SafePloy® THALES

前十件事项

你应该知道的关于医疗健康的信息安全

维护病人数据的安全性是一个复杂的命题，它影响到医疗设施的每一位员工、其 IT 系统的每一个领域，以及与医疗服务提供商合作的所有供应商、合作伙伴和保险公司。

虽然许多设施正在努力实现完全遵守 HIPAA、HITRUST 和其他隐私规则，但有许多因素需要考虑，这些因素超出了合规问题，以解决您的设施的总体风险。 考虑到这一点，我们提出了 10 件你应该知道的关于医疗信息技术安全的事情：

10

受保护的健康信息是主要目标

PHI 记录通常包含敏感数据，如：姓名、出生日期、社会保险号码、保险信息和病史。 这一信息受到了极大的追捧，因此毫不奇怪，Breach Level 指数显示身份盗窃是 2018 年最普遍的数据破坏类型。

09

医疗保健面临最大的安全威胁

根据“到达水平指数”，医疗公司在 2018 年 H1 中经历了所有行业中最多的安全事件。

大多数漏洞来自内部

在医疗保健行业，73%的违规行为是雇员未经授权或无意的行为造成的。 从滥用特权，通过错误的电子邮件和传真到丢失或被盗的笔记本电脑，敏感信息可能在过程的任何时候暴露。即使意图不是恶意的，数据也进入一个没有保护的环境。

08

成本可能是天文数字

Ponemon 研究所的 2019 年数据违约成本研究表明，医疗行业平均每次违约支付 429 英镑，是各行业的最高记录。 除了解决违约问题的直接成本外，病人数据安全的失败还会导致病人、利益相关者和社区之间失去信任，以及对组织声誉的损害、病人和收入流的损失以及责任的增加。

07

在线信息需要 24/7 保护

在线信息需要24/7保护。 由于医疗记录和处方正在上网，医院网络正在互联网上的医生、病人和保险公司之间共享这些数据，因此必须控制谁能够访问信息和应用程序，并通过强大的双因素身份验证确保适当的接入点，并确保数据在运动中和静止时都被加密。 例如，DEA 的 EPCS 法规要求从业人员在发布 EHR 时使用强双因素认证对 EHR 应用程序进行重新认证受控物质的电子处方。

06

05

规则总是在变化

从1996年的 HIPAA 到2018年的 GDPR，联邦和州立法正在增加对医疗信息技术系统的需求，以保护病人数据和报告违规行为罚款也在增加。因此，现在采取行动将让你满足州和全国的最后期限， 享受联邦奖励计划，同时最大限度地提高你的安全预算。

04

敏感信息无处不在..

医疗服务提供商和从业者已经通过智能手机、PDA和笔记本电脑来接受移动计算，在医疗 IT 系统中造成了新的漏洞。 这导致更多的数据面临暴露的风险，因为副本可以轻松制作，备份存储在传统数据中心的范围之外，虚拟环境和云。

03

时间是最重要的

从2015年开始，不使用电子健康档案的医院将受到经济处罚。相反，为了获得医疗保险或医疗补助 EHR 财政奖励，医院和 CAH 必须证明电子健康记录的“有益使用”，如第二阶段和第三阶段的目标。EPCS 的期限因州而异，一些遵守期限已经生效。

如果数据没有加密，就没有受到保护

无论是在数据库中，由最远的最终用户使用，还是在两者之间的任何时刻，未加密的数据都容易被窃取或滥用。加密的存在或不存在也可能是确定违约责任的决定因素。

02

个人需要承担责任

随着对病人数据安全的关注继续增加，法规正在转移，将个人责任增加到公司责任，为负责保护数据的负责人打开了罚款甚至监禁的大门。

01

虽然所有这些听起来都可能令人生畏，而且应该如此，
但是你只需要知道一件事就能解决整个前10项清单，
泰雷兹简化、可扩展的患者数据保护。

SafePloy THALES

前十件事项

你应该知道的关于医疗健康的信息安全

用医疗保健中最完整、集中和端到端解决方案简化您的病人数据安全。

泰雷兹提供了一个灵活的、集中的解决方案，以确保您的病人数据记录和健康历史、账单帐户信息、知识产权（例如医疗和药品专利）以及您的组织需要维护的任何其他数据或交易信息。

通过使用集中的身份和数据保护框架，结合加密、访问策略、密钥管理和身份验证，泰雷兹的身份和数据保护 (IDP) 解决方案允许医疗保健组织通过全面、智能、持久和可扩 展的方法将IT策略与未来的业务增长保持一致。所有关键加密和密钥管理要求都集中实施，消除了对来自不同供应商的不同系统进行投资的必要性。

在一个单一的、全面的平台中，医疗保健组织可以确保监管合规，并确保本地和远程访问关键应用程序和 ePHI。泰雷兹 IDP为身份、交易和应用程序提供端到端保护，帮助确保业务效率。

- 经过行业验证的基于硬件的加密和密钥存储平台保 护事务和应用程序，确保数据完整性（包括从纸张 到数字的过程），并保持审计跟踪。
- 数据加密和控制解决方案在整个生命周期中保护和维 护数据的所有权，从数据中心到端点（包括医生、临床医生和管理员使用的移动设备）和云。
- 高性能通信加密解决方案持续保护信息，确保超出位置或边界的控制，简化操作，促进灾难恢复，并降低合规成本。

简化执行有助于遵守最后期限和避免罚款

泰雷兹 IDP 解决方案的设计是为了快速和容易地集成到现有的 IT 基础设施。有了开箱即用的连接器和集成，以及集中的部署能力，泰勒斯大大减少了实施时间和成本，以确保最后期限得到满足和避免罚款。

不间断访问的最大性能

所有组成泰雷兹 IDP 的组件都是为优越的加密性能而设计的，以确保它们与您的业务流程和患者的体验无缝集成。向高度专业化的硬件设备卸载和集中数据加密处理提供了性能水平，轻松地支持最苛刻的处理环境。

- 具有硬件安全模块 (HSMS) 的多因素强身份验证为用户保护身份，并控制对数据的物理和逻辑访问，建立公众对组织的信任。
- 与硬件令牌或软件令牌（OTP 应用程序）的多因素强身份验证有助于控制对一系列医疗系统的访问，并能够遵守 DEA 的 EPCS 规则。 同样的令牌不仅可 以用于在发放受控物质的eRx时重新认证 EHR 系统，而且还可以确保在房地以外工作的从业人员 远程访问 EHR。

模块化灵活性和可伸缩性满足特定的遵从性和数据安全需求

不断演变的安全威胁需要一个渐进的解决方案。 泰勒斯提供了一个通用的、集成的框架内安全模块的全面基础， 允许您选择和添加适合您独特的战略数据保护需求的安全控制。这种综合方法使您能够在今天和将来以最高的保证和最低的所有权成本保护每一个数据资产。

关于 SafePloy 安策与 THALES 泰雷兹的关系

SafePloy 安策从与 Rainbow 的合作开始，到 SafeNet（并购Aladdin），再到 Gemalto，以致到今天与 THALES 泰雷兹的合作，我们见证了 SENTINEL 与 SafeNet 品牌的不断强大，作为这些专业技术过硬公司的中国区合作伙伴，我们已致力数字安全领域18年。

无论是从软件世界的商业化保护、许可、交付，还是人、设备、物连接网络空间的身份认证以及访问控制，再到数字时代的加密保护，按需加密和控制是我们一直以来秉持泰雷兹的服务理念。

关于 SafePloy 安策

SafePloy安策是一家专注于软件、数据、网站及终端安全的公司，18年的安全经验为众多国内外企业的在线应用和数据保驾护航，按需对：S.软件及代码加密保护并管理许可授权和交付；D.企事业敏感数据加密，合规化管理以及关键加密密钥管控；A.网络用户强认证与单点登录管理；

>safeploy.com<

联系我们: 400 600 9103 有关所有办事处地址和联系信息，请访www.safeploy.com