医疗健康网络安全手册

CSA GCR cloud security alliance
GREATER CHINA REGION ®

云安全联盟软件定义边界工作组的官方网址:

https://cloudsecurityalliance.org/research/working-groups/software-defined-perimeter/

序言

近年来，网络安全事件频发，事件造成的影响也日益增大，对于医疗健康行业，网络安全的重要性凸显。随着医疗信息化的普及，医疗设备与相关系统的安全性已经关系到医疗机构业务的正常运营。勒索软件，拒绝服务攻击造成的医院应用系统中断，已经给多家医疗机构和患者带来巨大影响。此外，在医疗健康大数据以及医患隐私数据的开发利用过程中，网络安全问题已成为新的行业痛点。网络安全不仅需要在技术层面投入预算提升安全防护水平，更需要在网络安全治理管理层面做好设计，在不同业务场景中控制安全风险，提升全员安全意识。

保证医疗健康行业的网络安全，需要企业和个人承担相应的网络安全职责，在中国的《网络安全法》、《数据安全法》、《个人信息保护法》已经明确要求企业需要委派专人负责，确保网络安全和数据的全生命周期安全。本白皮书从全球视角提出了网络安全的发展趋势分析，行业网络安全痛点以及相应的解决方案建议，为企业安全负责人和从业者提供了不错的参考。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

致谢

《医疗健康网络安全手册》(Healthcare Cybersecurity Playbook An Evolving Landscape)一文由 CSA 软件定义边界工作组专家编写，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）：

组　长：童　磊

翻译组：陈　皓　伏伟任　顾　伟　黄　晖　贾玉彬　刘雅梅　王　娜

审校组：顾　伟　郭鹏程　贺志生　李芊晔　沈　勇　姚　凯

感谢以下单位对本文档的支持与贡献：

北京北森云计算股份有限公司　　北京奇虎科技有限公司

北京威联科技有限公司　　成都云山雾隐科技有限公司

防特网信息科技（北京）有限公司（Fortinet ）　　上海碳泽信息科技有限公司

英文版本编写专家

作　者：Jim Angle　Vince Campitelli　John Di Maria　Eleftherios Skoutaris

审稿人：Alex Kaluza　Ashish Vashishtha

CSA 全球员工：Stephen Lumpe　Claire Lehnert　AnnMarie Ulskey

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

介绍

不断演变的格局

想要理解当代医疗健康技术所处的确切阶段，很有必要先回顾一下它的演化进程。医疗健康行业曾遇到过哪些障碍以及如何克服这些障碍的？医疗健康领域将会发生怎样的变革，又将是谁来引领这些变革呢？

20世纪50 年代，使用计算机动进行某些护理活动和记录的设想，标志着信息时代新旅程的开启。但当时并没有什么进展，一方面是因为信息计算还没有发展到一定程度。另一方面，医学界并没看到它的价值，也就对医疗健康电脑化兴致索然。

从 60 年代中期开始，商家已着手开发起了医院管理程序。60 年代末，医院会计系统共享开始出现，供中小型医院使用。此外，还尝试了用于临床的计算机系统，可惜并没有取得成功。

到了 90 年代，计算机已经发展得更为灵活、强大，成为了实用的信息管理工具。另外，当时引入的网络能够将来自不同地点的医疗健康数据链接起来。再加上以患者为中心的综合数据变得愈发重要，人们的重点慢慢转移到了记录终身健康档案上（Hannah、Ball 和 Edwards，2006 年）。在这之前，很少有关计算机在临床上应用。阻碍计算机发展的最大因素是医疗供应商不愿证实计算机在成本和患者健康方面的优势（mThink，2003）。

从此，医疗健康系统的健康记录迅速走向了计算机化。如今，患者的病历档案里已有着完整的病史记录，不同医生可以从不同地点检索、查看和修改。医疗健康行业开始进入了一个专注于临床护理的创新时代。

数字化转型彻底改变了医疗健康产业，这在几年前还不可能做到。随着云计算和大数据分析的蓬勃发展，加上以消费者为中心的医疗体系的转变，医疗健康服务正在重塑。卫生保健组织 (HDO) 能够访问大量数据，如果对其整理、分析和适当利用，这些数据可为 HDO 和患者带来巨大利益。

云计算的运用催生出了物联网 (IoT) 和可穿戴医疗设备，即医疗物联网 (IoMT)。这些技术创新提供了大量数据，可以有效提高患者护理水平、完善临床资料、增加效率并降低成本（Armis，2019）。

不久前医疗设备还是没有任何网络连接的独立设备。如今的医疗设备不仅有网络连接，而且还常常接入云端。这种连接大有益处。首先，它可以远程监控设备。医疗系统人员无需患者前来即可远程查看植入设备的传感状况。医院的护理人员也可以从一个中心区域监控患者，不再需要频繁查房。

在新冠疫情期间，远程医疗更成了医疗健康系统一个显著增长的方面。由于医疗健康服务逐渐转变为以患者为中心，远程医疗可以运用在各个方面包括远程患者监控或常规预约等等。此外，新冠疫情的爆发促使 HDO 开始采用视频会议进行常规在线门诊。如果得到有效运用，远程医疗可以极大地改善患者与其他患者、工作人员和弱势群体的接触问题，还可以为家中症状较轻的患者提供所需的护理，同时减缓致命病毒的传播。

这些先进技术通过与云计算结合，使我们现在拥有了庞大的数据集。这些数据集可同大数据分析一起使用

于管理人口健康、预测健康趋势以及处理流行疾病，如新冠疫情的应对。这种数据分析可以有效改善患者的治疗效果。

1 医疗健康行业作为首要目标

无论从哪个角度看，美国医疗健康行业是一个目标丰富的环境！ 该行业得到超过784,626个组织的支持，这些组织包括数千个复杂且动态的供应链。美国每8个公民中就有一个是这些组织的雇员。在6210多家注册医院中，每年的住院人数超过3600万。这还不包括新冠疫情后远程医疗和远程医疗服务的激增，这创造了一种新的患者服务、入院和治疗类别。[1]

自2010年以来，美国每年的医疗支出占国内生产总值（GDP）的17%以上，这一事实表明了美国在医疗健康行业的支出规模[2]。

1.1 云计算—大湖中的小池塘

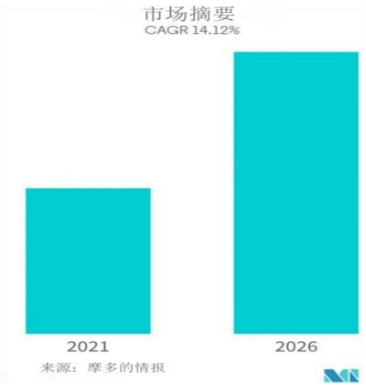
云计算仍处于起步阶段，该行业在20世纪50年代开始技术尝试。但如图1所示，预计采用的增长速度将越来越快[3]。

随着这种增长，预计由于本手册中提到的许多原因，网络安全攻击的风险将反映与目前该行业的现有传统技术平台所经历的频率相似，甚至更高。 根据2019年的泰雷兹报告70% 接受调查的医疗健康组织报告了数据泄露[4]，其中三分之一的机构自去年以来报告了数据泄露。 所有接受调查的组织都报告说使用数字转换技术收集、存储或共享敏感信息。

“2009 年至 2019 年间，共发生了 3,054 起医疗健康数据泄露事件，涉及 500 多条记录。 这些泄漏事件已导致 230,954,151 份医疗记录丢失、被盗、暴露或不允许披露。 这相当于美国人口的 69.78% 以上。 2019 年，每天报告的医疗健康数据泄露事件达1.4 起。”[5]

根据2021年1月5日发表在《Health IT Security》上的一篇文章，自2020年11月以来，针对医疗实体的网络攻击增加了45%。根据Check Point和Fortified Health Security的报告，按照这个比率，该行业占所有数据泄露报告事件的79%。

Check Point的研究为该行业目前面临的最大威胁提供了新的分析。在联邦机构就医疗服务提供商面临的勒索软件威胁发出告警后不久，研究人员发现攻击事件增加了45%，是其他行业的两倍多。



图表 1

[1] https://policyadvice.net/insurance/insights/healthcare-statistics/
[2] IBID
[3] https://www.mordorintelligence.com/industry-reports/global-healthcare-cloud-computing-marketindustry
[4] https://cpl.thalesgroup.com/healthcare-data-threat-report
[5] HIPPA Report https://www.hipaajournal.com/healthcare-data-breach-statistics/

这些威胁包括僵尸网络、远程代码执行和DDoS攻击，其中勒索软件攻击增幅最大。Check Point强调，恶意软件是医疗健康提供商面临的最大威胁。

这些信息证实了我们的论点，医疗健康行业面临着与其他行业不同的重大挑战，即：

供足够的医疗健康服务将会收集大量敏感数据，这些数据比其他行业具有更大的长期风险。此外，与可以访问和利用的其他类型的数据相比，这些数据本质上对黑客更具吸引力。 因此，可能会对成功受到攻击的组织产生一系列负面影响，例如： 监管机构（例如美国的 HHS、FDA 和欧盟和欧洲经济区的GDPR）处以巨额罚款/处罚或采取法律诉讼； 此外，患者和社会的信心丧失，所涉组织的声誉也受到损害。

从风险的角度来看，无法完全减轻未来受到损害的可能性。 例如，在金融服务中，可以取消信用卡并关闭银行账户。 在医疗健康领域，患者的私人数据可以在无休止的欺诈和滥用循环中重新出售、回收和再利用！更糟糕的是，患者可能永远不会意识到与他们的数据相关的欺诈行为！如果没有改进和更有效的干预措施，结果是可想而知且令人担忧的。

随着更敏感的医疗健康和相关个人数据迁移到云端，受独立提供商和市场新进入者增长的刺激，目标数量将增长，并且数据量将呈指数级增长。

全球患者将继续来到美国寻求只有在美国才能获得的出色医疗健康服务。 这就产生了来自欧盟的合规负担——通用数据保护条例，又名GDPR。此类活动引发了两项监管要求。根据美国 HIPAA 要求，定期风险评估必须记录这些跨境数据流的存在，而根据欧盟的 GDPR，必须记录实现合规所需的数据保护要求。 此外，随着英国于2021年1月1日退出欧盟，根据英国脱欧协议，英国目前存在的 GDPR 肯定会进行修改。

医疗健康也是管理供应链风险的一项研究。 组织不应天真地认为他们不必担心安全性，因为他们正在迁移到云。 根据 HIPAA的规定，供应商继续负责完成和记录企业风险评估，包括与外包给第三方相关的风险，尤其是第三方的第N方可能随后负责选定的安全和隐私控制的操作。现在，比以往任何时候都更需要一个安全公理，那就是组织是强大的取决于其最薄弱的环节是“强大”的，这是所有供应商尽职调查的精神和实践中的一个口号。

我们观察到，采用云服务的组织开始意识到，随着每个新 CSP 的采用，他们实际上已将其企业扩展为“云中某处”的另一个实体。 一个他们对其运营的控制措施有限，甚至可见性更低的实体，但仍然对持续运营、有效性能、适当的安全性、隐私和所有相关的法规遵从性要求负全部责任。虽然并非不可能，但如果没有深入的规划、持续的警惕和对整个供应链提供的技术服务的掌握，成功也不是必然的。这些新挑战可能会给那些试图平衡患者护理和在全球大流行病中运营的组织带来相当大的预算和培训负担。

解决医疗健康领域的网络安全和云技术技能差距。 进入2021年，大多数医疗健康组织面临的最普遍挑战之一将是掌握技能提升和新技能要求，以满足数字化转型和云技术平台的独特需求，包括治理、风险、合规性、安全性和隐私保护。

1.2 医疗健康行业网络安全的现状

为了反映美国网络安全现状的最新快照，在此分享2020年进行的最新调查的结果，以便对行业的当前趋势和挑战提供一些见解。

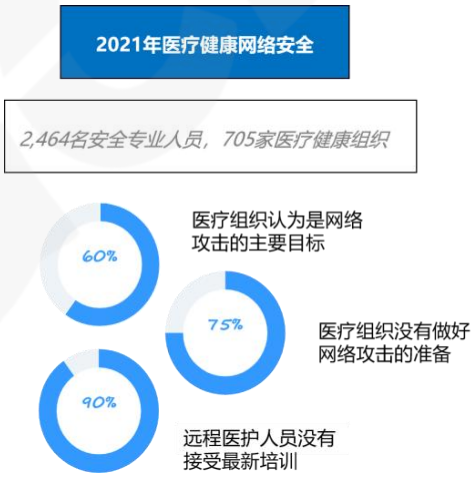
最近的一项市场研究调查[6]了来自 705 家医疗健康组织的 2,464 名安全专业人员，旨在了解为什么这些组织容易受到与医疗健康相关的数据泄露的影响。 如下图 1 所示，研究人员发现[7]：

> 1.73% 的卫生系统、医院和医生组织评估其基础设施没有做好应对网络攻击的准备。
>
> 2.96%的IT专业人士证实，数据攻击者的攻击速度超过了企业抵御攻击者的能力。
>
> 3.网络安全专业人才短缺的现象有增无减，远远满足不了卫生系统的需求。

在一项相关的黑皮书调查中，291名医疗健康人力资源高管接受了调查。

他们报告说，医疗IT职位的招聘具有挑战性，往往比其他IT职位的招聘时间长70%。另外 66 名卫生系统的 CISO 也接受了采访，他们认为许多安全专业人员不愿意在医疗机构中寻求工作。

总而言之，医疗健康网络安全方面的现有差距，加上医疗健康部门缺乏经验丰富的 IT 专业人员，增加了医疗健康数据泄漏的可能性。 这些网络安全风险只会因在家工作的情况增加而加剧，大量医护人员需要在家工作，而没有专门为这些新工作范式设计全面和量身定制的安全指南和最佳实践。



图表 2

1.3 医疗健康和网络安全—关键行业考虑 (3)

> • 据预测，医疗健康行业遭受的网络攻击将是其他行业平均数量的2-3倍。
>
> • 据预测，2017年至2020年间，针对医疗机构的勒索软件攻击将翻两番，到2021年可能增长到5倍。
>
> • 根据HIPAA杂志的一份报告，医疗健康电子邮件欺诈攻击在两年内增加了473%。
>
> • 根据Health IT Security的一份报告，超过24%的美国医疗健康员工表示，他们没有接受网络安全意识培训。
>
> • 超过93%的医疗健康组织在过去3年中经历过数据泄露，57%的医疗健康组织承认在同一时间段内有5次

[6] https://www.prnewswire.com/news-releases/attacks-predicted-to-triple-in-2021-black-book-state-of-the-healthcare-industry-cybersecurity-industry-report-301172525

[7] https://www.herjavecgroup.com/healthcare-cybersecurity-report-2021/

以上的数据泄露。

• 据称，医疗健康机构在其IT预算中，网络安全部分的平均比例为（4-7）%，而其他行业（如金融服务业）的这一比例约为15%。

• IT研究公司Gartner预测，到2020年，医疗服务机构中超过25%的网络攻击将涉及物联网（IoT）。

界定医疗健康行业的网络事实是无可辩驳的！这是一个被围攻的行业。由于其文化和对患者护理和健康的总体承诺，安全和隐私问题并非组织需要。因此，结果是可预见的，许多攻击都是成功的，并且这些成功通常具有长期的影响。

如果执行得当，云计算的采用可为医疗健康提供者提供独特的机会，以实现其护理和交付系统的现代化，并集成内部部署解决方案无法实现的安全和隐私功能。该论点得到了riskrecon(8) 最近进行的一项研究的证实，其中得出的结论是“我们可以把这些结果解释为宣称云计算还没有为医疗健康应用做好准备，应该避免使用”。

然而，另一种解释可能表明，这更多地是关于机构对云的准备，而不是云固有的不安全性。无论哪种方式，这些结果都应该鼓励所有迁移到云的医疗健康组织评估其处理模式转变（即云安全）的能力…”

2 安全医疗的承诺

只有在医疗健康领域，我们才会遇到这样一个悖论：越来越多的数据通过医生办公室和公共卫生部门流动：然而，在过去，这些数据的价值在很大程度上尚未开发，因为它们是非结构化的，并且被孤立在互不通信的系统中（Kelly，2019）。如今，大数据分析比以往任何时候都更加重要。大数据可用于帮助快速识别COVID-19的爆发，并提供更好的应对措施。大数据还可用于关联治疗数据，从而有助于结束大流行。

随着HDO继续通过改善服务、质量和成本获得竞争优势，他们依靠技术来提供优势。这一举措始于电子医疗记录，以及越来越依赖技术通过连接设备提供医疗健康，现在已转向虚拟医疗健康。主要由于COVID-19大流行，去年向虚拟医疗健康服务的转变加速了。

虚拟医疗和可穿戴个人健康监测设备的使用大大增加了攻击面。再加上商业性的非医疗机构现在也参与其中，亚马逊宣布扩展到全国范围内的远程医疗，谷歌收购了Fitbit。我们现在有一个更大的攻击面。问题是，随着这一增长，我们如何兑现获得高质量、低成本和安全医疗的承诺？

使用安全可靠的技术可以实现改善患者和提供者的实践和标准的承诺。 为了增强这项技术，HDO越来越多地将其迁移到云端。 云计算可以提高 HDO 的能力，但由于监管要求，医疗健康服务需要一个安全且可审计的平台。 云计算可以链接所有孤立的系统，允许收集和分析数据。 云计算有助于兑现改善患者治疗效果和改善医疗服务提供者与患者之间沟通的承诺。

2.1 时刻保护所有患者

云计算作为一项有望改变医疗健康行业的有前途的技术迅速进入我们的环境。 云计算具有许多优势，例如灵活性、成本和能源节约、资源共享和快速部署（Al-Issa、Ottom 和 Tamrawi，2019 年）。云计算还带来了许多安全和隐私问题。在当今的移动社会中，HDO 需要随时随地访问医疗记录。云计算促进了来自患者、医疗设备、医疗物联网 (IoMT) 和多个 HDO 的数据共享。 这种共享以及 HDO 和患者随时随地访问，需要更高级别的安全性。

无论数据驻留在何处，HDO都负责确保医疗数据的隐私和安全。 医疗健康数据很有价值，而 HDO 是网络犯罪分子的目标。 这使得始终HDO 必须保护所有患者信息。 除了保护患者信息的道德义务外，组织还需要满足监管要求。

世界上大多数国家/地区还制定了管理健康数据处理的数据保护法。 这些要求可能会在国家法律（一般适用于个人数据）和部门法律（适用于特定领域（如健康）或特定法律（适用于特定情况，如 COVID））中描述。每项法律都有其要求，这些要求可能是另一项法律的补充，也可能是另一项法律的例外。此外，由于国家之间的数据保护制度存在差异，大多数国家除非满足某些条件否则禁止个人数据（包括健康数据）的传输，HDO必须了解管理其数据收集、处理和存储地点的法律；这里法律包括所有国家和地方法律。

2.1.1 透明度和保证

人们越来越意识到，当前安全事件呈上升趋势，许多组织的表现不佳，与此同时公众信任度也在下降。 对公开报告中传达的信息缺乏信心可能会削弱披露的动机。 可以通过使用第三方独立保证来缩小可信度差距。然而，这并不是一个不合格的解决方案。迄今为止，许多验证和保证实践本身在稳健性、可靠性和一致性方面存在问题，并且所采用的保证模型不足以满足更广泛的能力维度方面的要求。

有必要建立一个通用框架，确保报告的透明性和道德性，并确保担保提供者本身的信誉。CSA STAR计划提供了解决这些差距的方法和工具。

安全信任保证和风险 (STAR) 计划包含透明度、严格审计和标准协调的关键原则。 使用 STAR 的公司指出最佳实践并验证其云产品的安全状况。云控制矩阵是STAR计划所依据的特定部门云控制的基准。

STAR 注册表记录了流行的云计算产品提供的安全和隐私控制。 这个可公开访问的注册表允许云客户评估他们的安全提供商以做出最佳采购决策。

要使用云推动业务成功，您必须了解责任共担模型（图 2），并且明确各个角色和职责至关重要。 STAR 要求组织考虑云服务提供商和用户的角色和责任。

图 2

停电、中断、漏洞和灾难仍然是一种风险，即使对于云也是如此。 因此，作为云用户，您必须识别风险并实施相关控制措施。

3 当前和未来的可扩展性

规模和可伸缩性是描述医疗健康行业和云计算的两个口号，这一点并不奇怪！它们适用于虚拟世界中的云计算，虚拟世界支持允许IT资源动态扩展或收缩的云技术流程。它们主要应用于医疗健康行业的物理世界，这是由大量潜在患者/消费者衡量。在过去一年中，我们观察到该行业如何以云计算解决方案的形式采用可伸缩性的概念，这种解决方案支持可归因于新冠病毒大流行的不可预见的患者疾病和护理高峰。

从历史上看，美国医疗健康行业的规模和范围需要在技术资源、流程和人员方面进行巨额投资。这些投资导致了持续的资本成本、遗留技术平台以及不变的基础设施和房地产承诺。今天，供给和需求都在不断变化，有时甚至是意料之外的变化——这就是明证新冠病毒大流行过去两年的影响——是使用新冠病毒的重要驱动因素。目前的趋势表明，对医疗健康的需求持续增长，这主要归因于人口老龄化和增长，再加上消费者日益增

长的兴趣和健康。在2025年至2025年期间[8]，与11 – 17%的增长率趋势相关的主要趋势有四个：

•消费主义升级。这导致供应商市场从基于数量的服务转向基于价值的服务。价值模型根据护理成本效益和临床病例结果奖励提供者。这些变化保证了通过云计算可实现的可变随需应变IT资源实现的快速创新。云计算使消费者能够识别和使用大量提供商提供的同类最佳医疗服务。

•医疗监管和金融风险重组的影响。医疗改革和监管已经并将继续改变医疗格局。监管影响市场结构，这将继续推动纵向和横向的整合。由此带来的组织规模和范围的增长，促进了对创新服务和产品的更大投资，吸引了广大消费者/患者。整合的进一步影响催生了新技术平台和服务的诞生，这些平台和服务创造了由云计算支持的新产品和服务，如大数据分析和人工智能。受影响的运营流程：在本用例中，信息促进了数据安全和隐私保护。需要考虑统一的安全管理机制。

•数字化的影响。IT，特别是云计算，是使消费者能够对其医疗健康拥有更大所有权，并让他们以更少的限制获得更多选择的促成因素。医疗健康行业正朝着以信息为中心的交付模式发展，该模式促进合作、协作和信息共享。云计算提供了虚拟基础设施，允许医院、医疗机构、保险公司、研究机构和医疗\生态系统中的其他参与者利用相同的计算资源。

•关注预防性保健。如今，消费者使用移动应用程序、物联网（IoT）和可穿戴技术——所有这些都可以通过云监控他们的健康、与他们的提供商通信和接受治疗。医疗健康正在从一个“修复我的系统”以“促进幸福”系统，主要归功于技术创新。需要医疗实践和医疗服务转型。今天基于云的技术的承诺，加上基于数据分析、人工智能、全球协作和无处不在的访问的许多技术创新，将加速行业转型n、 目前能够提供独立于时间和地点、协作、一致和实时的认知患者支持和服务。这些能力将有助于实现未来医疗健康的必要转型。

为了获得云计算所带来的诸多好处，并在整个医疗健康领域充分利用这些好处，消费组织应该遵循几个深思熟虑的步骤，以经济高效地利用云服务提供商提供的众多服务。 这些步骤必须考虑到消费组织的动态，以及他们需要提供的服务的规模和范围。

将云计算用于医疗健康的指导[9]：

1) 为云计算构建商业案例。
2) 确定特定的基于云的医疗健康解决方案并确定其优先级。
3) 确定合适的云部署和服务模型。
4) 执行符合HIPAA的测试。所有云服务和云服务提供商的企业风险评估。

[8] Cloud Standards Customer Council Impact of Cloud computing on Healthcare, version 2 (2017)

[9] IBID

5) 确保满足所有安全和隐私要求。

6) 记录与现有企业系统的集成和互操作性点。（这应包括整个供应链中所有其他受影响的应用程序/服务。）

7) 为所有SLA和KPI协商云服务协议和监控工具。

8) 开发用于监控/管理所有云服务和所有云服务提供商的责任矩阵/模型。

9) 为整个云服务组合和云服务提供商开发和监控风险仪表板。（注意，应定期与所有云服务和云服务提供商的单独清单进行核对。）

10) 保存一份关于所有高风险未决问题的相关分发报告。

11) 记录纠正措施计划和状态。

4 时间、金钱和资源

最近一项 CynergisTek 的 CAPP会议调查中[10]，54% 的医疗健康专业人士指出，资源（金钱、人员和工具）是满足组织安全和隐私需求的最大障碍。以 NIST 网络安全框架作为衡量标准， 79% 的医疗机构在合规性方面的评估得分低于“C”。

很多时候，根本原因是过于复杂。复杂性给系统和资源带来很大负担。即使安全技术有所改进，还是系统越复杂安全性越低。造成这种情况的原因有很多，但都可以追溯到复杂性问题。为什么？因为我们非常关注技术，并且增加了很多法规和标准。因此，我们变得支离破碎，过于复杂。

复杂系统：

•有更多的独立进程，会产生更多安全风险。

•有更多的接口和交互，会产生更多安全风险。

•更难监控，可能包含未经测试和审计的部分。

•更难安全地开发和实施。

•员工和利益相关者更难理解和接受培训。

[10] https://docs.google.com/document/d/1_2RqUOgWB3WWa8bto_dpeyJcyCXy_ZyV58p_lmCg0OQ/edit?ts=608f0a23#

为了应对这些日益增长的业务问题，云安全联盟 (CSA)创建了云控制矩阵(CCM)，与国际行业工作小组共同开发，明确了云安全相关的通用控件，是CSA STAR构建的基础。CCM映射到超过35种不同的标准和法规，这有助于显著减少安全程序的实施。

我们应该将 80% 的时间用于计划，20% 的时间用于实施，但实际上，大多数组织将 20% 的时间用于计划，20% 的时间用于实施，60% 的时间用于灭火，然后延续系统的生命周期或直至我们退休，以较早者为准。

我们逐个看下它们是如何影响项目的。

时间限制是指可用于完成项目的时间。

成本（金钱）约束是指项目可用的预算金额。

资源是指实现优质和有效的系统所需的人数、流程和技术。

但我们还须将范围纳入其中。项目范围的大小将对时间成本和资源产生重大影响。范围扩大通常意味着时间增多和成本增加，时间限制可能意味着成本增加和范围缩小，而预算紧张可能意味着时间增加和范围缩小。

最后，组织的安全性是复杂性的直接结果。集成系统可降低成本并提高安全性。

集成安全系统使组织能够将其流程和程序整合到一个完整的框架中，这有助于有效和高效地实现目标。

为了使这些系统成为公司整体系统的组成部分，流程之间必须无缝连接。

换种方式做事...

经验告诉我们，成功企业在整个组织中推行最佳实践，而不仅仅是在一个特定领域。当下的产品和服务必须满足各种认证和合规性要求。制定可重复使用的流程和一致框架让组织能够符合标准、发展业务和妥善经营。

制定全公司范围的战略可以打破长期以来部门相互隔绝的“孤岛效应”，对于许多组织来说，这代表着企业文化的重大变化。

集成安全系统将业务的所有组件集成到一个连贯的系统中，以实现其目的和使命，并以最少的成本、时间和资源维护系统，同时降低风险并提高弹性。

5 管理整个生命周期

任何关于云安全的讨论都应该从数据的生命周期开始。当我们在为云实施定义所需要的安全控制时，需要记住这些都是为数据而生的。计算机，包括云计算，生成，存储，处理和使用数据。核心价值就在数据中，这也就是我们需要尽力去保护的东西。为了保护数据，我们必须知道我们拥有哪些数据，这些数据存储在什么地方。为了确保你能够从所有的角度照顾到数据安全的方方面面，最好的办法就是贯彻整个数据生命周期去审视

它。数据的生命周期管理是及其重要的，因为随着时间的流逝，数据的价值可能会下降，但是数据存储的成本和数据暴露的风险并不会。数据生命周期为：

> •创建-数据的生成，获取或者是修改
>
> •存储-将数据发送到数据仓库
>
> •使用-对数据进行处理，查看或者是其他任何的使用活动
>
> •共享-数据或是信息为其他人所访问
>
> •归档-数据放置于长期的存储之中
>
> •销毁-当数据不再需要时，对它进行物理性的摧毁

5.1 创建

医疗健康服务组织(HDO)会因为众多的原因创建和收集数据，比如财务，供应链，人力资源和病患资料。第一步是需要识别创建了什么类型的数据。此数据是否是敏感数据诸如受保护的健康信息 (PHI)，个人可标识信息 (PII), 或者支付卡行业 (PCI)数据？ 在此阶段的关键性安全因素如下:

数据是如何创建，收集或是进行修改的？ 是否由外部资源所创建，比如一个新的患者或是员工输入了最初的数据？是否是通过其他数据源汇编而创建？是否是通过键盘输入，移动端应用或是联合数据？HDO必须知道所有收据的来源。

数据的用途是什么？这对于HDO们来说是至关重要的，因为PII和PHI法规都要求HDO能够告知收集的数据的内容和用途

谁能够创建和收集数据？当数据包含PHI时，识别谁能够创建或是收集数据就变得非常重要。“谁”是对数据的一致性的回顾。

数据是怎么进行分类分级的？数据的分类关系到此类数据的保密性要求。例如：是仅供内部使用，业务机密还是PHI敏感数据。联邦信息和信息系统安全分类199 (FIPS) 199建立了相关信息和信息系统的三个潜在的影响层级（低，中，高），针对三个层级各有三个明确的安全目标（保密性，一致性和可用性）(Stine, Kissel, Barker, Fahlsing, and Gulick 2008).

影响数据创建的工具的安全性如何？供应商是否部署了安全开发实践，包括应用代码扫描，针对代码的访问控制和知识产权保护？

了解数据的来源会帮助组织建立一个坚实的安全基础。

5.2 存储

HDO 的存储管理政策可以帮助HDO更有效的管理他们的存储资源，并同时满足所有法律和法规的合规要求。在HDO决定存储要求之前，他们必须要明白有多大数量的数据要进行存储，它们都是些什么数据。随后的问题可以对启动关于存储的对话有所帮助：

数据将会被存储在哪里？是云端，企业数据中心，本地存储或者是可移动的媒介。所以这些都有它们各自不同的要求，同时HDO应该考虑每种存储方式可能产生的影响。

谁可以访问存储中的数据？这是对于管理数据存储基础架构的人来说，想要了解访问特权的关键点。

对于云端的数据来说，它具体存储在什么地方？ 这是想要了解数据存储位置所首先要知道的，无论是主要数据还是备份数据。数据是否有离岸存储？ 法规要求可能会因为存储的具体位置而有所不同。

数据需要保留多长时间？ 数据保留要求可能会决定最终使用的存储方式

是否有针对静态数据的加密要求？基于数据保密性的考虑，可能会有法规或是业务要求对数据进行加密

了解存储的数据的种类，存储位置，访问权限，存储状态和保留期限可以帮助HDO 部署正确的安全控制。

5.3 使用

由于数据收集的速度和规模在不断的增长，用于处理数据集的分析技术越来越复杂，同时数据的使用也变得越来越多种多样。针对健康研究的大数据有着巨大的潜力；然而必须要对它进行正确的保护以防止相关数据的丢失和滥用。在医疗健康领域的数据安全可以助推积极的成果并阻止负面影响的产生。另外，透明度也对医疗健康业的数据安全提出了复杂的挑战。HDO需要在保证安全的同时，在如何使用它们的数据方面显示出更大的透明度。

了解数据和如何使用数据是非常重要的。HDO必须知道后面问题的答案：

谁是数据的用户？这些数据的用户可能并不是数据的拥有者。

数据将在什么地方进行使用？

数据的用途是什么，以及数据如何被使用？

数据的使用是否正确地基于数据类型和法规要求？

数据在将来会如何使用？

对于数据和用户进行全面的了解有助于HDO确保可以部署正确的控制，并让这些控制高效的保护数据。这些控制必须包含一个强健的识别和准入控制程序(IAM)。在云计算中，陈旧的网络边界不再那么有效，同时准入控制已经变成了新的边界。

5.4 共享

多年以来，HDOs建立了很多数据仓库，这些烟囱式系统导致了数据孤岛。这种烟囱式系统的大量使用导致所建立的系统中的数据更多的被复制而不是共享。而良好的数据安全则可以提供更有效的分享数据的流程。为此，HDO必须要回答出如下问题：

数据要共享给谁？比如，一家保险公司，计费资源，医院/治疗人员？

数据共享出于什么样的目的？这些人真的有必要知道吗？

根据数据类型和监管要求，这种使用是否合适？

数据是否会完全离开HDOs的云架构？数据在其他供应商那里使用和存储时是否都到了足够的保护？

有两项技术可以帮助HDOs 来安全的共享数据，它们是云访问安全代理(CASB)和权限管理服务 (RMS). CASB是一个策略执行中心，它可以把多个安全策略进行合并，然后将她们应用到HDO云端所有的实例上。CASB可以让HDO使用更细粒度的方法来进行数据保护和策略执行。RMS可以帮助HDOs提升他们的数据保护策略，通过持续一致的数据使用策略来保护信息，无论它存在什么位置上。HDOs可以定义谁有权限打开，修改，打印，转发或是对信息进行其他的操作行为。HDOs还可以创建定制的使用策略模板并直接应用到对应的信息上。

5.5 归档

法律法规诸如《健康保险流通与责任法案》(HIPAA)展示了如何制定一份有效的数据管理计划，来应对 HDOs所创建，处理和存储的那些无穷无尽的数据阵列。HDOs必须要执行这样的信息安全政策 ，不仅是为了减少支出，降低成本还要提升运营效率。那些HDO必须要保存但是不再活跃的数据就应当归档。数据是否需要归档是HDO必须要知道的：

HDOs控制范围内的各种数据类型的数据保留要求是什么？

每一个存储 ePHI的合作方，是否有对应的方法来满足数据归档的要求？

诉讼保留中的数据是否确实保存到了保留结束的时候？(Crosbie, 2020)

5.6 销毁

HDO不能忘记数据销毁，包括资产处置，这是数据生命周期中最后一步重要的阶段。由于敏感数据和受管制的数据可能跨多个站点存储，HDO必须有简明扼要的政策和流程定义如何销毁过期、受限访问的数据以及它所使用的未加密的存储媒介：

谁负责数据销毁？

合作方如何提供关于数据按照指导原则进行了安全的销毁的保证？

使用了什么样的销毁方式来确保数据无法再重新获得？

谁负责资产处置，另一个层面和维度的资产处置？

当资产不再需要时，上面的数据是否得到了正确的销毁？

资产上的物理存储能力是否被移除了,数据是否确实被销毁了？

数据销毁政策是否包含了确保所有敏感数据已经被销毁的流程？

在多租户的云环境下，数据销毁对于一个单个实体来说是很困难的，因为存储介质不可能为了单个实体而销毁；这是一个全有或是全无的局面。这里有两个行之有效的方式来确保数据已经被销毁。一是如果数据是被加密的，如果不再需要相关数据就将密钥销毁。当数据还以物理方式存在那里的时候，它将无法再被使用(Gillian 2019)。

关于这个方法有一点需要注意，HDO必须从合同责任上确保每一个租户使用不同的秘钥来进行数据加密。第二个方法，可以使用多次重写的方式直到数据无法再被获取。

6 提升你的安全态势

随着新闻中安全漏洞的数量呈指数级增长，您需要在下一个标题是关于您的组织之前采取行动。但是，提升你的安全态势可能会让你难以决定从哪里开始。提升到一个强大的安全态势需要时间和持续的改进，然而，有一些简单的关键行动，您可以采取，将促进长期安全成功。

建立一种安全意识的文化，让领导层参与进来，让全体员工参与进来。

对安全专业人士来说，最大的挑战之一是向他们的领导或管理证明投资安全的价值。虽然许多领导者可能传统上将安全视为组织生产力的障碍，但必须帮助他们认识到安全所带来的好处。

由于今天的许多入侵都是由员工的失误造成的，一个受过教育的员工是一个强有力的安全态势最关键的组成部分。确保你实施了一个涵盖所有员工的全面培训平台。深入程度应该由风险、员工角色和责任决定。

建立定期的安全内部审计。当涉及到识别安全环境中的漏洞时，内部审计是必要的。确保您对业务流程和相关的安全状况具有完全的可视性是至关重要的。

在医疗健康领域，从患者登记到控制和监控传输身体功能信息以及配药的活动医疗设备，软件被广泛使用。潜在的供应链攻击和破坏一直是一个问题，但最近的例子，如SolarWinds提醒我们，攻击者可以利用第三方代码直接危及代理系统。根据sonatype最近的一份报告[11]，开源软件供应链攻击增加了400%以上，指向一个越来越有吸引力的攻击途径。

年度Bitglass“医疗数据泄漏报告”[12]其分析数据发布到“耻辱之墙”.泄漏报告和由美国健康和人类服务部

[11] https://www.sonatype.com/campaign/wp-2020-state-of-the-software-supply-chain-report

[12] https://www.bitglass.com/press-releases/2021-healthcare-breach-report#:~:text=Bitglass%20

门运营的公众问责网站显示美国医疗数据泄露的总数从386年的2019上升到599年的2020人,增长55.1%。67.3%的入侵是由黑客入侵和IT事件造成的。拥有一个良好的信息安全管理系统，涵盖关键的人员、流程和技术，这是至关重要的。这包括很好地处理第三方云软件(SaaS)和基础设施公司(IaaS)服务提供商。

要求您的云提供商的安全性和有效性证据的透明度是降低风险和理解您的组织的角色和责任的重要步骤;正如本文透明度和保证部分所描述的，在证明尽职调查和“注意标准”方面有很长的路要走。CSA的共识评估计划问卷(CAIQ)和云控制矩阵(CCM)是很好的开始工具，有很好的文档说明。

7 结论

数字化转型和云计算改变了几年钱前无法实现的医疗健康方式。云计算和大数据分析的使用，以及转向以消费者为中心的医疗健康方式，正在重塑医疗健康服务。 如果如果使用得当，医疗健康机构通过访问大量数据，可以使患者和医疗健康机构都受益。物联网和 MedIoT(使用物联网的药品确认系统)的创新，一直都是以改善患者的护理为目标。 但随之而来也带来了对医疗数据及其患者资料的保护责任。

79%的医疗健康机构在合规性方面的评估得分低于“C”，美国卫生与公众服务部显示，美国医疗健康违规总数从2019年的386起上升到2020年的599起（增长55.1%）。因此有明确的要求，需要建立一种让全体员工参与进来，并获得领导层的支持的安全意识文化。

行业和患者要求云计算提供商和内部组织能提供更高透明度的安全性和有效性的证据。 如本文的透明度和保证部分所述，是为了降低风险并了解您组织的角色和责任。 以及在安全培训上的增加，将大大有助于在被传唤出庭的不幸事件中，证明有可能出现的“尽职调查”和“谨慎标准”这两个问题。 CSA的共识评估倡议问卷 (CAIQ) 和云控制矩阵 (CCM) 是帮您避免钉在“耻辱墙”上的绝佳工具。

7.1 培训和教育

如果您是云计算的新手，甚至是CSA和云安全的新手，我们建议您首先查看下表中的推荐阅读材料以及培训和教育机会，其中包括CSA相关认证。

这些文档可以极大地帮助您组织中的个人提高他们的能力，并扩展他们的能力，填补由世界各地医疗健康提供商使用的众多云平台所造成的知识缺口。

7.2 推荐阅读材料

以下这份阅读材料指南，可以帮助您了解云计算的基本原理，同时也是创建有效的安全、隐私和法规遵从

News-,Bitglass%202021%20Healthcare%20Breach%20Report%3A%20Over%2026%20Million%20People,in%20Healthcare%20Breaches%20Last%20Year&text=Each%20year%2C%20Bitglass%20analyzes%20data,protected%20health%20information%20(PHI).

性计划的最佳实践。

阅读材料	内容概述
CSA 云计算关键领域安全指南	本文概述了云计算中的安全变化以及无论使用哪家供应商的所有组织都应遵循的最佳实践。
云安全管理服务指南	这些指南基于云控制矩阵（CCM）中概述的控制，为云用户更好地选择安全合格的云服务提供商提供了指导。
云端远程医疗数据	解决在远程医疗方案中，云端处理、存储和传输患者数据相关的隐私和安全问题。
云端医疗大数据	检查大数据及医疗健康的一些用例,大数据对医疗健康的影响、云端受保护的健康信息（PHI）的监管要求以及保护云端PHI。
管理连接到云端的医疗设备的风险	介绍了基于医疗设备与患者距离的医疗设备管理概念，并介绍了确保医疗设备使用云计算的实践。
OWASP的安全医疗设备部署标准	本指南旨在作为在医疗机构内对医疗设备进行安全部署的综合指南。

如果您有兴趣了解CSA并为医疗健康行业创建的最新研究，参与到未来出版物的创建，您可以访问CSA健康信息管理工作组。该小组帮助整个医疗健康行业加速在医疗健康方面遇到的安全问题。例如，我们的成员可以通过参与该工作组解决遇到的物联网安全挑战。

7.3 我们为医疗健康行业推荐的云安全培训。

在云端对医疗专业人员进行培训和教育。

比获得证书更重要的是，为与医疗机构合作的社区提供强有力的培训。对于刚接触云的网络安全专业人员来说，云安全知识证书（CCSK）是一个很好的起点，因为它会让他们对云计算和安全最佳实践有一个中立的理解。一旦建立了知识基线，云审计知识证书（CCAK）应该对医疗健康领域的核心安全人员更加有所帮助。

健康信息管理工作组：您可以在此处（https://cloudsecurityalliance.org/research/working-groups/health-information-management/）查看该小组创建的最新研究

参考

Al-Issa, Y, Ottom, M, Tamrawi, A, 2019. eHealth Cloud Security Challenges: A Survey, Journal of Healthcare Engineering, Volume 2019, Article ID 7516035, https://doi.org/10.1155/2019/7516035

Armis (2019), Medical and IoT Device Security for Healthcare, Retrieved from https://www.armis.com/resources/iot-security-white-papers/medical-iot-device-security-for- healthcare/

Crosbie, Devon, 2020. Why Data Destruction is Essential to Information Governance, Complete Discovery Source, Retrieved fromhttps://cdslegal.com/insights/why-data-destruction-is-essential-to-information-governance/

Gillin, Paul, 2019. Data Destruction in the Cloud: It's Complicated, Retrieved from https://www.ironmountain.com/blogs/2019/data-destruction-in-the-cloud-its-complicated

Hannah K.J., Ball M.J., Edwards M.J. (2006) History of Healthcare Computing. In: Introduction to Nursing Informatics. Health Informatics (formerly Computers in Health Care). Springer, New York, NY. https://doi.org/10.1007/978-0-387-32189-9_3

mThink, 2003. Health Care Technology: A History of Clinical Care Innovation Retrieved from https://mthink.com/health-care-technology-history-clinical-care-innovation/

Stine, Kevin, Kissel, Rich, Barker, William C., Fahlsing, Jim, and Gulick, Jessica, 2008. Special Publication 800-60 Volume I Revision 1: Guide for Mapping Types of Information and Information System to Security Categories, National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from Https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final