医疗保健中的信息技术治理、风险与合规（第二版）

CSA GCR cloud security alliance GREATER CHINA REGION

CSA cloud security alliance

联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《医疗保健中的信息技术治理、风险与合规（第二版）》由 CSA 工作组专家编写，CSA 大中华区秘书处组织数据安全工作组专家进行翻译并审校。

中文版翻译专家组

组长：

王安宇

翻译组：

王彪、张明敏、易利杰、卜宋博

审校组：

王安宇、罗智杰、高健凯

研究协调员：

卜宋博、闭俊林

感谢以下单位的支持与贡献：

北京天融信网络安全技术有限公司　　杭州安恒信息技术股份有限公司

（以上排名不分先后）

英文版本编写专家

主要作者：

Dr. Jim Angle

贡献者：

Yutao Ma　　Akhil Mittal　　Michael Roza

审校组：

Anup Ghatage　　Tolgay Kizilelma, PhD　　Namal Kulathunga

Yuvaraj Madheswaran　　Vaibhav Malik　　Kenneth Moras

Meghana Parwate　　Akshay Shetty　　Rose Songer

Udith Wickramasuriya

CSA 全球工作人员

Alex Kaluza　　Claire Lehnert

在此感谢以上专家及单位。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给予雅正！ 联系邮箱 research@c-csa.cn； 国际云安全联盟 CSA 公众号。

目 录

序言

随着医疗保健行业进入数字化转型的深水区，信息技术的快速普及不仅为医疗服务的提升带来了巨大的机遇，同时也带来了前所未有的挑战。在这一过程中，信息技术治理、风险管理与合规（GRC）成为医疗保健机构不可忽视的关键领域。云计算、人工智能（AI）、物联网（IoT）以及区块链等技术的崛起，进一步加剧了这些挑战，要求医疗保健组织在采纳新技术的同时，确保患者数据安全、信息隐私保护、以及遵循复杂的行业法规。

《医疗保健信息技术治理、风险与合规（第二版）》从全球视角出发，全面剖析了云计算环境下的 GRC 框架如何帮助医疗保健机构应对当下的安全和合规挑战。报告深入探讨了 GRC 如何在确保合规的同时帮助机构最大化地降低技术风险，提升运营效率，简化流程，并且为组织的长期安全性和可持续性奠定基础。

报告指出，随着生成式人工智能等新兴技术的应用，医疗保健行业面临的安全威胁愈加复杂。AI 技术的双刃剑效应，不仅可以提升医疗诊断的精准度和效率，也可能因数据隐私、算法偏见等问题带来法律和伦理上的挑战。针对这些问题，报告建议医疗保健机构将 AI 的治理纳入 GRC 框架中，以确保技术发展符合道德标准和法规要求。

展望未来，全球医疗保健行业在技术进步的驱动下，将持续面临复杂的供应链风险、严格的监管要求以及新型攻击手段的不断涌现。为此，报告呼吁医疗保健机构采用前瞻性思维，构建具备自动化能力的 GRC 框架，并在零信任架构、云原生安全工具等方面加大投入，以确保组织在瞬息万变的技术环境中保持强大的适应能力和弹性。

李雨航 Yale Li

CSA 大中华区主席兼研究院长

摘要

医疗保健服务提供组织（HDO）使用云服务的情况正变得越来越普遍化，但向云端的迁移却带来了挑战。其中一个主要挑战是在云中建立治理、风险与合规（GRC），这需要重新定义业务和技术的流程，并依赖第三方提供商。为了确保 HDO 能够从云计算中获益，设计并实施一个稳健的云 GRC 计划非常重要，该计划能够解决这些挑战，并确保符合行业法规和标准。

1. 引言

HDO 意识到通过治理、风险与合规（GRC）计划能全面了解风险和合规的价值，该计划使 HDO 能够从业务角度解决技术风险，通过自顶向下的方法使业务和技术保持一致性。这种自顶向下的方法确保在符合行业法规和标准的同时也能识别和解决风险。

云 GRC 是组织收集重要风险数据、验证合规性并报告结果的有效手段。云管理是云 GRC 中的一个重要关注领域，它在很多组织中以孤岛的方式实施。（从而）未能将收集的结果整合到 GRC 计划中，可能导致重复性工作，并且不能充分利用 GRC。正确实施的 GRC 计划可以消除重复性工作，提供数据存储库，并促进自动化。本文将讨论一个良好的云 GRC 计划的要素以及建立该计划所需的条件。

人工智能（AI）的重要性正在快速增加，特别是在医疗保健行业。因此，GRC 也受到越来越多的关注。AI GRC 专注于人工智能和机器学习（ML）系统的数据质量和准确性、道德和法律问题、安全性和隐私性，因为可能涉及患者和其他敏感数据。GRC 的目标是建立必要的监督，以使 AI 行为符合道德标准和社会期望，并防范潜在的不利影响。

GRC 提供了一种共享相关信息的方法，有助于弥合差距并消除组织中的孤岛。

1.1 新兴技术对 GRC 的影响

区块链、物联网（IoT）、人工智能和高级分析等新兴技术在医疗保健领域的迅速采用，为 GRC 框架带来了新的挑战和机遇。这些技术可以帮助简化流程、增强数据完整性并改善患者治疗效果，但它们也在合规性和安全管理方面带来了复杂性。在 GRC 框架内解决这些技术问题，可确保它们符合医疗保健标准和法规，同时增强网络安全措施。

2. 治理

由于云计算相对于本地数据中心的独特性，,HDO 需要重新考虑如何实现 IT 治理。HDO 必须实施并维护一个治理生命周期，来规划、定义、实施和监控治理。HDO 必须考虑如何管理责任共担模型和多租户环境。此外，虽然 HDO 可能有云优先策略，但至少在最初，他们将处于混合云环境中。在医疗保健领域中，有效的 IT 治理确保技术投资与组织目标一致，高效分配资源，决策过程透明且负责任。这包括为 IT 系统和人员制定策略、程序和标准。

基于云的架构和业务运营比传统的本地数据中心架构更加多样化和复杂，因此依靠用于本地数据中心环境的相同策略和工具将不能确保在云上取得成功 1。云治理是基于风险和标准框架的 HDO 的策略和标准的集合。根据信息系统审计和控制协会（ISACA）的说法，云环境中的治理有助于实现使用云计算服务所带来的好处，同时最大限度地降低风险、优化投资并确保符合法律和法规要求。

通过创建云治理模型，HDO 可以避免许多云优先战略的陷阱。

将云计算引入 HDO 会影响角色、职责、流程和度量标准。如果没有适当的治理来提供标准和指南来驾驭风险以及有效采购和运营云服务，HDO 可能会发现自己面临一些常见问题：

- 与企业目标不一致

- 频繁的策略例外评审
- 项目停滞
- 合规或监管的处罚或失败
- 数据治理与管理
- 预算超支
- 不完整的风险评估[2]

根据面向服务架构（SOA）框架，云治理生命周期由四个阶段组成：

- 计划（Plan）
- 定义（Define）
- 实施（Implement）
- 监控（Monitor）

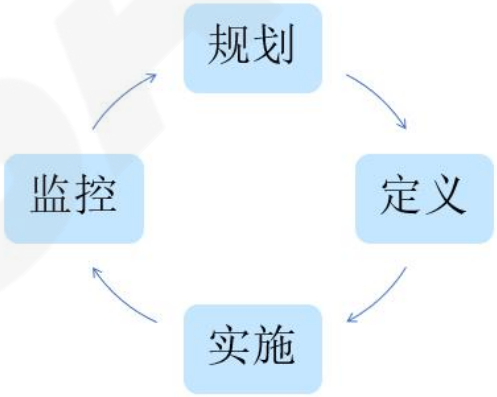

图 1：SOA 治理生命周期

2.1 规划

规划始于识别利益相关者的业务需求，并识别如何满足这些需求。云计算治理

生命周期的规划阶段包括：

1. **分析已实施的治理模型和流程。**

这包括评估公司治理的所有方面，以找到创建或维护云治理模型的起点，以便提供基于云计算治理成熟度水平的管理级别信息，来提升云计算治理。该水平分为 6 个级别：

- 级别 0：不存在云计算治理
- 级别 1：初始/临时的云计算治理
- 级别 2：可重复的云计算治理
- 级别 3：已定义的云计算治理
- 级别 4：可管理和可度量的云计算治理
- 级别 5：优化的云计算治理

2. **云治理愿景与战略。**

云治理愿景基于云治理的指导原则和商业战略。实现云计算愿景的战略应包括云治理评估以及衡量从云治理中获得价值的指标定义。

3. **云治理的范围。**

- 识别利益相关者的需求
- 识别云治理流程
- 识别治理级别并选择云治理的组成部分

4. **指导原则的适应性调整。**

此活动根据企业 IT 治理原则调整 HDO 的云治理指导原则。。ISACA 组织认为采

用和使用云有 6 个指导原则：赋能、成本收益、企业风险、能力、问责和信任。这些原则通过强调云计算的问题和关注点，为 HDO 提供了高层次的指导，并有助于在采用云解决方案的同时实现 HDO 的业务目标。

5. 规划云治理路线图。

云治理路线图定义了云治理生命周期的迭代次数。云治理的初始部署在第一个周期的实施过程中进行。在后续的迭代中，逐步实施完整的云治理愿景[3]。

在 HDO 开始规划和实施其治理模型时，有两个关键领域对于这一过程的成功至关重要，首先是数据分类。数据分类为整个生态系统中的数据访问、使用和共享设定规则。数据的安全要求决定了其分类。数据必须要多安全？它是个人可识别信息（PII）还是受保护的健康信息（PHI），或者数据可以自由共享吗？

其次，识别角色和责任。云计算处于一个责任共担环境中。以下来自微软的图表展示了不同职能的责任分配：

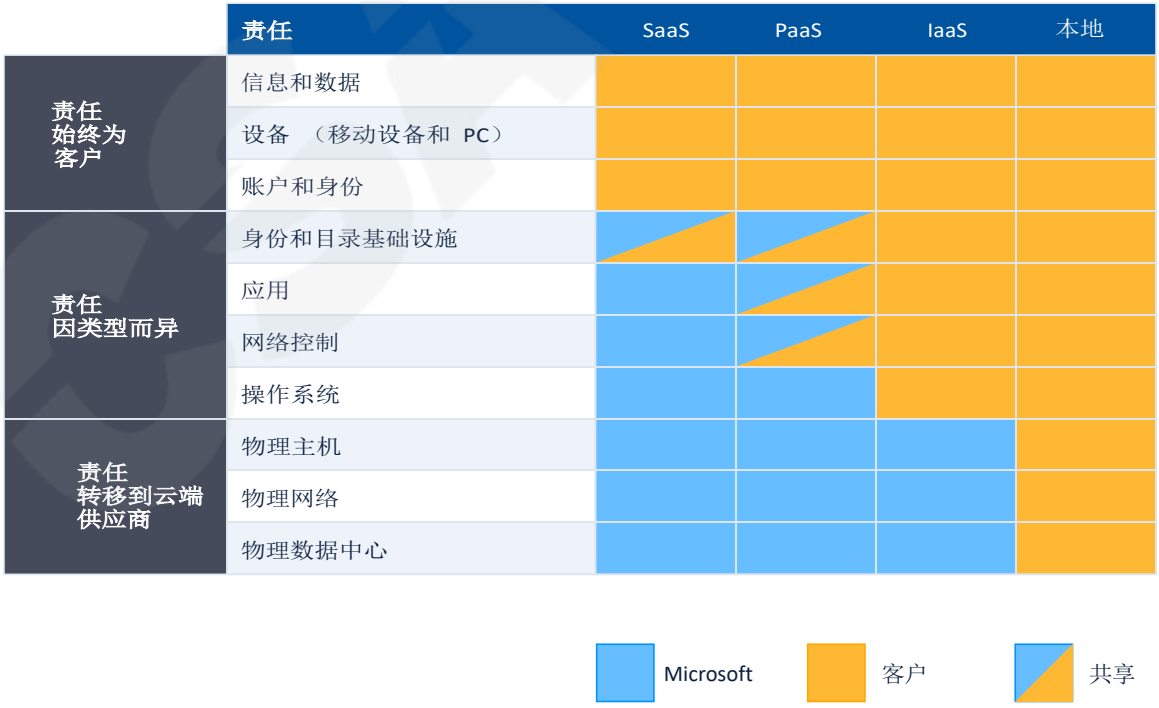

图 2：来自微软的云责任共担模型

如您所见，在责任共担模型下，基于本地数据中心的治理模型在混合云环境中将不再充分满足需求。

清楚了解从云服务提供商那继承的合规性至关重要。这是因为他们负责实施，适用于他们在责任共担中所负责部分的控制措施。作为客户，您也负责实施控制措施，以实现对法规的整体合规性。例如，如果您需要遵守《健康保险流通与责任法案》(HIPAA)，您的云服务提供商将根据他们在责任共担中所负责的部分，如数据中心和虚拟化安全，实施一套控制措施。然而，作为云服务的客户，您也负责实施来自合规性继承的其余控制措施，如实施适当的身份和访问管理（IAM)、对您的应用程序、系统和数据的访问控制、管理应用程序漏洞、确保您有安全软件开发生命周期、遵守数据保留和数据处置要求、实施安全控制、监控您的云资源是否有异常和恶意活动，并处理事件。IT GRC 是一个持续的过程，需要持续监控、评估和改进。医疗保健组织应定期审查其 IT GRC 框架，评估其有效性，并根据不断变化的风险、法规和业务需求进行必要的调整。

2.2 定义

"定义"是定义实现规划阶段目标所需步骤的过程。以下是此步骤中的一些活动。

1. 根据公认的治理成熟度模型评估当前云治理的现状。
2. 定义适用于 HDO 的治理策略和合规法规[4]。
3. 识别必须弥补的差距以满足 HDO 的云治理要求。
4. 定义执行所有治理流程的治理机构。
5. 定义一个治理框架。云安全联盟（CSA）的云控制矩阵（CCM）框架专注于整个信息安全生命周期[5]。

此外，实施和管理云治理所需的技术和工具也在此项活动中被定义。进行现有企业技术和工具的分析，并识别出差距。差距分析的结果作为获取技术和工具的基础，这些技术和工具应支持云治理的自动化能力。

2.3 实施

实施治理框架是一个具有挑战性的过程，它需要合作、沟通、监控和持续改进。HDO 在定义阶段定义了流程、技术和工具。现在，HDO 需要定义标准和程序。这些包括云计算各个方面的指导方针，如配置、访问管理和变更控制。这些标准和程序必须传达给所有利益相关者，明确说明每个利益相关者的角色和责任。此外，HDO 应提供培训，让所有利益相关者熟悉云治理策略、程序和标准[6]。

理解实施云治理将面对挑战是重要的。一些挑战包括安全和隐私。HDO 需要明确两者的要求。挑战可能来自业务部门的路线图和整体战略方面。这会导致在组织内推出治理框架时出现重大延误，特别是，当需要与工程部门、开发运营（DevOps）和开发人员合作时，这可能妨碍成功推出这些框架的能力。此外，对治理重要性以及控制措施实际意义的教育不足，会在实施过程中带来意想不到的挑战。

2.4 监控

持续监控对确保云治理的有效性至关重要。策略和标准并非一成不变；随着技术和法规的变化，它们也必须更新。当变化发生时，评审和更新策略及标准是必不可少的。HDO 应进行定期评估，以识别需要改进的领域并进行必要的调整。

监控使 HDO 能够收集有关云治理流程的性能信息，这些信息可以作为下一个周期的关键输入。然后 HDO 可以确保满足云治理的目标和目的。必须持续监控，以提供最新和准确的信息。根据业务需求[7]，测量数据会连续地或以设定的时间间隔进行评估。

实施云安全态势管理（CSPM）解决方案提供全面洞察云配置错误的情况，提供及时的建议和有效的策略来减轻技术风险的暴露。此外，基础设施即代码（IaC）的采用已经彻底改变了云计算基础设施的管理，促进了主动风险管理。通过使用静态代码分析技术，组织可以在将 IaC 脚本部署到生产环境之前识别和解决错误配置。这种主动的方法通过简化风险检测和促进快速补救，极大地提高了投资回报率（ROI），

加强了云治理框架。

2.5 讨论

云治理可以显著增强 HDO 利用云计算满足业务需求的能力。随着 HDO 持续以迁移向云，它们必须了解如何利用云服务并实现业务与 IT 的一致性。虽然并没有一个特定的云治理框架，HDO 需要选择一个框架并根据其需求进行调整。CSA 的 CCM 框架专注于整个生命周期，并可以使 HDO 在开发其框架时获益。

实施云治理影响业务价值的创造和使用云服务的收益。然而，HDO 可能会面临一些困难，例如将云治理整合到其现有的治理流程中、规划治理路线图以及设计治理结构。制定清晰的云治理实施指南将有助于克服这些困难[8]。

2.6 威胁

与旨在保护资产的传统网络安全不同，医疗保健行业的网络安全始终与人息息相关，它通常直接连接到面向患者的网络技术——例如，对患者生命至关重要的植入式医疗设备。另一方面，网络安全威胁在数量、种类（如勒索软件）以及对有漏洞的 IoT 系统的攻击方面都在增加。

2016 年，非特定目标的勒索软件 WannaCry，攻击了 150 多个国家，包括医疗保健系统。WannaCry 最深远的影响发生在英国，导致英国国家卫生服务（NHS）受到严重影响，勒索软件加密了文件，犯罪分子要求支付赎金以解锁医疗记录或关键设备。结果是超过 80 家独立医院的正常医疗运营受到干扰超过四天。这次网络攻击直接影响了生命，给 HDO 带来了新的威胁。在 5 月 12 日至 5 月 19 日之间，成千上万的预定手术和临床预约不得不取消。

3. 风险

网络安全风险是业务风险的一个子集，因此，应该用业务术语来讨论。HDO 应该在组织风险的环境下看待信息风险。当 HDO 实施信息安全控制时，他们的目标是降低风险。没有任何信息系统是百分之百安全的，因此控制的目的就是将风险降低到一个可接受的水平，并且管理风险。为了构建一个健壮的网络防御，HDO 必须理解风险。

云风险管理是在云关系的整个生命周期中识别、评估和控制在现代混合云环境中的风险的过程。由于采用了不同类型的云（IaaS、PaaS、SaaS），并且缺乏对 CSP 提供的服务和环境的可见性，责任共担模型下的风险管理是复杂的，这也是第三方风险管理（TPRM）的一部分。风险评估也可能因云部署的形式不同而有所不同——私有云、公有云或混合云。

识别风险是风险管理的基础活动；如果 HDO 未能识别风险，它将难以成功管理其风险。HDO 必须确保他们能够及时识别风险，然后将其传达给适当的利益相关者。风险识别中的重要活动包括：

• 建立风险类别。考虑威胁态势的一种常见方式是识别风险/威胁的来源。这种方法有助于将具有共同特征、策略和趋势的风险划分到合适的类别。

• 为依赖科技和信息资产的运营活动识别风险来源。回顾 HDO 在负面运营事件方面的历史经验，可以是识别风险来源的良好第一步。HDO 可以从这个列表开始，然后根据其风险管理活动的范围和独特的运营环境进行定制。

• 在风险登记册中记录已识别的风险，或采用其他跟踪机制。风险登记簿一般用于组织和记录已经识别的运营风险的信息。HDO 的风险管理策略必须将运营活动和流程按优先级排序，来区分出那些已经被管理的和那些较不重要的，需要较低关注水平的活动和流程[9]。HDO 应该使用风险登记册来记录和管理已识别的风险。下表是来自《网络韧性评审补充资源指南：风险管理》[10]中的一个示例。

• 建立一个与您的技术组织熟悉的工作方式相一致的报告机制，例如工程师使

用 Slack 频道报告他们想要报告的风险。这样做的好处是，GRC 不需要承担识别风险的责任，并创造了一个安全意识文化，这种文化拥抱并理解风险，并且员工可以报告风险。

风险编号	识别日期	风险描述	影响	可能性	风险级别	处置	缓解控制	风险所有人

图 3：风险登记册 《网络韧性评审补充资源指南：风险管理》 第 7 卷：风险管理

3.1 评估风险

风险分析过程确保所有已识别的风险都在HDO的风险驱动因素背景下进行评估，以形成风险处置决定。无论采用何种方法进行风险分析，记录这一过程都很重要，以确保一致性并为未来的改进提供背景信息[11]。在进行云风险评估时，理解责任共担模型非常重要。在传统的数据中心中，所有的安全责任都落在 HDO 上。最重要的是理解谁负责云部署的所有阶段[12]。在获取云服务之前，HDO 需要分析使用云解决方案所带来的风险，并规划针对云运营的风险应对和控制活动。为此，云消费者需要获得整个云生态系统的视角，它将服务于其基于云的信息系统的运营[13]。

在评估风险时，使用一个公认的风险管理框架很重要。来自 ISO 和 NIST 的公认框架是使用大型、多样化组织的输入所开发的。在评估风险之后，HDO 应该应用控制措施来管理风险。

在对云平台进行风险评估时，有必要结合多种评估方法，如配置检查和漏洞扫描。然而，云平台有更多有价值的资源，并且与租户有服务级别协议，因此一些评估方法需要根据云计算的特性进行调整。

- 问卷调查：问卷提供了一套关于管理和操作控制的问题，供系统技术或管理

人员填写。问卷应包括 HDO 的业务战略、安全需求、管理系统、系统和数据的敏感性、系统规模和结构等。

• 访谈：现场访谈涉及评估人员前往现场访谈系统技术或管理人员，并收集有关系统的物理、环境和操作方面的信息。访谈的内容应包括：

- 是否有数据存储完整性测试的设计
- 是否有清除数据副本的手段和措施
- 识别、警告和阻止持续大流量攻击的能力，以及是否有专门设备来检测网络入侵
- 虚拟机（VM）之间以及虚拟机与宿主机之间的隔离方法
- 退出云计算服务或变更云服务提供商的初步计划，以及相关客户人员的运营和安全培训计划

• 安全渗透测试：由于基础设施的影响，在 SaaS 环境中进行渗透测试可能是不被允许的。在 PaaS 和 IaaS 中进行云渗透测试是被允许的，但需要一定的协调工作。值得注意的是，合同中的 SLA 将决定哪种类型的测试是被允许的，以及测试应该多久进行一次。

3.2 降低风险

HDO 很可能无法评估 CSP 负责的控制措施。然而，云提供商应该能够向 HDO 提供来自独立评估者的报告，以验证适当的控制措施已经部署并且按预期工作。HDO 可以从云服务提供商那里要求第三方证明材料，例如 SOC2 报告。

HDO 基于责任共担模型对其责任范围内的领域开展风险评估。在大多数云服务模型中，HDO 仍然需要对用于访问云的设备、网络连接、账户和身份以及数据负责。[14] 风险评估会评估 HDO 安全控制的有效性、效率和适当性。包括但不限于检查数据在存储和传输中是否满足加密标准，日志记录和监控是否正确配置，安全组和网络访

问控制列表是否适当地限制了访问，身份和访问管理是否按预期工作，以及漏洞是否及时发现并进行了适当的管理。

HDO 必须将他们的风险和控制框架映射到一个能够以标准化方式解决云风险的框架上。如果 HDO 现有的风险评估模型不能解决云计算的特殊挑战，他们可以从被广泛采用和标准化的框架中受益，例如 ISO 27001、COBIT 和 NIST。

为了更好地理解与云计算平台相关的潜在威胁和风险，请参考 CSA 发布的《云计算十一大顶级流行威胁》报告[15]。这份报告提供了对云用户和提供商面临的最重大安全挑战的深刻见解，包括数据泄露、配置错误、不安全的接口和 API 以及内部威胁。通过了解这些威胁，组织可以采取积极的措施来降低风险，增强其云安全态势。

4. 合规性

云合规性指的是旨在保护和规范存储在云平台上的信息的准则、法律和法规。对于医疗保健服务提供组织（HDO），这指的是涵盖安全性和隐私性的法规和法律。这包括数据如何存储、保护和使用。无论是个人身份信息（PII）、个人健康信息（PHI）还是支付卡行业（PCI）数据，都必须得到保护。云合规性是确保云服务的使用满足合规要求的过程。当 HDO 使用云计算时，他们并没有将合规责任外包给云服务提供商（CSP）。监管机构和客户仍然可以追究他们的责任，因为 HDO 对遵守法律法规、监管和合同义务负有责任。[16]

在美国，当面对联邦法规时，你会遇到特定行业或法律领域的规则。也就是说，每种形式的信息都有其自己的规则。在美国，PHI 有《健康保险流通与责任法案》（HIPAA）。对于 PCI，是《支付卡行业数据安全标准》（PCI DSS）。不少国家、地区有保护其数据主体 PII 的国家法律。这包括存储在国内和国外的数据。在美国，虽然并非所有合规要求都有全面的联邦法律，但每个州都有自己的要求。例如，关于保护个人信息的要求在加利福尼亚州最为突出，有《加利福尼亚州消费者保护法》。

还有缅因州的《缅因州保护在线消费者信息隐私法案》，以及内华达州的《内华达州参议院第 220 号在线隐私法法案》。[17]

除了美国的法规外，加拿大和墨西哥也有自己的法规。加拿大有两项主要的隐私立法：《隐私法》和《个人信息保护与电子资料法》。在墨西哥，《保护私有主体持有的个人数据联邦法》后来得到了《义务主体持有的个人信息保护一般法》的加强。

欧盟实施了《通用数据保护条例》（GDPR），该条例定义了 PII 并要求处理过程的透明度。该指令还禁止将 PII 传输到任何未能证明有足够保护的国家。下图显示了 GDPR 的适用情况。

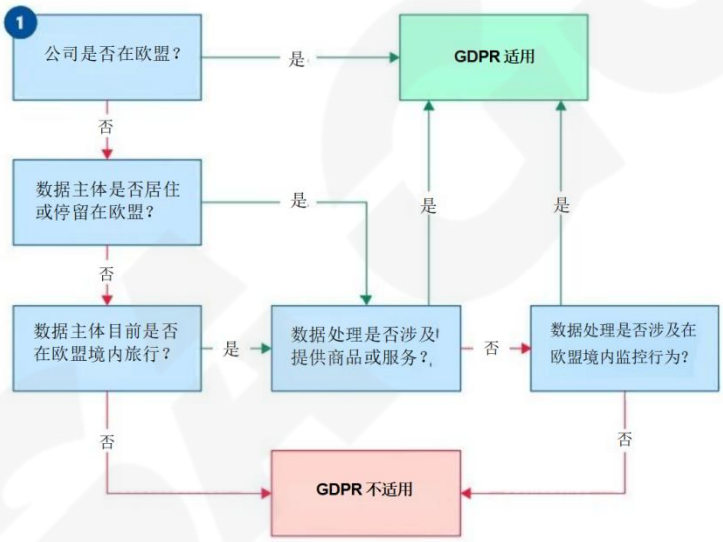

图 4:GDPR 适用范围[18]

这份法规列表让读者了解在确定合规性要求时必须考虑的主要法规。这只是合规要求的一小部分；医疗机构需要针对其特定数据存储地点和涉及对象进一步研究相关要求。

医疗保健组织通常依赖第三方供应商和服务提供商提供各种 IT 服务。评估第三方供应商的安全态势、对其安全实践进行尽职调查，并建立明确安全责任和合规要求的合同协议至关重要。

实施有效的云合规策略对于组织确保其云环境的安全性和符合法规至关重要。医疗保健服务提供组织（HDO）应建立与行业法规和其特定业务需求相一致的明确合规目标。通过进行全面的风险评估，HDO 可以识别潜在的安全风险和合规漏洞。制定明确且有文档记录的政策和程序至关重要。这些策略应涵盖访问控制、加密、数据处理、事件响应与管理、变更管理、漏洞管理以及数据泄露通知。对云环境的持续监控有助于及时识别和纠正不合规问题或安全事件。[19]

4.1 将伦理考量纳入 GRC

随着技术渗透到医疗保健的各个方面，伦理考量变得越来越重要。将伦理规范整合到 GRC 框架中是至关重要的，以解决数据隐私、患者知情同意以及人工智能应用中的算法偏见等问题。这种整合确保技术进步在不侵犯患者权利或自主性的情况下，为患者带来利益。

4.2 云合规框架

这些框架特别针对云合规要求。云服务提供商和客户都应该深入了解这些框架，包括全球采纳的框架以及所在国家、地区的监管框架。

4.3 全球云框架

云控制矩阵（CCM）：云安全联盟（CSA）发布了云控制矩阵（CCM），为评估云安全提供了框架。这个由 CSA 创建的安全控制矩阵为安全供应商提供了基本准则。此外，该框架帮助客户评估潜在云供应商的风险状况。CSA 还开发了一个名为“安全、信任、保障和风险”（STAR）的认证程序。STAR 注册表是一个公开的注册平台，展示了主流云服务提供商在安全和隐私方面的控制措施。

联邦风险与授权管理计划（FedRAMP）：FedRAMP 是一项覆盖整个政府的计划，为云产品和服务的安全评估、授权以及持续监控提供了一种标准化方法。对于希望与任何联邦机构开展业务的组织而言，遵守这一套针对云的特定数据安全法规是必要的。

ISO/IEC 27017：国际标准化组织（ISO）发布了多项网络安全标准，其中 ISO/IEC 27017:2015 是提供云服务信息安全控制指南的标准。

云合规框架帮助您应对监管环境，避免因不合规而带来的财务和声誉成本。此外，这些框架提供了维持客户所需安全级别的指南和规范。通过实施合规框架，HDO 可以展示其对隐私和数据保护的承诺。这将帮助监管机构提升与患者和第三方合作伙伴的信誉和信任。[20]

4.4 地方监管框架

有许多国家、地区特定的云框架。以下是一些示例：

三部委的两项指导方针（2G3M）：在日本，政府对医疗机构在与第三方服务提供商、云服务提供商以及相关方合作时，如何保护医疗信息进行监管。政府规定，云服务提供商有义务根据由两个日本政府部门发布的两项指导方针，审查云风险管理措施。这些指南定义了云服务提供商的义务。

- 《医疗信息系统安全管理指南 5.1 版（2021 年 1 月）》由日本厚生劳动省发布
- 《处理医疗信息的信息系统和服务提供商安全管理指南（2020 年 8 月）》由日本经济产业省发布

法国健康数据托管（HDS）：在法国，HDS 认证由法国政府机构引入。它要求托管个人健康信息（PHI）的服务提供商遵循其框架，以确保 PHI 的安全保护。

- 维护托管物理基础设施的物理场所的正常运行状态

- 维护托管信息系统的应用平台的正常运行状态
- 维护用于处理健康数据的信息系统的虚拟基础设施的正常运行状态
- 对包含健康数据的信息系统进行管理和操作。
- 健康数据的备份

5. 结论

治理、风险和合规（GRC）是一套帮助医疗保健服务提供组织（HDO）结构化其治理、风险管理和监管合规方法的流程、实践、框架和技术。其目标是统一和协调组织的风险管理和监管合规工作。一个精心规划的 GRC 策略可以帮助 HDO 实现多项优势。在采用云计算时，HDO 必须认真识别其安全需求，评估服务提供商的安全和隐私控制，并理解共享责任和合规责任的传递。通过深入理解合规要求和进行全面的风险评估，HDO 可以为安全和合规的云适应奠定基础。GRC 可以帮助将绩效活动与业务目标对齐，管理企业风险，并满足合规法规，确保医疗服务环境的安全和保障。

参考文献

[1] Capgemini,2021.*Cloud Governance Guide-Business Aligned Approach toCloud Utilization,*Retrieved from https://www.capgemini.com/fi-en/research-and-insight/cloud-governance-guide-business-aligned-approach-to-cloud-utilization

[2] Object Management Group,2019.*Practical Guide to Cloud Governance*,Retrieved from https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-governance.pdf

[3] Karkošková,S.&Feuerlicht G.,2016.Cloud ComputingGovernance Lifecycle,Acta Informatica Pragensia,5(1):56-71 DOI:10.18267/j.aip.85

[4] Arend,C.,&Helkenberg,R.2021.*Cloud Governance Success:A Practical Framework to Getting Started with Cloud Data Governance*,Retrieved from https://info.microsoft.com/WE-HCS-CNTNT-FY22-11Nov-10-Cloud-governance-eGuide-A-Practical-Framework-to-Starting-Cloud-Data-Governance-SRGCM5306_LP01-Registration---Form-in-

Body.html

[5] Object Management Group,2019.*Practical Guide to Cloud Governance*,Retrieved from https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-governance.pdf

[6] Ancoris,2023.*Cloud Governance Framework:How to Develop,Implement and Follow One*,Retrieved from https://www.ancoris.com/blog/cloud-governance-framework

[7] Karkošková,S.&Feuerlicht G.,2016.*Cloud Computing Governance Lifecycle*,Acta Informatica Pragensia,5(1):56-71 DOI:10.18267/j.aip.85

[8] Rasner,G.,2021.*Cybersecurity &Third-Party Risk:Third-Party Threat Hunting*,John Wiley&Sons,Inc.,Hoboken,NJ.

[9] Carnegie Mellon University,2016.*CyberResilience Review Supplemental Resource Guide:Risk Management*,Department of Homeland Security

[10] Rasner,G.,2021.Cybersecurity &Third-PartyRisk:Third-Party Threat Hunting,JohnWiley &Sons,Inc.,Hoboken,NJ.

[11] Carnegie Mellon University,2016.Cyber Resilience Review Supplemental Resource Guide:Risk Management, Department ofHomeland Security

[12] Rasner,G.,2021.Cybersecurity &Third-Party Risk:Third-Party Threat Hunting,John Wiley&Sons,Inc.,Hoboken,NJ.

[13] lorga,M.,Karmel,A.,Managing Risk inaCloud Ecosystem,doi.org/10.1109/MCC.2015.122

[14] Microsoft,2023.Risk Assessment Guide for Microsoft Cloud,Retrieved from https://learn.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide

[15] Cloud Security Alliance,2023.*Top Threats to Cloud Computing Pandemic Eleven*,Retrieved from https:/cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven

[16] Shacklett,M.,2023.*What is Cloud Compliance?A Comprehensive Guide*,Retrieved from https:/www.datamation. com/cloud/what-is-cloud-compliance/

[17] Moschovitis,C.,2021.*Privacy Regulations and Cybersecurity:The Essential Business Guide*,JohnWiley &Sons,Inc.New Jersey

[18] Varankevich,S.,2017.Teritorial Scope of GDPR,Retrieved from

https://www.linkedin.com/pulse/territorial-scope-gdpr-flowchart-siarhei-varankevich/?trackingId=U8nnOpslTgWPEcMXttfPVA%3D%3D

[19] Sutradhar C.,2023.*CloudCompliance -Protecting Your Data and Maintaining Trust*,Retrieved from https://www.paloaltonetworks.com/blog/prisma-cloud/cloud-compliance-protecting-your-data-and-maintaining-trust/

[20] Knowles,M.2023.*Cloud Compliance Frameworks:What You Need to Know*,Retrieved from https://hyperproof.io/resource/cloud-compliance-frameworks/

Health Security, 2020. *Healthcare Challenges in the Era of Cybersecurity*, Retrieved from https://bioethics network.org/sites/default/files/webinar/documents/hs.2019.0123.pdf

ISACA, 2014. *Controls & Assurance in the Cloud: Using COBIT 5*. New York: ISACA.

ISACA, 2012. *Guiding Principles for Cloud Computing Adoption and Use*, Retrieved from https://www.eurogeography.eu/SoC/sofia-workshop/SoC-implementation/ISACA-Guiding-Principles.pdf

CSA GCR cloud security alliance
GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905