PSCI PHARMACEUTICAL SUPPLY CHAIN INITIATIVE
Building responsible supply chains

2025 PSCI China Supplier Conference
PSCI 中国供应商大会（上海）

PSCI审计/AI应用中的信息安全与隐私数据保护

Information Security & Personal Data Protection in PSCI Audits/AI Application

麦璐 | 资深技术经理 | 德国莱茵TÜV

Minnie Mai | Senior Technical Manager | TÜV Rheinland

嘉宾介绍 Speaker Bio

- 姓名：麦璐
- 职位：资深技术经理
- 公司：德国莱茵TÜV
- 联系方式：(86) 138 0252 0004

- 背景：麦璐女士毕业于中山大学化学与化学工程学院，在企业社会责任和可持续发展审核领域拥有超过20年的专业经验，帮助多个品牌对供应链的社会责任及可持续发展表现进行管理，包括但不限于：
  - 供应商行为守则，供应商行为标准和供应商行为指南编写
  - 定制化风险评估工具开发
  - 供应链风险评估和分级管理项目执行
  - 审核方法论及审核工具的设计
  - 现场审核的执行
  - 供应链能力建设

议程 Agenda

Why it matters?

What it is?

How to identify and mitigate the risks?

What to do when using AI?

Key takeaway

Q&A

议程 Agenda

Why it matters?

What it is?

How to identify and mitigate the risks?

What to do when using AI?

Key takeaway

Q&A

迄今为止全球最大数据泄露罚款案例

2024/2025部分医疗行业个人信息泄露案例

Change Healthcare攻击事件于2024年2月22日首次披露，**美国医疗保健系统持续数周的大规模中断。为应对勒索软件攻击而被迫关闭IT系统**，使**许多药店和医院以及其他医疗保健设施和办公室无法处理索赔和接收付款。**2024年6月，Change Healthcare承认有敏感的患者医疗数据在这次攻击中暴露，具体可能涉及**诊断、药物、测试结果、图像、护理和治疗方案等。**

Ascension是**美国最大的医疗系统之一**，该公司于2024年5月透露，由于**一名员工无意中下载了恶意软件**，致使其遭受**勒索软件攻击。**此次攻击影响了**MyChart电子健康记录系统、电话**和用于订购测试、手术和药物的系统。

2024年6月，**英国病理实验室Synnovis**遭受网络攻击，导致**数周内患者服务广泛中断。**黑客攻击后，依赖该实验室的**地方国民健康服务信托基金推迟了数千次手术和医疗程序**，促使英国卫生部门宣布重大事件。这次攻击盗取了**3亿条与患者互动相关的数据。**

2024年6月，**澳大利亚电子处方服务公司MediSecure**，在5月份的大规模数据泄露事件（**6.5TB的患者和医生信息在黑客论坛上出售**）后进入**运营清算**状态，由咨询公司接手了管理权和清算权。

2024年11月的消息，在一名名为“nears”的威胁行为者利用了属于**法国医院Aléo Santé**的特权**MediBoard**帐户后，一场网络攻击泄露了**758,912名患者的医疗记录。**MediBoard是**Softway Medical Group**的**电子患者记录（EPR）解决方案**，为法国的多个医疗机构提供服务。被盗数据包括患者的**全名、出生日期、地址、联系方式、医生信息、处方和健康卡历史。**

南加州医疗服务提供商PIH Health于12月1日遭遇**勒索软件**攻击，黑客入侵其**三家医院及相关机构的网络系统**，声称窃取了**1700万患者记录**，并威胁公开。此次攻击导致PIH Health的**IT和电话系统中断**，迫使其采取**纸质临时流程，部分手术和检查被取消，药品处方服务受限。**

2024-12-16，**医疗软件服务公司Phreesia**通知**超过91 万用户**，其旗下子公司 **ConnectOnCall** 遭遇数据泄露。据信，泄露信息包括患者与医疗服务提供者的沟通内容，如**姓名、电话号码、出生日期、病历号、健康状况、治疗和处方信息，部分还涉及社会安全号码。**

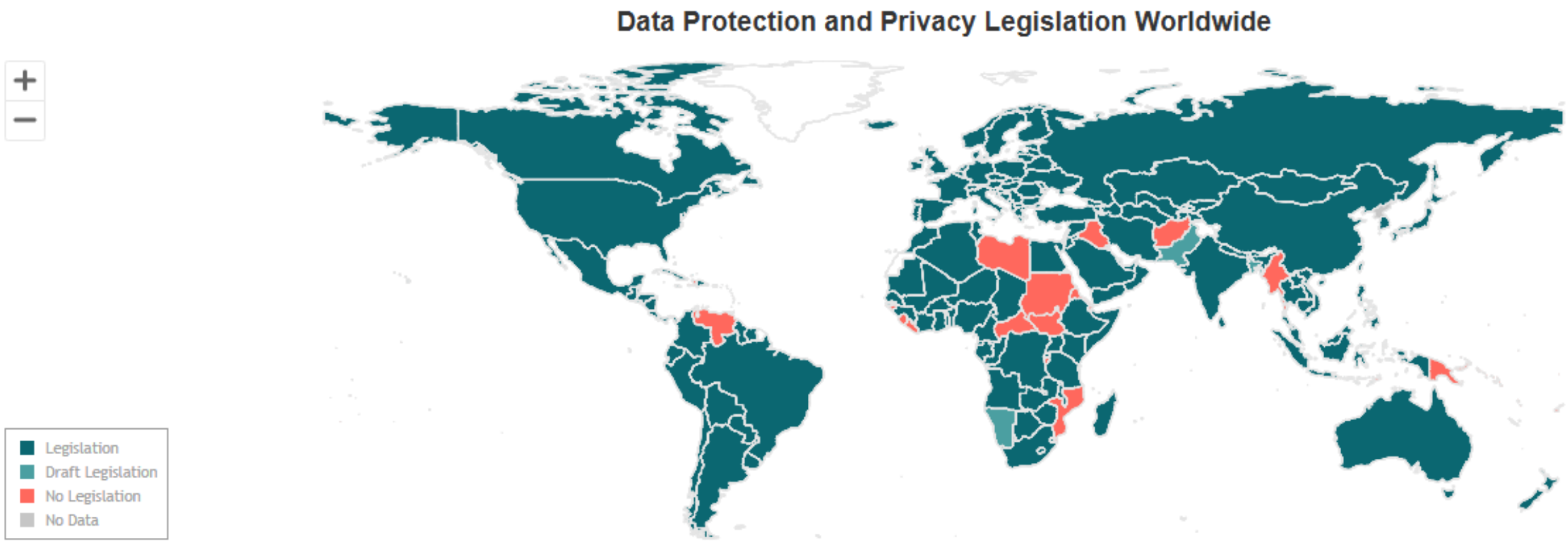
2024-12-16，**德克萨斯理工大学健康科学中心及其埃尔帕索分支机构网站**遭到**网络攻击**，导致约 **146.5 万患者**数据泄露。据信泄露信息包括**全名、出生日期、地址、社会安全号码、健康保险信息、医疗记录等。**

2024年12月，有网络安全研究员在vpnMentor发布消息，声称发现**加拿大眼科技术公司Care1**的**未受保护数据库**泄露了约**4.8百万条患者记录。**暴露信息包括**患者姓名、地址、病历、个人健康编号(PHN)及详细的眼科检查报告。**这些报告以PDF格式保存，包含**医生笔记和眼部图像**，同时还发现包含**患者家庭住址及健康数据的CSV和XLS文件。**Care1是一家专注于眼科人工智能技术的眼科技术公司，与170多家验光师合作，管理超过**15万次患者访问。**

2025年年初，黑客组织攻击并泄露了**美国社区健康中心（CHC）**的数据，涉及**超过100万名患者**的个人和医疗信息。CHC位于美国康涅狄格州，是该地区领先的医疗保健提供者，提供初级保健、牙科、行为健康及专业医疗服务。被泄露的数据可能包括**患者姓名、出生日期、联系方式、诊断信息、治疗记录、测试结果、社会保险号及健康保险详情。**

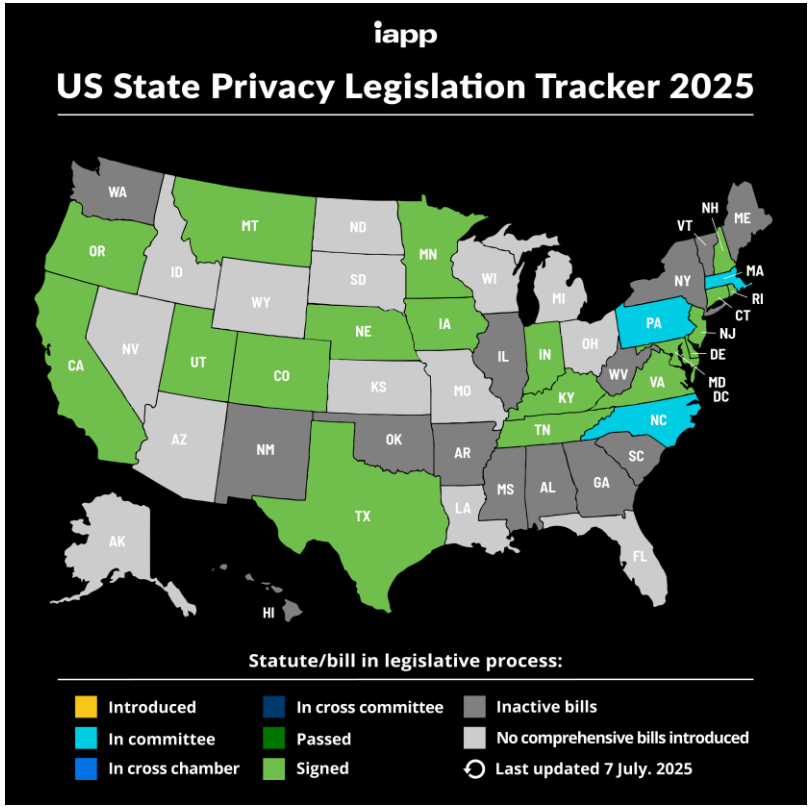
2025 年2月18日 一名网络安全专家在 Website Planet上发布消息，声称发现**DM Clinical Research位于德克萨斯州的临床试验中心网络的医疗保健数据库无需任何加密、密码保护或安全身份验证即可在线公开访问**，该数据库包含**超过160万条**与医学调查相关的记录，包括个人和医疗信息的宝库，包括**姓名、出生日期、电话号码、电子邮件地址、疫苗接种状态和当前药物。**一些调查甚至包括**有关 COVID-19 疫苗不良反应、医生姓名以及个人是否正在节育或怀孕的注释。**

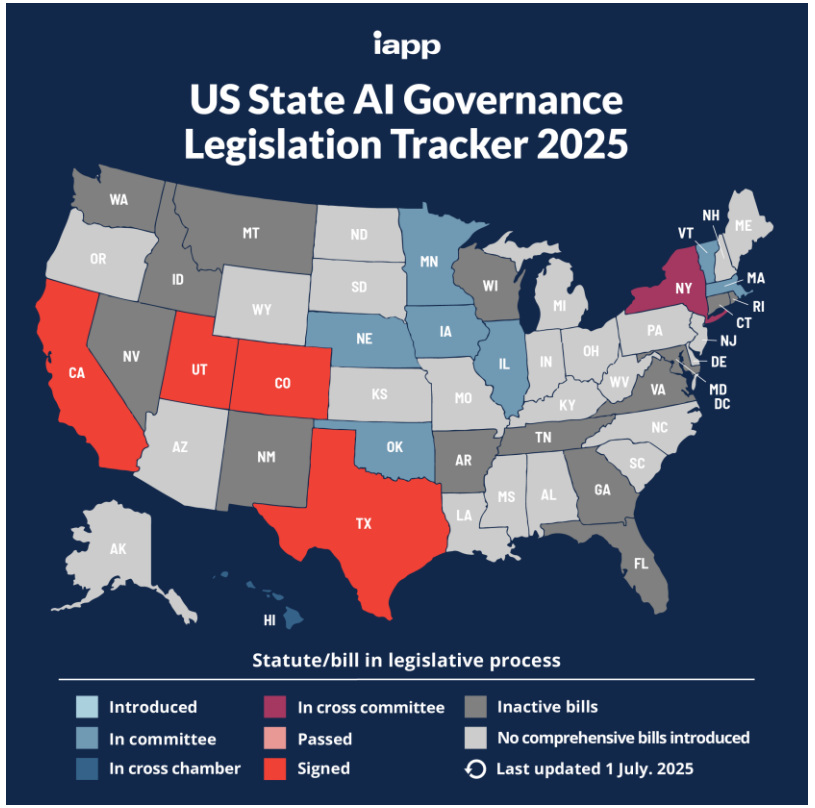
全球数据保护和隐私立法 - Overview



Data Protection and Privacy Legislation Worldwide | UN Trade and Development (UNCTAD)

全球数据保护和隐私立法 - US





Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Federal Trade Commission Act Incorporating U.S. SAFE WEB Act amendments of 2006

全球数据保护和隐私立法 - EU

General Data Protection Regulation (EU) 2016/679
apply from 25 May 2018

Data Act (EU) 2023/2854
apply from 12 September 2025

NIS 2 Directive (EU) 2022/2555
transposition by 17 October 2024
apply from 16 January 2023

Artificial Intelligence Act (EU) 2024/1689
apply from 2 August 2026

Data Governance Act (EU) 2022/868
apply from 24 September 2023

Cyber Resilience Act (EU) 2024/2847
apply from 11 December 2027

全球数据保护和隐私立法 - CN

中华人民共和国民法典 第四编 人格权
第六章 隐私权和个人信息保护
2021年1月1日起施行

中华人民共和国网络安全法
2017年6月1日起施行

中华人民共和国数据安全法
2021年9月1日起施行

中华人民共和国个人信息保护法
2021年11月1日起施行

- **新一代人工智能伦理规范**
  2021年9月25日起施行
- **互联网信息服务算法推荐管理规定**
  2022年3月1日起施行
- **互联网信息服务深度合成管理规定**
  2023年1月10日起施行
- **生成式人工智能服务管理暂行办法**
  2023年8月15日起施行
- **人脸识别技术应用安全管理办法**
  2025年6月1日起施行
- **人工智能生成合成内容标识办法**
  2025年9月1日起施行

全球数据保护和隐私立法 - CN

- GB/T 35273-2020 信息安全技术 个人信息安全规范
- GB/T 37964-2019 信息安全技术 个人信息去标识化指南
- GB/T 42460-2023 信息安全技术 个人信息去标识化效果评估指南
- GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南
- GB/T 42574-2023 信息安全技术 个人信息处理中告知和同意的实施指南
- GB/T 40660-2021 信息安全技术 生物特征识别信息保护基本要求
- GB/T 41819-2022 信息安全技术 人脸识别数据安全要求
- GB/T 39725-2020 信息安全技术 健康医疗数据安全指南
- GB/T 24364-2023 信息安全技术 信息安全风险管理实施指南
- GB/T 43269-2023 信息安全技术 网络安全应急能力评估准则
- GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
- GB/T 43697-2024 数据安全技术 数据分类分级规则
- GB/T 45574-2025 数据安全技术 敏感个人信息处理安全要求
- GB/T 41391-2022 信息安全技术 移动互联网应用程序(App)收集个人信息基本要求
- GB/T 45654-2025 网络安全技术 生成式人工智能服务安全基本要求
- GB 45438-2025 网络安全技术 人工智能生成合成内容标识方法
- GB/T 45674-2025 网络安全技术 生成式人工智能数据标注安全规范

PSCI要求

Privacy		Additional Auditor Guidance
16	**Does the facility or company ensure confidentiality and privacy of information concerning companies, individuals, workers, patient rights and intellectual property?** Data Privacy: General Data Protection Regulation (GDPR): Other? Please explain:	Does the company demonstrate and implement data privacy policies and procedures?

知识产权与研发数据

制造与供应链中数据

临床试验数据

员工个人数据

议程 Agenda

Why it matters?

What it is?

How to identify and mitigate the risks?

What to do when using AI?

Key takeaway

Q&A

信息安全与数据安全

信息安全

对**信息**的**保密性、完整性和可用性**的保持。

注：另外，也可包括诸如真实性、可核查性、抗抵赖和可靠性等其他性质。

GB/T 25069-2022 信息安全技术 术语

数据安全

指通过采取必要措施，确保**数据**处于**有效保护**和**合法利用**的状态，以及具备保障持续安全状态的能力。

数据，是指任何以**电子**或者其他方式**对信息的记录**。

中华人民共和国数据安全法

个人信息与个人敏感信息

个人信息

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**来识别特定自然人**身份**或者**反映其活动情况**的各种信息。

注 1：个人信息包括姓名、出生日期、公民身份号码、个人生物特征信息、住址、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加工处理后形成的信息，例如，用户画像特征标签，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，也属于个人信息。

GB/T 25069-2022 信息安全技术 术语

敏感个人信息

一旦**泄露**或**非法使用**，容易导致自然人的人格尊严受到侵害或人身财产安全受到危害的个人信息。

注：敏感个人信息包括**生物识别、宗教信仰、特定身份、医疗健康、金融账户和行踪轨迹等**信息和**不满十四周岁未年人的个人信息。**

GB/T 45574-2025 数据安全技术 敏感个人信息处理安全要求

个人信息与个人敏感信息

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账户、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

符合以下**任一条件**的个人信息,应识别为**敏感个人信息**:

1) 一旦遭到泄露或非法使用，容易导致自然人的**人格尊严**受到侵害;

注1:容易导致自然人人格尊严受到侵害的情形可能包括“人肉搜索”、非法侵入网络账户、电信诈骗、损害个人名誉和歧视性差别待遇等。歧视性差别待遇可能因个人信息主体的特定身份、宗教信仰、性取向、特定疾病和健康状态等信息泄露导致。

2) 一旦遭到泄露或非法使用，容易导致自然人的**人身安全**受到危害;

*注2:例如泄露或非法使用个人的**行踪轨迹信息**,可能会导致个人信息主体的人身安全受到损害。*

3) 一旦遭到泄露或非法使用，容易导致自然人的**财产安全**受到危害。

注3:例如泄露或非法使用金融账户信息,可能会造成个人信息主体的财产损失。

GB/T 35273-2020 信息安全技术 个人信息安全规范

个人信息与个人敏感信息

类别	描述
生物识别信息	个人基因[a]、人脸[b]、声纹[c]、步态[d]、指纹、掌纹、眼纹、耳廓和虹膜等生物识别信息
宗教信仰信息	个人信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动和特殊宗教习俗等个人信息
特定身份信息	残障人士身份信息、不适宜公开的职业身份信息等个人信息
医疗健康信息	——与个人的身体或心理的伤害、疾病、残疾和疾病风险或隐私有关的健康状况信息[e]，如病症、既往病史、家族病史、传染病史、体检报告和生育信息等； ——在疾病预防、诊断、治疗、护理和康复等医疗服务过程中收集和产生的个人信息，如医疗就诊记录（如医疗意见、住院志、医嘱单、手术及麻醉记录、护理记录和用药记录）、检验检查数据（如检验报告和检查报告）等
金融账户信息	个人的银行、证券、基金、保险和公积金等账户的账号及密码，公积金联名账号、支付账号、银行卡磁道数据（或芯片等效信息）和基于账户信息产生的支付标记信息和个人收入明细等个人信息
行踪轨迹信息	连续精准定位轨迹信息、车辆行驶轨迹信息和人员连续的活动轨迹信息等个人信息
不满十四周岁未成年人个人信息	不满十四周岁未成年人的个人信息
其他敏感个人信息	精准定位信息[f]、居民身份证照片、性取向、性生活、征信信息、犯罪记录信息[g]和显示个人身体私密部位的照片或视频信息等个人信息

GB/T 45574-2025 数据安全技术 敏感个人信息处理安全要求

按前一页识别收集和产生的敏感个人信息，敏感个人信息**类别**应符合本页。

注4:如有充分理由和证据表明处理的个人信息达不到上一页条件的，不识别为敏感个人信息。

既要考虑单项敏感个人信息识别，也要考虑**多项一般个人信息汇聚后的整体属性**，分析其一旦泄露或非法使用可能对个人权益造成的影响，如符合上一页所述条件，应将**汇聚后的个人信息整体**参照敏感个人信息进行识别与保护。

匿名化与去标识化

匿名化

通过对个人信息的技术处理，使得**个人信息主体无法被识别或者关联**，且**处理后的信息不能被复原**的过程

不再属于个人信息

无法回溯复原，因此大多用于数据调查、数据统计和数据分析等

去标识化

通过对个人信息的技术处理，使其在**不借助额外信息的情况下，无法识别或者关联个人信息主体**的过程

强化数据安全

必要时可以复原，但需要将**用于恢复识别个人的信息**与**去标识化之后的信息**分开存储并加强访问和使用的权限管理

个人信息处理过程中的各方

个人信息主体

个人信息所**标识或关联**的自然人

General Data Protection Regulation (EU) 2016/679

控制者

单独或与他人共同**决定个人数据处理目的和方式**的自然人或法人、公共当局、机构或其他团体

处理者

代表控制者处理个人数据的自然人或法人、公共当局、机构或其他团体

接收者

接收被披露个人数据的自然人或法人、公共当局、机构或其他团体，无论其是否为第三方

第三方

除数据主体、控制者、处理者以及在控制者或处理者直接授权下有权处理个人数据的人员以外的自然人或法人、公共当局、机构或团体

个人信息的处理 —— 前提

符合任一前提

- 取得个人同意
- 为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需
- 为履行法定职责或者法定义务所必需
- 为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需
- 为实现公共利益实施新闻报道、舆论监督等行为
- 处理个人自行公开或者其他已经合法公开的个人信息
- 法律、行政法规规定的其他情形

中华人民共和国劳动合同法实施条例

第八条　劳动合同法第七条规定的职工名册，应当包括**劳动者姓名、性别、公民身份号码、户籍地址及现住址、联系方式、用工形式、用工起始时间、劳动合同期限**等内容。

禁止使用童工规定

第四条 用人单位招用人员时，必须**核查被招用人员的身份证**；对不满１６周岁的未成年人，一律不得录用。用人单位**录用人员的录用登记、核查材料应当妥善保管。**

个人信息的处理 —— 要求

合法、正当、必要和诚信的原则

明确、合理的目的

公开、透明的原则

保证个人信息的准确和完整

确保个人信息的安全

收集	存储	使用	加工	共享、转让和传输	公开披露
合法性	时间最小化	访问控制措施	用户画像的使用	事先评估	事先评估
最小必要	去标识化处理	展示限制	个性化展示的使用	告知并征得明示同意	告知并征得明示同意
授权同意	控制者停止运营	使用的目的限制	对个人信息的汇聚融合	通过合同规定接收方的责任和义务	准确记录公开披露的情况

个人敏感信息的处理 —— 通用安全要求

特定的目的　　**充分的必要性**　　**采取严格的保护措施**

取得个人信息主体的单独同意

单独同意是指处理敏感个人信息**不应与一般个人信息一并取得个人同意**

法律、行政法规规定下取得书面同意

包括但不限于采集**人类遗传资源**、向**征信机构**查询个人信息、从事信贷业务的机构向其他主体提供**信贷信息**和使用房地产经纪服务过程中提供**房地产交易相关信息**等

收集合法性

- 通过**隐私政策**等方式明确收集敏感个人信息的必要性和对个人权益的影响
- 不应通过**非法方式**收集或通过**非法渠道**购买敏感个人信息
- 不应通过技术手段**自动收集**敏感个人信息
- 不应**基于任何违反法律法规规定的目的**收集或利用敏感个人信息
- 不应为**犯罪活动**收集敏感个人信息，或将所收集的敏感个人信息用于犯罪活动

收集的要求

- 收集**非敏感个人信息可实现处理目的的**，不应收集敏感个人信息
- 应**仅在个人信息主体使用业务功能期间**，收集该业务功能所需的敏感个人信息
- 应按业务功能或服务场景，**分项收集**敏感个人信息
- 利用移动互联网应用程序收集应符合**GB/T41391**的要求

GB/T 45574-2025 数据安全技术 敏感个人信息处理安全要求

个人敏感信息的处理 —— 通用安全要求

应向个人信息主体**告知**的事项

- **个人信息处理者**的名称或姓名、联系方式等基本情况
- 敏感个人信息的**处理目的、处理方式和必要性**
- 敏感个人信息的**种类、保存期限和对个人权益的影响**
- 个人信息主体**行使个人信息主体权利的方式和途径**

多项敏感个人信息处理活动，或单项敏感个人信息被用于**多个处理目的或业务功能**的，应提供**单独同意**机制

在公共场所**安装图像采集或个人身份识别设备**

- 应设置显著的**提示标识**
- 除取得个人信息主体**单独同意**外，所收集的个人图像和身份识别信息类敏感个人信息**原则上只能用于维护公共安全目的**

GB/T 45574-2025 数据安全技术 敏感个人信息处理安全要求

个人敏感信息的处理 —— 特殊安全要求

生物识别信息 | **宗教信仰信息** | **特定身份信息** | **医疗健康信息** | **金融账户信息** | **行踪轨迹信息**

在可采用收集**非个人敏感信息实现处理目的**时，不应将基于个人敏感信息的方式作为**默认选项或强制选项**

建立相应的**访问控制权限审批机制**

应**去标识化**显示个人敏感信息，确需完整显示的，应**进行个人信息主体或授权人员身份验证**

公开个人敏感信息，应基于**个人信息主体主动要求或书面同意**

通过**无需个人信息主体配合的方式收集**个人敏感信息前，应取得个人信息主体的**书面同意**

将个人敏感信息用于**科学研究**，应取得个人信息主体的**书面同意**

持续收集个人敏感信息的，应提供**持续提示机制**

不应使用个人敏感信息**构建用户画像**

实现处理目的后，应**删除**所收集的原始个人敏感信息

不满十四周岁未成年人的个人信息

仅在**未成年人相关法律法规有明确要求**时方可收集

应当取得未成年人的父母或者其他**监护人的同意**

应制定**专门的未成年人个人信息处理规则**并公开显示

个人信息主体的权利

知情权

决定权

个人信息查询	**个人信息更正**	**个人信息删除**
个人信息主体撤回授权同意	**个人信息主体注销账户**	**个人信息主体获取信息副本**

时限	收费	不响应请求的回应
在验证个人信息主体身份后，**三十天内**或法律法规规定的期限内作出回应，并**告知外部纠纷解决途径**	对合理请求原则上**不收取费用**，但对**一定时期内多次重复**的请求，可收取**成本费用**	决定不相应请求的，应向个人信息主体**告知该决定的理由**，并**提供投诉的途径**

议程 Agenda

Why it matters?

What it is?

How to identify and mitigate the risks?

What to do when using AI?

Key takeaway

Q&A

个人信息安全风险评估

数据映射分析

个人信息类型
个人信息处理的目的
个人信息控制者
个人信息处理者
是否涉及跨境传输
是否涉及第三方共享

待评估的个人信息处理活动

个人信息项目
收集来源
收集方式
存储方式/加密措施
传输方式/加密措施
存储期限
删除/匿名化方式

个人权益影响分析

个人信息敏感程度分析
个人信息处理活动特点分析
个人信息处理活动问题分析
个人权益影响程度分析

风险源识别

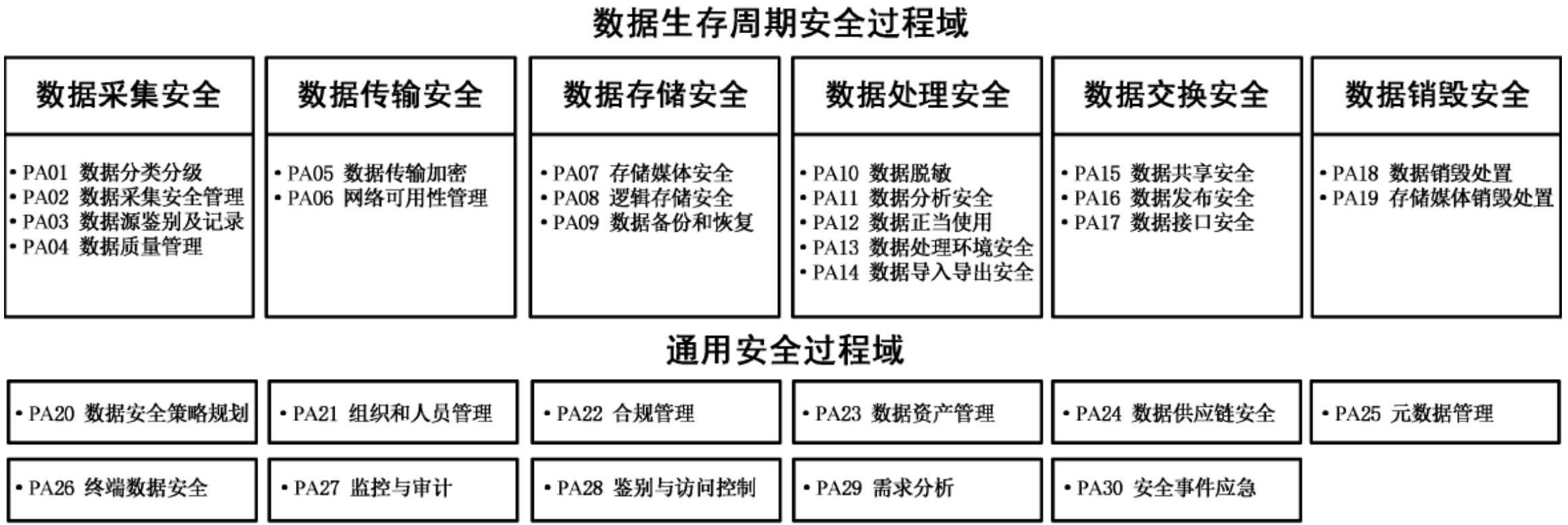
网络环境和技术措施
个人信息处理流程
参与人员与第三方
业务特点和规模及安全态势

个人权益影响程度 × **安全事件可能性** = **风险级别**

- 数据泄露
- 数据篡改
- 数据损毁
- 非法获取数据
- 非法使用数据
- 非法共享数据

GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南

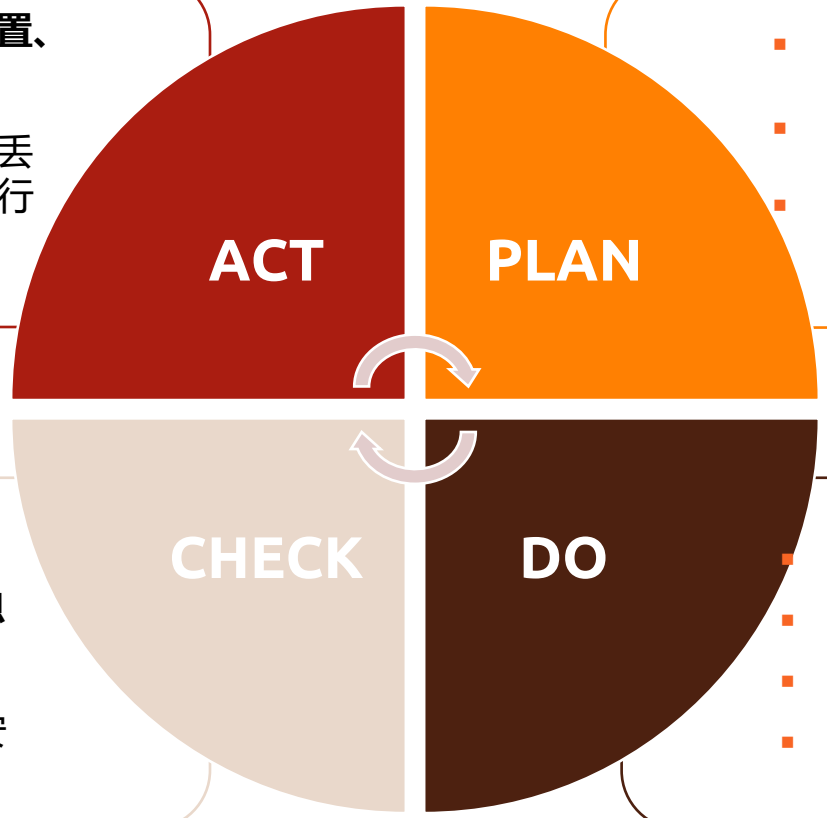
个人信息安全风险管控



GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

个人信息安全风险管控

- 审计过程形成的记录应能**对安全事件的处置、应急响应和事后调查提供支撑**
- 发生或者可能发生个人信息泄露、篡改、丢失的，应当**立即采取补救措施**，并**通知**履行个人信息保护职责的部门和个人



- 制定内部**管理制度和操作规程**
- 开展**个人信息安全影响评估**，至少保存**三年**
- 制定并组织实施**个人信息安全事件应急预案**

- 定期进行**漏洞检测**
- 建立**自动化审计系统**，**检测记录个人信息处理活动**
- 定期对个人信息保护政策、相关规程和安全措施的有效性进行**合规保护审计**

- 对个人信息实行**分类管理**
- 采取相应的加密、去标识化等**安全技术措施**
- 合理确定个人信息处理的**操作权限**
- 定期对从业人员进行**安全教育和培训**

个人敏感信息安全风险管控

ISO/IEC 27701:2019
信息安全、网络安全和隐私保护 – 隐私信息管理系统 - 要求和指南

ISO/IEC 20889:2018
隐私增强数据去标识化术语和技术分类

- 建立敏感个人信息**安全风险监测预警和响应机制**
- 对敏感个人信息**处理和操作**情况进行记录，**日志记录应保存三年**
- **加密存储和加密传输**
- **解密操作与加密操作应分别授权**
- 应按**最少够用原则**，**严格限制**敏感个人信息**访问权限和有效期**
- 敏感个人信息显示界面应添加包括访问主体标识和访问时间等内容的**水印**，涉及集中显示的，应**默认禁用复制、打印和截屏等功能**
- **定期梳理可访问敏感个人信息的应用和数据接口**，应采用身份鉴别、访问控制、最小授权、安全通道、加密传输和时间戳等**安全措施**
- 规划建设涉及敏感个人信息的产品服务时，宜按开展个人信息安全工程实践，**同步规划、同步建设、同步部署和同步使用个人信息安全措施**
- 敏感个人信息出境应符合国家有关部门**数据出境有关规定**
- 至少**每月**对敏感个人信息处理**日志和用户权限**进行**安全审计**

GB/T 45574-2025 数据安全技术 敏感个人信息处理安全要求

议程 Agenda

Why it matters?

What it is?

How to identify and mitigate the risks?

What to do when using AI?

Key takeaway

Q&A

AI服务中的个人信息保护测评方法

01

查看**个人信息保护相关制度**，检查其中是否包含训练数据中使用个人信息、敏感个人信息的安全要求

02

如使用包含个人信息的训练数据，从**全部包含个人信息的训练数据中随机抽取不少于1000条或10%的数据**，检查是否取得对应**个人同意**

03

如使用包含敏感个人信息的训练数据，从**全部包含敏感个人信息的训练数据中随机抽取不少于1000条或10%的数据**，检查是否取得对应**个人单独同意**

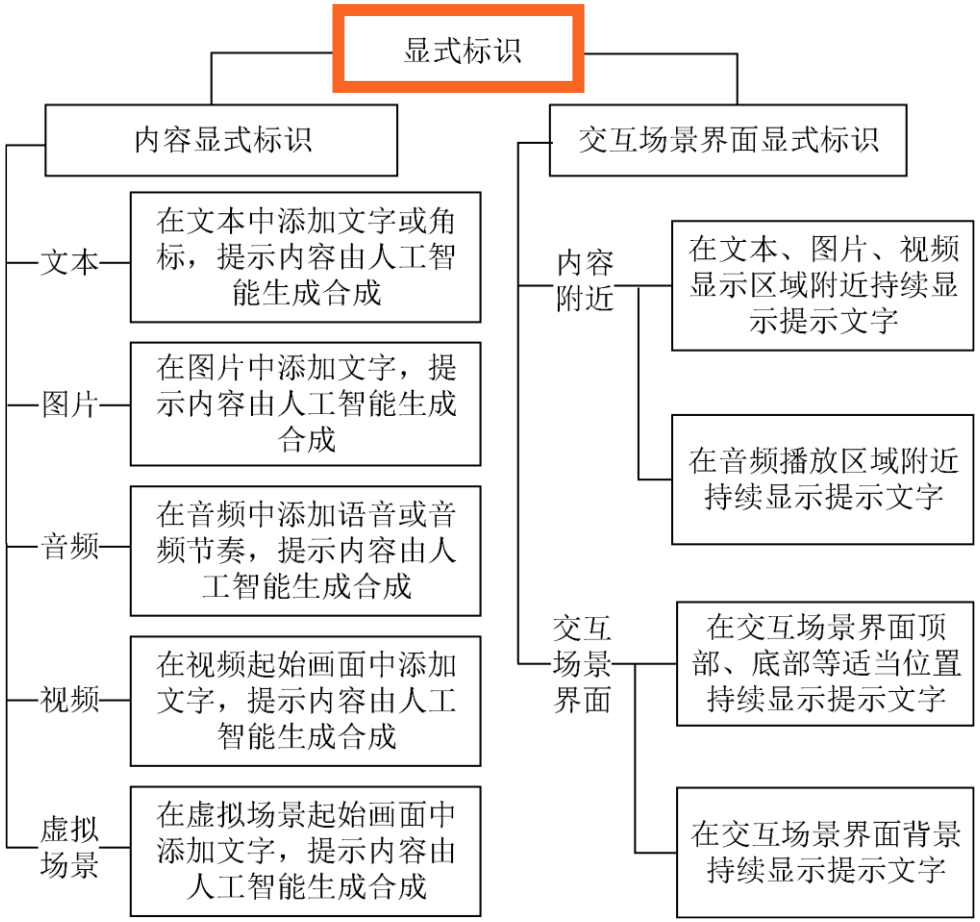
04

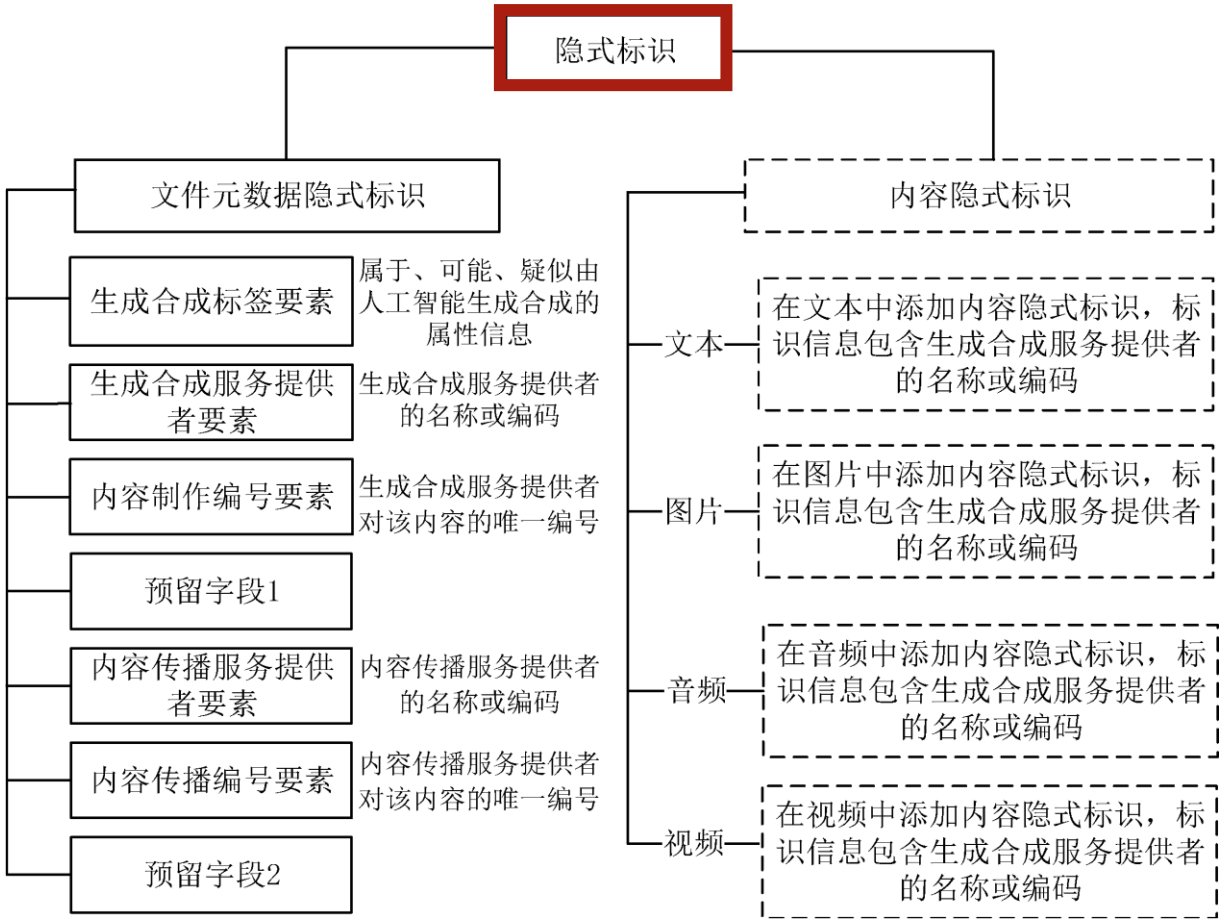
从**全部训练数据中随机抽取不少于4000条数据**，检查所抽取数据中是否包含**个人信息**，如包含个人信息，检查是否取得**对应个人同意**

05

从**全部训练数据中随机抽取不少于4000条数据**，检查所抽取数据中是否包含**敏感个人信息**，如包含敏感个人信息，检查是否取得对应**个人单独同意**

AI生成合成内容标识方法





GB 45438-2025 网络安全技术 人工智能生成合成内容标识方法

学术出版中AIGC使用边界指南

01 透明度和问责制

02 质量和诚信

03 隐私和安全

04 公平

05 可持续发展

PSCI PHARMACEUTICAL SUPPLY CHAIN INITIATIVE
Building responsible supply chains

Key takeaways