

迪安诊断技术集团股份有限公司

隐私保护制度与流程

第一章 总则

（一）编制目的

迪安诊断技术集团股份有限公司高度重视信息安全和隐私保护，将客户、患者、员工、合作伙伴及其他相关方的个人信息和敏感数据保护作为公司合规运营和业务持续发展的重要基础。为规范个人信息和相关数据的收集、使用、存储、传输、共享、披露、留存和销毁等处理活动，防范数据泄露、滥用、未经授权访问或其他隐私保护风险，依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》和 GB/T 35273-2020《信息安全技术 个人信息安全规范》等法律法规及标准，结合公司信息安全管理体实际情况，制定本制度与流程。

（二）适用范围

本制度与流程适用于迪安诊断技术集团股份有限公司及下属子公司涉及个人信息、客户数据、业务数据、经营管理数据及其他敏感信息处理的活动。供应商、承包商、合作伙伴及其他第三方在为公司提供产品或服务、接触公司数据或参与数据处理活动时，应遵守本制度与流程的隐私保护要求。

（三）术语定义

1. 个人信息：指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、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。

2. 敏感个人信息：指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

3. 个人信息的处理：包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

4. 个人信息主体：个人信息所标识或者关联的自然人。

第二章 管理组织与职责

（一）治理架构

公司建立四级信息安全与隐私保护管理架构，包括决策层、管理层、执行层和监督层：

1. 决策层——信息安全委员会。委员会领导小组由公司高级管理层组成，主任由公司首席执行官（CEO）担任，执行主任由公司首席信息官（CIO）担任，领导小组成员包括首席财务官（CFO）、首席人力资源官（CHO）及各大区总负责人。信息安全委员会负责审定信息安全总体战略、方针和策略，研究决定信息安全管理重大事项，审批信息安全预算计划和风险评估报告，决策启动重大信息安全事件应急处置流程。

2. 管理层——信息安全委员会办公室。办公室设在信息管理中心，主任由 CIO 担任，执行主任由信息安全工作主要负责人担任，成员至少包含信息管理中心、业务、法务、财务、人力、行政、公共事务部等部门及各大区主要负责人。办公室负责拟定信息安全中长期规划和年度工作计划，组织制定和修订信息安全管理制度和应急管理体系，协调督促制度落实执行。

3. 执行层——各部门信息安全员及全体员工。信息安全员负责本部门信息安全工作传达、信息资产梳理、风险评估配合和安全事件上报。全体员工遵守信息安全管理规定，妥善使用和保护所涉及的信息资产，及时上报发现的安全事件或隐患，积极参与安全教育和培训。

4. 监督层——信息安全监督小组。由集团总部的 IT 监督员和审计部的信息安全审计员组成，负责信息安全工作监督检查和违规行为调查处置。

（二）分工职责

1. 信息安全委员会办公室：作为个人信息保护的决策者和本办法的制定及维护主体，负责贯彻执行国家个人信息保护相关法律法规，审定个人信息保护发展战略和重大决策。

2. 信息管理中心：作为个人信息保护的管理部门，负责个人信息保护政策和制度的制定与定期更新，建立自动化审计系统监测记录个人信息处理活动，制定个人信息安全事件应急预案并组织应急演练。

3. 法务部：作为个人信息保护的支持部门，负责提供个人信息保护相关法律法规支持，协同开展个人信息安全影响评估。

4. 人力资源中心：作为个人信息保护的支持部门，负责人员入职背景审查、保密协议签署、离岗保密管理和个人信息保护培训组织。

5. 审计部：作为个人信息保护的监督部门，负责监督各部门对个人信息保护策略和规程的执行，受理个人信息相关投诉和举报，开展个人信息保护内部审计。

6. 公司各部门及下属子公司：作为个人信息保护的执行主体，负责落实本部门个人信息保护措施，建立个人信息保护清单，制定应急预案并处置安全事件，各部门负责人为本部门个人信息保护第一责任人。

第三章 基本原则

公司在个人信息处理活动中遵循以下基本原则：

1. 权责一致：公司对其个人信息处理活动负责，采取技术和其他必要措施保障个人信息安全，对因处理活动对个人信息主体合法权益造成的损害承担责任。

2. 目的明确：处理个人信息具有明确、清晰、具体、合理的目的，处理活动与处理目的直接相关。

3. 选择同意：向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意。收集年满十四周岁未成年人的个人信息前，征得未成年人或其监护人的明示同意；不满十四周岁的，征得其监护人的明示同意。

4. 最小必要：只处理满足授权同意目的所需的最少个人信息类型和数量。目的达成后，及时删除个人信息。

5. 公开透明：以明确、易懂和合理的方式公开处理个人信息的规则，明示处理的目的、方式和范围。

6. 确保安全：具备与所面临的安全风险相匹配的安全能力，采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

7. 主体参与：向个人信息主体提供查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等途径。

第四章 生命周期管理流程

（一）个人信息收集

收集个人信息前，应明确业务目的和使用场景，向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得授权同意。收集范围应与业务需求相匹配，不得超出业务必需范围收集信息。个人信息收集应做到标准统一、术语规范、内容准确、身份标识唯一。通过纸质表单采集个人信息并转换为电子信息时，由收集部门指定负责人对纸质表单流转的全过程进行监控和审计。

（二）个人信息存储

公司明确个人信息的存储期限为实现处理目的所必要的最短时间。存储个人信息应采用加密、安全存储、访问控制、安全审计等安全措施。对于以纸质档案形式在系统外保管的个人信息，建立严格的调用权限、审批权限与档案管理制度。存储期限届满时，对个人信息进行删除或匿名化处理。

（三）个人信息传输

应用系统间的个人信息传输应通过系统定义的接口和安全传输通道（如 SSL 证书、VPN 等）进行，并对重要的传输请求进行日志记录。通过网络传输个人信息时，应采取加密措施，禁止在互联网上明文传输敏感个人信息。通过电子介质（U 盘、光盘等）传输个人信息时，需进行加密或脱敏处理。包含敏感个人信息的介质如需提供给外部机构，不应通过第三方（如快递等）传递，介质交接应保留完整的接收方签收记录。

（四）个人信息使用

1. 权限管理：对直接或间接接触个人信息的岗位人员进行角色划分，根据工作需要，按照最小必须原则限定可查看个人信息的内容范围与相应权限。原则上各部门仅可调用由本部门收集、存储的个人信息。涉及敏感数据的访问、查询、展示和使用，应按照权限控制和审批要求执行。对个人信息的批量修改、拷贝、下载等重要操作设置内部审批流程。对个人信息的访问和操作进行记录（包括业务操作日志和系统日志），保证日志的完整性、可用性和可追溯性，日志至少保存六个月。

2. 信息展示：在操作终端查询、展现个人信息时，应采取去标识化处理、对展示界面增加水印等措施，降低信息泄露风险。向个人信息主体提供业务功能时使用个性化展示的，应区分个性化展示和非个性化展示内容，并提供不针对个人特征的选项。

3. 委托处理：委托第三方处理个人信息时，不超出已征得授权同意的范围，对委托行为进行个人信息安全影响评估，通过合同形式明确受委托者的责任和义务并进行监督。

4. 共享与转让：共享、转让个人信息前，开展个人信息安全影响评估，告知个人信息主体共享或转让的目的、数据类型接收方类型及可能产生的后果，并取得授权同意。与数据接收方签订合同，明确其责任和义务。个人生物识别信息原则上不共享或转让。

5. 信息提取：根据最小化原则确定个人信息提取的场景、范围和权限规则。个人信息提取应有详细的操作记录。开发人员和外包人员不得从事个人信息的提取工作。提取后和使用完成后，个人信息应立即从本地设备安全删除。

（五）个人信息删除

当个人信息超出存储期限、个人信息主体撤回同意或注销账户时，公司应及时对相关个人信息进行删除或匿名化处理。存储个人信息的介质进行报废处理时，应采用物理损毁等方式销毁，确保信息不可恢复。

第五章 人员管理与培训

公司对大量接触个人敏感信息的岗位人员实施入职背景审查。从事个人信息处理岗位的相关人员应签署保密协议，在调离岗位或终止劳动合同时继续履行保密义务。可能访问个人信息的外部服务人员应签署保密协议，遵守个人信息安全要求。

公司定期（至少每年一次）或在个人信息保护政策发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，确保相关人员熟练掌握个人信息保护政策和相关规程。

第六章 安全事件管理

公司制定个人信息安全事件应急预案，明确安全事件处置流程和各岗位职责。信息安全委员会办公室定期（至少每年一次）组织应急响应培训和演练。

发生个人信息安全事件后，公司立即采取必要措施控制事态、消除隐患，评估事件影响和产生原因。根据相关法律法规和行业主管部门的规定，及时向监管机构报告并告知受影响的个人信息主体。

公司建立投诉与申诉管理机制，向个人信息主体提供投诉渠道，在规定时间内对投诉和申诉进行响应和处理。

第七章 第三方管理

公司在产品或服务中接入具备收集个人信息功能的第三方产品或服务时，建立第三方接入管理机制和工作流程。通过合同等形式明确双方的安全责任及应实施的个人信息安全措施。向个人信息主体明确标识由第三方提供的产品或服务。

公司监督第三方产品或服务提供者加强个人信息安全管理，发现未落实安全管理要求的，及时督促整改，必要时停止接入。对嵌入或接入的第三方自动化工具（如代码、脚本、接口、算法模型、SDK、小程序等）开展技术检测，确保其收集和使用行为符合约定要求。

第八章 审计监督与考核

审计部协同信息管理中心和法务部，定期对公司各部门及下属子公司处理个人信息遵守法律和公司制度的情况进行合规审计，及时处理审计过程中发现的个人信息违规使用和滥用等情况。信息管理中心建立自动化审计系统，监测记录个人信息处理活动。

信息管理中心协同法务部建立个人信息安全影响评估制度，在涉及敏感个人信息处理、自动化决策、委托或共享个人信息、跨境传输等情形时，事前进行个人信息保护影响评估，评估报告和处理记录保存不少于三年。

信息安全委员会办公室每季度至少组织一次信息安全体系运行沟通会议，每年至少组织一次信息安全检查和一次信息安全综合应急演练或专项演练。信息安全委员会全体会议每季度召开一次。

公司建立考核与奖惩机制。对信息安全工作成绩突出的部门与个人给予奖励。违反国家法律法规、行业规章或公司信息安全管理规定，造成安全事故或犯罪的，根据有关法律法规和公司规定追究相关责任。

第九章 持续改进

公司结合业务发展、法律法规变化、技术变化、风险评估结果、安全事件复盘和利益相关方反馈，每年至少组织一次信息安全管理评审，评估改进机会和变更需要，持续完善隐私保护制度、流程和技术措施。

第十章 附则

本制度与流程经信息安全委员会审议通过后生效，自发布之日起施行。

下属子公司可根据本制度的基本原则和业务实际情况，制定具体的实施细则，细则标准不得低于本制度要求。

本制度与流程由信息安全委员会办公室负责解释和维护。