 所示。

表B.1 健身数据安全级别变化

措 施	安全级别调整
汇聚融合	3级升至4级
生产健身数据脱敏后用于健身健康机构内部业务经营或管理工作	3级降至2级
汇聚融合，特定机构特定时间或事件后信息具有高安全等级	2级升至4级
脱敏，从健身数据中去除能够直接定位到个人主体的内容，删除涉及商业秘密的内容等，特定时间或事件后信息失去原有敏感性	4级降至2级
涉及用户为 14 岁以下未成年人	2级升至4级，3级升至4级
对健身数据内容进行分析或统计，得出结论	以健身数据结果敏感度为准

附 录 C
（资料性）
健身核心数据的性质和内容

C.1 健身核心数据是指在我国境内由政府、企业或个人收集、产生的涉及国家秘密，或与公共健康安全、社会发展及公共利益密切相关的加深数据（包括原始数据和衍生数据）。一旦这些健身数据未经授权披露、丢失、滥用、篡改或销毁，或经过汇聚、整合、分析后，可能造成以下后果：

a) 导致公共卫生危机，影响社会秩序和公共安全；
b) 影响关键医疗设施、健康信息系统的安全，导致健身服务中断或数据泄露；
c) 扰乱健身市场秩序，影响行业的健康发展；
d) 通过健身数据分析推断出涉密敏感信息；
e) 影响或危害其他公共安全事项。

C.2 健身核心数据可包括但不限于以下几类：

a) 宏观特征数据：
   1) 描述：反映不可更改或长时间保持稳定的健身特征、社会特征的数据；
   2) 示例：全国性的健身统计数据等。
b) 海量信息汇聚得到的衍生特征数据：
   1) 描述：通过大量健身信息汇聚、整合、分析后得到的数据；
   2) 示例：覆盖多地区的健身消费者真实健身记录和运动数据。
c) 行业监管机构决策和执法过程中的数据：
   1) 描述：行业监管机构在履职或执法过程中收集和产生的涉及国家秘密或可能产生严重影响的未公开的受控健身数据；
   2) 示例：监督检查记录、行政处罚决定书等。
d) 关键信息基础设施网络安全缺陷信息：
   1) 描述：涉及关乎国家安全的健身信息系统关键基础设施的网络安全漏洞信息；
   2) 示例：健身信息系统的安全漏洞报告、软件缺陷信息等。

C.3 不属于健身核心数据的范围：

a) 不涉及国家机构或关键国央企的生产经营和内部管理信息；
b) 不涉密的个人信息，除非这些信息的泄露会对公共健康安全或社会秩序造成严重影响；
c) 所有需要面向全社会公开或公示的信息。

附 录 D
（资料性）
健身数据保护方法

表D.1提供了典型健身数据保护方法的参考。对于隐私等级较低的数据，采用较为通用的方式进行传输与存储，可以同时实现保护隐私与不影响健身数据的可用性。而对于隐私等级较高的健身数据，必要时根据不同需求采取不同的保护方式代替加解密操作，满足健身数据隐私性和可用性的需求。

表D.1 健身数据保护方法

安全级别	数据需求	数据示例	保护方法
5	略	所有涉密数据	略
4	公开发布	所有4级数据	部分屏蔽（高强度）
4	统计计算	包括极度敏感的体检指标，账单、纳税信息、位置信息等在内的所有4级数据	差分隐私
4	模型训练	所有4级数据	联邦学习
4	内容比对/判断	用户密码、身份验证信息在内的所有4级数据	哈希
4	精确计算	极度敏感的体检指标，账单、纳税信息、位置信息等在内的所有4级数据	同态加密计算
3	内容比对/判断	用户姓名、身份证号在内的所有3级数据	哈希
3	公开发布	明显异于常人的身高、体重、血型等数值型体检数据	匿名化/泛化
3	公开发布	个人姓名、身份证号、家庭住址、电子邮件、电话号码、社交媒体账号、学号等长文本类信息	部分屏蔽
3	精确计算	与疾病相关的敏感体检指标，明显异于常人的身高、体重、血型等数值型体检数据在内的所有3级数据	加密
2	公开发布	性别、民族、国籍、籍贯、婚姻状况等非精确基本信息，非公开的睡眠时间、运动时长、跑步距离等健身健康信息在内的所有2级数据	匿名化/假名化/泛化
2	精确计算	用户身高、体重、身体质量指数BMI、血压、脉搏、肺活量等非敏感体检指标等在内的所有2级数据	元数据隐藏
1	公开数据	所有用户主动公开或可在网络上公开查询到的内容在内的所有1级数据	无须保护