简译版

安全专家如何帮助患者保护医疗数据

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	How Security Pros Can Help Protect Patients from Medical Data Theft		
原文作者	Reza Chapman	**原文发布日期**	2017 年 7 月 13 日
作者简介	Reza Chapman 是埃森哲全球医疗业务网络安全总监，负责为提供商、健康保险公司和业务伙伴开发和推动安全产品。 http://www.darkreading.com/author-bio.asp?author_id=3781		
原文发布单位	Dark Reading		
原文出处	http://www.darkreading.com/attacks-breaches/how-security-pros-can-help-protect-patients-from-medical-data-theft/a/d-id/1329326?		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

安全专家如何帮助患者保护医疗数据

Reza Chapman

医疗行业在处理黑客攻击风险方面步履缓慢，数据泄露事件不断增加。安全专家必须更积极主动地保护患者的安全。

想象一下，一家当地医院的 IT 系统被黑客入侵，黑客威胁要在网上发布患者的姓名、地址和病历。在 2016 年 9 月，俄克拉何马州的 6000 名患者就遭遇了这样的事情。

正如安全专家所知，这只是医疗数据盗窃的其中一个例子。埃森哲（Accenture）的最新研究发现，多达 26%的美国消费者遭遇了医疗数据泄露事件，在这其中，有 50%的人之后又遭遇了医疗身份盗用。

大多数消费者都意识到了在线交易的风险，但是很少有人能够意识到医疗身份盗用及其可能造成的损害，这就要求安全专家提供更强大的防盗措施，要求医院在遭遇数据泄露期间和之前更好地进行管理。

身份危机

医疗数据包括测试结果和诊断，还包括社保号、出生日期、联系信息和驾照号码。这些信息共同构成了一个在线身份。安全专家知道黑客能够利用这些信息来做什么。这些个人信息或医疗数据被售卖，黑客可能以此威胁医院支付赎金，否则就“在网上公布数据”（如俄克拉荷马州事件），或阻止医院访问这些重要信息。

其他行业正在加紧步伐应对数据安全，所以旨在窃取个人数据的黑客不得不换个目标。而且，大多数医疗信息是以电子方式存储的，可以追溯到好几年前，因此对黑客来说医疗行业就是瓮中之鳖。在 2016 年，医疗行业发生了 377 起数据泄露事件，占所有数据攻击事件的 34.5%。在 2017 年，截至 2 月中旬，已经发生了 144 次数据泄露事件。看来，这种趋势正在加速。

一个合乎逻辑的问题是：“这些数据泄露事件发生在哪里，应该如何阻止？”根据埃森哲的研究，数据泄露事件最有可能发生在医院，其次是急诊室、药店、医生办公室和健康保险公司。通常情况下，医疗机构无法及时发现问题：在遭遇数据泄露的美国消费者中，有一

半是因为信用卡对账单或利益解释有误而自己发现了数据泄露。只有三分之一是被医疗机构告知了数据泄露事件，只有 15%是被政府机构告知的。安全专家了解医疗信息泄露的潜在机会，能够帮助医院系统和整个医疗行业加强防御措施，以确保消费者数据安全。

安全专家能做什么

医疗机构有义务（和固有的利益）来保护医疗和金融数据。当安全措施不足时，就会导致数据泄露和之后的数据窃取。埃森哲的研究表明，许多受影响的消费者会采取行动。受影响的受访者或者更换了医疗服务提供商（25% ）或保险计划（21%），或寻求法律顾问（19%）。根据最近的趋势和事件来看，安全专家的作用只会越来越重要。

许多消费者首先了解数据泄露对其财务状况和健康状况的影响。每起医疗身份盗用事件的受害者平均损失为 2500 美元，与信用卡数据泄露不同，身份盗用的受害者通常没有追回损失的权利。有趣的是，埃森哲的调查发现，当医疗机构主动与消费者进行沟通时，追回损失的几率仍然很高。在安全专家看来，这再一次说明了提前准备好应对潜在攻击的重要性，这样，医疗机构能够迅速采取行动，在事件发生期间或之后帮助减轻消费者的恐惧心理。

医疗服务提供商是时候更加认真地看待数据窃取了，安全专家也是时候在患者和医疗机构之间建立更强大的信任关系了。首先，以下几个措施能够帮助保护消费者数据：

- **敦促消费者监督医疗记录并阅读所有声明。**如果病历不准确，那么他们的数据可能与其他人的混合了。敦促患者密切关注医疗服务提供商给出的病历和声明，并要求他们至少每年一次给出摘要。
- **提醒消费者查看其信用报告。**信用报告的任何差异都有可能意味着消费者的医疗数据已经受到了侵害。
- **不要过分分享信息。**消费者只应该提供所需的最低限度的个人信息，例如医疗服务提供商不需要患者的社保号。消费者还应该警惕虚假通信：在 2015 年的 Anthem 数据泄露事件之后，受害者报告称接到了钓鱼电话和电子邮件。
- **立即发出警报。**如果消费者发现任何异常，应立即通过用户友好的渠道告知医疗服务提供商或保险公司。