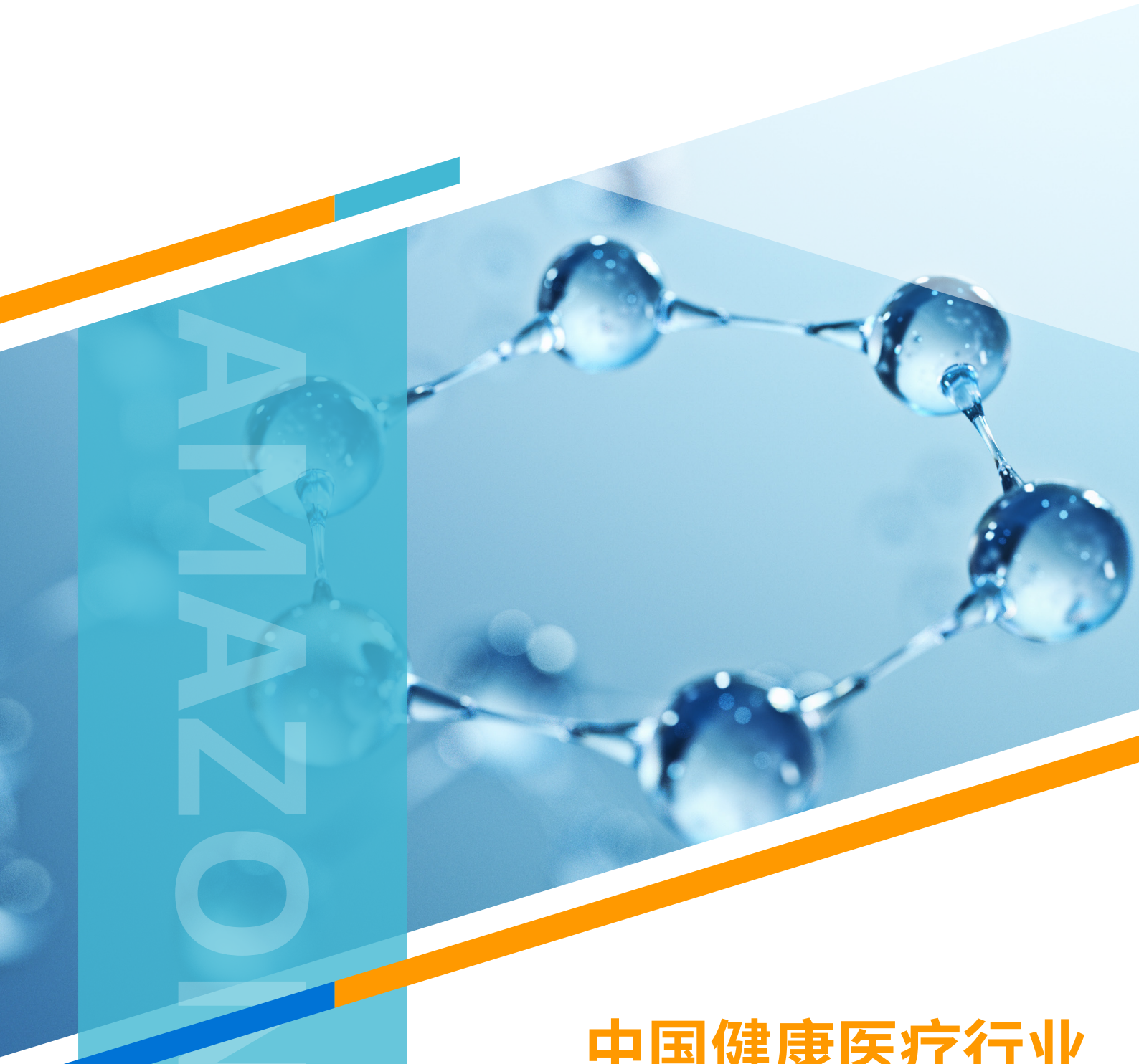


中国健康医疗行业企业数据出境实用指南及方案介绍

2023年04月

声 明

本《中国健康医疗行业企业数据出境实用指南及方案介绍》（“本指南”）由上海国瓴律师事务所和Amazon Web Services, Inc.或其关联方（“亚马逊云科技”）分别撰写，双方就各自撰写的内容分别、独立享有相关知识产权。其中上海国瓴律师事务所对其撰写的部分（包括关于本指南国瓴部分的声明、国瓴引言、摘要、第一章“数据出境”、第二章“健康医疗大数据出境”、第三章“遗传数据出境”、第四章“药企经营数据出境”和第五章“健康穿戴设备数据出境”）单独享有知识产权；亚马逊云科技对其撰写的部分（包括关于本指南亚马逊云科技部分的声明、亚马逊云科技引言以及第六章“亚马逊云科技助力健康医疗行业”）单独享有知识产权。

关于本指南亚马逊云科技部分的声明：

本部分内容陈述了亚马逊云科技在封面页所示日期的有关服务产品及实践，该等信息可能变化且我们不会另行通知。客户对于本部分的信息以及亚马逊云科技的产品或服务应自己做出独立的判断，该等内容都是“依现状”提供，不包含任何明示或者暗示的保证。本部分内容并没有创设来自亚马逊云科技、北京光环新网科技股份有限公司（“光环新网”）、宁夏西云数据科技有限公司（“西云数据”）、或其各自的关联方、提供方或许可方的任何保证、陈述、合同性承诺、条件或者担保。亚马逊云科技、光环新网、西云数据对其各自的客户的义务和责任均由适用的客户协议管辖。本部分内容不是亚马逊云科技、光环新网、西云数据和其各自的客户之间任何协议的组成部分，也不构成对任何协议的修改。

关于本指南国瓴部分的声明：

本指南中上海国瓴律师事务所拟写部分（以下简称：“本指南国瓴部分”，包括声明、引言、摘要中涉及国瓴部分的内容及本指南第一章至第五章）所涉内容的依据为本指南封面页所示日期以前已经颁布并生效的中华人民共和国法律、法规、规范性文件、国家标准等，借鉴了尚未生效的法律、法规、规范性文件的内容及其中体现的立法趋势，并结合了上海国瓴律师事务所在本指南封面页所示日期以前的有关服务经验及实践经验，该等信息可能变化且我们不会另行通知。

本指南国瓴部分所含内容为一般性信息，上海国瓴律师事务所及其律师并不因此构成提供任何法律建议、其他专业性建议或服务，在做出任何影响您的法律决策、商业决策或其他决策之前，您应咨询合格的专业顾问。本指南没有为上海国瓴律师事务所及其律师、员工、合作方、关联方、代理方创设任何保证、陈述、合同性承诺、条件或者担保，任何上海国瓴律师事务所或其律师、员工、合作方、关联方、代理方均不对任何方因使用本指南而直接或间接导致的任何损失或损害承担任何责任。上海国瓴律师事务所及其合作方、关联方均为具有独立法律地位的法律实体，相互之间不因第三方而承担任何责任或约束对方。

引 言

国瓴引言

根据《健康产业统计分类（2019）》，健康医疗行业(Health Care Life Science，以下简称："HCLS")指以医疗卫生和生物技术、生命科学为基础，以维护、改善和促进人民群众健康为目的，为社会公众提供与健康直接或密切相关的产品（货物和服务）的生产活动集合。

健康医疗数据包括个人健康医疗数据以及由个人健康医疗数据加工处理之后得到的健康医疗相关数据。随着健康医疗数据应用、"互联网+医疗健康"和智慧医疗的蓬勃发展，健康医疗数据跨境交互的机会越来越多、场景也越来越丰富，与之相对的是对于数据出境行为的监管力度不断加强，健康医疗数据出境给企业带来的风险和挑战也越来越大。

国家计算机网络应急技术处理协调中心（CNCERT/CC）发布的《2020年中国互联网网络安全报告》在"2020年我国网络生物安全态势专题分析"部分提到：在2020年，共发现国内基因数据通过网络出境717万余次，涉及我国境内近2.4万个IP地址，覆盖境内31个省（直辖市、自治区），我国基因数据流向境外170个国家和地区，涉及境外IP地址近4.7万个。2020年我国新冠肺炎病毒数据出境次数达99万余次，占生物数据出境总次数的13.8%。在2020年，发现境内医学影像数据通过网络出境497万余次，我国医学影像数据流向境外128个国家和地区，涉及境外IP地址近4.7万个，涉及境内3347个IP地址。2020年我国未脱敏医学影像数据出境近40万次，占出境总次数的7.9%。

本指南旨在解读中国健康医疗企业数据出境相关的法律、法规、标准及规范性文件，分析中国健康医疗企业所面临的问题和挑战，并提出企业应当关注的出境路径、合规要点及法律+管理+技术的解决方案，旨在为中国健康医疗企业出海尽一份绵薄之力。

亚马逊云科技引言

随着人类步入由互联网、云技术催生的大数据时代，大到国家决策，小到日常生活都在走向数字化，在健康医疗领域，中国庞大的人口和全民医疗体系更是提供了丰富的数据来源。

健康医疗大数据是国家重要的基础性战略资源。健康医疗大数据蓬勃发展，带来健康医疗模式的深刻变化，有利于激发深化医药卫生体制改革的动力和活力，提升健康医疗服务效率和质量，扩大资源供给，不断满足人民群众多层次、多样化的健康需求，有利于培育新的业态和经济增长点。《"健康中国2030"规划纲要》要求加强健康医疗大数据应用体系建设，推进基于区域人口健康信息平台的健康医疗大数据共享开放、深度挖掘和广泛应用。为加强健康医疗大数据服务管理，促进"互联网+健康医疗"发展，充分发挥健康医疗大数据作为国家重要基础性战略资源的作用，进一步强化对健康医疗大数据的政策指引，充分发挥健康医疗大数据作为国家重要基础性战略资源的作用，国家相关部门也积极研究、制定、发布各项规范、办法

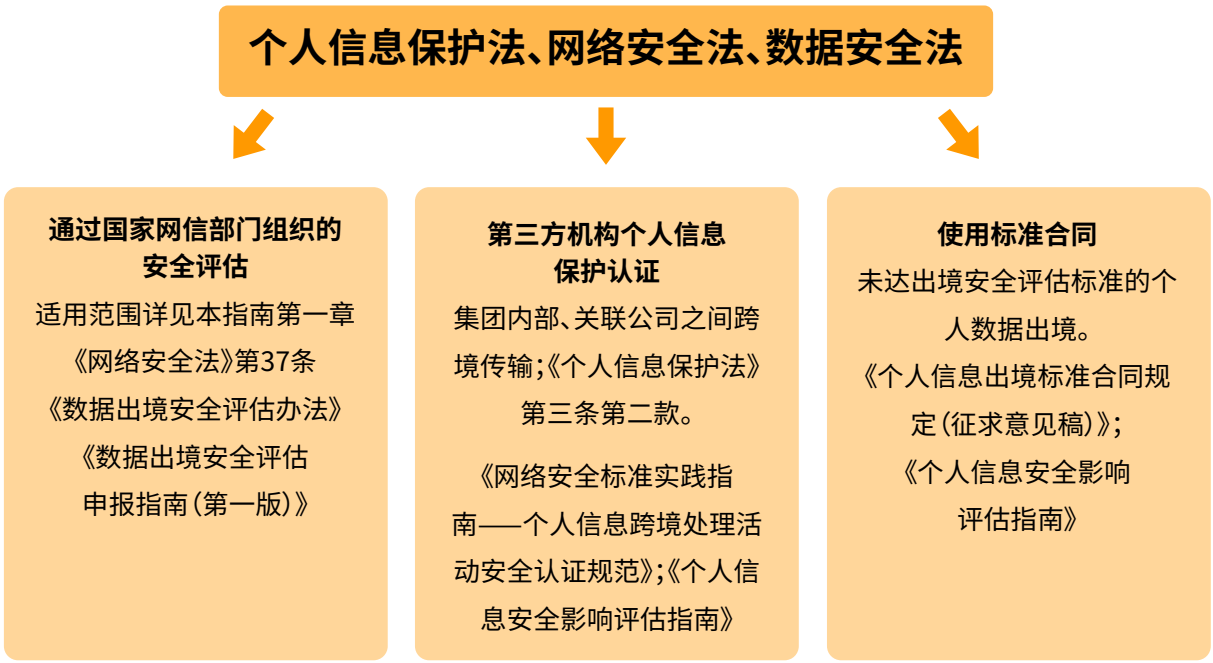
对健康医疗大数据管理使用加以引导和规范。

2015年，国务院发布《关于印发促进大数据发展行动纲要的通知》提出在健康医疗等领域开展大数据应用示范，鼓励和规范有关单位开展创新应用研究。2016年，国务院发布《关于促进和规范健康医疗大数据应用发展的指导意见》，提出健康医疗大数据是国家基础性战略资源，其发展将带来健康医疗模式的深刻变化，不断满足人民群众多层次、多样化的健康需求，并制定了发展目标、主要任务和组织框架。并明确指出："到2020年，健康医疗大数据相关政策法规、安全防护、应用标准体系不断完善,适应国情的健康医疗大数据应用发展模式基本建立"。2018年，国家卫生健康委员会发布《国家健康医疗大数据标准、安全和服务管理办法（试行）的通知》，不仅首次对"健康医疗大数据"做出了官方定义："在人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据"并且提出"我国公民在中华人民共和国境内所产生的健康和医疗数据，国家在保障公民知情权、使用权和个人隐私的基础上，根据国家战略安全和人民群众生命安全需要，加以规范管理和开发利用"。今年5月，国务院办公厅印发的《"十四五"国民健康规划》提出要全面推进健康中国建设，促进全民健康信息联通应用，推广应用人工智能、大数据、第五代移动通信（5G）、区块链、物联网等新兴信息技术，实现智能医疗服务、个人健康实时监测与评估、疾病预警、慢性病筛查等。

通过将强大的数据资源与新技术相结合来解决现有的诸多挑战，不仅能提供更好的循证决策，还可以为改变现有医学模式提供指引。从尚未出生的胎儿到新生儿检查、定期体检，直至临终关怀，人生中所有的医疗健康数据都被存储记录下来，为医生的诊断提供参考。同时，大数据让覆盖全生命周期的健康服务成为可能。健康大数据分析可以为医生做出精准的医疗方案提供重要的科技支撑。基于健康医疗大数据的技术，将实现个性化的治疗、提高疗效、降低副作用、降低费用。数据流动将促进数据使用，从而更好的发挥数据价值。健康医疗数据依法合规跨境流动，既可以满足科研合作的需要，又能满足全球化的商业合作需求。国际科研合作，有助于知识的共享，开拓研究视野，促进国内学科能力建设，提升科研水平。对于跨国药企来讲，业务全球化有利于优化资源配置，实现正确的商业布局，开拓发展空间，增强创新能力，推动产业发展。数据共用共存，单个数据价值或创造价值有限，聚合后的大量数据处理才能够带来巨大价值，所以数据的开发、许可、转让权能的行使非常重要。

摘 要

与其他行业企业一样，健康医疗行业数据处理者在重要数据出境时需要通过国家网信部门组织的安全评估，如果出境数据涉及个人信息，应当根据出境个人信息的数量和敏感程度等通过国家网信部门组织的安全评估、第三方机构个人信息保护认证或使用标准合同出境，相关法律体系和数据出境路径可参考下图



在健康医疗行业企业数据出境的过程中，国瓴的数据合规团队与技术专家可以为客户提供包括法律+技术+管理的一站式解决服务，将协助需要申报数据出境安全评估的处理者完成包括但不限于：初步尽职调查（法律+管理+技术），合规整改及差距分析（法律+管理+技术），盘点数据资产及信息系统资产，梳理数据链路，出具数据出境相关法律意见和技术意见，协助拟写数据出境风险自评估报告，协助申报、反馈及与网信部门沟通，协助应对监管问询和调查等工作。在项目整改过程中，国瓴的数据合规团队与技术专家可以协助客户建立完善的组织保障体系，协助客户搭建数据合规、个人信息保护及隐私保护、网络安全保障相关管理体系、管理制度及控制流程，协助客户建立个人信息保护影响评估机制，起草或审核数据出境处理协议、隐私政策等法律文本，提供数据保护培训、APP治理等服务。在后续落地的第三方机构个人信息保护认证出境场景及使用标准合同出境场景中，国瓴的数据合规团队与技术专家亦可为客户提供包括法律+技术+管理的一站式解决服务。

从企业数据合规体系搭建、数据保护培训到跨境数据合规甚至数据合规刑事风险防范、企业上市及投融资中的数据合规尽职调查，国瓴数据合规团队可以为各类数据合规业务提供专业的服务。

根据《信息安全技术　健康医疗数据安全指南》(GB/T　39725-2020)及相关法律、法规、规范性文件的规定,不涉及国家秘密、重要数据或者其他禁止或限制向境外提供的数据,经个人信息主体授权同意,并经数据安全委员会讨论审批同意,健康医疗大数据的控制者可向境外目的地提供个人健康医疗数据,累计数据量应控制在250条以内,否则应提请相关部门审批。

根据遗传资源的分类,人类遗传资源信息出境需要科学技术部门备案(非基因遗传资源信息)或审批(基因识别数据及关联信息)+科学技术部门安全审查(涉及公众健康、国家安全和社会公共利益的);人类遗传材料运送、邮寄、携带出境需要科学技术部门许可+海关审批。

对于业务范围涉及药物研发或医疗器械研发的企业而言,临床实验需要依法通过伦理审查,取得知情同意,并履行临床试验申请/备案/批准等程序;此外,若拟出境的临床实验数据中若涉及重要数据的,需通过网信部门组织的安全评估,拟出境的临床实验数据涉及个人信息的,需依据数据处理者情况、出境的个人信息数量及敏感程度等判断并选择适用网信部门组织的安全评估、第三方机构个人信息保护认证、使用标准合同出境(自2023年6月1日起施行)。

第一章 数据出境

一、数据从中国出境的几条路径

数字化经济背景下，数据在技术层面上不再受限于地域，其中个人信息不仅占比大，且事关每个个体的信息安全。因此，为保护个人信息安全和重要数据等的安全，《中华人民共和国网络安全法》（以下简称："《网络安全法》"）、《中华人民共和国数据安全法》（以下简称："《数据安全法》"）、《中华人民共和国个人信息保护法》（以下简称："《个人信息保护法》"）、《数据出境安全评估办法》、《数据出境安全评估指南》等法律、法规、规范性文件对于中国企业的数据出境行为提出了规范性要求。

1. 个人信息出境的三条路径

根据相关法律、法规、规范性文件的规定，目前数据处理者向境外传输个人信息有三条路径：

（1）通过国家网信部门组织的安全评估后出境（详见本指南第一章第二节介绍）。

（2）第三方机构个人信息保护认证出境：

按照《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》等进行个人信息保护认证出境，适用情形：

a.跨国公司或者同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动（此种个人信息跨境处理活动可以由境内一方申请认证，并承担法律责任）；

b.《个人信息保护法》第三条第二款适用的在中国境外处理中国境内自然人个人信息的活动。

基本要求：个人信息处理者和境外接收方之间应当签订具有法律约束力和执行力的文件，确保个人信息主体权益得到充分的保障；个人信息处理者和境外接收方均应指定个人信息保护负责人（DPO）及个人信息保护机构；个人信息处理者和境外接收方遵守统一的个人信息跨境处理规则；事前进行个人信息保护影响评估。

（3）使用标准合同出境（自2023年6月1日起施行）：

适用情形：个人信息处理者同时符合下列情形的，可以通过签订标准合同的方式向境外提供个人信息：

a.非关键信息基础设施运营者；

b.处理个人信息不满100万人的；

c.自上年1月1日起累计向境外提供未达到10万人个人信息的；

d.自上年1月1日起累计向境外提供未达到1万人敏感个人信息的。

基本要求：个人信息处理者应当事前开展个人信息保护影响评估+在标准合同生效之日起10个工作日内向所在地省级网信部门备案。

2. 健康医疗行业的数据处理者数据出境的路径

（1）具体来说，健康医疗行业的数据处理者数据出境涉及个人信息部分的出境合规要求包括：

a.数据涉及敏感个人信息。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、行踪轨迹等信息。

i.自上年1月1日起累计向境外提供1万人敏感个人信息的→国家网信部门安全评估；

ii.自上年1月1日起累计向境外提供未达到1万人敏感个人信息的→签订国家网信部门制定的标准合同/经专业机构进行个人信息保护认证。

b.健康医疗行业的数据处理者出境数据不涉及敏感个人信息：

i.自上年1月1日起累计向境外提供10万人个人信息的→国家网信部门安全评估；

ii.自上年1月1日起累计向境外提供未达到10万人个人信息的→签订国家网信部门制定的标准合同/经专业机构进行个人信息保护认证。

(2)健康医疗行业的数据处理者向境外提供重要数据的，需由国家网信部门进行安全评估。

(3)健康医疗行业的关键信息基础设施运营者向境外提供个人信息的，需由国家网信部门进行安全评估。

二、需进行数据出境风险评估的主体范围及申报程序简介

1. 主体范围

根据《数据出境安全评估办法》及《数据出境安全评估申报指南》等相关规定，自2022年9月1日起，数据处理者向境外提供数据，有下列情形之一的，应当每两年一次通过所在地省级中国国家互联网信息办公室（以下简称："网信部门"或"网信办"）向国家网信部门申报数据出境安全评估：

(1)数据处理者向境外提供重要数据；

(2)关键信息基础设施运营者和处理100万以上个人信息的数据处理者向境外提供个人信息；

(3)自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息的数据处理者向境外提供个人信息；

(4)国家网信部门规定的其他需要申报数据出境安全评估的情形。

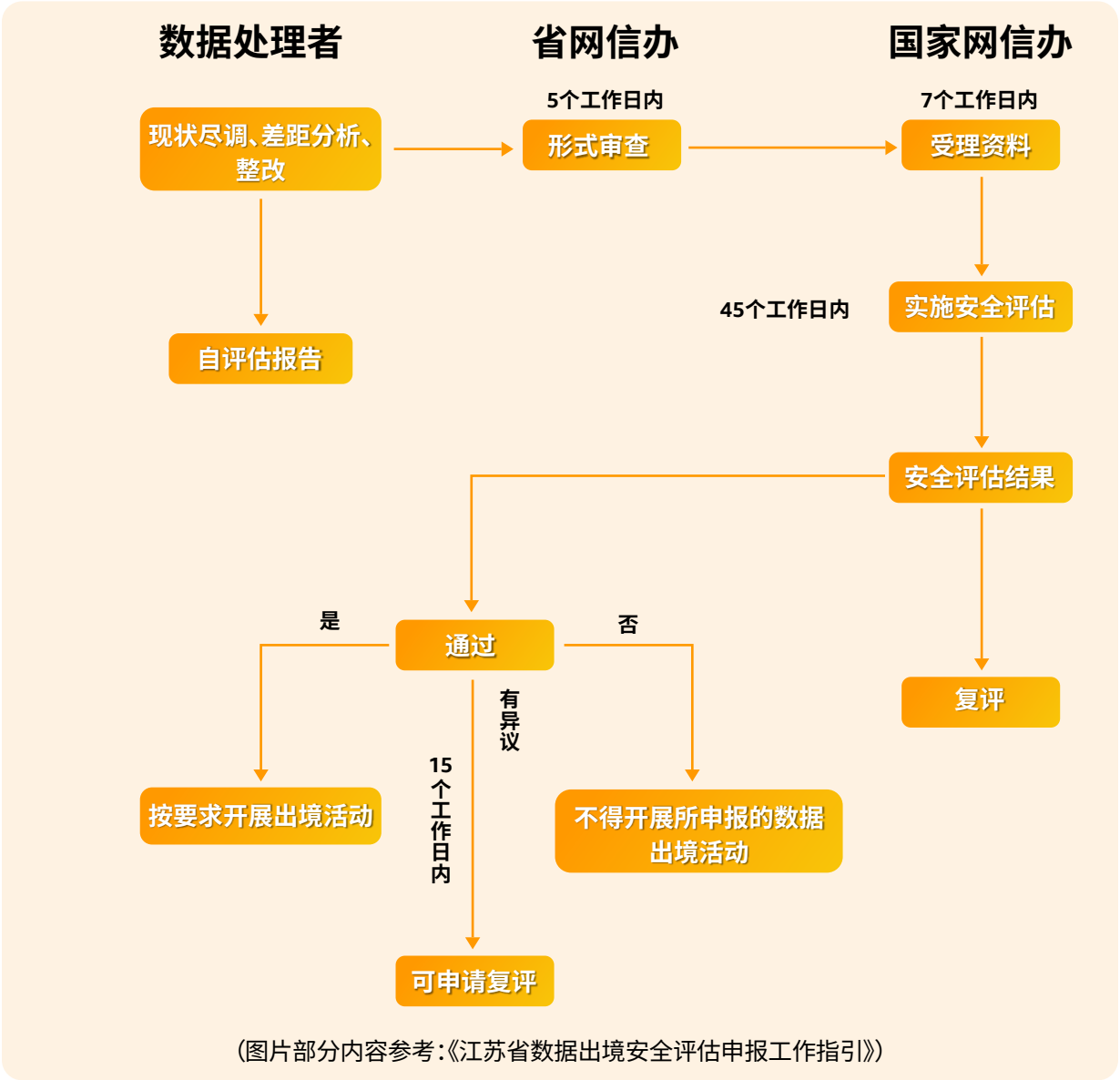
2. 数据出境风险评估的申报程序及申报资料

(1)数据出境风险评估申报所需资料如下：

序号	材料名称	要求	
1	统一社会信用代码证件	影印件加盖公章	
2	法定代表人身份证件	影印件加盖公章	
3	经办人身份证件	影印件加盖公章	
4	经办人授权委托书	原件	
5	数据出境安全评估申报书		
5.1	承诺书	原件	
5.2	数据出境安全评估申报表	原件	

6	与境外接收方拟定的数据出境相关合同或其他具有法律效力的文件	原件或影印件加盖公章	对数据出境相关约定条款做高亮、线框等显著标识。法律文件以中文版本为准，若仅有非中文版本的，需同步提交准确的中文译本。
7	数据出境风险自评估报告	原件	
8	其他相关证明材料加盖公章	原件或影印件加盖公章	相关材料以中文版本为准，若仅有非中文版本的，需同步提交准确的中文译本。

(2) 数据出境风险评估的项目流程及申请流程如下：



(图片部分内容参考：《江苏省数据出境安全评估申报工作指引》)

三、相关核心术语解释

1. 关键信息基础设施与关键信息基础设施运营者（CIIO）

关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。关键信息基础设施运营者（CIIO）负责关键信息基础设施的运行、管理，对本组织关键信息基础设施安全负主体责任。

2. 敏感个人信息

敏感个人信息是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. 跨境

跨境是指从一个司法管辖区域到另一个司法管辖区域的行为，而其中司法管辖区域是既包括具有独立主权的国家，也包括具有司法独立主权的地区。

4. 数据出境

以下情形属于数据出境行为：

（1）数据处理者将境内运营中收集和产生的数据传输、存储至境外；

（2）数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；

（3）国家网信部门规定的其他数据出境行为。

5.1 重要数据

重要数据指：一旦遭到篡改、破坏、泄露或者非法获取、非法利用等可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。如未公开的政府信息、大面积人口、基因健康、地理矿产资源等。

数据处理者需按照相关行业标准确定，以下为江苏版出境评估指南，仅供参考：

（1）未公开的政务数据、工作秘密、情报数据和执法司法数据；

（2）重点行业和领域安全生产、运行的数据，关键系统组件、设备供应链数据；

（3）达到国家有关部门规定规模或者精度的基因、地理、矿产、气象等国家基础数据；

（4）影响关键信息基础设施安全稳定运行的数据，国防设施、军事管理区、国防科研生产单位等重要敏感区域的地理位置、安保情况等数据；

（5）出口管制物项涉及的核心技术、设计方案、生产工艺等相关数据，密码、生物、电子信息、人工智能等领域对国家安全、经济竞争力有直接影响的科学技术成果数据；

（6）国家法律、行政法规、部门规章明确规定需要保护或者限制处理的国家经济运行数据、重要行业和领域业务数据、统计数据等；

(7) 其他一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

5.2 健康医疗行业的重要数据认定参考

健康医疗行业企业作为数据处理者时需根据法律、法规及相关行业标准界定相关出境数据是否为重要数据，由于目前健康医疗行业并未颁布对于“重要数据”识别的相关标准，在无相关参照下，可参考《信息安全技术 重要数据识别指南（征求意见稿）》规定的识别因素及过往《信息安全技术 数据出境安全评估指南（征求意见稿）》中针对不同行业给出的重要数据识别指南。

实践中，健康医疗行业企业需特别关注：涉及大面积人口、基因、公共健康和安全的数据构成重要数据，例如：反映群体健康生理状况、族群特征、遗传信息等的基础数据（如非公开的人口普查资料、生命登记信息、人类遗传资源信息、基因测序原始数据）；涉及人类遗传资源的临床试验数据；其他应当取得“重要数据”地位的健康医疗行业企业数据（如涉及国家战略安全的临床研究数据、涉及国家战略安全的药品生产过程数据及药品生产配方数据等）。

四、数据出境企业的合规要点

1. 企业进行数据出境风险自评估，需主要关注以下事项：

(1) 数据出境的目的、范围、方式等的合法性、正当性、必要性；

(2) 境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；

(3) 出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；

(4) 数据安全和个人信息权益是否能够得到充分有效保障；

(5) 数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；

(6) 遵守中国法律、行政法规、部门规章情况。

2. 数据处理者进行数据出境行为需要注意遵守的合规要点包括但不限于：

(1) 数据出境及境外接收方处理数据的目的、范围、方式需要具有合法性、正当性、必要性。

数据出境遵循本地化存储+最小必要化出境原则，即要求在履行工作职责和智能的安全主体，在法律和相关安全策略允许前提下，对受到保护的个人信息等数据仅能在最小必要范围内被共享和传输出境，尽量避免数据出境行为对国家安全、公共利益、个人或者组织合法权益带来风险。

(2) 数据资产情况、信息系统情况、数据出境涉及的数据中心（包含云服务）情况及数据出境链路相关情况的梳理和盘点。

对于出境数据的权属、规模、范围、种类、敏感程度等进行盘点，对于数据出境涉及的信息系统情况、数据

中心(包含云服务)情况及数据出境链路相关情况、境外接收方处理数据的流程等进行梳理和盘点。

(3)提升数据处理者及境外数据接收方的数据安全保障能力,降低数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险。

从技术、法律、管理三个维度提升数据处理者及境外数据接收方的数据安全保障能力,加强数据安全管理能力(包括管理组织体系和制度建设情况,例如全流程管理、分类分级、应急处置、风险评估、个人信息权益保护等制度及落实情况),提升数据安全技术能力(包括数据收集、存储、使用、加工、传输、提供、公开、删除等全流程所采取的安全技术措施等,并提供数据安全保障措施有效性证明)。

(4)个人信息主体的权益保护及个人信息权益维护的渠道。

个人信息处理者需建设完善的企业隐私合规体系及个人信息主体授权同意机制。个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制,个人信息处理者拒绝个人行使权利的请求的,应当说明理由。

(5)签订数据出境相关合同

与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等需充分约定数据安全保护责任义务,内容需包括:

a.数据出境的目的、方式和数据范围,境外接收方处理数据的用途、方式等;

b.数据在境外保存地点、期限,以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施;

c.对于境外接收方将出境数据再转移给其他组织、个人的约束性要求;

d.境外接收方在实际控制权或者经营范围发生实质性变化,或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时,应当采取的安全措施;

e.违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式;

f.出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时,妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

3.健康医疗行业企业数据出境合规要点详见本指南第二章之“三、健康医疗大数据出境及相关合规要点”。

五、违法数据出境的行为处罚措施及依据

违法数据出境行为可能给企业带来罚款、暂停相关业务、停业整顿、甚至是吊销相关业务许可证或者吊销营业执照的处罚风险,例如:

(1)《网络安全法》第66条规定:关键信息基础设施运营者违反相关该法规定在境外存储网络数据,或者向境外提供网络数据的,由有关主管部门责令改正,给予警告,没收违法所得,处五万元以上五十万元以下罚款,并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

(2)《数据安全法》第46条规定:违反该法相关规定,向境外提供重要数据的,由有关主管部门责令改正,给予警告,可以并处十万元以上一百万元以下罚款,对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款;情节严重的,处一百万元以上一千万元以下罚款,并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照,对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

(3)《个人信息保护法》第66、67条规定:违反该法规定处理个人信息,或者处理个人信息未履行该法规定的个人信息保护义务的,由履行个人信息保护职责的部门责令改正,给予警告,没收违法所得,对违法处理个人信息的应用程序,责令暂停或者终止提供服务;拒不改正的,并处一百万元以下罚款;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。有前款规定的违法行为,情节严重的,由省级以上履行个人信息保护职责的部门责令改正,没收违法所得,并处五千万元以下或者上一年度营业额百分之五以下罚款,并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照;对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款,并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。有该法规定的违法行为的,依照有关法律、行政法规的规定记入信用档案,并予以公示。

(4)《数据出境安全评估办法》第16、17条规定:任何组织和个人发现数据处理者违反该办法向境外提供数据的,可以向省级以上网信部门举报。国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的,应当书面通知数据处理者终止数据出境活动。数据处理者需要继续开展数据出境活动的,应当按照要求整改,整改完成后重新申报评估。

六、向境外监管机构、境外司法机构或境外执法机构提供数据

企业运营过程中可能经常会遇到境外政府部分因为国家安全、行政管理与市场监管、司法程序等原因要求企业向境外政府或监管机构提供或披露数据的情况。

“证据开示”指根据《联邦民事诉讼规则》(“Federal Rules of Civil Procedure”)第26条等相关规定,美国民事诉讼程序中的一方需要向另一方披露可能用于支持其主张或抗辩的自然人的姓名、其知晓的联系方式等;民事诉讼程序中的一方还需向另一方披露占有、存储或控制的文件、搜集的数据、有形资产等的复印件、分类描述及存储地(该法另有规定除外);原告必须在向被告送达诉状后召开双方当事人会议,以计划证据开示程序,各方应提议并就证据开示程序的时间安排达成一致,并在会议后14天内向法院提交证据开示计划。例如Philips Medical Systems (Cleveland), Inc. v. Buan案中,被告以禁止对外提供国家安全及其他敏感利益相关数据对于证据开示进行抗辩,但是法庭认为被告没有提供任何理由让他们认为提供与本案有关的信息会违反这些法律,没有证据表明中国政府可能会将被告掌握的相关信息视为涉及其国家安全或其他利益。

2020年12月,美国签署《外国公司问责法案》(Holding Foreign Companies Accountable Act),除了对于

受到该法规制的企业提出更高的信息披露要求之外，还表示如果美国上市公司会计监督委员会连续三年无法对一家在美上市公司的美国境外审计机构进行审查，美国证监会应当禁止该公司证券在美国的交易所或在美国境内以其他形式（比如通过场外OTC市场）进行交易。

与此相反，中国法律、法规对向外国行政机构提供或者外国行政机构调取我国境内数据存在限制，例如：

《个人信息保护法》第41条规定："中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息"。

《数据安全法》第36条规定："中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据"。

2022年4月2日，证监会会同财政部、国家保密局、国家档案局联合发布《关于加强境内企业境外发行证券和上市相关保密和档案管理工作的规定（征求意见稿）》，对于境内企业（或通过境外上市主体）向境外监管机构提供、披露文件资料提出了进一步的规范性要求，明确：境内企业向有关证券公司、证券服务机构、境外监管机构等单位和个人提供、公开披露，或者通过其境外上市主体等提供、公开披露涉及国家秘密、机关单位工作秘密的文件、资料的，应当依法报有审批权限的主管部门批准，并报同级保密行政管理部门备案，并且规定如果提供、公开披露其他泄露后会对国家安全或者公共利益造成不利影响的文件、资料，应当按照国家有关规定，严格履行相应程序，并与有关证券公司、证券服务机构依照《中华人民共和国保守国家秘密法》等法律、法规及该规定签订保密协议，明确有关证券公司、证券服务机构承担的保密义务和责任。此外，为境内企业境外发行证券和上市提供相关证券服务的证券公司、证券服务机构在境内形成的工作底稿等档案应当存放在境内，境内企业、有关证券公司、证券服务机构发现国家秘密已经泄露或者可能泄露的，应当立即采取补救措施并及时向有关机关、单位报告。境内企业向有关证券公司、证券服务机构、境外监管机构等单位和个人提供对国家和社会具有重要保存价值的会计档案或会计档案复制件的，应当按照国家有关规定履行相应程序。

因此，企业涉及需向境外监管机构、境外司法机构或境外执法机构等提供或披露存储于中国境内的数据或个人信息时，应当依法报有审批权限的主管部门批准，另外还需履行数据相关网信部门组织的安全评估等申报/备案手续（详见本指南正文部分第一章第一节和第二节）。

第二章 健康医疗大数据出境

一、健康医疗大数据

根据《信息安全技术 健康医疗数据安全指南》(GB/T 39725-2020)的规定,健康医疗大数据包括以下数据(该标准附录A对于个人健康医疗数据具有更为细致的列举,可按需参阅):

1.个人属性数据:具体包含姓名、年龄、性别、民族等人口统计信息;身份证、工作证、社保卡、住院号、检查检验单号和可识别的个人影像图像等个人身份信息;电话号码、邮箱等个人通讯信息;基因、指纹、声纹、虹膜等个人生物识别信息和个人健康监测传感设备ID等共计五小类。

2.健康状况数据:主要指患者主诉、现病史、既往病史、体格检查(体征)、家族史、症状、生活方式等相关信息。

3.医疗应用数据:主要包含门(急)诊病历、处方、检查检验报告、用药信息、病程记录等诊疗判断与行为,以及相关检查检验信息等。

4.医疗支付数据:一是指交易金额、交易项目、医保支付信息等医疗交易信息;二是指保险账号、保险金额、保险状态等保险信息。

5.卫生资源数据:包含医院基本数据、医院运营数据等。

6.公共卫生数据:具体包含环境卫生数据、传染病疫情数据、疾病监测数据、疾病预防数据、出生死亡数据等。

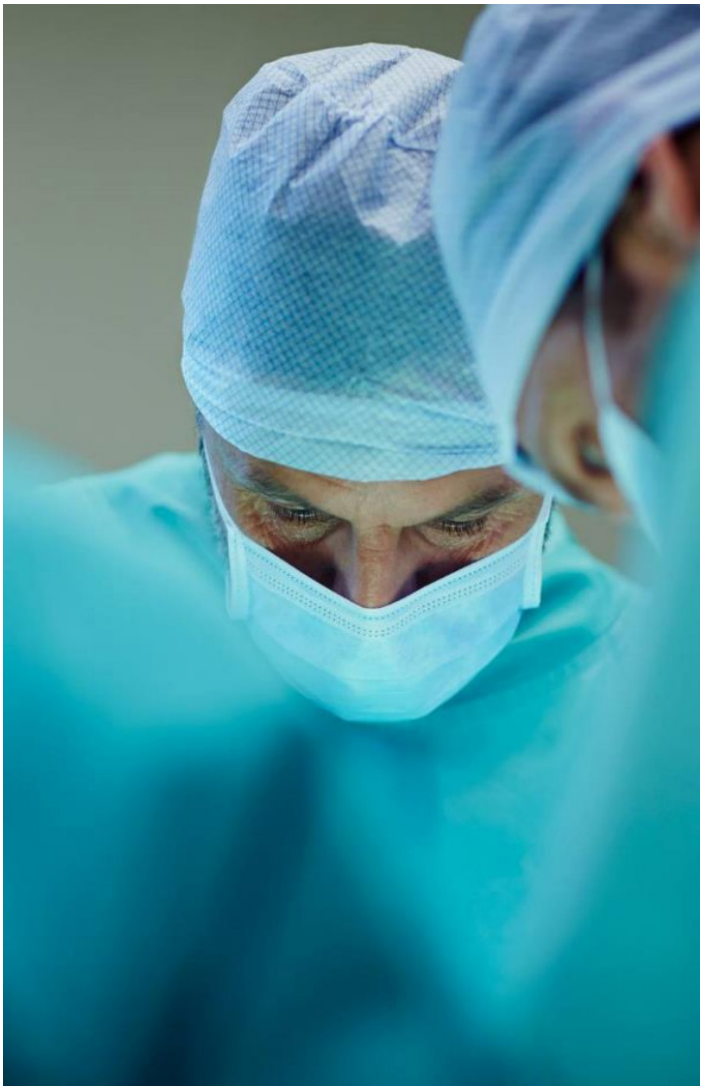
二、健康医疗大数据出境的可行性

根据《信息安全技术 健康医疗数据安全指南》(GB/T 39725-2020)的规定,健康医疗大数据的控制者因为学术研讨需要,需要向境外提供相应数据的,在进行必要的去标识化处理后,经过数据安全委员会讨论审批同意,数量在250条以内的非涉密、非重要数据可以提供,否则宜提请相关部门审批。不涉及国家秘密、重要数据或者其他禁止或限制向境外提供的数据,经个人信息主体授权同意,并经数据安全委员

会讨论审批同意，健康医疗大数据的控制者可向境外目的地提供个人健康医疗数据，累计数据量应控制在250条以内，否则应提请相关部门审批。

健康医疗大数据原则上只与有相应资质的境内单位开展合作研究，在未获得政府行业主管或监管部门批准合作项目批准的情况下，数据不予境外单位（含外国组织和个人以及在我国注册的外商独资企业和中外合资、合作企业）使用。

此外，由于健康医疗大数据与《网络安全法》、《数据安全法》以及《个人信息保护法》项下的“重要数据”和“个人信息”等概念存在部分重叠，因此健康医疗大数据的出境除了上述规定外，还需要依照《网络安全法》《个人信息保护法》《数据安全法》的规定履行相关程序（详见本指南第一章相关介绍）。



三、健康医疗大数据出境及相关合规要点

健康医疗大数据出境合规要点包括但不限于：

（1）与其他行业的企业一样，健康医疗数据出境需遵循“最少必要原则”，数据出境的目的、范围、方式需要具有合法性、正当性、必要性；

（2）数据开放的目的、内容、使用方等经过健康医疗大数据企业内部的数据安全委员会审批，确保符合合法性、正当性和必要性的要求；

（3）根据使用目的尽可能地去标识化；

（4）明确数据开发和使用目的、使用方需要承担的安全责任、安全措施等，并签署相应的协议；

（5）宜依规进行安全评估，涉及重要数据的应依规进行评估审批；

（6）需加强对健康医疗大数据的存储管理，健康医疗大数据应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律、法规及有关要求进行安全评估审核。此外，人口健康信息管理

责任单位不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。

此外，健康医疗大数据出境中对于数据处理者的合规要求包括但不限于：

1. 建立完善的组织保障体系

与其他行业的企业一样，出境健康医疗大数据的数据处理者宜建立完善的组织保障体系、健全的健康医疗大数据安全管理人才培养机制、健全的制度规范体系及完整的个人信息访问控制措施。

个人信息控制者在以下情况下需设立专职的个人信息保护负责人和个人信息保护工作机构：

（1）主要业务涉及个人信息处理，且从业人员规模大于200 人；

（2）处理超过100万人的个人信息，或预计在12个月内处理超过100万人的个人信息；

（3）处理超过10万人的个人敏感信息的。

此外，需注意处理健康医疗大数据的企业应建立健全相关安全管理制度（其中“数据使用管理办法”可参考《信息安全技术　健康医疗数据安全指南》附录C的示例）、操作规程和技术规范，落实“一把手”责任制，加强安全保障体系建设，强化统筹管理和协调监督，保障健康医疗大数据安全。处理健康医疗大数据的企业的组织架构中至少包括健康医疗数据安全委员会和健康医疗数据安全工作办公室，并需指定专人（例如DPO）负责健康医疗数据安全日常工作，以确保做好健康医疗数据安全管理工作，并形成相应的文档记录。处理健康医疗大数据的责任单位应当结合服务和管理工作需要，及时更新、甄别、优化和维护健康医疗大数据，确保信息处于最新、连续、有效、优质和安全状态。

2. 个人信息主体权益保护

（1）与其他行业的企业一样，出境健康医疗大数据的数据处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

a.制定内部管理制度和操作规程；

b.对个人信息实行分类管理；

c.采取相应的加密、去标识化等安全技术措施；

d.合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

e.制定并组织实施个人信息安全事件应急预案；

f.法律、行政法规规定的其他措施。

（2）个人信息主体的权益保护及个人信息权益维护的渠道

a.与其他行业的企业一样，出境健康医疗大数据的数据处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。出境健康医疗大数据的数据接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。出境健康医疗大数据的数据接收方变更原先的处理目的、处理方式的，应当依照本法规

定重新取得个人同意。单独同意过程不应捆绑与被同意事项不相关的任何业务功能或处理目的。

个人信息主体授权同意的例外。根据《信息安全技术 健康医疗数据安全指南》(GB/T 39725-2020)的规定，数据控制者即使没有获得主体的授权，在以下情况可以使用或披露相应个人健康医疗数据：

(i)向本人提供其本人健康医疗数据时；

(ii)治疗、支付或保健护理时；

(iii)涉及公共利益或法律、法规要求时；

(iv)受限制数据集用于科学研究、医学/健康教育、公共卫生目的时。在上述情况下，出境健康医疗大数据的数据处理者可依靠法律法规要求、职业道德、伦理和专业判断来确定哪些个人健康医疗数据允许被使用或披露。

b.基于个人同意处理个人信息的，个人有权撤回其同意，处理涉及健康医疗大数据的个人信息处理者应当提供便捷的撤回同意的方式。处理涉及健康医疗大数据的个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务（处理个人信息属于提供产品或者服务所必需的除外）。

c.个人请求查阅、复制其个人信息的，处理涉及健康医疗大数据的个人信息处理者应当及时提供。个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，处理涉及健康医疗大数据的个人信息处理者应当提供转移的途径。

d.个人发现其个人信息不准确或者不完整的，有权请求处理涉及健康医疗大数据的个人信息处理者更正、补充。个人请求更正、补充其个人信息的，处理涉及健康医疗大数据的个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

e.个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

f.有下列情形之一的，出境健康医疗大数据的数据处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

(i) 处理目的已实现、无法实现或者为实现处理目的不再必要；

(ii) 个人信息处理者停止提供产品或者服务，或者保存期限已届满；

(iii) 个人撤回同意；

(iv) 个人信息处理者违反法律、行政法规或者违反约定处理个人信息；

(v) 法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，出境健康医疗大数据的数据处理者应当停止除存储和采取必要的安全保护措施之外的处理。

(2) 处理敏感个人信息的特殊要求

由于健康医疗大数据可能涉及众多敏感个人信息，出境健康医疗大数据的数据处理者在数据全生命周期中均需注意：

a.只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，出境健康医疗大数据的数据处理者方可处理敏感个人信息。

b.个人信息主体需要对于种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等个人敏感信息场景下的授权同意，应进一步选择使用单独同意的方式以充分保障个人信息主体能充分知情和自主授权。如果出境健康医疗大数据的数据处理者处理不满十四周岁未成年人的个人信息的，应当取得未成年人的父母或者其他监护人的同意。

c.传输和存储个人敏感信息时，应采用加密等安全措施；存储个人生物识别信息时，应采用技术措施确保信息安全后再进行存储，例如将个人生物识别信息的原始信息和摘要分开存储，或仅收集、存储、使用摘要信息。

(3)制定个人信息保护政策

与其他行业的企业一样，出境健康医疗大数据的数据处理者应制定个人信息保护政策，内容应包括但不限于：对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及各自的安全和法律责任。

(4)建立个人信息保护影响评估机制

与其他行业的企业一样，出境健康医疗大数据的数据处理者向境外提供个人信息前应当事前进行个人信息保护影响评估，并对处理情况进行记录。

个人信息保护影响评估应当包括：个人信息的处理目的、处理方式等是否合法、正当、必要；对个人权益的影响及安全风险；所采取的保护措施是否合法、有效并与风险程度相适应。

3.制定并实施个人信息安全事件应急预案及安全审计机制

与其他行业企业一样，出境健康医疗大数据的数据处理者应对个人信息处理活动进行日常化的审计，确保安全管理措施到位、安全技术措施有效；此外，发生个人信息泄露、篡改、丢失时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。

4.数据共享或转移

处理健康医疗大数据的责任单位在选择健康医疗大数据服务提供商时，应当确保其符合国家和行业规定及要求，具备满足相关法律法规要求、落实相关标准、确保数据安全的能力，建立数据安全管理、应急响应管理等方面管理制度。

处理健康医疗大数据的责任单位发生变更时，应当将所管理的健康医疗大数据完整、安全地移交给承接延续其职能的机构或本行政区域内的卫生健康行政部门，不得造成健康医疗大数据的损毁、丢失和泄露。

5.健康医疗数据的分类分级

与其他行业企业一样，出境健康医疗大数据的数据处理者需建立并实施完善的数据分类分级制度。

健康医疗数据根据数据的重要程度、风险级别以及对个人健康医疗数据主体可能造成的损害和影响的级别进行分级，可将健康医疗数据划分为以下5级，并按照《信息安全技术　健康医疗数据安全指南》(GB/T

39725-2020）等相关规定的要求管理和使用，实施不同的安全措施：

（1）第1级：可完全公开使用的数据。包括可以通过公开途径获取的数据，例如医院名称、地址、电话等，可直接在互联网上面向公众公开。

（2）第2级：可在较大范围内供访问使用的数据。例如不能标识个人身份的数据，各科室医生经过申请审批可以用于研究分析；

（3）第3级：可在中等范围内供访问使用的数据，如果未经授权披露，可能对个人健康医疗数据主体造成中等程度的损害。例如经过部分去标识化处理，但仍可能获得重标识的数据，仅限于获得授权的项目组范围内使用。

（4）第4级：在较小范围内供访问使用的数据，如果未经授权披露，可能会对个人健康医疗数据主体造成较高程度的损害。例如可以直接标识个人身份的数据，仅限于参与诊疗活动的医护人员访问使用。

（5）第5级：仅在极小范围内严格限制条件下供访问使用的数据，如果未经授权披露，可能会对个人健康医疗数据主体造成严重程度的损害。例如特殊病种的详细资料，仅限于主旨医护人员访问且需要进行严格管控。

6. 强化安全保障措施、落实网络安全等级保护制度

出境健康医疗大数据的数据处理者应严格落实网络安全等级保护制度，遵守国家有关网络安全审查制度，并建立健全安全保障机制，强化安全保障措施。具体责任如下：

（1）加强健康医疗大数据相关系统安全保障体系建设，提升关键信息基础设施和重要信息系统的安全防护能力；

（2）定期对相关信息系统开展定级、备案和测评工作；

（3）建立健全涉及国家秘密的健康医疗大数据管理与使用制度，严格管理制作、审核、登记、拷贝、传输、销毁等环节；

（4）采取数据分类、重要数据备份、加密认证等措施；

（5）建立可靠的数据容灾备份工作机制，定期进行备份和恢复检测；

（6）为健康医疗大数据在不同系统间的交互、共享和运营提供安全与便利条件；

（7）提供安全的信息查询和复制渠道，确保公民隐私保护和数据安全；

（8）严格规范不同等级用户的数据接入和使用权限，确保数据在授权范围内使用；

（9）建立严格的电子实名认证和数据访问控制；

（10）建立健康医疗大数据安全监测和预警系统，建立网络安全通报和应急处置联动机制；

（11）依法对网络安全重大事件进行报告并处置。

7. 大数据服务提供者、大数据处理者须遵循大数据管理相关要求

若出境健康医疗大数据的数据处理者同时为大数据服务提供者（指拥有大数据平台和应用，提供大数据服务的组织或企业），还需满足大数据服务安全能力、大数据安全管理等要求。

法律、法规及参考文件(部分列举):

1.《中华人民共和国网络安全法》

2.《中华人民共和国数据安全法》

3.《中华人民共和国个人信息保护法》

4.《数据出境安全评估办法》

5.《数据出境安全评估指南》

6.《国家健康医疗大数据标准、安全和服务管理办法（试行）》

7.《人口健康信息管理办法(试行)》

8.《信息安全技术 健康医疗数据安全指南》（GB/T 39725-2020）

9.《信息安全技术 个人信息安全规范》（GB/T 35273-2020）

10.《信息安全技术 个人信息告知同意指南（征求意见稿）》

11.《信息安全技术 大数据服务安全能力要求(征求意见稿)》（20220157-T-469）

12.《信息安全技术 大数据安全管理指南》（GB/T 37973-2019）

第三章 遗传数据出境

一、遗传数据出境的可行性

人类遗传资源，包括人类遗传资源材料和人类遗传资源信息。人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料；人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料。

人类遗传资源的“出境或对外提供”方式根据遗传资源的分类包括：

a.材料出境：可能通过运送、邮寄或携带等方式；

b.信息出境：信息出境包括向外方提供或向外方开放使用。

人类遗传资源在符合国家法律、法规规定的情况下可以出境。人类遗传资源出境需符合伦理，不得危害公众健康、国家安全和社会公共利益，尊重人类遗传资源提供者的隐私权，取得其事先知情同意，并保护其合法权益，不包括以临床诊疗、采供血服务、查处违法犯罪、兴奋剂检测和殡葬等为目的采集、保藏人类遗传资源及开展的相关活动，并且符合国家法律法规规定的程序。禁止买卖人类遗传资源，为科学研究依法提供或者使用人类遗传资源并支付或者收取合理成本费用，不视为买卖。

具体来看，根据采集信息的主体不同。国内主体，在采集、保藏、利用、将我国人类遗传资源材料运送、邮寄、携带出境时，应当经过国务院科学技术主管部门批准；境外组织、个人及其设立或者实际控制的机构不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源。外方单位需要利用我国人类遗传资源开展科学研究活动的，应当采取与我国科研机构、高等学校、医疗机构、企业（以下简称：“中方单位”）合作的方式进行。由合作双方共同提出申请，经国务院科学技术行政部门批准。

根据遗传资源的分类。遗传资源材料的出境应当经过国务院科学技术主管部门批准，并由中方单位凭科技部人类遗传资源材料出境证明办理海关出境事宜；遗传资源信息的出境应当向国务院科学技术主管部门事先报告并提交信息备份。此外，如果将人类遗传资源信息向境外组织、个人及其设立或者实际控制的机构提供或者开放使用可能影响我国公众健康、国家安全和社会公共利益的，应当通过科技部组织的安全审查。

基因识别数据指使用技术手段，从人类遗传物质中提取的表征个体或群体遗传信息的数据，该数据可以直接或间接识别到人类个体或群体。基因识别数据主要包括：基因组核酸序列数据、功能基因组数据，以及提取过程中生成的原始数据和中间数据。根据法律规定，基因识别数据属于人类遗传资源信息的范畴。基因识别数据及关联信息不应出境，但取得数据主体的知情同意并获得有关部门批准的除外。

二、遗传数据出境需要履行的程序

1.根据遗传资源的分类，人类遗传资源信息出境需要科学技术部门备案（非基因遗传资源信息）或审批（基因识别数据及关联信息）＋科学技术部门安全审查（涉及公众健康、国家安全和社会公共利益的）；人类遗

传材料运送、邮寄、携带出境需要科学技术部门许可＋海关审批。

其中，非基因遗传资源信息出境需要向科技部提交备案，备案材料应当包含以下内容：

（1）对外提供或者开放使用我国人类遗传资源基因、基因组信息的目的、用途；

（2）向外方单位提供或者开放使用的人类遗传资源基因、基因组信息；

（3）信息接收单位信息；

（4）对我国人类遗传资源保护可能造成潜在风险的评估。

上述备案程序如下：

申请人登录网上平台，提交信息备份，并确定备份成功，获得信息备份号。 → 信息备份成功后，申请人可登录网上平台（网址：https://grants.-most.gov.cn）在线提交备案材料，获得备案号。 → 申请人获得备案号，即可将人类遗传资源信息向外国 组织、个人及其设立或者实际控制的机构提供或开放使用。

2.开展国际合作，需要我国人类遗传资源材料出境的，可以单独提出申请，也可以在开展国际合作科学研究申请中列明出境计划一并提出申请，由科技部合并审批。由中方单位凭科技部人类遗传资源材料出境证明办理海关出境事宜。为获得相关药品和医疗器械在我国上市许可，在临床机构利用我国人类遗传资源开展国际合作临床试验、不涉及人类遗传资源材料出境的，不需要审批，但是合作双方在开展临床试验前应当将拟使用的人类遗传资源种类、数量及其用途向国务院科学技术行政部门备案。

利用我国人类遗传资源开展国际合作科学研究的，应当符合下列条件：

（1）对我国公众健康、国家安全和社会公共利益没有危害；

（2）合作双方为具有法人资格的中方单位、外方单位，并具有开展相关工作的基础和能力；

（3）合作研究目的和内容明确、合法，期限合理；

（4）合作研究方案合理；

（5）拟使用的人类遗传资源来源合法，种类、数量与研究内容相符；

（6）通过合作双方各自所在国（地区）的伦理审查；

（7）研究成果归属明确，有合理明确的利益分配方案。

3.如果人类遗传资源信息的对外提供可能会影响我国公众健康、国家安全和社会公众利益的，应当通过科技部组织的安全审查。

根据《人类遗传资源管理条例实施细则（征求意见稿）》，安全审查的情形包括对外提供或者开放使用以下信息：

（1）重要遗传家系的人类遗传资源信息；

（2）特定地区的人类遗传资源信息；

(3)500人以上人群的外显子组测序、基因组测序信息资源;

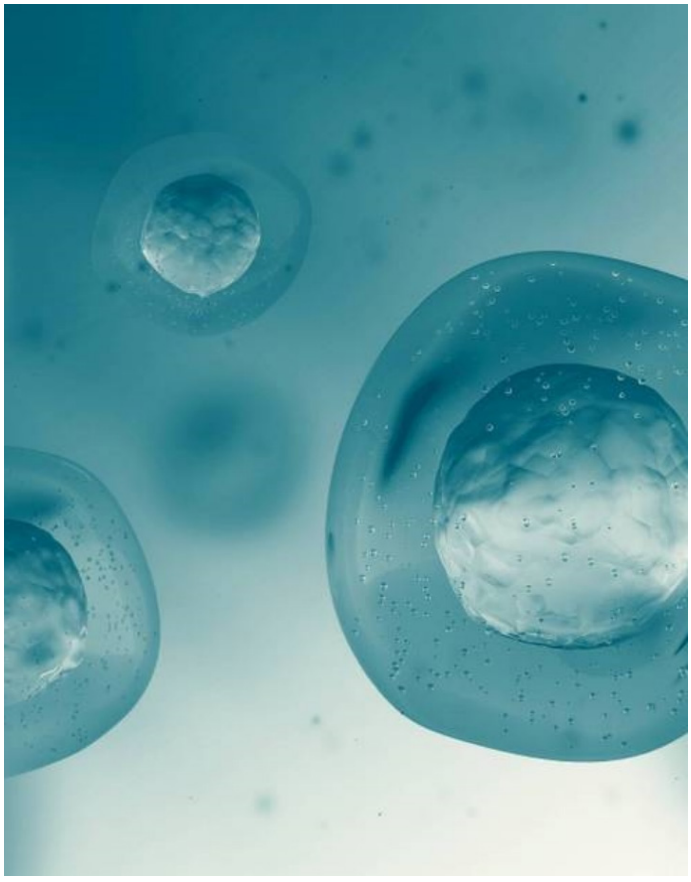
(4)可能影响我国公众健康、国家安全和社会公共利益的其他信息。

4.根据《信息安全技术　重要数据识别指南(征求意见稿)》关于重要数据的识别因素的规定,人类遗传信息及基因测序原始数据属于重要数据,并且人类遗传信息甚至可能构成"关系国家安全、国民经济命脉、重要民生、重大公共利益等"的国家核心数据。不过是否所有类型的人遗资源信息都将被认定为重要数据,目前尚未有明确的答案。因此,向境外提供人类遗传资源信息的,还应注意遵守《网络安全法》的规定,进行网信部门要求的安全评估(如需)。

遗传资源信息中的基因识别信息具有识别性,可能构成个人信息,而其他人类遗传资源信息除非在经过匿名化处理或者该自然人没有被识别或者无法被识别的情况下,也可被视作为个人信息。对于属于个人信息的部门的数据出境,除了前述需要科技部门审批或者许可外,还需要依照《网络安全法》、《个人信息保护法》等法律、法规、规范性文件的规定进行安全评估和需要个人同意,履行数据出境相关申报/备案等程序(详见本指南第一章相关介绍)。

三、遗传数据出境的合规要求

遗传数据出境中对于数据处理者的合规要求包括但不限于:



1.对于拥有基因识别数据的数据控制者,应要履行以下义务:

(1)设立专门数据管理机构(如:数据管理委员会),制定个人信息保护政策,建立数据安全管理机制,形成完整的信息安全管理体系,确保基因识别数据及关联信息全生命周期的安全性,保障数据主体的合法权益。

(3)应针对基因识别数据相关的特有智能设备(如:测序仪、质谱仪、生物计算服务器等)和业务特点,制定和实施相关的安全管理制度和技术措施(如:网络隔离措施、访问控制措施、入侵防范措施等)。

(4)当发生基因识别数据及关联信息被窃取、篡改、丢失、泄露、损毁等安全事件

时，应按照规定向相关部门报告；及时采取应急处置及补救措施；应按照规定通过邮件、信函、电话、推送通知等方式及时告知数据主体；难以逐一告知数据主体时，应采取合理、有效的方式公开发布相关的警示信息。

(5) 应建立数据主体撤回授权、投诉及跟踪处理机制，并在承诺时限内对数据主体的相关请求进行响应。

2.采集、保藏、利用、对外提供我国人类遗传资源，应当

(1) 符合伦理原则，按照国家有关规定进行伦理审查，符合相关规定要求的范围的还需取得行政许可；

(2) 尊重人类遗传资源提供者的隐私权，取得其事先知情同意，并保护其合法权益；

(3) 遵守国务院科学技术行政部门制定的技术规范。

3.参见本指南第二章第三部分之“三、健康医疗大数据出境及相关合规要点”中列举的其他合规要点。

法律、法规及参考文件(部分列举)：

1. 《中华人民共和国网络安全法》
2. 《中华人民共和国数据安全法》
3. 《中华人民共和国个人信息保护法》
4. 《数据出境安全评估办法》
5. 《数据出境安全评估指南》
6. 《中华人民共和国人类遗传资源管理条例》
7. 《人类遗传资源管理条例实施细则（征求意见稿）》
8. 《中华人民共和国生物安全法》
9. 《人类遗传资源采集、收集、买卖、出口、出境审批行政许可事项服务指南》
10. 《信息安全技术 基因识别数据安全要求》（征求意见）》
11. 《信息安全技术生物特征识别信息保护基本要求（征求意见）》
12. 《人类遗传资源管理条例实施细则（征求意见）》
13. 《信息安全技术 个人信息处理中告知和同意的实施指南（征求意见稿）》
14. 《互联网个人信息安全保护指南》

第四章 药企经营数据出境

一、药企经营数据出境的可行性

药物生产、销售企业（以下简称："药企"）作为特殊行业企业，无论其ERP系统数据出境还是药物研究数据出境均需按照出境数据的性质、数量等履行审批或备案手续。

场景1：药企ERP系统数据出境

《工业和信息化部关于进一步推进中小企业信息化的指导意见》中鼓励和支持中小企业充分利用云计算、大数据、移动互联网等信息技术，并提倡进一步推广经营管理信息化软件（ERP/OA/CRM等）的应用，其中，企业资源计划（Enterprise Resource Planning，ERP）是企业运用信息技术提升企业经营效率和管理水平的重要手段。在云计算的大趋势下，现代ERP系统可以一站式提供财务、营销、制造、采购、人力等领域的系统服务，全面赋能企业在供应链、生产、财税、营销等领域的创新升级。

药企ERP系统数据出境可能触发法律规制的情形例如：

（1）药企内部员工个人信息，若药企ERP系统收集和处理药企内部员工的个人信息，涉及个人信息（特别是个人敏感信息）出境达到一定数量。

（2）顾客信息，若药企ERP系统收集和处理顾客的个人信息，涉及个人信息（特别是个人敏感信息）出境且达到一定数量。

（3）药企ERP系统收集和处理的信息涉及健康医疗数据。

（4）ERP系统出境数据涉及重要数据，例如中国家战略安全药品的生产过程数据。

场景2：药企经营中产生的员工数据、财务数据出境

同其他行业的企业一样，药企的其他非行业特殊的经营数据（例如员工数据、财务数据等）需根据其数据

性质，依照《网络安全法》《个人信息保护法》《数据安全法》等规定履行数据出境相关申报/备案等程序（具体参考第一章相关介绍）。

二、药企运营数据出境的合规要求

药厂的企业运营数据出境的合规要求具体如下：

1. 药企ERP系统数据

药企作为其客户信息以及内部员工的个人信息的收集和处理者，数据出境主要关注点在于敏感个人信息或非敏感个人信息的出境数量，采取不同的数据出境合规路径。《个人信息保护法》第38条明确，境内企业向境外提供个人信息，可以通过国家网信部门安全评估、个人信息保护认证或者签订国家网信部门制定的标准合同等三种路径依法实现数据出境。药企应当注意三种路径的适用的要求各有不同，尽可能选择符合自身需求的路径。

此外，药企涉及重要数据出境的，需要申报数据出境安全评估。药企涉及健康医疗数据出境的，需根据数据性质履行相关申报/备案等程序（详见本指南第二章相关介绍）

2. 药企的药物临床试验数据

临床试验阶段所产生的源数据指临床试验中产生的原始记录、文件和数据，如医院病历、医学图像、实验室记录、备忘录、受试者日记或者评估表、发药记录、仪器自动记录的数据、缩微胶片、照相底片、磁介质、X光片、受试者文件，药房、实验室和医技部门保存的临床试验相关的文件和记录，包括核证副本等。

2022年5月9日，国家药监局发布《中华人民共和国药品管理法实施条例（修订草案征求意见稿）》，该条例第23条明确了境外数据接受的相关要求。药品注册申请人在境外取得的临床试验数据，在符合NMPA要求时可用于药品上市许可申请，且境外药企在境内进行的国际多中心临床试验，符合相关要求的，临床试验数据可用于药品在境内进行上市申报。从该条例可以看出，以药品取得境内上市许可为目的，无论研制活动在境外还是境内进行，都应当符合我国相关法律、法规的要求。

该条例第40条（对于该条例现行有效版本第34条进行修订）规定：国家对获批上市部分药品的未披露实验数据和其他数据实施保护，药品上市许可持有人以外的其他人不得对该未披露试验数据和其他数据进行不正当的商业利用。在该药品数据保护制度下，第三人若使用未披露的该等数据则有可能构成不正当的商业利用。同时，该条例第178条规定了药监部门及其工作人员泄露未披露试验数据或者其他数据的情况下应当承担的赔偿责任以及相应的行政处分。

临床试验的数据在不涉及人类遗传资源等其他重要数据的情形下，包含个人信息（特别是敏感个人信息）出境如达到《数据出境安全评估办法》的数量要求则需要申报数据出境安全评估，未达上述标准则可选择签订国家网信部门制定的标准合同出境或第三方机构个人信息保护认证出境。

此外，需要关注的临床试验中有关数据保护的合规要点包括但不限于：

(1)受试者的姓名以受试者鉴认代码(指临床试验中分配给受试者以辨识其身份的唯一代码)代替以保护其隐私,研究者在报告受试者出现的不良事件和其他与试验有关的数据时应使用该代码。

(2)药物临床试验不仅触及人类遗传资源信息保护,同时触及受试者的个人敏感信息保护。在临床药物试验中,须在受试者签署的知情同意书中列明法律法规中约定的信息(例如境外接收方相关信息),并取得受试者的单独同意。

(3)开展药物、医疗器械临床试验和其他医学研究均应当遵守医学伦理规范,依法通过伦理审查,取得知情同意。药物临床试验用药品的管理应当符合药物临床试验质量管理规范的有关要求。获准开展药物临床试验的,申办者在开展后续分期药物临床试验前,应当制定相应的药物临床试验方案,经伦理委员会审查同意后开展,并在药品审评中心网站提交相应的药物临床试验方案和支持性资料。

3. 药企的科学数据

根据《科学数据管理办法》第25条规定,涉及国家秘密、国家安全、社会公共利益、商业秘密和个人隐私的科学数据,不得对外开放共享;确需对外开放的,要对利用目的、用户资质、保密条件等进行审查,并严格控制知悉范围。药企在药品研发的过程中形成的相关科学数据的数量或者性质如符合上述范围的要求,在数据出境场景也应当进行审查。

药企的药物临床试验、药物生产数据中的重要数据和相关个人信息在面临数据出境时需要考虑的数据出境合规范围较大,应遵守相应法律、法规对需要进行安全评估的重要数据和个人信息开展系统全面的自评估工作,结合药企的医药创新需求,规范药企数据出境行为,降低我国医药数据出境风险。

三、与药企数据相关的企业上市要求

2022年7月29日,中国证监会公布《公开发行证券的公司信息披露编报规则第25号——从事药品及医疗器械业务的公司招股说明书内容与格式指引》中要求相关发行人应披露报告期内下列与公司研发情况有关的信息,其中包含主要研发项目已进入或已完成临床试验的,披露临床试验情况,包括:主要临床前研究数据、临床试验境内外获批和准许情况,临床试验进展,试验方案重大调整或变更、临床试验暂停或终止,临床试验期间是否发现存在安全性问题或者其他风险等;相关发行人应对临床试验进度、安全性、有效性等进行分析。由此可见,药企上市程序中的药物临床试验数据管理及安全性问题受到证监会重点关注。

法律、法规及参考文件(部分列举):

1. 《中华人民共和国网络安全法》
2. 《中华人民共和国数据安全法》
3. 《中华人民共和国个人信息保护法》
4. 《数据出境安全评估办法》

5.《数据出境安全评估指南》

6.《科学数据管理办法》

7.《药品注册管理办法》

8.《中华人民共和国药品管理法实施条例（修订草案征求意见稿）》

9.《药物临床试验质量管理规范》

10.《药品记录与数据管理要求（试行）》

11.《药物临床试验质量管理规范》

12.《工业和信息化部关于进一步推进中小企业信息化的指导意见》

13.《公开发行证券的公司信息披露编报规则第25号——从事药品及医疗器械业务的公司招股说明书内容与格式指引》

第五章 健康穿戴设备数据出境

一、健康穿戴设备数据

健康传感数据是指通过健康传感器采集的,在软件支持下感知、记录、分析,与被采集者健康状况相关的,应用于医疗服务和健康生活的一切数据。例如:监测诊疗数据(血氧饱和度、血压、血糖、心率、睡眠)、行为情绪数据(跑步距离、行走轨迹、步数、消耗能量、锻炼时长)、环境数据(紫外线指数、污染指数、温度、湿度、噪声)。

一般情况下,当可穿戴设备的目标人群为健康人群且仅用于非医疗目的的记录统计健康信息(如睡眠监测、体重监测、生活方式记录等)时,该等可穿戴设备可被视为普通的电子消费产品;而当可穿戴设备是预期用于疾病管理的,实现一项或多项医疗用途(如无创血糖监测、无创血液监测、远程诊疗等)的设备或是含有实现一项或多项医疗用途的软件的设备时,属于移动医疗器械。

根据《信息安全技术 健康医疗数据安全指南》(GB/T 39725-2020)相关规定,可穿戴设备采集的与个人健康相关的数据属于个人健康医疗数据,具体表现为:

(1)本身或者明显为健康医疗相关数据;

(2)或是由传感器采集的,并且可以单独或者与其他数据结合用来对可穿戴设备的用户的健康状况或者疾病风险进行判断的数据;

(3)或是可穿戴设备采集的数据并且为对用户中的健康状况或者疾病风险进行判断后的结论;

(4)或是通过可穿戴设备相连的 APP 或者系统进行提供的,并非可穿戴设备使用者另行提供的。

目前,在中华人民共和国境内所产生的健康和医疗数据的相关安全管理和服务管理工作的监管主要由国家卫生健康委员会/县级以上卫生健康行政部门会同相关部门依据《国家健康医疗大数据标准、安全和服务管理办法(试行)》的规定负责。除了传统的疾病防治过程中产生的健康医疗数据,如远程诊疗过程中产生的诊治情况、病史、病症、用药记录等,人们在日常生活中利用可穿戴设备进行健康管理过程中产生的健康医疗相关的数据也在《国家健康医疗大数据标准、安全和服务管理办法(试行)》管理和保护范围内。因此,除了医疗机构、医疗器械设备生产/销售企业或医疗器械软件运营企业外,即使企业所生产和销售的可穿戴设备并不属于移动医疗器械,只要其在提供健康管理服务过程中涉及与健康医疗相关的数据,其可能属于国家健康医疗大数据标准、安全和服务管理办法(试行)》所规定的责任单位,并因此需要遵从该办法关于健康医疗大数据的安全管理和服务管理等的要求。

二、健康穿戴设备数据出境的可行性

健康穿戴设备数据出境与其他健康医疗大数据出境所需经过的审批流程相一致,在不涉及国家秘密、重要数据或者其他禁止或限制向境外提供的数据时,经佩戴健康传感设备的人员的授权同意,并经数据安全委员会讨论审批同意,健康穿戴设备数据的控制者(指使用健康传感设备采集健康医疗数据的机构包括但不限

于医疗机构、医保机构、健康服务企业，下同）可向境外目的地提供个人健康医疗数据，但是累计数据量宜控制在250条以内，否则宜提请相关部门审批（参见本指南第二章“健康医疗大数据出境”相关内容）。

三、健康穿戴设备产生的个人信息出境的合规要求

健康穿戴设备产生的个人信息出境中对于数据处理者的合规要求包括但不限于：

1.与其他健康医疗大数据出境一致，健康穿戴设备产生的个人信息出境应遵循“最少必要原则”，并且在程序上，数据开放的目的、内容、使用方等要经过数据安全委员会审批，确保符合合法性、正当性和必要性的要求，涉及需要进行数据出境风险评估审批的应当进行审批后方可出境（详见本指南第一章相关介绍）；涉及重要数据的应依规进行出境风险评估审批并根据使用目的尽可能地去标识化，明确数据使用目的、使用方需要承担的安全责任、安全措施等。

2.与其他健康医疗大数据出境一致，出境健康穿戴设备数据的处理者需要根据数据开放的形式有针对性做出相应安全措施。

3.与其他健康医疗大数据出境一致，在隐私保护方面，出境健康穿戴设备数据的处理者需要注意：

（1）使用和披露健康传感数据宜征得主体同意；

（2）健康传感数据集成之后宜向主体说明应用目的和共享对象。

4.与其他健康医疗大数据出境类似，在数据采集方面，出境健康穿戴设备数据的处理者需要注意：

（1）健康传感设备宜支持用户认证，确保合法的控制和使用健康传感设备，用户认证手段包括但不限于虹膜识别、指纹识别、密码技术。

（2）采集控制措施，用户可开启或关闭数据采集，可选择上传的内容。

（3）如果健康传感设备通过网络向终端应用传输采集的健康数据，宜支持节点认证机制。

5.与其他健康医疗大数据出境一致，传输安全方面，出境健康穿戴设备数据的处理者需要注意：宜采用校验技术或密码技术保证个人健康医疗数据在传输过程中的保密性、完整性，加密方法的选择宜考虑应用场景、传输方式、数据规模、效率要求等。设备宜默认开启数据加密功能。

6.与其他健康医疗大数据出境类似，在数据存储方面，出境健康穿戴设备数据的处理者需要注意：

（1）采用电子签名及时间戳等技术来保证数据的完整性和可追溯性。

（2）确保数据可用性。制定数据备份及恢复策略，定期进行数据备份，建立介质存取、验证和转储管理制度。通过高性能、可扩展的数据库服务确保各类业务对数据获取服务的性能要求。

（3）建立远程控制措施，一旦设备被窃或丢失，可自行选择删除设备中存储的数据。

（4）健康传感设备宜支持个人健康数据的存储加密。

7.与其他健康医疗大数据出境一致，在数据使用方面，出境健康穿戴设备数据的处理者需要注意：

（1）建立数据访问认证和授权机制。建立完善的身份认证以及基于角色的权限控制，严格区分不同用户

角色对数据访问的权限。合理、精细的定义角色权限，避免不必要的、超过角色合法职责之外的授权。

(2)对健康传感数据的使用活动进行审计，重点对健康医疗数据的访问及操作的合规性进行审计，确定必要的审计控制范围和需要审计的数据，宜采取相应技术手段，保证审计日志的完整性。

8.为使医疗健康可穿戴设备对其设备和应用中处理的数据提供完善的安全保护机制，基于泄露对用户隐私造成的影响，将医疗健康可穿戴设备的数据分为2级，分别是敏感级数据、一般级数据。其中，敏感级指一旦泄露对用户生命、财产、健康等产生严重影响，例如个人身份信息、个人生物特征信息、疾病史等，一般级指一旦泄露对用户生命、财产、健康产生较少或可控的影响、或不会产生影响，例如一般的个人健康数据、监测诊疗数据、行为情绪数据、环境数据、设备数据等。

出境健康穿戴设备数据的处理者需要对于敏感级的数据做好进行境内储存、加密、分类分级、去标识化、备份恢复等工作。

9.参见本指南第二章第三部分之“三、健康医疗大数据出境及相关合规要点”中列举的其他合规要点。

法律、法规及参考文件(部分列举)：

1.《中华人民共和国网络安全法》

2.《中华人民共和国数据安全法》

3.《中华人民共和国个人信息保护法》

4.《数据出境安全评估办法》

5.《数据出境安全评估指南》

6.《医疗器械生产监督管理办法》

7.《医疗器械监督管理条例》

8.《移动医疗器械注册技术审查指导原则》

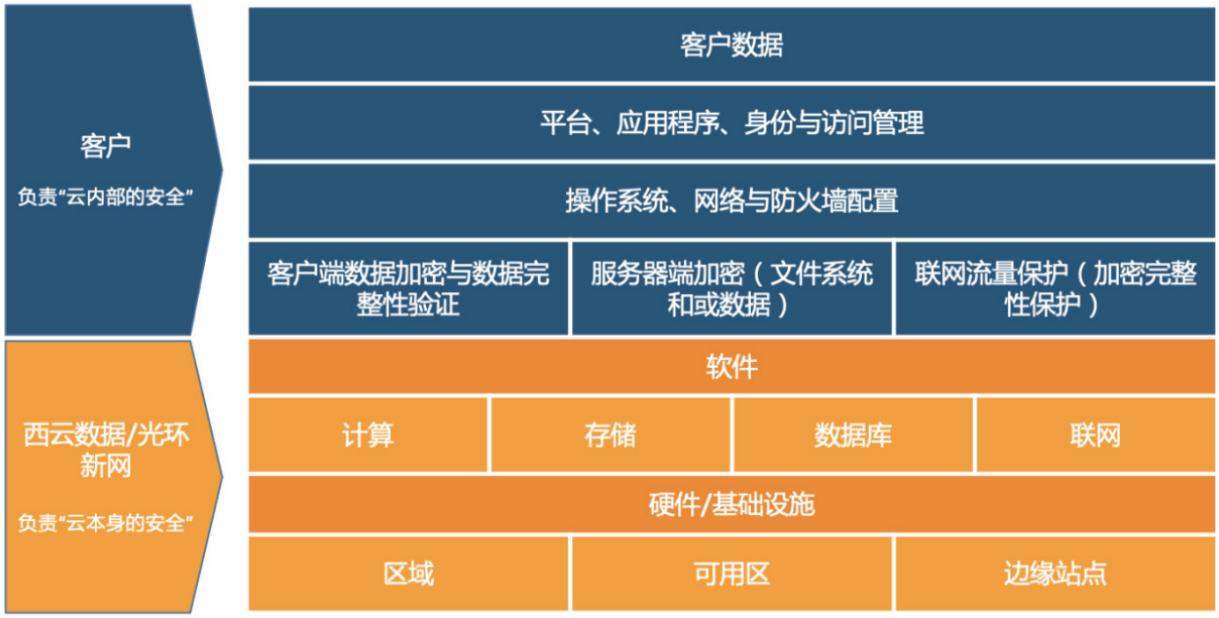
9.《国家健康医疗大数据标准、安全和服务管理办法（试行）》

10.《信息安全技术 健康医疗数据安全指南》（GB/T 39725-2020）

第六章 亚马逊云科技助力健康医疗行业

一、亚马逊云科技服务的责任共担模型

安全性和合规性是亚马逊云科技运营方和客户的共同责任。这种共担模型可以减轻客户的运营负担，因为西云数据/光环新网（分别作为亚马逊云科技中国（宁夏）区域和（北京）区域的运营方）负责运行、管理和控制从主机操作系统和虚拟层到服务运营所在设施的物理安全性的组件。客户负责管理来宾操作系统（包括更新和安全补丁）、其他相关应用程序软件以及亚马逊云科技运营方提供的安全组防火墙的配置。客户应该仔细考虑自己选择的服务，因为他们的责任取决于所使用的服务，这些服务与其 IT 环境的集成以及适用的法律法规。责任共担还为客户提供了部署需要的灵活性和控制力。如下图所示，这种责任区分通常涉及云“本身”的安全和云“内部”的安全。



西云数据/光环新网负责“云本身的安全”–西云数据/光环新网负责保护其各自运营的所有亚马逊云科技服务的基础设施。该基础设施由运行亚马逊云科技服务的硬件、软件、网络和设备组成。

客户负责“云内部的安全”– 客户责任由客户所选的亚马逊云科技服务确定。这决定了客户在履行安全责任时必须完成的配置工作量。例如，Amazon Elastic Compute Cloud (Amazon EC2) 等基础类型的服务，因此要求客户执行所有必要的安全配置和管理任务。部署Amazon EC2实例的客户需要负责来宾操作系统（包括更新和安全补丁）的管理、客户在实例上安装的任何应用程序软件或实用工具，以及每个实例上亚马逊云科技运营方提供的防火墙（称为安全组）的配置。 对于抽象化类型的服务，例如Amazon S3 和Amazon DynamoDB，西云数据/光环新网运营基础设施层、操作系统和平台，而客户通过访问终端节点存储和检索数据。客

户负责管理其数据(包括加密选项),对其资产进行分类,以及使用Amazon IAM工具分配适当的权限。

亚马逊云科技的“责任共担模型”,为云安全的建设设定了基本的原则。亚马逊云科技运营方负责云自身的安全,客户负责云中自身业务的安全,亚马逊云科技运营方会提供多层次的安全防护服务帮助提升客户云中的安全防护。亚马逊云科技的“责任共担模型”降低了客户管理、运营底层基础设施的复杂性并节省了成本,同时为客户提供了部署需要的灵活性和控制力。

二、广泛且严格的安全性与合规性

亚马逊云科技旨在帮助客户在云中运行和管理最敏感的医疗保健和生命科学工作负载,提供行业领先的服务和功能,让客户能够(i)控制其数据的存储位置和访问权限以及(ii)保护数据、账户和工作负载免受未经授权的访问。亚马逊云科技支持众多安全标准与合规性认证,客户可利用亚马逊云科技继承全面的合规性控制,并借助其提供的自动化合规工具、最佳经验及专家指导,保持和加强企业健康医疗数据的控制,并负责根据其特定需求实施额外的安全措施,包括内容分类、加密、访问管理和安全凭据,降低安全与合规的复杂性、成本并节省时间。亚马逊云科技定期对数千个全球合规性要求进行第三方验证,并持续监控这些要求。

三、全球领先的安全理念和全方位的安全服务

为帮助客户提升云中的安全防护,亚马逊云科技提出云上安全三大理念,并包括全方位的涵盖威胁检测和事件响应、身份认证和访问控制、网络和基础设施安全、数据保护与隐私以及风险管控及合规五大领域超过280个安全合规服务和功能。

利用云上的事件驱动型架构去构建自动化防护栏,而非设立关卡。亚马逊云科技认为,自动化是实现云上规模化安全的重要一环。只有建立起一套从威胁检测到事件响应、原因分析、恢复的自动化防护,才能在实现安全的同时解放开发团队的精力,使之专注于业务创新。亚马逊云科技提倡通过服务间的深度集成实现安全的自动化并降低风险,通过一套完整的API管理和安全工具,实现自动执行安全任务,包括持续进行的运行状态检测和保护、威胁修复和响应等,减少人工配置错误,让开发团队将更多时间精力投入到其他关键业务中去。

云中安全是主动设计出来的,而不仅是被动响应。应该将“安全”与“业务”视为硬币的两面,彼此紧密融合。因此安全应该是基于主动设计,而不是出现事件之后才响应。亚马逊云科技的安全团队从一开始就深入参与新服务和新功能开发,如果存在任何已知的安全问题,新服务将不会部署。亚马逊云科技上的服务均有安全基线,客户无论规模大小均可基于亚马逊云科技强扩展性、高度可靠的基础设施和服务,快速、安全地部署应用程序和数据,开展云上业务创新。

云中安全必须是一个洋葱型的多层防护,而不是一个鸡蛋。相比于像鸡蛋有一层看起来坚硬的外壳,云上安全更需要洋葱式层层递进的防护机制。亚马逊云科技构建了安全的全球云基础设施,客户无论规模大小

均可获得一致的云安全体验。亚马逊云科技的基础设施不仅根据安全最佳实践和最高标准来建立和管理，而且还考虑了云的独特需求，采用冗余和分层控制、持续验证和测试，大量使用自动化，确保底层基础设施得到7X24小时全天候的监控和保护。在适用法律法规允许的前提下，亚马逊云科技使用相同的安全硬件和软件来构建和运营全球每个区域。

威胁检测与事件响应：检测是安全生命周期的重要组成部分，可用于支持安全流程，还可以用于威胁识别和响应工作。客户使用检测服务和功能，可以识别潜在安全配置错误、威胁或其他行为。重点服务：威胁检测服务Amazon GuardDuty可持续监测恶意活动和未经授权的行为，该服务具有丰富的情报源并集成了机器学习的能力，可实现威胁的精准定位，并对安全事件进行快速响应；Amazon Security Hub安全事件统一管理平台为客户提供了一个统一的安全事件视图，并可根据不同的标准和最佳实践持续对客户的云环境进行合规性检查，快速发现技术差异并提供修复方案。

身份认证与访问控制：亚马逊云科技为客户提供强大的身份管理和权限管理，确保只有得到授权的人员才能访问对应的资源。亚马逊云科技提供了大量帮助客户管理用户身份及其权限的服务及功能，客户可以根据业务的需要，进行最小化的授权，并且对授权策略进行审核，以确保访问策略的安全性。重点服务：Amazon Identity and Access Management以细颗粒度的身份认证与访问控制机制，结合对安全事件的持续监控和精准的安全权限设置，保障相关资源被有相应权限的人员访问。

网络与基础设施安全：亚马逊云科技在主机、网络和应用程序级别边界为客户提供细粒度的保护。其中，Amazon Virtual Private Cloud (Amazon VPC)安全组在主机级别为客户在亚马逊云科技工作负载中的资源提供保护。对于Web应用程序保护，Amazon WAF允许客户过滤Web请求的与规则不匹配部分，以阻止常见的攻击模式。客户还能通过与Amazon Firewall Manager的集成，对不同账号的网络安全防护实施统一的策略。

数据保护与隐私：亚马逊云科技数据保护服务提供加密、密钥管理和威胁检测功能，可以持续保护客户数据、监控和保护客户的账户和工作负载。亚马逊云科技上有很多不同的方法帮助用户实施数据保护。其中，Amazon Key Management Service (Amazon KMS)为客户提供数据加密，可帮助用户大幅减少人工操作，降低出错概率。

四、植根中国的配套技术解决方案

近年来，生命科学行业跨国企业持续“植根中国”、“加码中国”。如今，中国市场不仅仅是增长引擎，更是创新引擎，随着经济发展、产业升级、创新能力提升，跨国HCLS企业纷纷在中国建立研究和创新中心，加大研发投入。这就意味着企业在中国市场产生出越来越多的数据。这些在中国产生的数据应当按照中国相关法律法规和行业合规要求进行保存、流转、追溯，保障数据的完整性、安全性、隐私性、机密性等。

亚马逊云科技从2013年起进入中国，致力于在中国长期投资和发展。2016年9月，由光环新网运营的亚马逊云科技中国（北京）区域正式商用。2017年12月，由西云数据运营的亚马逊云科技中国（宁夏）区域正式

上线。

西云数据运营的亚马逊云科技中国（宁夏）区域和光环新网运营的亚马逊云科技中国（北京）区域严格按照中国法律法规的监管要求依法合规经营。亚马逊云科技向西云数据和光环新网提供行业领先的技术、指导和专业知识，西云数据和光环新网运营并向客户提供亚马逊云科技云服务。前述两个中国区域所提供的云服务与其它亚马逊云科技区域所提供的云服务相同，但是又与所有其它亚马逊云科技区域隔离，客户可以通过将其数据存储在亚马逊云科技中国区域来满足数据驻留中国大陆境内的要求。

西云数据运营的亚马逊云科技中国（宁夏）区域和光环新网运营的亚马逊云科技中国（北京）区域通过独立的第三方机构验证其标准符合能力，已经完成了网络安全等级保护三级测评，还获得了可信云服务评估，以及在国内也通行的ISO9001质量管理体系认证、ISO20000信息技术服务体系认证、ISO27001信息安全管理体系认证、ISO27017云服务信息安全管理体系认证、ISO27018云隐私安全管理认证、ISO22301业务连续性管理认证、ISO27701隐私信息管理体系认证、PCI-DSS支付卡行业数据安全标准认证、SOC认证以及TISAX可信信息安全评估交换认证。

亚马逊云科技提供了以下一系列技术解决方案，助力跨国HCLS企业数据出境的需求，并帮助这些企业在中国建立安全的云上数字底座和数据平台。目前，这些解决方案已经助力多家跨国HCLS企业在中国境内，成功落地了基于现代化架构的云上数字底座与数据平台，并实施了来自亚马逊云科技的安全最佳实践。客户企业如今可以快速、安全地在亚马逊云科技上进行大数据分析，更快取得市场洞察，为企业发展中国市场提供稳固可靠的基础，帮助企业深耕中国，在中国这个战略市场上做大做强，帮助客户提升科学研发效率，更快取得创新成果，为增进人民健康、抗击疾病作出贡献。

1. Cloud Foundations

Cloud Foundations系统地定义了HCLS企业云上生产环境所需的数十种信息技术“功能”，范围涵盖基础设施、安全、业务连续性、运维、治理与合规等六大支柱，是继云上着陆区后，对企业上云基础能力的全面提升。Cloud Foundations是专为亚马逊云科技中国区域的客户打造，完全按照数字底座的理念开发的云上基础设施部署工具。旨在利用云原生技术和自动化方案，快速搭建一个包括着陆区、安全基线和运维功能的上云就绪环境，覆盖必须的身份与访问管理、网络与基础设施安全等安全功能，以迅速供生产系统使用。客户可以此为基础，持续构建和加强 Cloud Foundations 定义的技术功能。

Cloud Foundations带来的优势：

快速交付：Cloud Foundations 快速启动包缩短了客户实现价值的时间并降低了实施成本，促进了安全最佳实践的使用。客户可以将有限的信息技术资源集中在诸如大规模迁移、构建下一代无服务器应用程序和云上重塑业务流程等高价值的机会上。

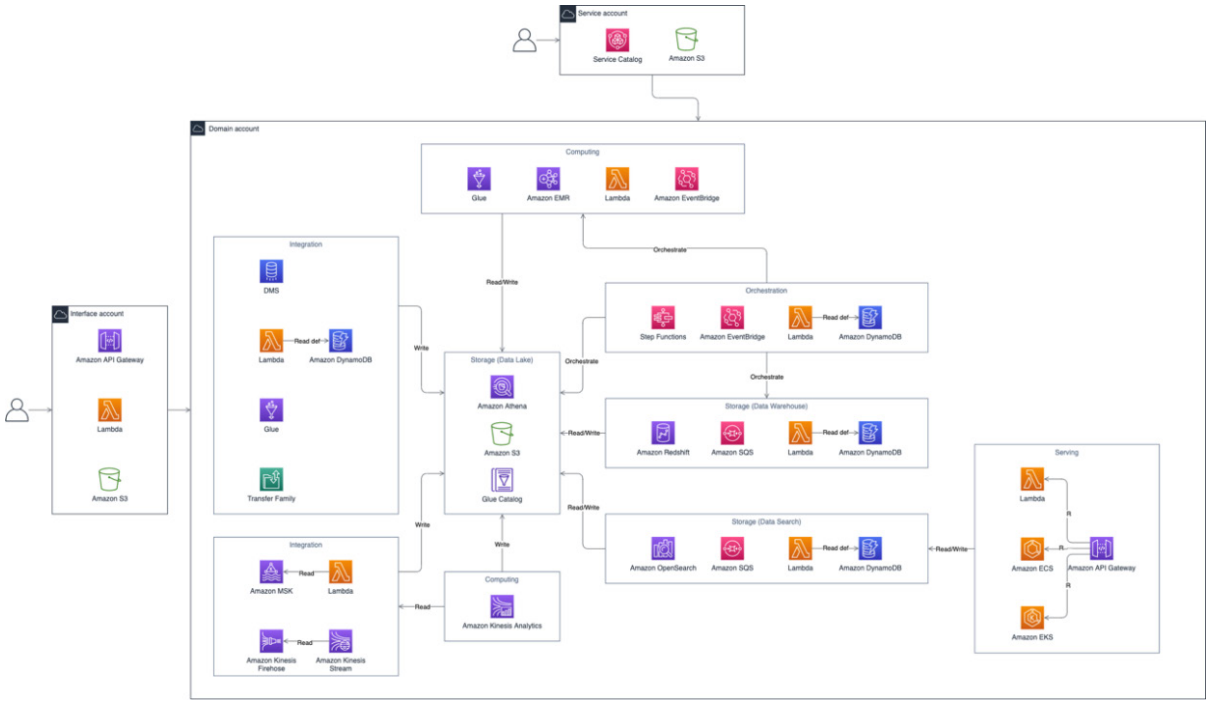
提高安全性：用户使用一套集中管理的部署代码，可以提高质量和安全性。Cloud Foundations 快速启动包内置了安全和合规的基本配置。用户提出的新安全要求可以很容易的集成到目前的代码中，有利于持续改善安全状况。

简化工作：Cloud Foundations 快速启动包简化了为客户构建多账户亚马逊云科技环境所采用的复杂方法。通过预先完成大部分工程、代码的开发和测试工作，从而降低了出现缺陷的可能性。

2. Data Analytics Foundations

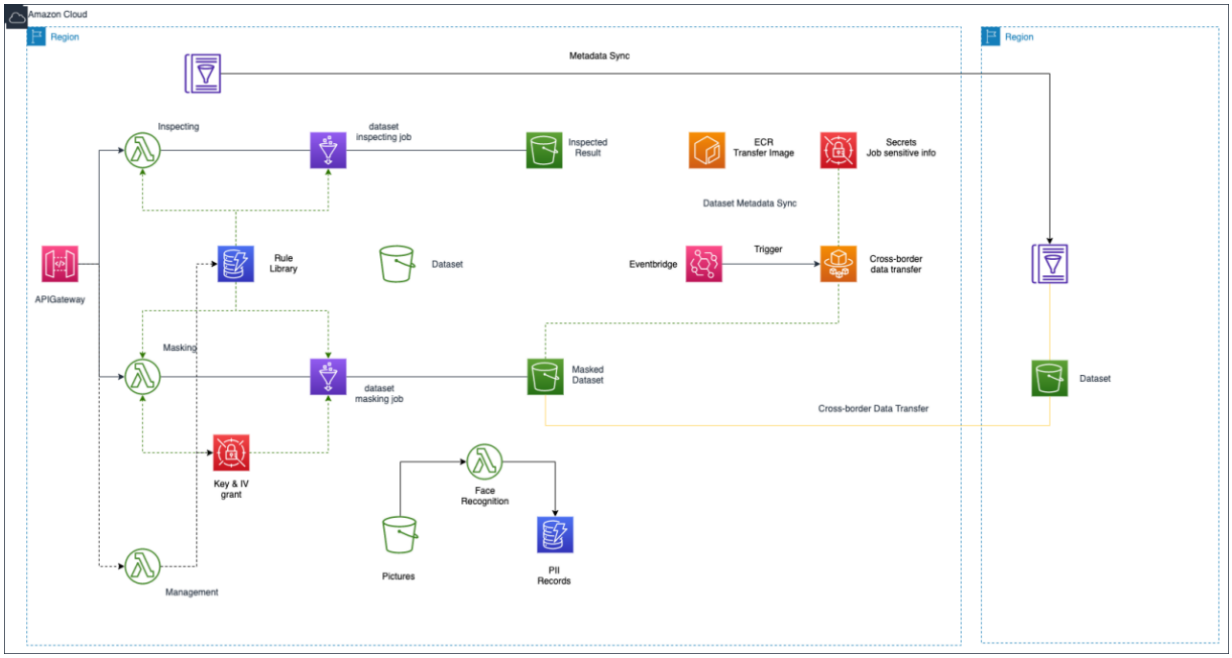
Data Analytics Foundations（DAF）提供了一套以事件驱动封装的功能模块，并基于亚马逊云科技的云原生服务进行了基础设施即代码的开发，现有25个功能模块涵盖数据采集、数据存储、数据处理、流程编排、目录和发现、数据仓库、数据消费、数据质量管理和数据安全控制等。客户可以根据自身业务的需求在DAF的模块菜单中选取特定组合并一键部署到亚马逊云科技账号环境中。例如，客户可以将数据处理模块配置为具有自动缩放容器来托管自定义程序，为大数据启动弹性内存计算集群，启用流功能以加速实时事件分析。

DAF也是一套经过实战验证的组件，结合了亚马逊云科技专业服务团队过去多年构建企业级数据分析平台的项目经验，辅之以云原生服务的最佳实践，集成了数据保护、加密传输等数据安全功能，可促进数据网格架构 Data Mesh 的开发，并将数据作为资产集成到其他数据管理方案中。尤其对于使用亚马逊云科技中国区域的客户，DAF在开发中进行了功能适配，完全满足亚马逊云科技中国区域的功能要求。基础设施即代码的部署方式既快捷又易于迭代升级，让客户能够对于在多区域环境中部署的多套数据分析基础设施，进行统一管理和维护，大大提升了运维效率。客户可以借助亚马逊云科技专业服务团队的实施经验和最佳实践，在短时间进行数据分析基础设施的标准化部署。



3. 数据海关

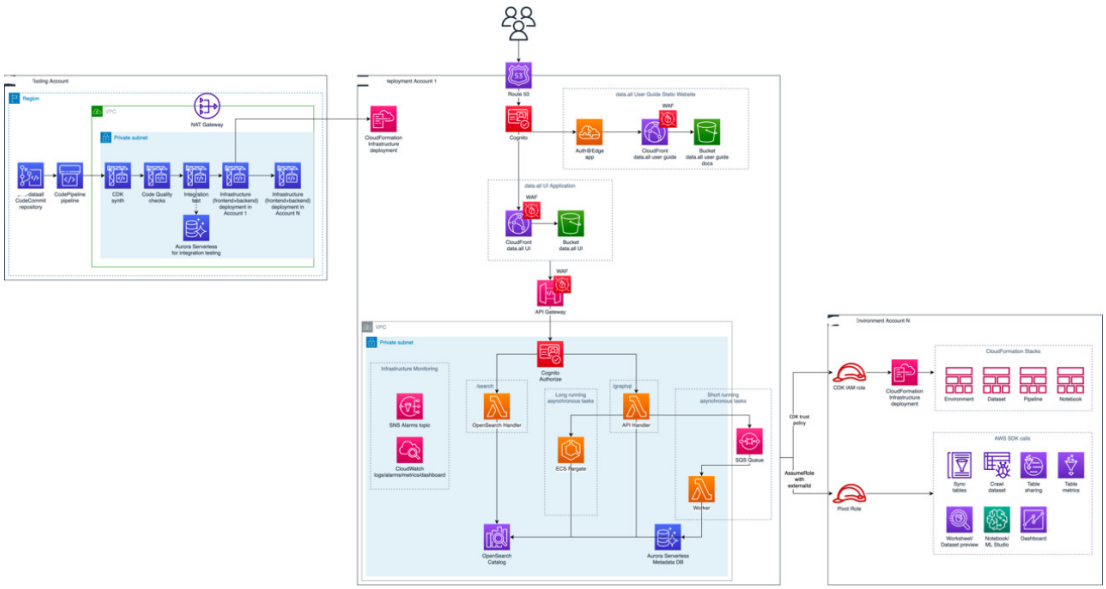
数据海关解决方案本身不提供对相关法律的合规解读，而是根据客户的输入（客户可以通过与“国瓴”等机构的合作对隐私或敏感数据进行分析、得出结论并将结论输入数据海关解决方案中），数据海关利用技术方法识别和屏蔽此数据类型，实现去标识化和匿名化，并进行所需的数据脱敏。数据海关可以支持多种语言的识别和脱敏，支持数据类型的自定义，支持湖仓数据及流式数据，支持多种脱敏模式，采用基于开放API的无服务架构，基础设施即代码的交付模式，运营成本低，投产周期短。



4. 企业数据管理中心

HCLS企业在数据治理过程中，需要对数据架构、数据标准、数据资产进行统一管理。而面对多角色构成的数据团队，如：分析师、数据科学家、工程师、业务用户，需要提供一个统一的管理界面，帮助他们既能根据各自工作，获取正确的数据和分析工具，又可以互相协同工作。为了满足企业客户的这一系列需求，亚马逊云科技专业服务团队推出了适合中国区域部署的“企业数据管理中心”解决方案。通过该管理中心的实施，不同组织形态的企业，可以根据自己的业务和管理需求，创建集中式、分布式或混合式的数据湖。使用企业数据管理中心，可以建立统一的数据资产目录，管理统一的数据权限，同时，又能跨业务部门发布和订阅数据，从全局的视角助力实现数据传输最小化的要求。

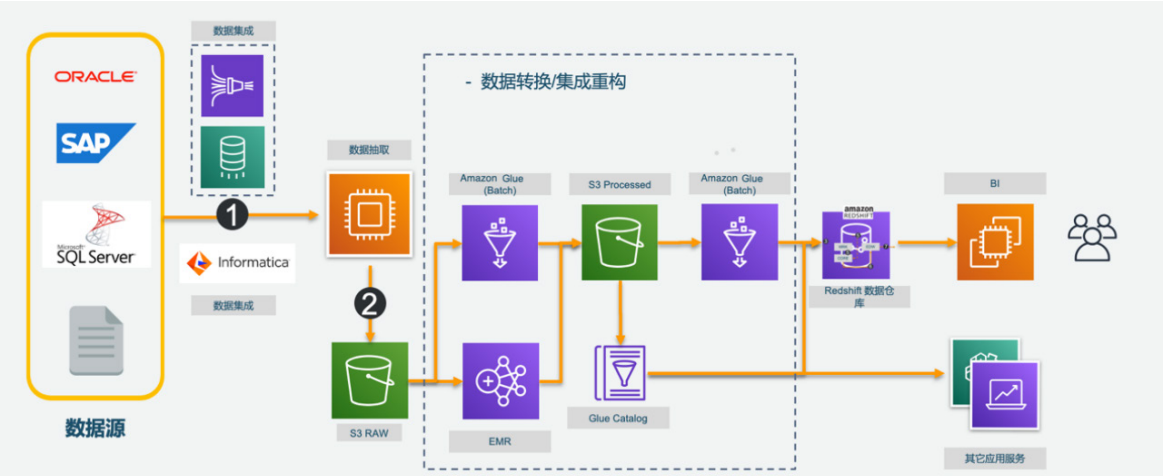
企业数据管理中心提供简洁的Web可视化界面，方便客户使用亚马逊云科技强大的数据存储和技术能力，加速构建自己的数据分析业务，深挖数据价值。根据业务定义的数据标准构建企业数据目录；方便企业内部数据的生产者快速构建数据处理管道，生产、发布数据和管理数据权限；方便数据使用者查看数据、申请数据权限、利用各种工具进行数据探察、数据分析、数据可视化；方便数据技术人员运维数据湖。为企业各类人员，提供统一数据试图、统一数据权限、统一工作界面，整合利用整个组织的数据资源，加速向数据驱动型企业转型。



5. 现代智能湖仓

中国市场是HCLS行业跨国企业的增长引擎，亚马逊云科技的云上智能湖仓方案，为企业落地中国，深耕中国市场提供了数据湖、数据仓库、数据分析等一系列技术支持。亚马逊云科技帮助多个跨国HCLS企业在中国区设计、构建数据湖、Redshift数据仓库，协助客户进行ETL(Extract-Transform-Load)流程优化、数据仓库调优，集成商业智能分析系统，不仅帮助企业满足数据安全治理的要求，也帮助企业快速搭建数据分析流程，优化查询效率，为企业深度分析市场、全角度分析客户数据、经销商数据、分析财务运营数据等各种维度的数据提供安全、稳固的基础。

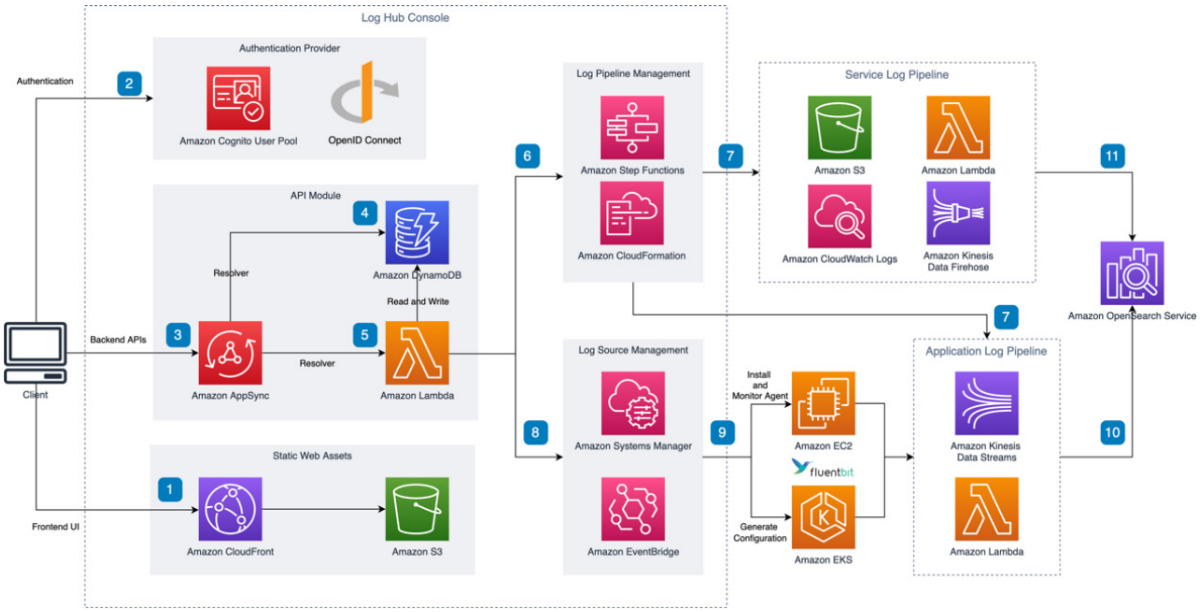
数据仓库是HCLS企业的核心部分，允许跨部门的用户收集数据并生成运行业务所需的每日报表。过去的数据仓库常常无法持续扩展以满足其业务需求，导致 ETL 流程超时，即席查询耗时过长，无法和数据湖集成。这些问题让越来越多企业IT 部门考虑优化重构数据仓库。



Amazon Redshift是亚马逊云科技提供的快速、可扩展的联机分析处理(OLAP)数据仓库,采用一致的安全和治理策略,可轻松且经济高效地分析数据仓库和数据湖中的所有数据:1)可以充分利用实时分析和ML/AI 使用场景而无需重新设计架构;2)为工作负载提供高性能,而无需完成定义排序键和分配键等无差别的繁重任务来优化数据仓库,而且还提供了物化视图、自动刷新和自动查询重写等新功能;3)不仅为未来的增长提供了充分的弹性,还提供了并发扩展等功能以覆盖高需求峰值,无论是 GB 还是 PB 级数据,无论是几个用户还是成千上万的用户,都可以稳定地快速提供结果;4)作为一个完全托管式数据仓库,消除了繁琐的基础设施管理或性能优化负担,可以专注于获取洞察,而不是执行诸如预置基础设施、创建备份、设置数据布局之类的维护任务;5)与商业智能BI工具兼容,为在 BI 工具中进行操作的企业用户带来了 Amazon Redshift 的强大功能和集成能力。

6. Log Hub

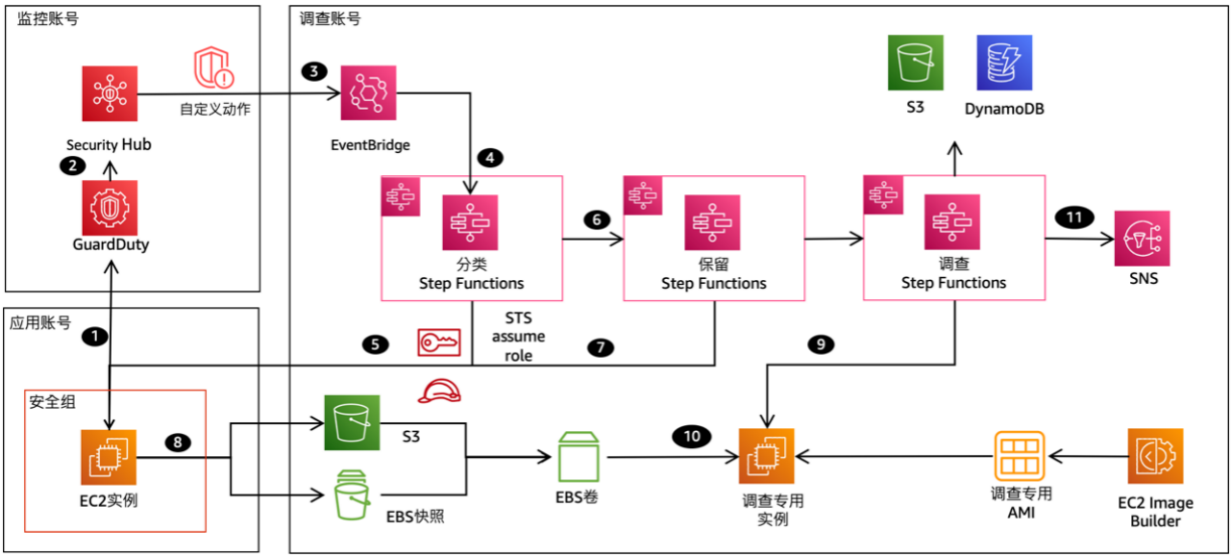
日志通(Log Hub)是亚马逊云科技提供的综合日志管理和分析平台,帮助客户轻松创建日志分析管道,并获取业务洞察。日志通基于Amazon OpenSearch构建,可同时高效完成日志摄取、日志处理和日志可视化。日志通支持摄取多种来源的日志数据,包括亚马逊云科技服务日志、应用程序日志以及安全日志,在经过客户的合理设置后也可助力满足客户数据出境日志的留存和数据访问的审计需要。同时,可通过丰富的仪表板展示分析处理后的日志数据。该解决方案结合了无服务器技术、内置的高可用性,和按使用付费的计费模式,减少了基础架构管理工作,使客户技术人员可专注于构建业务用例。



安全合规要求:根据客户的需要和自主设置,可用于遵守MLPS、PCI DSS中的相关安全要求。将设备、网络和应用程序日志集中存储到一个位置,以进行日志审计和威胁检测。

业务运营和数据分析：迅速识别趋势和模式，并构建交互式和直观的可视化图表。从日志中获取业务洞察力，并通过数据支持业务决策。

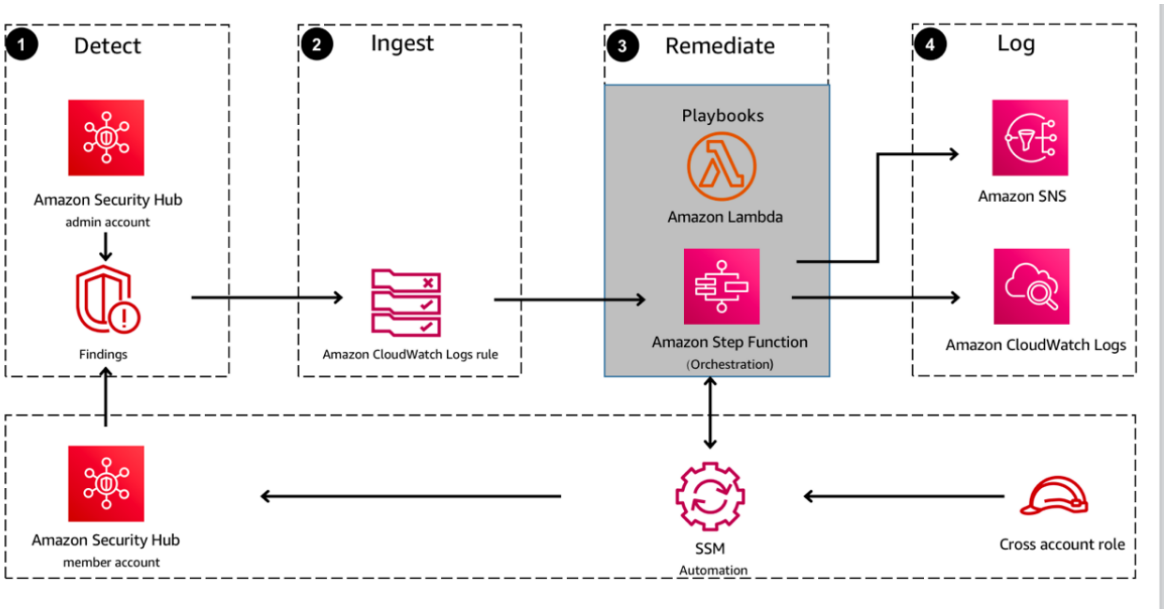
应用程序和基础架构故障排除：轻松监控应用程序和云基础架构日志，探寻问题的根本原因从而快速解决问题。提高工作负载的可观察性，并实现更好的业务稳定性。



7. 安全事件取证与自动响应

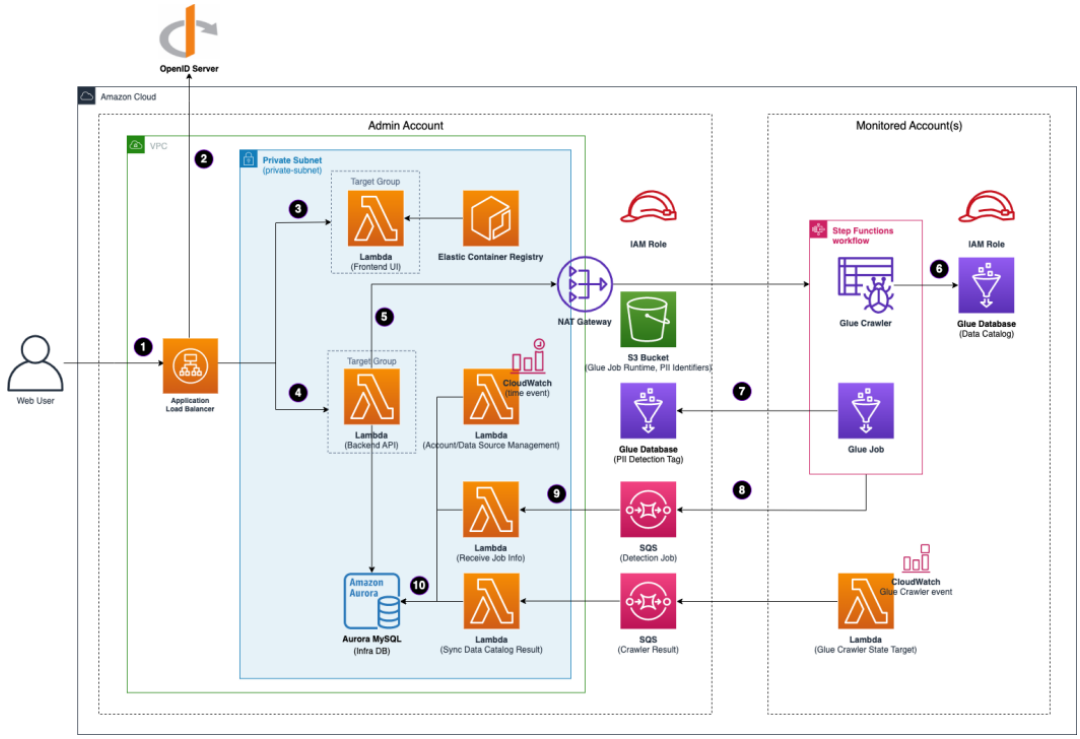
安全事件取证方案：帮助企业提升在检测到安全事件后立即收集、保存、保护和分析数字证据的能力。通过引入自动化，可以最大限度地降低调查成本，加快流程并避免人为错误。通过在检测到事件后立即收集证据，可以减少证据被删除或操纵的机会。该解决方案通过基础设施即代码的交付模式，结合前述多个解决方案，轻松定制客户的要求。

自动安全响应方案：与亚马逊云科技Amazon Security Hub服务结合使用，并根据针对安全威胁的行业合规性标准和最佳实践提供预定义的响应和修复操作。通过该方案，可以帮助客户处理Amazon Security Hub服务检测到的常见安全问题并改善自身的安全状况。整个过程包含四个步骤：事件检测、事件匹配、事件修复和记录通知。自动响应修复支持自定义，默认包含以下标准的部分操作：the Center for Internet Security (CIS) 标准、Amazon Web Services Foundations benchmarks v1.2.0、Amazon Web Services Foundational Security Best Practices (AFSBP) v1.0.0以及 PCI-DSS v3.2.1。



8.敏感数据保护解决方案

敏感数据保护解决方案（Sensitive Data Protection Solution）是一个开源的、云原生的数据安全及数据隐私解决方案。该方案基于Amazon Glue 的数据目录（Data Catalog）功能，使用机器学习和模式匹配等技术帮助客户识别多种数据源（如Amazon S3、Amazon RDS等）中的敏感数据，帮助客户构建企业敏感数据资产地图。



国瓴律师事务所

联系我们: 上海市秀文路69B号西子国际中心2号楼3层/
上海市华山路1389弄14号国瓴研究院

TEL: 021-33883626

WEB: www.guolinglaw.com

编写指导:

亚马逊云科技

余昶、梁超慧、石皓、王鹏、黄庆春、方康、苏卓、刘春华、
刘采薇、朱林、屈铭、刘玉恒、张一卫、白帆

上海国瓴律师事务所

何渊(数据与知识产权研究院院长)、高慧(管委会主席)

主编人员:

亚马逊云科技

黄帅、李勤、倪宜峥、王俊峰、周盈、江学森、苏璠、李国建、
刘育新、郭技

上海国瓴律师事务所

指南主编:阮芳洋(高级合伙人)

其他编委成员:黄佳旺、刁雪慧、鲁璘麾、王玥辉

亚马逊云科技 - 优惠大礼包

亚马逊云科技 - 微信订阅号

亚马逊云科技 - 微信服务号