保护云中医疗健康数据隐私

CSA GCR cloud security alliance®
GREATER CHINA REGION

云安全联盟健康信息管理工作组研究的官方网址：

https://cloudsecurityalliance.org/research/working-groups/health-information-management/

序言

数字经济时代，医疗健康数据的开发利用有利于广大民众的健康生活，但同时作为一类特殊的隐私数据，患者、医生包括医疗机构等全产业链的数据安全面临着巨大的泄漏风险。随着云计算技术在医疗行业的广泛普及，网络和平台安全受到云服务商的有效保护，但是数据的交换与传输不仅需要云服务商技术层面的保护，还需要企业从数据治理，合规层面做出相应的安全管控。

如何保证云端的医疗健康数据尤其是敏感的隐私数据的安全，需要数据控制者和数据处理者从数据的全生命周期考虑安全，数据安全是数据治理的重要组成部分，在企业数字化转型中需要重点考虑。本白皮书结合业内最佳实践从隐私工程、风险评估、隐私监管几个方面阐述了云端医疗健康数据的保护策略，对企业和从业者有非常好的借鉴作用，可作为云安全治理，隐私安全评估工作的参考。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

致谢

《保护云中医疗健康数据隐私》(Protecting the Privacy of Healthcare Data in the Cloud)一文由CSA 健康信息管理工作组专家编写，CSA 大中华区秘书处组织翻译并审校。

中文版翻译专家组（排名不分先后）：

中文版翻译专家组（排名不分先后）：

组　长：童　磊

翻译组：黄　瑞　侯汉书　李娇娇　罗　春　罗晓兰　马　嘉　魏　东　薛　琨

周星宇

审校组：史宇航　王　岩　赵晨明　张　亮　姚　凯　郭鹏程

感谢以下单位对本文档的支持与贡献：

北京奇虎科技有限公司　　北京威联科技有限公司

北京北森云计算股份有限公司　　北京谷安天下科技有限公司

浙江大华技术股份有限公司　　杭州世平信息科技有限公司

杭州虎符网络有限公司　　启明星辰信息技术集团股份有限公司

上海物盾信息科技有限公司　　兴业数字金融服务（上海）股份有限公司

任子行网络技术股份有限公司

英文版本编写专家

主要作者: Dr. James Angle

合作者: Michael Roza

CSA 全球工作人员: Vince Campitelli　Alex Kaluza　Claire Lehnert (Design)

AnnMarie Ulskey (Cover)

在此感谢以上专家。如译文有不妥当之处，敬请读者联系CSA GCR秘书处给与雅正!

联系邮箱：research@c-csa.cn；云安全联盟CSA公众号。

目录

摘要

隐私安全取决于合法访问、使用和更改信息的决策。隐私安全搭建了一个框架，用于决定合法获得访问和更改信息权力的主体（Bamauer,2013）。科技推动了前所未有的创新、经济发展以及社会服务的改善。特别是在医疗领域，科技赋予的价值与个人健康信息的收集息息相关。理想情况下，科技在最大化个人利益的同时保护个人隐私安全。考虑到医疗数据迁移上云的趋势，且由于云上存储的大量受保护的健康数据，加剧了对于隐私安全的担忧。

介绍

尽管已经有很多关于云安全和云隐私安全的文章和论文，但以云隐私为主题的文章却少之又少。我们从如何看待和保护这两个角度将隐私安全和安全区分开来，并赋予全新的意义。安全与隐私安全理应视为具有差异但又紧密相关的话题。传统意义上以机密性、完整性和可用性（缩写为CIA）为基本原则的数据安全广为人知，而本文所指的隐私安全则是在预定义和批准的前提下（如同意），充分处理和利用个人信息的一种数据保护形式。隐私安全可以通过不同方法和工具实现，通常是依据法律、地方政策或个人（如患者）对医疗信息使用的意愿。隐私安全讨论包含合法访问、使用以及更改信息等很多具有争议的决策（Bamauer,2013）。在医疗领域，由于出现了针对于云信息系统的高级持久性威胁和针对性攻击，侵犯患者隐私问题的关注度日益增加.

将隐私安全从安全中独立分离具有重要的实际意义。隐私安全搭建了一个框架，用于决定合法获得访问和更改信息权力的主体。在医疗领域，由于出现了针对于信息系统的高级持久性威胁和针对性攻击，侵犯患者隐私问题的关注度日益增加。在新冠状病毒（COVID-19）和民权办公室（OCR）规则变革的推动下，远程医疗的采用量和大数据的使用量呈显著增长（美国卫生与人力资源服务部，2020）。这种增长需要提高对隐私安全问题的意识。

科技推动了前所未有的创新、经济发展以及社会服务的改善。特别是在医疗领域，科技赋予的价值与个人健康信息的收集息息相关。理想情况下，科技在最大化个人利益的同时保护个人隐私安全。考虑到医疗数据迁移上云的趋势，且由于云上存储的大量PHI数据，加剧了对于隐私安全的担忧。

目前，许多网络安全控制框架适用于医疗领域，如美国国家标准技术研究所（NIST），国际

标准化组织（ISO）以及健康信息信任联盟（HITRUST）。虽然这些框架为隐私安全风险提供了缓解措施，但远远不够，因为隐私安全风险并不全都是由网络安全事件引起的（NIST,2020）。

医疗健康服务组织 （HDO）需要了解隐私安全和安全之间的关联，特别是两者之间的差异。这种理解共识将使HDO能够实施隐私安全风险管理计划解决隐私安全顾虑。HDO须同时关注受保护的隐私健康信息（PHI）和个人可识别信息（PII），并为这两类数据提供缓解控制措施。

本文中，作者将解决讨论隐私安全工程和风险管理、多种隐私安全法律法规以及整个云信息生命周期的合规问题。隐私安全工程师、隐私安全官以及信息安全专家都能从本文中获益。

1 隐私工程

什么是隐私工程？为什么有必要？其实安全专家早就知道，建设时同步考虑安全比事后增补安全性价比更高[1]。安全工程专家作为开发团队的一部分，可以在开发过程中确定安全需求并实施安全实践。安全工程能够指导开发人员了解系统设计的漏洞，并尝试消除或缓解这些漏洞。隐私工程师为系统设计的隐私方面提供同样的功能。隐私工程师确定隐私要求并采用隐私设计（PbD）构建隐私。

将信息安全等同于隐私是大家最容易犯的常识性错误。虽然安全肯定能够在隐私方面发挥作用，但有一个重要的区别：安全是保护和控制信息，而隐私则是认识到信息的支配权不再属于医疗服务机构。虽然医疗服务机构保留了对数据的物理控制，但有关个人信息的决定则受法律或法规的约束。安全部门执行这些决策，但不做出决策（Cavoukian、Shapiro和Cronk，2014）。

在过去十年中，医疗服务机构对隐私健康信息和个人识别信息的收集、使用和披露，以及隐私健康信息和个人可识别信息的价值和管理需求，都有了显著的增长。医疗服务机构处理数据的信心取决于其对核心隐私的承诺和能力。隐私工程和隐私设计旨在通过促进问责制和用户信任来增强对隐私的保护（Cavoukian等人，2014年）。

隐私工程中一种有用的方法是LINDDUN方法。LINDDUN是一种隐私威胁建模方法，可帮助分析员识别隐私威胁。这是一种基于模型的方法，因为该方法需要将数据流图（DFD）作为系统的代表性模型进行分析。

[1] CSA, DevSecOps-Automation-SafeCode的六大支柱，图1，第10页

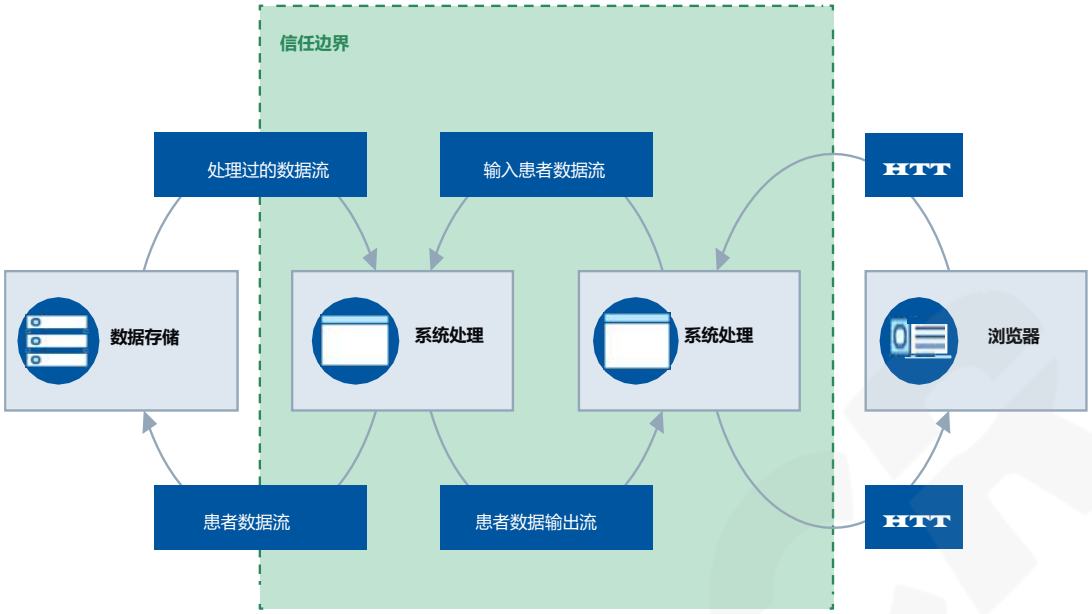


图1 数据流图

图1中所示的数据流图将作为分析的基础，它的每个元素都会被仔细检查，以防隐私威胁。该方法的原理主要是提供了与一组隐私威胁相关的最常见攻击路径。首字母缩略词LINDDUN代表：

1) 可链接性(Linkability)，指即使不知道可链接兴趣项目主体的实际身份，也能充分区分两个兴趣项目是否有链接的能力。可链接性过程假设，在数据迁移到云存储/处理环境（数据库存储）之前或迁移过程中，执行了所有相关隐私措施以合并患者私有和敏感数据。因此，可链接性提供了即使在屏蔽、匿名或加密时也能关联数据的能力；
2) 可识别性(Identifiability)，在一组主体中充分识别主体的能力；
3) 不可抵赖性(Non-repudiation)，无法拒绝索赔；
4) 可检测性(Detectability)，充分区分感兴趣项目是否存在的能力；
5) 信息披露(Disclosure of information)，信息披露树不是LINDDUN的一部分，而是微软STRIDE的一部分。由于隐私依赖于安全，LINDDUN包括了微软STRIDE的信息披露威胁；
6) 无意识(Unawareness)、缺乏了解共享信息的后果，用户通常不知道共享数据的影响；
7) 不合规(Non-compliance)、不配合遵从法律、法规和公司政策。

攻击路径表示为威胁树，详细说明了与主要威胁类别相关且特定于DFD元素类型的威胁的可能原因（Wuyts、Scandariato和Joosen，2014）。

隐私专业人士需要了解隐私存在于个人和他人之间的边界。技术对这一边界施加压力（NIST，2017）。远程医疗、医疗设备和大数据分析方面的技术进步使个人受益；然而，这项技术可能会对隐私产生不利影响。保护隐私需要多学科方法，包括法律、社会学、信息安全、伦理和经济学（NIST，2017）。隐私工程是隐私专业的技术表述。隐私工程师确保隐私方面的考虑通过设计集成到产品中。隐私工程师现在作为产品团队、设计团队、IT团队和安全团队的一部分工作。隐私工程可能包括法律和安全合规性，并为数据所有者提供自由裁量权和同意权。

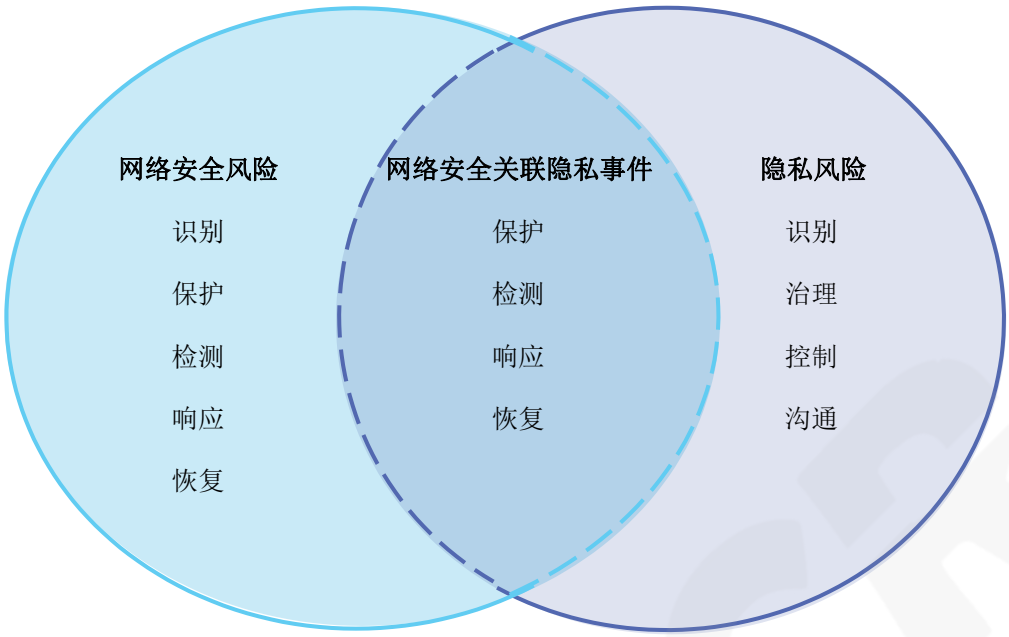
隐私工程是第一步。一旦发现威胁并想进一步减轻影响，那么下一步就必须执行隐私风险评估。风险评估有助于确定医疗服务机构需要额外强调控制措施的地方。

2 风险评估

医疗服务机构在制定隐私计划时应采取的第一步是确保他们充分了解个人数据处理的不同阶段，即如何创建、存储、使用、共享、归档和销毁数据。此外，根据医疗服务机构业务模型或医疗健康信息的特定处理，个人数据生命周期的某些阶段甚至可能不存在于特定情况下（例如，不涉及存储或归档个人数据的处理）。这意味着医疗服务机构必须执行隐私风险评估，了解数据生命周期每个阶段的隐私风险。

从安全分析员的角度看，“威胁”和“脆弱性”这两个词有非常具体的含义；然而，在隐私方面，这些术语并不能充分反映隐私问题。例如医疗记录窥探问题。本案中的威胁是一名内幕人士正在查看他们不应该查看的记录。例如，如果一个非常重要的人（VIP）来到医疗机构接受治疗，则不参与治疗的员工可能会想知道为什么VIP会在那里。如果他们访问VIP的医疗记录，则不会违反安全规定，因为员工已批准访问。虽然不是安全违规，但这是隐私违规，因为员工没有了解该信息的有效需求。

尽管未授权访问被保护的医疗信息是信息安全的一个子集，也是隐私的一个重要方面，但对于如何识别和解决超出授权访问被保护的医疗信息范围这样的个人隐私风险，人们的理解还远远不够。风险管理是一个过程，使医疗健康服务组织 (HDO)能够实现其目标，同时最大限度地减少不利后果。虽然隐私风险的概念并不新鲜，但直到最近，美国联邦政府还没有关于如何评估这种风险的指导。随着NIST隐私框架的发布，情况发生了变化。



使用功能管理网络安全和隐私风险，NIST 2020

完整过程见隐私框架附录D（NIST，2020）。

一旦医疗服务机构了解了其数据的收集、使用和共享，下一步就是进行隐私风险评估。隐私风险评估的目的是向医疗服务机构提供实施检测和预防控制措施所需的信息，并促进知情决策。

为了区分隐私威胁和安全威胁，隐私风险评估引入了一些更适合系统隐私性质的新术语。如上例所述，潜在情况或关注事件是个人作为授权处理被保护的医疗信息的副产品所经历的问题。因此，隐私风险模型的一个信息更丰富的因素不是在“威胁”一词中添加更多的概念，而是识别系统在被保护的医疗信息上执行的操作，该操作可能会对个人造成不利影响或问题，简言之，即有问题的数据操作。“有问题的数据操作是指对个人造成不利影响或问题的数据操作” (NIST, 2017 p. 21)

就向在安全风险评估中一样，医疗服务机构关注可能性和影响。医疗服务机构可以使用隐私风险模型考虑系统和流程易受问题数据行为影响的程度，以及问题数据行为的可能性及发生时的影响。

考虑到一个组织的有限资源，隐私风险评估的一个重要功能是确定风险的优先级并确定适当的响应。与安全风险一样，隐私风险可以管理，但无法消除。虽然隐私风险评估是医疗服务机构隐私风险管理的总括，但还需要完成另外两个流程：隐私影响评估（PIA）和数据保护影响评估（DPIA）。

在隐私风险评估中，这两个术语经常互换使用；但是，它们有不同的功能。

1）PIA旨在分析HDO如何收集、使用、共享和维护PII和PHI。PIA样本见附录A。

2）DPIA用于识别和最小化处理PII和PHI时的风险。DPIA的样本见附录B。

PIA和DPIA都是整体隐私风险管理框架（RMF）的一部分。当为新程序或流程获取PHI和PII时，执行PIA。DPIA纳入欧盟（EU）通用数据保护条例（GDPR），作为识别和降低隐私风险的持续流程。

一旦医疗服务机构完成了对有问题数据操作可能性的评估，就可以评估影响。这种影响发生在隐私和组织风险的交叉点（NIST，2020年）。医疗服务机构在组织风险管理这种级别上管理这些类型的影响。通过承认隐私风险是一种组织风险，领导层可以利用知情决策加强隐私计划。

3 隐私法规

隐私涉及关于合法访问、使用和更改信息的决定。隐私框架规定了谁应该合法地拥有访问和更改信息的资格（Bamauer，2013年）。在医疗健康领域，随着信息系统面临各种高级持续性威胁和针对性攻击，侵犯患者隐私成为一个日益严重的问题。

大多数国家都制定了管理健康数据处理的数据保护法。在国家法律(适用于一般个人数据)和行业法律(适用于特定领域，如医疗健康领域)或特定法律(适用于特殊情况，如新冠疫情)中都可能会提出健康数据管理的相关要求。每一部法律都有自己的要求，这些要求可以是另一部法律的补充，也可以作为另一部法律的例外。 此外，由于国与国之间的数据保护制度存在差异，大多数国家都禁止将个人数据（包括健康数据）跨境传输到其他国家，除非满足某些特定条件。本文提到了两部法规要求，《健康保险携带与责任法案 (HIPAA) 》 和《通用数据保护条例 (GDPR) 》。我们不仅要关注HIPAA和GDPR两部法规，还应该了解管辖区域内数据收集、处理和存储相关的所有法律，包括国家法律和地方法律。

HIPAA 隐私规则的主要目标是，在允许为了提供和促进高质量医疗健康服务而传播健康数据的同时，妥善保护受保护的健康信息(PHI)。在披露 PHI 之前，必须获得患者的书面授权。 若披露PHI数据并非为了治疗、支付和医疗健康服务，HDO必须获得患者的书面授权。所有授权都必须使用通俗易懂的语言，并包含详细的待披露信息，包括PHI数据的接收者、数据的有效期、

以及撤销披露的权利。美国卫生与公众服务部的相关规定如下：

> “HIPAA 隐私规则建立了美国保护个人医疗记录和其他个人健康信息的国家标准，并适用于医疗计划、医疗健康数据处理机构、以及某些电子医疗健康交易的医疗服务提供商。规则要求采取适当的安全措施保护个人健康信息的隐私，并对未经患者授权而使用和披露个人健康信息设定了限制和条件。规则还赋予患者对其健康信息的权利，包括检查和获取其健康档案副本，以及要求更正的权利。”（美国卫生与公共服务部，2003 ）

医疗健康信息激发了前所未有的创新，推动了经济价值和服务水平的提升。在医疗健康领域，数据价值通常与个人信息的收集有关。个人可能并不了解个人信息收集的后果和影响。我们面临的挑战是，如何在保护个人隐私的同时，从健康信息中获益。隐私保护提供有效的风险缓解措施时，必须允许个人的选择（NIST，2020）。

此外，根据数据收集对象、数据收集地点和数据存储位置，欧盟《通用数据保护条例(GDPR) 》可能会适用。GDPR 的主要目的是确保欧盟数据主体的个人数据受到保护，并赋予欧盟数据主体对其个人数据的权利。 无论企业位于何处，只要向欧盟数据主体提供服务并收集、处理或存储欧盟数据主体数据，都必须遵循 GDPR条例。在欧盟存储或处理的任何数据都受GDPR的约束，并在整个数据生命周期中都将被检查，以确保遵循GDPR相关条款。

注：*近代历史上最重要的国际隐私案件之一是奥地利隐私倡导者马克斯·施雷姆斯向爱尔兰数据保护委员会提出的针对 Facebook 的投诉。在诉状中，施雷姆斯先生对Facebook 爱尔兰分公司将他的数据（以及欧盟公民的数据）传输到美国提出质疑。该案件（“施雷姆斯第一案”）促使欧盟法院于 2015 年 10 月 6 日宣布《安全港协议》无效，该协议管控欧盟和美国之间的数据传输。《安全港协议》被《隐私盾》取代。 2020 年 7 月 16 日，欧盟法院作出裁决，宣布欧盟委员会(EU) 2016/1250号决定无效，该决定于 2016 年 7 月 12 日颁布，为欧盟-美国《隐私盾》提供保护效力”。受该决定的影响，当个人数据从欧盟传输到美国时，欧盟-美国《隐私盾》框架不再是遵守欧盟数据保护要求的有效机制。截至目前，双方依然没有达成新的协议 。*

3.1 创建

“创建”是指生成、采集新数据或修改现有数据。 PHI/PII 指包含可用于识别特定个人或个人群体的“身份标识”的任何信息。 对于PHI，它是健康信息也是身份标识。 在收集个人数据时，被收集数据的个人有权知道收集数据的具体内容、数据的用途、以及这些数据是否会被共享，

这一点非常重要。收集者必须获得同意，即必须征得用户的许可才能处理他们的数据。HDO 必须用通俗易懂的语言说明他们的数据收集行为，且用户必须明确地同意他们的做法。 此外，HDO 必须明确谁可以收集 PHI/PII 数据，并将数据映射到访问权限，确保具有访问权限的人才能访问。这也是根据敏感性和价值对数据进行分类的最佳时机。

3.2 存储

“存储”指将数据提交到存储仓库。 在隐私保护方面，数据存储意味着个人信息的存储和管理。 “存储”包括电子存储和硬拷贝存储。医疗健康服务组织 （HDO） 负责确保数据存储的机密性。在存储数据时，医疗健康服务组织（HDO）必须确保实施基于数据分类的控制措施。数据存储后，数据主体保留对其个人数据访问、纠正错误和要求删除的权利。 此外，必须明确说明数据存储方式，包括是否有多种存储策略？如何交叉引用数据？ 每类数据保留多长时间？

3.3 使用

“使用”指的是查看或处理数据（数据的修改属于创建）。当个人数据被使用时，隐私条例赋予了个人特定的权利。 以下列举了其中一些权利：

- 个人有权知情数据收集和使用的方式，包括明确声明数据使用目的和医疗健康数据的生命周期。
- 个人有权询问被收集数据的具体内容。
- 如果数据有误，个人有权要求更正。
- 个人有权要求从记录中删除他们的数据（个人可以提出要求，但医疗组织/医生不需要批准该请求）。
- 个人有限制数据处理权，例如拒绝将数据用于市场营销活动。

所有的HDO都需要制定隐私政策说明他们如何处理用户的信息。 隐私政策必须：

- 包括公司及其代表的详细联系方式
- 说明公司收集数据的原因
- 说明数据存档期限
- 说明用户拥有的权利
- 使用简单易懂的语言
- 指定个人数据的接收者（如果公司与其他组织共享数据）

3.4 共享

“共享”描述了他人（无论组织内部和组织外部）可以访问数据的行为。NIST 提到用数据处理生态系统描述不同组织之间如何共享数据。医疗健康服务组织 （HDO）必须确保部署数据防泄漏系来检测未经授权的敏感数据共享或复制行为。数据处理生态系统包括多个实体和角色，这些实体和角色彼此之间可能具有复杂的、多向关系。在数据共享方面（包括云服务提供商CSP之间的数据交换），互联互通问题可能会引发人们更多的担忧。在其他地方联合和复制本地医疗机构的安全策略可能会比较困难和麻烦。

数据处理生态系统关系图（NIST, 2020年）

这样做还可能需要改变或调整健康信息系统 (HIS) 中已实施的现有访问控制模型，以便患者数据的安全管理可以由患者(明确同意)和系统管理员共同操作（https：//link.springer.com/article/10.1007/s10916-020-01631-5）。实体在数据处理生态系统中的角色是隐私风险管理的一个关键因素，这会影响其法律义务。在医疗健康生态系统中，医疗健康服务组织（HDO) 和云服务提供商(CSP) 之间需要签署正式的协议/合同。

数据处理生态系统中风险管理的功能和类别表明，组织的优先级、约束、风险承受能力和假设已建立并用于支持与管理数据处理生态系统内和第三方相关的隐私风险决策。该组织已经建立并实施了识别、评估和管理数据处理生态系统内隐私风险的流程。了解 隐私健康信息（PHI）/个人识别信息（PII） 可以共享给谁、在什么情况下共享、以及以何种方式共享是非常重要的。

3.5 存档

根据各个国家的相关法律法规，医疗健康信息可能需要长期存储。数据存档可以作为纠正医疗操作和决策、患者历史医疗健康服务以及电子健康记录 (EHR)完整可视的证据。但是，一般而言，除 PHI 外，所有个人信息不再使用时可能需要删除。个人信息存储最小化原则。个人数据不能被无限期地存储。如果将来可能需要基础数据，可以在存档之前将个人信息与基础数据分离。数据分离指在不关联超出操作要求的个人或设备情况下，依然能够处理数据或事件的流程（NIST，2020）。有法律要求PHI要保存一段时间，其中一些甚至允许数据离线存储。

3.6 销毁

不再需要的数据将安全地销毁。在未确保所有受保护数据已被安全删除之前，不应处置包含隐私数据的可移动介质。所有包含受保护数据的存储介质在处置前确保数据已完全删除。在云端，可以通过数据加密、销毁密钥或匿名化方式达到数据销毁目的。尽管最初声明了数据生命周期、目的和患者授权，但医疗健康数据的销毁可能会受到患者请求的约束。HDO应该记录PHI/PII的销毁时间、法律依据，以及销毁责任人。

此外，可以实施多种措施保护数据。

- 桌面清理要求：所有员工离开工位之前，应确保桌面上没有任何包含隐私数据的材料，并且电脑要锁屏。
- 口令安全：禁止将口令书写记录。 应该尽可能设置较长且复杂的口令。
- 安全存储：任何包含个人隐私数据的材料都必须安全存储，隐私数据必须加密存储。
- 移动设备安全：移动设备应充分安全，并设置密码保护。
- 数据的安全传输：隐私数据应通过安全的方式发送。
- 数据的安全处置：在未确保所有受保护数据已被安全删除之前，不应处置包含隐私数据的可移动介质。
- 违规报告：在大多数情况下，如果发生违规行为，组织要在72 小时之内报告。

培训所有员工，让员工了解各种隐私规则下的责任，并严格遵守政策和程序将风险降到最低，这是至关重要的。

4 讨论

云计算在医疗健康领域中的应用未来将继续增加，随着这一点，存储在云中的隐私健康信息（PHI）数量也将持续增加。此外，物联网(IoT)设备的使用增加将加速云计算的应用。与医疗健康相关的云服务是非常复杂的，几乎涵盖了医疗健康服务的各个方面。医疗健康云服务可以向医疗健康服务组织(HDO)提供应用程序，否则无法使用。虽然医疗信息的隐私性是医疗健康服务组织关注的一个主要问题，但是云计算并非没有风险，为此，云安全联盟(Cloud Security Alliance)等组织已经做出了显著努力，确保这些风险得到解决和减轻。医疗健康服务组织按照提供的指导做尽职调查，可以将云计算所带来的风险降至最低，并从云计算中获益。

最近有关隐私的法律法规的激增，大大增加了保护个人隐私的复杂性和挑战。除了关注保密性的信息安全观点外，还涉及到确保隐私健康信息（PHI）的完整性及可用性。(NIST SP 800-53 r5, 2020)在与云提供商签订云服务协议时，医疗健康服务组织（HDO）应确保以下问题得到回答:

1) 云服务提供商(CSP)是否在隐私通知中描述了PHI被收集、使用、维护和共享的目的?
2) 云服务提供商(CSP)是否拥有、传播和和实施操作隐私政策和程序，以管理涉及PHI的程序、信息系统或技术的适当隐私和安全控制措施？这些文件是否包括如何联系云服务提供商（CSP）的数据隐私官(DPO)，以及患者或权威机构如何请求对个人的医疗健康数据采取行动？
3) 云服务提供商(CSP)是否有进行私隐影响评估?他们是否愿意分享
4) 云服务提供商(CSP)是否对在欧盟或欧盟数据主体上存储、处理或传输的数据进行了数据保护影响评估?
5) 医疗健康服务组织 是否对承包商和服务供应商有隐私角色、责任、访问的准入要求?
6) 云服务提供商(CSP)是否监控和审计隐私控制和内部隐私政策，以确保其有效的实施?
7) 云服务提供商(CSP)设计信息系统是否通过自动实现隐私控制来支持隐私?
8) 云服务提供商(CSP)是否对其控制下的每个记录系统中所保存的信息进行了准确的披露，包括a)每次披露纪录的日期、性质及目的?b)被披露的个人或组织的姓名和地址?
9) 云服务提供商(CSP)是否通过现有的安全控制来记录其流程，以确保受保护的隐私健康

信息（PHI）的完整性？

10) 云服务提供商(CSP)是否确认实现合法授权收集目的所需的最小必要原则PHI？

11) 在收集受保护的健康信息之前，云服务提供商(CSP)是否为个人提供了授权收集、使用、

12) 维护和共享受保护的健康信息的方式？

13) 云服务提供商(CSP)是否有接收和响应来自个人关于组织隐私实践的法律请求、投诉、关注或问题的流程?对检查隐私和医疗健康信息管理的审计，是否仅限于特定人员/角色，或受已声明的法规/合同的约束？

14) 云服务提供商(CSP)是否就其影响隐私的活动向公众和个人发出有效通知，包括收集、使用、共享、保护、维护和处置PHI？

15) 云服务提供商(CSP)是否对外共享受保护的健康信息(PHI)?

16) 如果需要，云服务提供商(CSP)是否具有聚合和关联存储/处理在其他地方的医疗信息的能力?

这些问题将确保云服务提供商（CSP）拥有一套结构化的隐私控制系统，有助于遵守所有适用的法律。此外，对云服务提供商（CSP）的隐私控制措施与安全控制措施一起查看，证明了隐私与安全之间的关系。

5 结论

虽然这篇文章的重点是关于《健康保险流通与责任法案（HIPAA）》中隐私条款和《通用数据保护条例》（GDPR）中的隐私安全，但医疗健康服务组织 （HDO）还须关注除此之外的法律法规。纽约修订了《纽约盾牌法案》，扩大了对违规行为的定义以及隐私信息的构成。这改变了违约通知要求（Ashkenazi,2020）。加利》福尼亚州通过并实施了《加州消费者隐私法（CCPA）》，加强了隐私安全法。2020年11月，《加州隐私权益法案（CRPA）对《加州消费者隐私法（CCPA）》进行了修订，新增的额外的保护条款将于2023年1月1日生效。受其影响的各医疗健康服务组织（HDO）将需要重新审查以确保遵守这些新修订内容。此外，各医疗健康服务组织（HDO）还需重新审查其数据所存储、处理或传输的所有司法管辖区域的法律法规。

参考

Ashkenazi, Asaf, 2020. NY Shield Act Sets in Motion Sweeping Privacy Regulations, Information Systems Security Association Journal, Vol.18 No 7 Retrieved from www.issa.org

Bambauer, Derek E., 2013. Privacy Versus Security, The Journal of Criminal Law & Criminology Vol. 103, No. 3

Cavoukian, Ann, Shapiro, Stuart, and Cronk, Jason R., 2014. Privacy Engineering: Proactively Embedding Privacy, by Design, Information and Privacy Commissioner, Ontario, Canada Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/pbd-priv-engineering.pdf

Department of Health & Human Services, 2020. OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, Retrieved from https://www.hhs.gov/about/news/2020/03/17/ocr-announces-notificationof-enforcement-discretion-for-telehealth-remote-communications-during-the-covid-19.html

Department of Health and Human Services, 2013. Summary of the HIPAA Privacy Rule, Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

Fennessy, Caitlin, 2019. Privacy engineering: The what, why and how, The International Association of Privacy Professionals, Retrieved from https://iapp.org/news/a/privacy-engineering-the-what- why-and-how/

National Institute of Standards and Technology, 2020. NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, National Institute of Standards and Technology, Gaithersburg, MD Retrieved from https://www.nist.gov/privacy-framework/privacy-framework

National Institute of Standards and Technology, 2017. NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems, National Institute of Standards and Technology, Gaithersburg, MD Retrieved from https://doi.org/10.6028/NIST.IR.8062

National Institute of Standards and Technology, 2020. Security and Privacy Controls for Federal Information Systems and Organizations, Gaithersburg, MD. Retrieved from https://doi.org/10.6028/ NIST.SP.800-53r5

United Kingdom Information Commissioner's Office, 2018. Data Protection Impact Assessment Template, Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection- impact-assessments/

Wuyts, Kim, Scandariato, Riccardo and Joosen, Wouter, 2014. LIND(D)UN Privacy Threat Tree Catalog, Retrieved from https://www.nist.gov/privacy-framework/linddun-privacy-threat- modeling-framework

附录A - 隐私影响评估样本格式

1.签署日期：

2.系统所有者：谁对系统负责？

3.名称：系统名称是什么？

4.PIA唯一标识符：HDO的系统唯一FQDN

5.该PIA的主题是以下哪一项：主要应用、次要应用、一般支持系统，

6.确定系统的企业性能生命周期阶段：

7.该系统是否包括可供公众使用的网站或在线应用程序？是/否

8.确定操作员：生产线（例如：财务、人力资源、供应链）

9.这是新系统还是现有系统？新的/现有的

10.系统是否具有安全授权（SA）？是/否 按照以下两点明确更新此PIA的原因：描述系统的用途；描述系统将要创建、存储、使用、共享或归档的信息类型。

11.提供系统概述，并描述系统将要创建、存储、使用、共享或归档的信息。

12.系统是否收集、维护、使用或共享PHI/PII？是/否

13.指出系统将创建、存储、使用、共享或存档的PHI/PII类型，例如：社会保险号、出生日期、姓名、邮寄地址、电话号码、医疗记录、就业状况、纳税人ID

14.指出创建、存储、使用、共享或归档PHI/PII的用户类别。雇员及公众人士；供应商/供应商/承包商

15.系统中个人PHI/PII数量是多少？

16.PHI/PII的主要用途是什么？

17.描述使用PHI/PII的其他用途。

18.确定系统和程序法律机构所允许的最大信息使用和披露的权利。

19.系统上的记录是否可以通过一个或多个PHI/PII数据元素检索？是/否

如果是，列出所有使用PHI/PII数据的系统

20.确定系统中PHI/PII的来源。

21.PII是否可以与其他组织共享？是/否

22.确定可共享或披露PII的对象并阐明目的。

23.描述授权信息共享或披露的协议。

24.描述授权披露的会计程序。

25.描述通知个人将收集个人信息的过程。如果没有事先通知，请解释原因。

26.个人提交PHI/PII信息是自愿的还是强制性的？

27.描述个人选择不想被收集和使用他们PHI/PII信息的原因。如果信息收集是强制性的，请说明原因。

28.当系统发生重大变化时，通知系统中存在PHI/PII的个人并获得其同意的流程是什么？

29.描述当个人认为其PHI/PII的获取、使用或披露不当，或PHI/PII不准确时，解决个人问题的流程。

30.描述对系统中包含的PHI/PII进行定期审查的流程，以确保数据的完整性、可用性、准确性和相关性。

31.确定谁可以访问系统中的PHI/PII，以及他们需要访问的原因。

用户：

32.描述确定系统用户（管理员、开发人员、承包商等）可以访问PHI/PII的流程。

33.描述允许访问PHI/PII的人员仅允许访问执行其权限范围内最小权限的方法。

34.确定针对不同的系统人员（系统所有者、经理、操作员、承包商和/或项目经理）针对性的提供培训，使他们意识到保护收集信息的责任。

35.描述用户接受的系统性培训（超过一般安全和隐私意识培训）。

36.合同是否包括收购条例和其他确保遵守隐私规定和惯例的适当条款？是/否

37.描述与PHI/PII留存和销毁相关的流程和指南。

38.简要但需要具体描述如何通过管理、技术和物理控制手段在系统中保护PHI/PII。

附录B – 数据保护影响评估(DPIA)模板示例

该模板是记录DPIA过程和结果的一个示例。它遵循我们DPIA指南中所列的流程，应当和DPIA指南一同阅读，也可以同欧洲DPIA指南所规定的可接受DPIA标准一起阅读。

在任何涉及使用个人隐私数据的重大项目开始时，或者在对现有流程做出重大改变时，数据控制人员需要填写该模板。将最终结果整合到项目计划中。

提交数据控制人员详细信息

数据控制人员姓名	
数据隐私专员议题/头衔	
数据控制人员联系人姓名/数据隐私专员姓名(酌情删除)	

第1步：确定DPIA的需求

大致解释项目的目的和涉及到的处理类型：参考和链接到其他文件，例如项目建议书，可能会有所帮助。总结DPIA的需求。

第2步：描述处理流程

描述处理的本质：如何采集、使用、存储和删除数据？数据的来源是什么？数据是否会共享给任何人？参考流程图或其他描述数据流的方式可能很有用。哪些处理类型被认为可能是高风险的？

描述处理的范围：数据的本质是什么，它是否包括特殊类别或者刑事犯罪数据？将要采集和使用多少数据？频率是怎样的？持续多久？有多少人受影响？覆盖的地理面积是多少？

描述处理的上下文：数据控制人员和数据拥有者之间的关系是什么性质？数据拥有者有多少控制权？数据拥有者希望以何种方式使用数据？数据拥有者是否包括儿童或其他弱势群体？之前是否有对这种处理方式或安全缺陷的担忧？数据是否在任何方面都是新颖的？该领域目前的技术状况如何？是否有任何当前大众关注的问题应当被考虑在内？数据控制人员是否签署了任何经批准的行为准则或认证计划(一旦已获任何批准)？

描述处理的目的：数据控制人员想到达的目的是什么？数据拥有者的预期效果是什么？数据拥有者、数据控制人员以及更多的人能从处理过程中收获什么？

第3步：协商过程

考虑如何与利益相关者协商：数据控制人员何时以及以何种方式寻求数据拥有者的建议，或者为什么不适合那样做？组织内还有谁需要参与？是否需要请处理人协助？是否有计划咨询信息安全专家或其他方向的专家？

第4步：评估必要性和相称性

描述合规和相称性的方法，特别是：处理过程的法律依据是什么？处理过程是否确实达到了预期目的？是否有其他方法实现相同结果？如何防止功能蠕变？如何确保数据质量和数据最小化？将提供哪些信息给数据拥有者？数据控制人员如何帮助支持他们的权利？采取什么措施以确保处理者遵守？如何保障任何的国际转让？

第5步：识别和评估风险

描述风险来源和对个人潜在影响的性质。必要时包括相关合约和公司风险。	**危害的可能性**	**危害等级**	**总体风险**
	遥远的、可能的或很可能	轻微，显著或严重	低、中或高

第6步：确定减少风险的措施

确定可以采取的额外措施，以减少或消除第5步中确定为中等或高等风险。				
风险	**减少或消除风险的方案**	**对风险的影响**	**剩余风险程度**	**批准措施**
		消除、减少或接受	低、中、或高	是/否

第7步：签收并记录结果

项目	名称/职务/日期	备注
措施批准人：		将行动重新纳入项目计划，并注明完成日期和职责。
剩余风险批准人：		如果接受任何剩余的高风险，在进行之前咨询ICO。
提供建议的数据隐私专员：		数据隐私专员应根据合规性、第6步的措施以及是否可以继续提供建议。
数据隐私专员建议概要：		
数据隐私专员建议接受或否决：		如果否决建议，必须解释原因。
评论：		
协商答复的审查人员：		如果数据控制人员的决策偏离了数据拥有者的意见，必须解释原因。
评论：		
本DPIA通过以下方式审查：		数据隐私专员还应该审查DPIA的持续遵守情况。