第10章

界限

他们不断地试图逃跑
从内外的黑暗中
通过梦想系统如此完美以至于没有人需要成为好人

– TS 艾略特

您的计算机可以为您做的任何事情都可能为其他人做。

– 艾伦考克斯

无论如何,您的隐私为零。克服它。

– 斯科特麦克尼利

10.1 简介

当我们限制信息流动以保护隐私或机密时,政策目标通常不是防止信息“向下”流动,而是防止信息在较小的群体之间“流动”。

1. 如果你让数百万拥有绝密许可的美国联邦雇员和承包商访问太多绝密数据,那么幸运的话你会得到像埃德斯诺登这样的举报人,否则你就会得到像奥尔德里奇艾姆斯这样的叛徒.

2. 随着手机在世界范围内的普及,野生动物犯罪变得更加容易。游戏管理员和其他打击偷猎的人在各个层面都面临着有组织的犯罪、暴力和内部威胁,但与国家情报部门不同的是,这里没有中央机构来管理许可和反间谍活动。

3. 如果你让医疗服务中的太多人看到病人记录,就会出现工作人员查阅名人数据的丑闻。大型中央系统的存在可能会导致重大丑闻,例如十年前的十亿份英国病历被卖给多家制药公司。

4. 类似的问题出现在社会关怀和教育领域。人们经常呼吁数据共享,但在实践中尝试这样做会导致各种问题。

5. 如果你让银行或会计师事务所的每个人都能看到所有的客户记录,那么不道德的经理就可以通过查看客户竞争对手的机密财务信息,向客户提供非常好的建议。

基本问题是,如果您将包含敏感信息的系统集中化,您会创造出更有价值的资产,同时让更多人可以访问它。正如网络的好处可以超过线性扩展一样,危害也是如此。

一个常见的缓解措施是限制任何个人的信息量
看到。在我们上面的五个示例案例中:

1. 情报部门将敏感信息放入隔间,这样在阿根廷工作的分析师可能只能看到与阿根廷及其邻国有关的绝密报告;

2. 支持游戏保护的系统必须做类似的事情,但访问控制必须是涉及多个保护机构、研究人员、护林员和其他参与者的联合努力;

3. 许多医院系统在合理可行的范围内限制员工进入他们工作的病房或部门,并且患者有权禁止在他们的直接护理之外使用他们的数据。随着系统变得越来越复杂,并且它们的操作员缺乏做出努力的动力,两者都变得越来越难以实施;

4. 2010 年,英国议会关闭了一个本应让医生、教师和社会工作者共享所有儿童数据的系统,因为他们意识到这既不安全又非法。然而,信息共享的压力一直存在,学校和其他机构使用可疑的云服务也存在各种问题;

5. 金融公司在业务的不同部分之间有“中国墙”,银行员工现在通常只能访问他们最近获得客户授权的记录,例如客户通过电话回答安全问题。

我们将在本章中讨论这些类型的访问控制。有几个方面:什么样的技术设计是可行的,它们给组织带来的运营成本,以及 通常是关键因素 组织是否有动力去实施和适当地监督它们。

在上一章中,我们讨论了多级安全性,并看到很难使机制正确。在本章中,我们将看到,当我们寻求细粒度的访问控制时,也很难获得正确的策略。组或角色是静态的还是动态的?它们是由国家政策、商业法、职业道德制定的,还是 就像你的 Facebook 群组一样?

朋友 系统用户?当人们为规则争吵或互相欺骗时会发生什么?即使每个人都为同一个老板工作,组织的不同部门也可能有截然不同的激励机制。有些问题在技术上可能很复杂,但在政策方面却很简单（野生动物）,而另一些问题则使用标准机制,但存在棘手的政策问题（医疗保健）。

从一个更简单的案例开始,假设您正试图在税收部门设置安全策略。 Sta 过去曾被发现不当访问名人的记录、向外界出售数据以及在赡养费案件中泄露收入详情 [188]。你会如何阻止它?

图 9.1 – 多级安全

你的要求可能是停止员工查看属于不同地理区域或不同行业的税务记录 除非受到严格控制。因此,如图 9.1 中经典公务员模型中的信息流控制边界不是水平的,我们实际上需要边界大部分是垂直的,如图 9.2 所示。

图 9.2 – 多边安全

横向信息流控制可能是组织性的,例如情报机构将在一个外国工作的代理人姓名保密,不让负责监视另一个国家的部门知道。它们可能是基于关系的,例如在律师事务所中,不同客户的业务和不同合伙人的客户必须分开。它们可能是两者的混合体,例如在医学中,患者保密是基于患者权利的法律,但可以通过限制进入特定医院部门或医疗实践来强制执行。它们可能是体积庞大的,因为当一个游戏保护协会不介意解密少量豹子照片但不希望偷猎者获得整个收藏时,因为这可以让他们找到设置陷阱的最佳位置。

医生、银行家和间谍都知道,除了防止公开的信息流动外,他们还必须防止通过账单数据等旁路渠道泄露信息。患者 X 向 Y 医生付费这一事实表明 X 因 Y 的专长而受苦。

10.2 分隔和点阵模型

美国及其盟国通过密码和分类来限制对秘密信息的访问。这些是用于表达访问控制组的前计算机机制,例如第二次世界大战中的代码字 Ultra,它指的是英国和美国对使用德国 Enigma 机器加密的消息的解密。Enigma 已被破解这一事实值得不惜一切代价加以保护。因此,只有一小部分人获得了超级许可 除了密码学家、翻译和分析师之外,名单还包括盟军领导人和他们的高级将领。任何曾经持有 Ultra 许可的人都不会面临被捕的风险;绝不能以让希特勒怀疑他的主要密码已被破译的方式使用情报。因此,当 Ultra 告知一个目标时,例如意大利前往北非的车队,盟军会在袭击发生前一小时左右派飞机“发现”它。该政策由特殊处理规则执行;例如,丘吉尔在一个特殊的发送箱中获得了他的 Ultra 摘要,他有钥匙但他的工作人员没有。 (超安全性由 David Kahn [1002] 和 Gordon Welchman [2007] 描述。)

今天也有很多相同的预防措施。泄露可能会暴露情报来源或方法的信息被标记为 TS/SCI,表示“绝密 - 特种情报”,并且可能有一个或多个代码字。一个分类加上一组代码字给出了一个隔间或安全上下文。所以如果你有 N 个码字,你可以有2N 个隔间;一些情报机构有超过一百万的活跃人员。这种谨慎是对一系列灾难性内部威胁的反应。奥尔德里奇·埃姆斯是一名中情局官员,凭借长期服役和资历积累了对大量隔间的访问权限,并且因为他从事反间谍工作,几乎可以出卖整个美国在俄罗斯的特工网络。克格勃的海外行动同样受到 Vassily Mitrokhin 的破坏 他是一名对共产主义感到失望并在等待退休金期间被派往档案馆工作的军官 [118]。沃克间谍案还有更早的先例。在那里,将海军舰艇放在舱室中的尝试根本行不通,因为一艘船可以在没有通知的情况下被派往任何地方,而且一艘船没有本地密钥材料在操作上是不可接受的。因此,美国海军的 800 艘舰船最终都配备了同一组密码,沃克家族将其卖给了俄罗斯人 [876]。您显然不希望任何人访问太多,但您如何才能做到这一点?

尝试使用强制访问控制来实现隔间,从而产生格模型。分类与代码字形成一个格子 一种数学结构,其中任意两个对象 A 和 B 可以处于支配关系 A>B 或 B>A。它们不一定是:A 和 B 可能只是无法比较(但在这种情况下,对于晶格结构,它们将具有最小上限和最大下限)。例如,假设我们有一个代码字,比如“Crypto”。然后,获得“最高机密”许可的人将有权阅读分类为“最高机密”和“秘密”的文件,但除非他也有加密许可,否则将无法访问分类为“秘密加密”的文件。这可以表示为图 10.3 所示。

碰巧的是,Bell-LaPadula 模型或多或少可以保持不变。

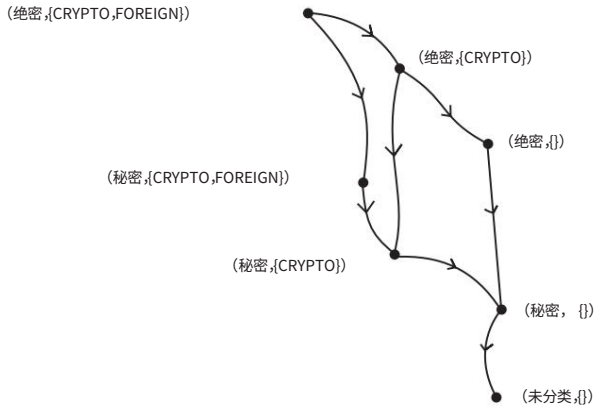

图 10.3：- 安全标签的格子

我们仍然像以前一样在 High 和 Low 之间有信息流,其中 High 是支配 Low 的隔间。如果网格中的两个节点不兼容 如图 10.3 中的“Top Secret”和“Secret Crypto” 那么它们之间根本就没有信息流。事实上，晶格模型和 Bell-LaPadula 模型本质上是等价的,并且是并行开发的。大多数 20 世纪为多层次安全市场打造的产品都可以在隔离模式下使用。如需更完整的历史,请参阅本书的第二版。

在实践中,事实证明,强制访问控制产品对于分隔并不是那么有效。使用这样的系统很容易将不同隔间中的数据分开 只需给它们不兼容的标签（“Secret Tulip”、“Secret Da odil”、“Secret Crocus”……）。但是操作系统现在已经变成了一种隔离机制,而不是一种共享机制;智能系统用户面临的真正问题与合并不同隔间中的数据,并在净化后降级有关。格安全模型在这里提供的帮助很小。

9/11 之后,美国情报界发生了翻天覆地的变化。领导人声称数以百万计的隔间阻碍了反恐战争,更好的信息共享可能使社区能够预防袭击,因此布什总统下令在情报界进行更多的信息共享。美国国家安全局局长基思·亚历山德 (Keith Alexan der) 推动“全部收集”,而不是最大限度地减少数据收集,而是最大限度地收集数据,让一切都可搜索。所以现在,政府系统使用强制访问控制来使机密系统与未分类的 stu 分开,并使用数据二极管和我们在前一章讨论的其他机制将绝密系统与两者分开。 Top Secret 之上的 stu 现在似乎主要使用自主访问控制进行管理。

斯诺登泄密事件告诉我们所有关于 XKeyscore 等搜索系统的信息,这些系统搜索过去有很多隔间的系统。如果搜索可以抛出带有许多代码字的结果,那么读取该结果将需要所有这些许可。在这样的世界中,本地标签只会成为阻碍。但如果没有他们,正如我在本书第二版中所问的那样,你如何预防未来的奥尔德里奇·埃姆斯?或许是美国情报界

幸运的是,失败模式是埃德·斯诺登。作为系统管理员,他能够规避自主访问控制并访问大量隔间。

后来我们了解到,在中央情报局,分隔并不总是有效。 2017 年,其黑客工具在 Vault 7 事件中泄露,在对涉嫌泄密者进行审判后,内部报告的编辑版本于 2020 年发布。它揭示了大多数敏感的网络武器没有隔离,用户共享系统管理员密码,没有用户活动监控,历史数据无限期可用。直到一年后这些工具出现在维基解密上,他们才注意到损失。事实上,英特尔社区用于绝密数据的全球联合英特尔通信系统 (JWICS) 尚未使用双因素身份验证 [2051]。

埃德·斯诺登 (Ed Snowden) 没有涉及到一些隔间,例如 NSA 可以利用哪些加密系统以及如何利用的详细信息 这被标记为“极端隔间信息”(ECI)。商业公司也可能有特殊机制来保护材料,例如未公布的财务结果;在我的大学里,我们在甚至没有连接到网络的机器上编写试卷。在这种情况下,正在发生的事情与其说是一个隔间,不如说是一个高于最高机密的全新级别。

10.3 老虎的隐私

参与打击野生动物犯罪的人们面临着一系列令人着迷的问题。
威胁的范围从通过小规模偷猎丛林肉导致的栖息地侵占,到有组织的犯罪团伙以工业规模采集象牙、犀牛角和老虎身体部位。这些帮派可能会受到心怀不满的社区的保护;即使是政府首脑也可能成为威胁,无论是通过破坏环境法还是通过保护偷猎团伙。最好的偷猎者往往是前护林员。

即使在没有主权威胁的地方,公共部门的捍卫者也经常为相互怀疑的政府工作;保护雪豹免遭偷猎者涉及印度、巴基斯坦、中国、尼泊尔和塔吉克斯坦的护林员,而东非的非法象牙贸易从肯尼亚蔓延到南非。技术让事情变得更糟;随着欠发达国家的移动电话信号越来越多,偷猎也越来越多。因此,它的军事、内部威胁和政治方面在许多方面与传统的安全和情报工作相似。关键的区别在于,捍卫者是非政府组织、公园管理员和执法机构的松散联盟。没有一个中央官僚机构来管理分类、许可和反情报。

我们与 Wildbook 的领导者 Tanya Berger-Wolf 有一个项目,Wildbook 是一个生态信息管理系统,它使用图像识别来匹配和分析通过旅游照片、相机陷阱、无人机和其他数据源收集的动物数据 [92]。她的想法是,如果我们可以将拍摄的许多野生动物照片联系起来,我们就可以极大地改进生态学和种群生物学科学,以及依赖于它们的资源管理、生物多样性和保护决策。现代的

图像识别软件使这成为可能,特别是对于具有独特标记的大型动物,例如大象、长颈鹿和斑马。 Wildbook 现在部署在十多个地点的十几个物种。

2015年,两名西班牙公民在纳米比亚Knersvlagte自然保护区携带49株小型多肉植物被捕;搜查他们的酒店房间后发现了 2000 多个,其中数百个是受威胁的物种。事实证明,他们通过网站出售这些植物,进行了多次收集之旅,并通过植物列表服务和社交网络发现了稀有标本。他们认罪,支付了 160,000 美元的罚款,并被终身禁止进入该国。事实证明,他们还使用了另一个公民科学网站 iSpot [2009]。像这样的事件表明野生动物聚合器需要访问控制,并且还导致植物学家、动物学家和其他人重新思考开放数据 [1166]。那么政策应该是怎样的呢?

需要保护的东西因物种和地点而异。对于稀有植物,我们不希望小偷知道哪怕是单个标本的 GPS 位置。对于濒临灭绝的 Coahuilan 箱龟,我们不希望小偷从野外偷走它们并将它们作为宠物出售,并提供虚假文件声称它们是人工饲养的。在那里,目标是建立一个包含所有已知陆龟的公共数据库,保护人员正忙于拍摄其范围内的所有野生标本,该范围位于墨西哥 360 平方公里的地区。这将使美国鱼类和野生动物服务局能够检查货物。对于雪豹,Wildbook 从一个尼泊尔保护区获得了三年的相机陷阱数据,并希望制定一项安全政策来帮助将其扩展到尼泊尔、印度和巴基斯坦的五个地点。这是一个红色名录物种,在这三个国家中每个国家都只有几百只。在非洲,情况相似。 Wildbook 从追踪斑马开始,其中 Gr´evy 斑马濒临灭绝。动物跨越相互怀疑的国家之间的边界,游客发布带标签的照片,尽管传单和警告他们不应进行地理标记 [2074]。有些游客根本不知道如何关闭标签;有些人愚蠢到下车被吃掉。保护要求也因国家/地区而异;在纳米比亚,当局热衷于阻止游客张贴带有标签的犀牛照片,而在肯尼亚,犀牛都有自己的武装警卫,当局对此并不在意。

新的野生动物聚集点可以使用图像识别来识别个体动物并将目击事件与位置历史联系起来;然后其他机器学习技术将这些历史汇总到运动模型中。我们可以快速找到敏感的输出,例如哪个水坑有很多豹子,或者哪个岛屿有很多繁殖中的鲸鱼。这是动物隐私与人类隐私不同的方式之一:高度抽象的数据通常更敏感而不是更不敏感。实际上,我们的机器学习模型获得了一名护林员在保护区工作十年后可能学到的“知识”。如果这些人转向黑暗面,他们就会成为最好的偷猎者,我们需要让学习他们技能的模型远离偷猎者之手。我们需要对敏感性保持警惕:如果偷猎者还可以通过追踪它们吃的山羊来追踪它们,那么仅保护雪豹的数据和运动模型是不够的。

我们的主要保护目标是不给野生动物罪犯提供可操作的情报,例如“物种 A 的动物更有可能在时间 T 出现在地点 X”。特别是,我们不希望我们建立的公民科学数据平台

使情况变得更糟。我们的出发点是使用一个运筹学模型作为指导来推导 (a) 最近的地理标记照片、(b) 预测模型和 (c) 照片集的访问规则。我们需要能够根据物种和地点调整规则。

有四个级别的访问权限。核心 Wildbook 团队负责维护软件并拥有对几乎所有内容的操作访问权;我们可以称这个级别为零。第一级是管理员,每个物种可能有 20 名管理员;随着访问控制的授权,每个保护区或每个保护区都会有更多的管理员。二级是数百名为保护工作收集和贡献数据的人,他们目前在某种程度上为 Wildbook 所熟知;随着系统规模的扩大,我们需要应对委托管理。在第三级,有成千上万的随机公民提供照片并获得访问非敏感输出的奖励。我们的威胁模型是第 3 级的公民科学家组将始终包括偷猎者; 2 级的管理人员集合将包括少数粗心或不忠诚的人;我们希望 1 级管理员通常不会与偷猎者勾结。

我们缓解内部威胁的重点是可能会叛逃的保护人员 。鉴于保护区通常在弱国运作,最终被发现和监禁的威胁似乎很遥远。最强大的威慑力是来自保护同行的社会压力:对同事的忠诚、团队合作意识和使命感。任务是找到支持团队凝聚力和忠诚度的技术手段。在欠发达国家 (LDC) 的条件下,雇用 10 或 20 名低工资员工的财政紧张的保护机构无论如何,让部门安全官员始终监督每个人的公务员方法是不可行的。

问题不仅仅是提供分析,以便我们可以在工作人员开始查看大量犀牛记录或塞伦盖蒂水坑的大量记录时发出警报。我们已经有每个物种和每个位置的管理员。

问题在于激励人们注意并采取行动。我们的核心战略是在二维透明度的基础上,对态势感知和威慑进行地方公众审计。所有的保护区工作人员都至少属于一个组,与他们感兴趣的物种或他们工作的公园有关。因此,犀牛组的工作人员可以看到谁一直在查看犀牛记录 包括个人目击记录和模型 而在塞伦盖蒂工作的工作人员可以看到谁对那里的数据和模型感兴趣。实际上,它是 2 级员工的矩阵系统;如果您身临其境或者您是犀牛专家,您就可以看到塞伦盖蒂犀牛,无论哪种情况,您都肩负着保持警惕的第一线责任。

1 级人员 可以注册 2 级人员并与其他保护组织进行对等安排,但 2 级同事可以看到他们的相关行为。我们将不得不看看这在现场是如何运作的。

10.4 健康记录隐私

也许在临床信息系统中可以找到访问控制支持隐私的最复杂和最具启发性的安全策略示例。医疗保健部门在国民收入中的支出比军方大得多

在所有发达国家都处于领先地位,尽管医院的自动化程度仍然较低,但它们正在迅速赶上。因此,医疗信息的保护对我们所有人来说都是一个重要的案例研究,其中有许多丰富而复杂的权衡取舍 。

许多国家/地区都有监管医疗保健安全和隐私的法律,这有助于塑造健康 IT 部门。在美国,在一系列隐私保护失败之后,国会于 1996 年通过了健康保险流通与责任法案 (HIPAA)。在一个臭名昭著的案例中,一名被定罪的儿童强奸犯在马萨诸塞州牛顿的牛顿 - 韦尔斯利医院担任骨科技术员,被发现使用一名前雇员的密码查看 954 名患者(主要是年轻女性)的记录以获取电话号码然后他给女孩打了淫秽电话 [317]。他最终入狱,马萨诸塞州参议员爱德华肯尼迪是 HIPAA 的发起人之一。

HIPAA 法规随时间发生了变化。第一组由克林顿政府于 2000 年 12 月发布,比较稳健,其依据是对因隐私问题而不敢及时寻求治疗的人所受伤害的评估。在规则制定的准备阶段,HHS 估计隐私问题导致 586,000 名美国人推迟寻求癌症治疗,超过 200 万人推迟寻求心理健康治疗。

同时,超过 100 万人根本没有寻求性传播感染的治疗 [873]。 2002年,布什总统改写并放宽为“隐私规则”;这要求医院和保险公司等相关实体为受保护的健康信息 (PHI) 维持一定的安全标准和程序,并对违规行为进行民事和刑事处罚(尽管在最初几年实施的处罚很少)。该规则还赋予患者索取其记录副本的权利。涵盖的实体可以披露信息以支持治疗或付款,但其他披露需要患者同意;这引起了研究人员的抱怨。继隐私规则之后,2006 年又出台了进一步的“行政简化”规则,以促进医疗保健系统的互操作性。当奥巴马总统的刺激法案拨款数十亿美元用于健康 IT 并略微增加对侵犯隐私的处罚时,这得到了进一步的推动; 2013 年,他的政府将规则扩展到适用实体的商业伙伴。但抱怨仍在继续。

健康隐私倡导者指出,该制度授权健康数据持有者自由和秘密地汇总和代理受保护的健康信息,而医院抱怨这增加了他们的成本,而患者权益倡导者十多年来一直抱怨医院工作人员经常将其用作无助的借口 例如阻止人们追踪受伤的亲属 [827]。

尽管 HIPAA 法规提供的隐私比欧洲少得多,但它仍然是医疗保健信息安全的主要驱动力,医疗保健占美国经济的 10% 以上。另一个驱动因素是本地市场效应:例如,在美国,系统在某种程度上是由生成账单记录的需要驱动的,而且市场也很集中,Epic 在美国的电子病历系统中占有 29% 的市场份额2019 年,而 Cerner 有 26% [1351]。

在欧洲,数据保护法设定了真正的界限。 1995 年,英国政府试图集中所有医疗记录,这导致了与医生专业团体英国医学协会 (BMA) 的对抗。

BMA 聘请我制定临床信息安全和隐私政策

化,我将在本章后面讨论。 25 年来医疗隐私的演变是一个有价值的案例研究;值得注意的是,尽管技术发生了巨大变化,但问题却几乎没有改变。

关于与医疗信息有关的安全和隐私权衡的争论也在这个时候在其他欧洲国家开始。德国人将当前处方、过敏等汇总数据放在居民随身携带的医保卡上;其他国家对此持保留意见,理由是如果将紧急数据从人类可读的 MedAlert 手环转移到智能卡上,这可能会危及在飞机上或国外度假时生病的患者。早期的中心化系统被用来获取名人信息,引发了一系列丑闻。关于人们是否可以停止将他们的记录用于研究也存在激烈的争论,无论是出于隐私问题还是出于宗教原因 例如,一名天主教妇女可能希望禁止将她的妇科记录出售给一家从事堕胎研究的制药公司药丸。

2010 年,欧洲人权法院在 I v Finland 案中阐明了有关同意和获取记录的欧洲法律。申诉人是芬兰一家医院的护士,也是艾滋病病毒感染者。她的病情在同事中传开了,她的合同也没有续签。医院的访问控制不足以阻止同事访问她的记录,其审计追踪也不足以确定谁泄露了她的隐私。法院的观点是,不参与患者护理的医护人员必须无法访问该患者的电子病历:“这方面需要的是实用且有效的保护,以排除任何未经授权的可能性访问首先发生。”

该判决于 2010 年成为最终判决,从那时起,医疗服务提供者就应该设计他们的系统,以便患者可以有效地选择退出对他们数据的二次使用。

10.4.1 威胁模型

研究健康 IT 威胁的适当背景不仅仅是隐私,而是安全和隐私。主要目标是安全,隐私往往是次要的。两者也交织在一起,尽管在很多方面。

医疗系统存在各种危险,最显着的是安全技术故障,据估计造成的死亡人数与道路交通事故相当。我将在系统评估和保证一章的第 3 部分中讨论这些问题。他们直接与安全交互;漏洞特别有可能导致 FDA 强制召回输液泵等产品。如果公众有安全角度,他们对安全问题就会更加敏感;与非个人风险相比,我们对敌对行动的容忍度要低得多。

第二个危险是,对医疗隐私失去信心会导致人们逃避治疗,或者寻求治疗的时间太晚。

1. 在 Pres 制定 HIPAA 规则之前,美国卫生与公众服务部收集了最全面的数据

认同克林顿。 HHS 估计,隐私问题导致 586,000 名美国人推迟寻求癌症治疗,超过 200 万美国人推迟寻求心理健康治疗。同时,超过 100 万人根本没有寻求性传播感染治疗 [873];

2. 兰德公司发现,超过 150,000 名在伊拉克和阿富汗服役的士兵未能寻求创伤后应激障碍 (PTSD) 的治疗,据信这导致退伍军人的自杀率大约是同类平民的两倍 a重大障碍是获得保密待遇[1861];

3. 最权威的文献综述得出结论,许多患者,尤其是青少年、男同性恋者和妓女,出于保密考虑而隐瞒信息或干脆不寻求治疗。

匿名 HIV 检测使男同性恋者的检测率增加了一倍多 [1650]。

因此,隐私不佳是一个安全问题,也是为一系列公民(从退伍军人到高危和边缘化群体)提供平等医疗服务的关键因素。主要的隐私威胁来自内部人员,包括疏忽和恶意,大致分为三类:

1. 有针对特定个人的针对性攻击,从在医院计算机上查找约会记录的令人毛骨悚然的医生,到跟踪政客或名人的记者。这些直接对个人造成伤害;

2. 大量攻击,例如政府或医院向制药公司出售数百万条记录,有时是秘密的,有时是声称这些记录已“匿名化”,因此不再是个人健康信息;

3. 大多数报告的违规行为都是意外事故,例如医生将笔记本电脑留在火车上,或者配置错误的云服务器在网上留下了数百万人的记录 [767]。这些报告的违规率是私营公司的五倍,因为医疗保健提供者有报告义务。有时意外泄漏会导致机会主义攻击。

由此产生的新闻报道主要是大规模袭击和事故,这让许多人担心他们的健康数据的隐私,尽管他们可能不会直接面临风险。批量攻击还侵犯了许多人的正义感,侵犯了他们的自主权和代理权,并破坏了对系统的信任。

那么直接风险有多大呢?有多少风险是由于技术造成的?
随着事情变得集中,我们遇到了一个基本的扩展问题。资源被滥用的可能性取决于它的价值和有权使用它的人数。将个人信息汇总到大型数据库中会同时增加这两个风险因素。在过去的 25 年里,我们已经从一个每个医生的接待员可以访问纸质图书馆或实践 PC 上的大约 5,000 名患者记录的世界,转变为一个拥有数千个医疗实践记录的世界。常见的

平台。一些共享系统可以访问许多患者的数据,但已被滥用。 25 年前,当人们开始构建集中式系统来支持紧急护理、计费和研究时,这已经是一个问题,从那以后它已经成为现实。甚至本地系统也可以大规模公开数据:一家大型地区医院可能拥有超过一百万前患者的记录。隐私问题不仅限于直接治疗患者的组织:一些最大的个人健康信息集合掌握在健康保险公司和研究组织手中。

为了防止滥用扩展,需要横向信息流控制。允许所有员工访问所有记录的早期医院系统导致了许多隐私事件,其中最引人注目的是导致欧洲法院对 I v Finland 作出判决的事件;但早在 20 世纪 90 年代中期,英国就发生过类似事件。已经尝试了各种临时隐私机制,但到 20 世纪 90 年代中期,我们觉得需要一个适当的访问控制策略,从第一原则考虑并由威胁的现实模型驱动。

10.4.2 BMA 安全政策

到 1995 年,大多数医疗实践都有计算机系统来保存记录;供应商是一些小公司,通常是由爱好计算而不是高尔夫或游艇的医生创办的,他们会根据医生的实际需要进行调整。医院有中央管理系统来处理账单,有些医院正在将纸质记录转移到计算机上。来自政府的压力,政府通过国家医疗服务体系支付英国约 90% 的医疗费用;当地人认为,如果他们能够获得所有信息,他们就能更好地管理事情,这导致了与关心专业自主权的医生之间的紧张关系。玛格丽特·撒切尔 (Margaret Thatcher) 政府在 1991 年所做的最后一件事是在医疗服务领域创建一个“内部市场”,在该市场中,地区专员的行为类似于保险公司,而医院则向他们收取治疗费用;实施这项工作是一项正在进行的工作,既混乱又有争议。因此,卫生部宣布要集中所有医疗记录。互联网热潮刚刚开始,医生们开始通过私人电子邮件发送信息;爱好者们开始构建系统,以电子方式从医院到医疗机构获取测试结果。 BMA 询问个人健康信息是否应该在网络上加密,但政府甚至拒绝考虑这一点(加密战争正在进行;请参阅 26.2.7.3 了解该故事)。

这是最后一根稻草; BMA 意识到他们最好找一位专家,并问我他们的安全政策应该是什么。我与他们的员工和成员一起开发了一个。

我们很快遇到了一个问题。政府策略采用单一电子病历 (EPR),从受孕到尸检全程跟踪患者,而不是在不同医院和医生办公室对同一患者进行不同记录的传统系统,信息以推荐信和出院信的形式在他们之间流动。为 EPR 制定遵守现有道德规范的安全政策的尝试变得复杂得无法控制 [821],有 60 多条规则。不同的人有

在您人生的不同阶段访问您的记录;你的出生记录也是你母亲记录的一部分,你在军队或监狱中的记录可能属于政府,当你接受性传播疾病治疗时,你可能有权完全保密。

卫生部接下来提出了一个多层次的安全政策:性传播疾病将处于对应于机密的级别,正常患者记录处于机密级别,而管理数据（例如药物处方和发票)处于受限级别。但这显然是行不通的。例如,抗逆转录病毒药物的处方应该如何分类?既然是处方,就应该限制使用;但由于它将一个人识别为 HIV 阳性,因此它应该是 Secret。它在其他各种方面也是错误的;一些 HIV 感染者对自己的病情持开放态度,而另一些患有轻微疾病的人则对自己的病情非常敏感。敏感性是患者决定的事情,而不是总理。患者同意是核心:只有在患者同意的情况下,或者在有限范围的法律例外情况下,才能与第三方共享记录,例如结核病等传染病的接触者追踪。

医学同事和我意识到我们需要一个比生命周期记录更细粒度的安全上下文,所以我们决定让现有的法律和实践设定粒度,然后以此为基础制定政策。我们将记录定义为同一个人可以访问的最大事实集:患者 + 医生、患者 + 医生加手术人员 、患者 + 患者的母亲 + 医生 + 人员 ,等等。所以一个病人通常会有不止一个记录,这冒犯了 EPR 的提倡者。

一个真正困难的问题是记录的二次使用。在过去,这意味着研究人员或临床审计员坐在医院或医疗机构的图书馆里,耐心地收集统计数据;同意书包括在候诊室张贴的通知,上面写着类似“我们在医学研究中使用我们的记录以改善所有人的护理;如果您不希望以这种方式使用您的记录,请告诉您的医生。到 1995 年,我们已经看到一家公司向全科医生 (GP)1 提供补贴计算机,以换取允许制药公司进行远程查询以返回所谓的匿名数据。

因此,BMA 安全政策的目标是执行同意原则,并防止太多人访问太多记录。

它并没有尝试做任何新的事情,而只是将现有的最佳实践编纂成法典,并将其浓缩成一页文本,每个人 医生、工程师或管理人员 都能理解。

从这些原则和见解出发,我们提出了九项原则。

1. 访问控制:每份可识别的临床记录都应标有访问控制列表,列出可以阅读和附加数据的人员。

2. 记录打开:临床医生可以打开自己和患者的记录

1英国的全科医生相当于美国的家庭医生;他们历来充当系统的看门人和每位患者终生医疗记录的保管人。他们还充当患者的代言人,并参与医疗实践、医院和社区之间的护理。与美国相比,这有助于降低英国的医疗保健成本。

在访问控制列表中。在患者被转介的情况下,她可以在访问控制列表上打开关于她自己、患者和转介临床医生的记录。

3. 控制:访问控制列表中的一名临床医生必须被标记为负责。只有她可以更改访问控制列表,并且她只能向其中添加其他医疗保健专业人员。

4. 同意和通知:负责的临床医生必须在打开其记录的访问控制列表时通知患者其姓名、所有后续添加内容以及每当责任转移时。除非在紧急情况下或法定豁免情况下,否则还必须获得他的同意。

5. 持久性:在适当的时间段到期之前,任何人都不能删除临床信息。

6. 归属:所有对临床记录的访问都应在记录上标明受试者姓名,以及日期和时间。还必须保留所有删除的审计线索。

7. 信息流:当且仅当 B 的访问控制列表包含在 A 的访问控制列表中时,从记录 A 派生的信息可以附加到记录 B。

8. 聚合控制:应有有效措施防止个人健康信息聚合。特别是,如果建议添加到其访问控制列表中的任何人已经可以访问大量人员的个人健康信息,则患者必须收到特别通知。

9. 可信计算基础:处理个人健康信息的计算机系统应有一个子系统,以有效方式执行上述原则。其有效性应由独立专家进行评估。

从技术角度来看,这个策略比上一章的 Bell-LaPadula 模型更严格地表达,因为它包含原则 7 中的信息流控制机制,但也包含状态。事实上,它需要隔室达到逻辑极限,因为隔室比病人多。可以在 [59] 中找到针对技术受众的讨论。完整的政策处理了更多的问题,例如可能被胁迫的弱势患者访问记录 [58]。

包括瑞典和德国医学协会在内的其他医学机构也制定了类似的政策;加拿大健康信息学协会和一个欧盟项目(这些在 [1077] 中进行了调查)。 BMA 模型于 1996 年被欧洲医学组织联盟 (UEMO) 采纳,公众咨询对该政策的反馈可在 [60] 中找到。

10.4.3 最初的实际步骤

来自现场的反馈来自医疗实践中的试点实施 [870],这是积极的,并且来自黑斯廷斯开发的医院系统,

它使用角色和功能的混合来控制访问,而不是表达 BMA 模型的 ACL。事实证明,在医院范围内进行访问控制的实用方法是通过诸如“病房护士可以看到过去 90 天内到过她病房的所有患者的记录”、“初级医生可以看到在她的科室接受过治疗的所有患者的记录”,以及“高级医生可以看到所有患者的记录,但是如果她访问从未在她的科室接受过治疗的患者的记录,那么负责的高级医生将通知该患者的护理 2。

在 [535, 536, 870] 中讨论了吸取的技术教训。事后看来,BMA 模型是对医生说他们所做的事情的无损压缩,而基于角色的模型是一个稍微有损的版本,但它实现了医院在实践中所做的事情,并且在这种情况下运作良好。但是,BMA 规则之一在这两种情况下都造成了困难:对小型可信计算基础的渴望。 GP 最终不得不信任他们从供应商那里获得的所有应用程序代码,虽然他们可以影响其发展,但没有有用的可信子集。医院记录系统要糟糕得多:它必须依靠患者管理系统 (PAS) 来告诉它哪些患者和哪些护士在哪个病房。 PAS 不稳定且经常出现故障,因此让安全关键系统依赖于它是不可接受的。下一次迭代是给每个医院工作人员一张智能卡,其中包含他们部门或病房的凭证。

卫生部的政策回应是成立一个由菲奥娜·卡尔迪科特夫人领导的调查委员会。她承认 NHS 内约 60 条已建立的信息流是非法的,并建议在每个医疗保健组织中任命一名负责任的隐私官 [367]。这至少是一个开始,但它造成了道德风险:虽然隐私主管(通常是高级护士)在出现问题时受到指责,但实际政策是由部长们制定的 导致我们在第 4 章中讨论的经典安全经济学陷阱8,Bob 保护系统,而 Alice 支付失败的代价。不管怎样,政府发生了变化,托尼·布莱尔的新政府寻求的是法律而非技术修复 数据保护法允许数据控制者假装数据是匿名的,只要他们自己无法重新识别数据,即使其他人可以通过将它们与其他数据匹配来重新识别它们。我们将在下一章讨论匿名化的局限性。

10.4.4 实际出了什么问题

在担任首相的第二个任期内,托尼·布莱尔宣布了一项耗资 60 亿英镑的计划,旨在实现英格兰医疗服务计算的现代化。众所周知,国家 IT 计划 (NPfIT) 是世界上最昂贵的计划

2黑斯廷斯系统最初是独立于 BMA 项目设计的。当我们相互了解时,我们惊讶于我们的方法如此一致,并确信我们以合理一致的方式抓住了行业的期望。

3 英国法律本应将欧盟数据保护指令 (95/46/EC) 转化为英国法律,以提供公平的隐私竞争环境;这个漏洞是让英国公司有很大回旋余地的几个漏洞之一,惹恼了法国人和德国人 [597]。欧盟最终推动通过了更严格的通用数据保护条例 (2016/679)。

民用 IT 灾难。大卫卡梅伦 2010 年上台后,国家审计署的一项调查指出,总支出约为 100 亿英镑,其中约 20 亿英镑用于宽带网络和数字 X 射线成像,导致大部分系统运行正常,而其余部分则没有。如果物有所值,每位患者都应拥有电子护理记录的核心目标将无法实现 [1390]。卡梅伦正式终止了该项目,但由于根深蒂固的供应商合同,其影响持续了多年,而健康 IT 被搁置了十年 [1559]。

NPfIT 曾呼吁在 2004 年至 2010 年间将所有医院系统替换为标准系统,以便为每位 NHS 患者提供一份电子护理记录。
安全策略具有三个主要机制。

1. 有基于角色的访问控制,就像黑斯廷斯首创的那样。

2. 为了访问患者数据,工作人员还需要合法关系。这抽象了黑斯廷斯关于“她的部门”的想法。

3. 有一项计划是患者可以密封他们记录的某些部分,只对特定的护理团队可见。然而,供应商从来没有抽出时间来实施这一点。它不符合单一电子健康记录的教义,部长们经常重复这一点,以至于它已成为一种宗教信仰。直到 2007 年,议会的卫生委员会才注意到供应商甚至还没有获得规范 [925]。

结果,在医院接受精神科门诊治疗的患者发现接待员可以看到他们的病例记录。以前,这些笔记以纸质形式保存在精神科医生的档案柜中;接待员只知道琼斯医生每个月会见史密斯夫人一次。但现在接待员角色必须获得访问患者记录的权限,以便他们可以查看和修改预约时间等管理数据;琼斯医生所在的医院翼楼接待处的每个工作人员都有合法的关系。所以他们都可以访问所有内容。这说明了为什么每个患者具有单个安全上下文的单个记录的文档是一个坏主意。

由于项目管理不善,只有不到 10% 的英格兰医院实际安装了这些系统,尽管“RBAC + 关系”的学说此后影响了其他医院。现在看来,无法支持每位患者的多个安全上下文将成为美国的一个问题,因为公司开始推动 FIHR 标准支持的健康应用程序,我将在第 10.4.5 节中返回。

10.4.4.1 急救

接下来出问题的是紧急医疗记录。政客用来推销 NPfIT 的故事之一是“假设你在阿伯丁生病,而医院想要访问你在伦敦的记录……”。这过去是,现在仍然是假的。护理人员和急诊室医生接受过治疗他们看到的东西的培训,并且不承担任何责任;他们依靠计算机来判断昏迷患者的血型的想法简直是愚蠢的。但政策就是政策,而且

在苏格兰,政府创建了处方和过敏的“紧急护理记录”,该记录保存在中央数据库中,供急诊室的医生、护理人员和非工作时间医疗热线服务的接线员使用。

250 万人的敏感信息被数万人获取,不可避免的事情发生了;邓弗姆林 Queen Mar Garet 医院的一名医生因浏览时任首相戈登·布朗、首席部长亚历克斯·萨尔蒙德以及各种体育和电视名人的健康记录而被捕并受到指控。此案最终因“不符合公共利益”而被撤销起诉 [1741]。患者有权选择退出这个系统,但这是一个非常奇怪的选择:如果你什么都不做,你的数据就会从你的全科医生那里收集,并提供给爱丁堡的卫生部和救护车服务。如果您选择退出,您的数据仍会从您的全科医生处收集并提供给卫生部;他们只是没有与救护人员共享。

这也是英格兰的一项政策,在那里它被称为“同意观看”:国家将收集所有内容并只向用户展示他们被允许看到的内容。每个人的记录都将在线,医生只有在声称患者同意的情况下才能查看这些记录。 Ocials 向议会保证,这是建立 NPfIT 的唯一可行方法;他们将此描述为“现状的电子版本”[925]。英国的急救系统 Summary Care Record (SCR) 也有大多数公民的敏感数据,可以广泛访问,但很少使用;如果你最终上了救护车,他们会在去医院的途中向你索取病史,就像他们一直做的那样4。荷兰也发生了类似的事情,公民医疗保险详细信息的数据库最终不仅可供医生和药剂师访问,还可供替代治疗师甚至出租车公司访问,结果完全可以预见 [186]。

10.4.4.2 弹性

转向集中式系统通常会使故障变得更罕见但更大,卫生系统也不例外。 NPfIT 唯一真正的成就是在英国使用数字机器和云存储标准化了所有 X 射线成像。 2005 年 12 月 11 日发出了脆弱性的预警,当时邦斯菲尔德储油库 250,000 升汽油泄漏形成蒸汽云并引爆 这是欧洲和平时期最大的爆炸。石油公司后来因违反安全规定被罚款数百万英镑。我们当地的医院失去了 X 光服务,因为与云服务的主要和备用网络连接都在附近经过。 2017 年,Wannacry 蠕虫感染了附近另一家医院的机器,进一步发出了警告;管理人员愚蠢地关闭了网络,希望防止进一步感染,然后发现他们不得不关闭急诊室并将患者转移到其他地方。在没有网络的情况下,他们无法进行 X 光检查(并且也得不到病理学检查结果,即使是来自医院自己的实验室)。自那以后,医院因勒索软件而关闭的事件不断发生,尤其是在美国。

4在冠状病毒危机中,SCR 通过从 GP 记录中添加大量数据“丰富”,使其可供规划人员使用,并默认选择退出。目前还不清楚它是否有任何有价值的用途。

10.4.4.3 二次使用

与付款相关的数据库通常不允许真正的选择退出,英国的例子是医院事件统计 (HES) 数据库,该数据库收集医院发送给支付费用的委托机构的账单,并包含关于每项费用的大量信息自 1998 年以来在英格兰和威尔士进行的国家资助医院访问和测试 总共约有 10 亿条记录5。这些记录已被证明无法保护,不仅因为对完整记录进行匿名化不切实际,还因为要求研究人员访问的巨大政治压力。

越来越多的人在 1997-2010 工党政府的领导下获得了访问权; 2010 年戴维·卡梅伦 (David Cameron) 成为首相后,闸门打开了。
卡梅伦聘请了一位之前经营过健康 IT 业务的“透明沙皇”,并在 2011 年宣布了“开放数据措施”,目标是让每个 NHS 患者都成为研究患者,以使英国成为制药研究的世界领先者. Ocials 声称,“所有必要的保障措施都将到位,以确保保护患者的详细信息 数据将被匿名化,并且该过程将受到仔细和强有力的监管”[1807]。匿名化意味着您的个人详细信息被删节到您的邮政编码和出生日期;这是相当不够的,我们将在下一章讨论。

2013 年,政府宣布将从 GP 系统中收集记录;全科医生有八周的时间通知他们的病人即将上传。这引起了足够多的不安,以至于隐私活动家、全科医生和其他人聚在一起成立了一个医疗隐私活动组织 medConfidential.org。最初的推动力是同意,特别是那些试图行使欧洲法律权利选择退出此类系统的患者最终被忽视,甚至被医疗服务注销。活动家敦促政府遵守新近澄清的欧洲同意法;政府扭动着躲避着。如果有些病历不能上传,医生的奖金怎么算?

2014 年 1 月,一些挖掘显示,HES 数据已出售给全球 1000 多家制药公司、大学和其他机构 通常以一套 DVD 的形式出售,其中包含可追溯到 1998 年的 10 亿集。一位医生透露,数据出现在网上;它很快被取下[1800]。

这种“care.data”丑闻在收集所有 GP 数据的提议后广为人知,成为主流。调查显示,大多数人都准备好让他们的数据用于学术研究,只要有人提出要求;但大多数人不准备与营利性研究人员分享它,而且大多数人反对简单地获取它。经过检查,事实证明重新识别患者很容易,即使他们的邮政编码和出生日期没有包含在数据集中;我们将在下一章讨论技术细节。有一个财务丑闻:尽管部长们谈论研究数据对卫生服务的巨大价值,但这些数据是在成本回收的基础上出售的,

5HES 被宣传为“包含英格兰 NHS 医院所有入院、门诊预约和 A 和 E 就诊详情的数据仓库”,包括在 NHS 医院接受治疗的私人和外国患者,以及在 NHS 支付的私立医院接受的治疗。现在声称‘我们根据 NHS 数字协议对所有已发布的 HES 数据应用严格的统计披露控制。这抑制了少数人以阻止人们识别自己和他人的身份,以确保患者的机密性得到维护。请参阅 https://digital.nhs.uk/data-and-information/data-tools-and-services/data-services/hospital-episode-statistics。

几千元一套。还有一个管辖权问题:事实证明,PA Consulting 已将 HES 数据加载到 Google 云系统中,以便转售给其客户,因为 20Gb 对于 Excel 来说太大了。

但是等等,议会成员说,这怎么可能合法?谷歌在英国没有任何数据中心,并且有各种各样的规定禁止将 NHS 数据带到海外 [1573]。另外,ocials承诺英国数据不会卖到海外,却在美国打广告;事实证明,即使是监管机构,药品和保健产品监管机构 (MHRA)6,也一直在出售个人数据 [1645]。部长们进入了损害遏制模式;隐私监管机构被说服相信导出的数据足够匿名,一家声称能够从这些记录中识别患者身份的公司的英国网站已被关闭 [1574]。部长们谈到了吸取的教训,并委托对所有数据发布进行审查;但是当出现这种情况时,它只调查是否遵循了内部准则,而不是它们是否合法 [1496]。

从那以后,英国的健康隐私丑闻一直以大约每年一次的速度持续发生:

- 2015 年,Google DeepMind 从伦敦皇家自由医院获得了所有 160 万患者记录的副本,声称要开发一款检测急性肾损伤的应用程序(它拿走了所有记录,而不仅仅是肾脏的记录)患者)。没有寻求患者的同意,后来发现该交易是非法的,当该应用程序是使用从 VA 获得的美国数据开发时,它并不令人印象深刻 [1541]。信息专员对医院进行了训斥,但未能命令 Google DeepMind 删除数据。最终 DeepMind 将记录转移给了谷歌,这与之前的保证相反 [1281]。

- 同样在 2015 年,一家小报发现在线药店 Pharmacy2U 将数千名患者的详细信息出售给掠夺性营销商,其中包括针对身体不适的老年男性的彩票欺诈者,以及一家已经因误导广告和未经授权而受到制裁的保健品供应商。健康声明[662]。该公司被罚款 130,000 英镑,其商务总监被通用制药委员会停职。英国最大的 GP 软件供应商 EMIS 的主要支持者出售了其股权。

- SCR 数据也被卖给了 Boots,这是一家商业连锁药店,迫使其员工积极营销,导致监管听证会 [405]。

- 2017 年,领先的 GP 软件供应商 TPP 拥有 6,000 名客户,其中包括 2,700 家 GP 诊所 占英格兰所有诊所的三分之一,有 2600 万患者的记录 开启“增强型数据共享”,以便当地医生可以看到记录医院。很快人们就注意到,在作为 TPP 客户的所有其他实践中都可以看到记录;全科医生并不知道这一点[577]。记录也可见

6 MHRA 也不太热衷于将不良临床试验结果的数据提供给需要它的医生。对它的投诉的实质是它更多地是为了制药公司和医疗设备制造商的利益而不是为了患者的利益行事,实际上成为一个被俘虏的监管机构。

疗养院、监狱和移民拘留中心的 TPP 客户。
TPP 未能回答有关其在印度、中国和阿联酋的任何客户是否可以访问的问题。

- 2018 年,英国公共卫生部将 2008 年至 2013 年在英国诊断出的所有 180,000 名肺癌患者的记录提供给了一家烟草公司,该公司声称癌症登记数据只会出于“医疗目的”出售。

标准中央系统确实具有真正的优势。在美国,退伍军人管理局为其医院网络运行此类系统;在飓风 Katrina 之后,来自路易斯安那州的退伍军人最终成为德克萨斯州或佛罗里达州甚至明尼苏达州的难民,他们可以直接前往当地的 VA 医院并在医生的指尖找到他们的笔记,而新奥尔良许多其他医院的患者完全丢失了他们的笔记。

但在美国也有争议。 2019 年 11 月,有消息称谷歌代表 Ascension 完成了一项处理 5000 万美国人医疗记录的外包交易,一名举报人透露,这些数据甚至没有被轻微去识别化； Google 和 Ascension 的员工都可以完全访问患者数据。一项联邦调查开始调查该安排是否符合 HIPAA [121]。

谷歌还从美国获得了 VA 数据,一旦 ICO 在那里做出裁决,谷歌就用它来代替伦敦数据。除了一些极端案例中的例外情况,政策制定者发现很难拒绝营销人员和研究人员的游说以获取访问权限。欧盟通用数据保护条例对“研究”有一个方便的豁免,由制药游说团体提出,不排除市场研究。当然,执法部门和情报机构也需要访问权限。这始于 1990 年代阿片类药物处方记录的收集,并已大大扩展。

10.4.5 机密性 未来

在 BMA 政策颁布近四分之一个世纪之后,我们现在能对医疗保健隐私说些什么?好吧,有些事情会改变,但令人惊讶的是,很多事情保持不变。我们在第 2 章中注意到,网络犯罪生态系统并未因过去十年的巨大技术变革而发生太大变化;健康隐私生态系统也是如此。向基于云的医疗记录的转变是难以抗拒的,因为它为个人护理提供者节省了维护服务器和备份的麻烦和费用。转向更复杂的外包似乎也是势不可挡的。我们可以预期专业公司将处理 X 光图像、病理学测试等,而学科专家将支持特定疾病（如糖尿病)的护理。

自 2014 年以来,出现了快速医疗保健互操作性资源（FHIR,发音为“fire”)的标准草案,它描述了两个系统如何在您允许的情况下相互通信。安全工程不在本标准范围内;例如,DeepMind 的智能手机应用程序使用 OAuth 2。FIHR 从 2021 年起在 NHS 中强制执行。在美国,新的联邦信息共享规则可能要求提供商将您的记录发送给第三方

第三方应用程序,如 Apple 的健康记录,在您授权数据交换后。这些细节提醒医生,他们注意到一旦你这样做,你将面临严重的滥用,因为数据将不在 HIPAA 范围内,应用程序可以随意出售它。药物滥用等数据不仅会限制获得保险的机会,而且雇主和其他人甚至可能会要求提供此类数据。政府回应说,开放健康数据将使人们能够更好地管理他们的护理并了解成本,同时开放该部门以进行竞争性创新 [1815]。除了人们是否会信任微软、亚马逊和谷歌的健康数据之外,你还必须全部或根本不共享这些数据;没有比您的整个生命周期记录更细粒度的访问控制的规定。

过去 25 年的经验表明,这不会令人满意。

在英国,医学教授和制药公司正在再次推动收集所有 GP 数据,谈论基于医疗记录、人工智能和基因组学的三大新健康产业。研究政策是,虽然研发应占 GDP 的 2%,但其中只有三分之一来自国家,其余来自工业。2019 年宣布有五家医院与一家由前部长经营的制药公司达成交易:他们提供“匿名”数据用于研究以换取股权 [500]。另一方面,英国最大的医学研究慈善机构 Wellcome Trust 预测,如果再发生 care.data 规模的丑闻,多达 40% 的患者可能会选择不将他们的数据用于研究。当然,数据表明,虽然大约 80% 的人相信医生会提供他们的健康数据,但健康保险公司和药房的这一比例下降到略高于 50%,研究人员约为 40%,制药公司为 20%,科技公司为 10% [1100] .我们如何才能在这片丛林中穿行?

英国竞选团体 medConfidential 的观点是需要三件事。

1. 首先,为了使我们能够根据欧洲法律行使我们的权利,必须得到患者的真正同意。这意味着从二次使用中选择退出,而不是像目前的 Facebook 那样每年或每两年更改一次退出机制并迫使人们再次选择退出。

2. 其次,保护他们的数据不应该是患者的工作,因此隐私架构和安全工程都必须默认是安全的。人们不得悄悄地选择使用被错误描述或根本未提及的二手数据;并且必须有适当的安全机制,让患者知道真相,尤其是当他们失败时。

3. 第三,仍然要有真正的透明度。目前我的全科医生可以看到谁访问了我的记录,但我也想看看。如果数以千万计的患者可以审核访问权限,那么即使实际上只有几十万患者这样做,这也应该阻止大部分滥用行为。

历史应该告诉我们,最好对患者诚实。在英国,我们已经浪费了 20 年:十年与 NPfIT 一起,还有十年试图假装不卖数据。然而,医院在 70-80% 的时间里都获得了在研究中使用数据的积极同意,而且我们有大型合作研究项目,例如 UK Biobank,其中 500,000

人们不仅在 2006-10 年同意进行终生监测,而且还提供了血液样本,以便研究人员可以对他们的 DNA 进行测序并将其与健康结果相关联。还有一个进一步的研究数据库,其中包含从其他同意的患者那里收集的 100,000 个基因组。

另一个发展是 OpenSAFELY 合作,它通过在现场使用 TPP 持有的实时医疗记录,率先对 Covid-19 流行病进行快速分析,TPP 是一家大型云电子健康记录服务提供商,支持英国约 40% 的全科医生.他们导入了一份死亡通知清单,不仅能够像社会统计那样按年龄和性别分析死亡率,还能够按社会剥夺、种族、吸烟史、体重指数和特定合并症分析死亡率,确定超过 1700 万的风险因素2020 年 2 月至 2025 年 4 月期间,有 6,000 多人死亡。

例如,他们首先确定在黑人和亚裔患者中观察到的超额死亡率明显高于仅用社会剥夺来解释的死亡率,这项研究的速度和规模是前所未有的,并为进行伦理批准的查询提供了理由直接访问实时数据并仅带走统计数据,而不是抽象匿名子集以供场外使用,但仍存在隐私风险（我们将在下一章详细讨论）。隐私风险可能更可控,因为数据副本较少,并且可以强制患者选择退出。虽然这可能被视为一种“新”研究技术,基于云的医疗记录的出现使之成为可能,但它实际上是一种非常古老的技术。在没有计算机的日子里,观察流行病学意味着坐在医院或手术室的图书馆里,筛选成千上万的纸质记录,寻找感兴趣的诊断,并在数周或数月的工作后离开统计表而不是可识别的个人信息。

10.4.5.1 伦理

因此,研究健康数据的研究人员最好注意道德规范。
2014-5 年,Nueld 生物伦理委员会委托我们中的十几位来自技术、遗传学、医学、保险和伦理学等不同背景的人撰写一份详细报告,说明在基于云的医疗记录和普适基因组学 [1600]。从历史上看,正是医学研究中的一系列伦理滥用更普遍地推动了研究伦理的发展。

- 在塔斯基吉梅毒实验中,美国医生研究了农村非裔美国男性未经治疗梅毒的进展情况,这些男性被引导相信他们正在获得免费医疗保健。该实验从 1932 年持续到 1972 年,但即使在 1947 年出现有效的抗生素治疗之后,受感染的男性仍未得到治疗。

- Karl Brandt 博士是希特勒的私人医生,从 1939 年开始实施安乐死计划。他还未经同意对战俘和被占领国家的平民进行人体实验,他的同事 Josef Mengele 博士也在比克瑙对双胞胎进行了实验。 1943–5；受试者经常被杀死并随后被解剖。勃兰特在纽伦堡审判中被定罪,并于 1948 年被绞死。

- 在英国Alder Hey 丑闻中,媒体发现病理学家在未经任何形式的同意的情况下,例行公事地从活着的和死去的病人身上保存“有趣”的身体样本。父母发现他们死去的孩子的身体部位在他们不知情的情况下被保存了下来。这严重损害了公众的信任,其后果损害了英国的病理学研究。爱尔兰也发生过类似的丑闻。

纳粹医生的审判导致了 1948 年的纽伦堡法典,根据该法典,受试者的自愿和知情同意是必不可少的。受试者必须有选择的自由,不受欺骗或胁迫,必须能够随时退出实验。这导致了 1964 年关于医学研究伦理的赫尔辛基宣言,该宣言于 1975 年在塔斯基吉之后进行了修订,以纳入对独立机构审查委员会或伦理委员会的需求,随后又于 1983 年、1989 年、1996 年、2000 年和 2008 年进行了修订。

该宣言由世界医学协会管理,在道德上对医生具有约束力。该宣言支持患者在开始和之后就参与研究做出知情决定的权利。

直到大约 20 世纪 90 年代中期,主要的伦理争论都与药物试验有关:一旦有效的抗逆转录病毒药物存在,给 HIV 患者服用安慰剂是否错误?如果欠发达国家的公民或医疗服务无法负担药物费用,那么在欠发达国家进行药物测试是否合乎道德?从那时起,越来越多的问题都是信息性的:将整个人群用作观察流行病学和研究的对象而不赋予他们选择退出的权利是否合乎道德?低成本的人类基因组测序会引发哪些伦理问题?

在花了一年时间详细考虑我在本节中总结的历史和问题后,我们得出结论,在如此复杂和快速发展的道德领域工作时,它有很多希望,但也充满了既得利益和政治诡计,研究人员躲在法律后面或只是按照今年政府的指导方针行事是不够的。

一套道德上合理的期望应该体现四个原则。引用报告:

1. 关于如何在数据计划中使用数据的一系列期望应基于尊重人的原则。这包括承认一个人在控制他人访问和披露在他们认为保密的情况下持有的与他们有关的信息方面的深刻道德利益。

2. 关于数据将如何在数据倡议中使用的一系列期望应该根据既定的人权来确定。这将包括限制国家和其他人出于公共利益(包括保护他人利益)干涉公民个人隐私的权力。

3. 关于数据将如何在数据计划中使用(或重新使用)的一系列期望,以及确保满足这些期望的适当措施和程序,应在具有道德相关利益的人的参与下确定。这种参与应包括提供和接收公众说明建立的原因,

以所有人都认为合理的方式开展和参与倡议。如果不可能让所有具有相关利益的人都参与进来 实践中经常会出现这种情况 应该公平地代表所有的价值观和利益。

4. 数据计划应服从有效的治理和问责制度,这些制度本身在道德上是合理的。这应包括援引合法司法和政治权威的问责制结构,以及因人们参与社会而产生的社会问责制。维持有效的问责制必须包括有效的措施,以向受影响的人和更广泛的社会传达治理、执行和控制的期望和失败。

简而言之,你必须把人当作目的而不是手段,而不是仅仅把他们的数据当作工业原材料;你必须提前告诉人们你在做什么,如果你不能告诉每个人你必须告诉一个好的样本,而不仅仅是你伦理委员会的一些朋友;你必须遵守法律,包括人权法中令人厌恶的部分;你必须告诉人们你之后做了什么 包括公开违规披露 [1600]。

但是请注意,道德流程存在很多道德风险;滥用数据的大公司通常会设立道德机构来为他们的行为找借口。我将在 11.4.4 节中回到这种道德清洗。

从那时起,我们就使用这个模型来指导我们自己对网络犯罪的研究,这在很多方面都是相似的。例如,我们有时可能会使用来源可疑的数据,并可能从中推断出未给予同意的活着的人。然而,在许多情况下,可以提出调查的道德案例,但需要仔细考虑做出和记录此类决定的过程。透明度至关重要;我们把我们写的所有论文都放在我们的网站上,这样每个人都可以看到对数据做了什么。

同样的原则可能是思考机器学习伦理的一个很好的起点。到目前为止,现实世界中的许多(如果不是大多数的话)人工智能伦理争议都围绕着健康数据。

10.4.6 社会关怀与教育

同样的问题已经蔓延到教育和社会关怀领域。在为 IT 建立 NHS 国家计划的同时,英国政府还开始建立一个所有儿童的国家数据库,用于儿童保护和福利目的,其中包含每个儿童接触过的所有专业人员的名单。 2006 年,英国信息专员要求我们中的一组人研究这方面的安全和隐私问题。现在孩子 X 在家庭医生 Y 注册的事实可能是无害的,但孩子在社会工作部门注册是不同的;教师对他们知道与社会工作者接触过的孩子的期望较低。与吸毒成瘾服务或卖淫服务的接触记录是高度耻辱的。我们得出结论,未能将此类元数据保密是不安全和非法的 [101]。

这在 2007 年 11 月成为一个更热门的政治问题,当时税收

当局丢失了两张包含英国整个儿童福利数据库的 DVD 英国每个有孩子的家庭的个人信息。一个与自由民主党有关联的慈善机构委托编写了一份题为“数据库状态”的进一步报告,内容涉及一系列公共部门系统的安全、隐私和合法性 [102];自由民主党在 2010 年大选后加入的联合政府关闭了儿童数据库并终止了 NPfIT,废除了前工党政府强制要求身份证的立法,并销毁了与该项目相关的数据和硬件。经过进一步审查,它还放弃了一项新的“eCaf”系统计划,以组织参与儿童保护的社会工作者。那里的问题不仅在于隐私,还在于糟糕的设计,因为 eCaf 需要如此多的信息,以至于社会工作者开始花更多的时间“喂养野兽”,而不是与儿童及其家人实际交谈 [1354]。

尝试通过直接电子访问在医学和社会保健之间共享数据引发了完整性和隐私问题。例如,当牛津的社会工作者可以访问 GP 记录时,社会工作者可以输入“糖尿病?”直接进入全科医生系统 这会将其解释为诊断并开始尝试安排所有其他糖尿病护理机器。全科医生会停止工作,因为医疗记录只是附加的;他们可能开始无法实现为糖尿病患者安排眼科检查的目标,这会减少他们的收入。护理服务和学校之间的自动化交流也存在问题;事实上,不同类型专业实践之间的任何自动化交互都需要通过广泛咨询和大量边缘案例的探索来设计。

“数据库状态”报告还强调了教育中的隐私。在英国,教育部建立了一个国家学生数据库,最初保存人口普查数据,但逐渐增加测试结果、行为和倾向数据,孩子是否穷到可以得到免费学校餐以及他们是否得到照顾。此外,学校开始增加进一步的监控,从指纹扫描仪到记录出勤和图书馆借书,再到闭路电视连续记录课堂(销售宣传是教师可以保护自己免受儿童的诬告)。

在苏格兰,政府于 2014 年提出了一项“指定人员”计划,根据该计划,将为每个儿童分配一名公共部门工作人员(通常是教师或健康访问员),以促进和保障他们的福祉。与其侮辱拥有社会工作者的贫困儿童,不如给每个人一个?这引起了广泛的反对,于 2016 年在最高法院被击败,并最终在 2019 年因部长们无法找到一种既合法又在政治上可接受的方式而被放弃。一个为制定法定行为守则而设立的机构认为它“不可取,因为它的复杂性意味着它在实践中不容易理解或应用”[520]。

在父母零星的抗议之后,现在至少有一个非政府组织在为儿童权利工作[7]。关注范围从生物识别到云服务在教育中的广泛采用,许多小型供应商出售大量的教学支持和其他服务,儿童数据无处不在。甚至隐私监管机构信息专员也

7https://www.defenddigitalme.org

因对儿童问题视而不见而受到批评,例如使用 Vimeo 在她的网站上提供教学视频,而其服务条款禁止 13 岁以下儿童使用。如果连监管机构都管不了自己的网站,一般学校还有什么机会?更根本的是,学校应该将每个学生视为公民/客户 负责和控制 还是作为嫌疑人/惯犯进行跟踪、扫描和指纹识别?对年轻人的诱惑是后者。

回顾近四分之一个世纪以来围绕健康 IT 的安全和隐私以及 IT 在教育和社会保健方面的相关主题的争论,我们可以看到符合政治刻板印象的失败。 1997 年至 2010 年的英国工党政府以典型的左翼方式失败。他们是善意的,但很天真;他们只能考虑官僚集中制和数十亿英镑的合同(有些公司在部长任期之前或之后雇用他们);他们不知道如何编写规范;当事情出错时,他们疯狂地撒谎;他们是特殊兴趣的傻瓜,例如要求获得一切的医学研究人员。自 2010 年以来,保守党政府以典型的右翼方式失败了8:谈论权利和自由,但愤世嫉俗地向制药公司的朋友出售 o 数据,而且价格微薄;当事情出错时像疯了一样撒谎;同时破坏监管机构并任命倾向于对安全和隐私失败视而不见的领导人。

10.4.7 中国墙

我们最后的多边安全模式是中国墙模型,由 David Brewer 和 Michael Nash [319] 正式提出。监管机构要求从投资银行到会计师的金融服务公司制定内部规则,以防止在两个客户是竞争对手的情况下发生利益冲突,这些控制被称为 Chinese Walls。

该模型的范围比金融更广。许多服务公司的客户可能相互竞争:广告公司是另一个例子。一个典型的规则是“最近在一家公司工作的合伙人可能看不到同一部门任何其他公司的文件”。因此,一旦撰稿人在 Shell 帐户上工作,他们将不会被允许在某个固定时间段内在另一家石油公司的帐户上工作。

因此,中国墙模型混合了自由选择和强制访问控制:合作伙伴可以选择为哪家石油公司工作,但一旦做出决定,他们在该部门的行动就会受到限制。它还将职责分离的概念引入到访问控制中;给定的用户可以执行事务 A 或事务 B,但不能同时执行两者。访问控制因此变得有状态。

Chinese Wall 模型对安全研究社区的部分吸引力来自于它易于形式化这一事实;事实上,它可以用类似于 Bell-LaPadula 的术语来表示。如果我们写 ,对于每个对象 c,y(c) 代表 c 的公司,x(c) 代表 c 的利益冲突类,那么就像 BLP 它可以

8尽管事实上 2010-15 年政府有自由民主党联盟伙伴

用两个属性表示：

- 简单的安全属性：主体 s 可以访问 c 当且仅当，对于
  s 可以读取的所有c0 ，y(c) 2/ x(c0) 或 y(c) = y(c0)
- *-属性：只有当 s 不能读取任何具有 x(c0) 6= 和 y(c) 6= y(c0) 的 c0 时，主体 s 才能写入 c。

Chinese Wall 模型引发了关于它在多大程度上与 BLP 宁静属性一致的争论，以及一些关于此类系统的形式语义的工作 9。还有一些关于隐蔽通道的有趣的新问题。例如，一家石油公司是否可以通过询问哪些专家可以咨询并注意到他们的人数突然减少来了解使用同一家投资银行的竞争对手是否正在计划竞标第三家石油公司？

在实践中，中国墙仍然使用手动方法实现。一家大型软件咨询公司让每个员工都保留一份“未分类”的简历，其中包含经过过滤并与客户达成一致的条目。一个典型的条目可能是：

9 月 17 日至 4 月 18 日：就美国一家主要零售银行的新分行会计系统的安全要求进行咨询

这不是唯一的控件。顾问的经理应该意识到可能的冲突，如果有疑问，不要将简历转发给客户；如果失败，客户可以自己从简历中发现潜在的冲突；如果这也失败了，那么顾问有义务在出现任何潜在冲突时立即报告。

仍然存在微观层面的问题。如果银行经理只看他最好的客户的竞争对手的银行报表怎么办？在这里，现代系统倾向于限制访问，除非工作人员为该客户建立了安全上下文，例如让客户回答一些身份验证问题。我将在有关银行业务和簿记的章节中进一步讨论这个问题。

中国墙的一个显着故障模式是冲突时间太短。政府通常有冲突规则，阻止部长在离开办公室后六个月内在他们监管的任何部门工作。

这太少了。六个月前担任能源部长的人仍然认识该行业的所有顶尖人物，任何从他们的政策中受益的人都可以通过雇用他们来表达他们的感激之情。五年可能更明智，但如果你认为你可以让当地立法机关通过这样的法律，祝你好运。

9 例如，参见 Foley [700] 关于与不干涉的关系。平静的实际解决方案通常是一段冷静期：在一家石油公司工作过，你可能被禁止在另一家公司工作两年

10.5 总结

在本章中,我们研究了当系统扩展以收集大量敏感信息时设置边界的问题,许多人需要访问这些信息才能完成工作。这是许多信息安全问题中的一个问题,从保护国家情报数据和有关野生动物遭受偷猎风险的数据,到医疗和社会保健信息的隐私和机密,再到一般的专业实践。

我们非常详细地查看了医疗记录,发现最简单的问题是在直接护理环境中设置访问控制,以便将对每条记录的访问限制在合理数量的人员内。这样的系统可以通过自动化现有的工作实践来设计,而基于角色的访问控制是实现它们的自然方式。然而,医疗保健系统中的激励措施往往执行不力,需要监管来强制遵守。传统的隐私保护方法可能被概括为“同意或匿名”,但由于许多外包系统的复杂性不断增加,这些系统甚至对医生(更不用说患者)也常常是不透明的,这种方法正在受到破坏。

更棘手的问题是越来越多的中央系统,尤其是与支付相关的系统,无法选择退出;基因数据的使用越来越多,以及社交媒体的影响,通常可以从中推断出敏感的个人健康信息。在这里,治理问题也比技术问题更难处理。唯一现实的解决方案在于监管,而美国和欧盟在这方面的分歧越来越大。欧洲赋予其公民将其个人健康信息限制在直接参与其案件的临床医生的权利;美国没有。然而,欧洲人可能很难行使我们的权利。美国和欧洲都面临着来自制药公司和其他想要我们所有数据的人的巨大游说和财务压力;政治家倾向于站在行业一边并破坏监管机构。

自 1990 年代以来,医疗服务提供者和服务机构一直试图通过建立医疗记录(或学校记录或人口普查报告)的“匿名”数据库来分得一杯羹,以便研究人员能够在不损害个人隐私的情况下进行统计查询。在某些应用中,这是完全不可能的,例如打击野生动物犯罪;在那里,汇总数据对偷猎者来说甚至比个人目击更有价值。

就病历而言,计算机科学家自 1980 年代以来就知道,对丰富的数据进行匿名处理比看起来要困难得多,近年来,我们已经获得了一个强有力的理论,可以让我们计算出它何时可以工作以及何时可以工作。它不会。我将在下一章讨论这个问题。

另一个外卖信息是这样的。正如多级安全是信息安全的“刺猬”方法一样,您希望通过只做对一件大事来获得好的结果,多边安全需要“狐狸”方法;你需要详细了解你的应用程序,了解过去出了什么问题 如果你想预测未来可能出现的问题,还需要善于对抗性思维。

研究问题

冠状病毒大流行可能会使健康监测更加普遍,因此个人健康信息将变得更加普遍,这里讨论的冲突将蔓延到医疗保健领域之外。这将带来什么,技术和政策机制应如何发展以应对?

此外,在不久的将来,越来越多的医疗将涉及基因信息。是否有任何明智的方法可以扩展隐私模型以处理多个人?例如,在许多国家/地区,您有权不知道亲属对亨廷顿舞蹈症等遗传性疾病进行的 DNA 检测结果,因为它可能会影响您也患有此病的几率。您的亲戚确实有知情权,并且可以告诉其他人 因此您可能会间接收到不受欢迎的消息。在我撰写本文时,英国和德国的法院审理了一些案件,这些案件对被诊断患有亨廷顿舞蹈病的人的子女的权利提出了不同的要求 [606]。这种信息权的紧张关系早在互联网出现之前就已经存在,并且不能仅通过技术机制来管理。但是社交媒体改变了比例因子,使它们更加广泛和尖锐。长期解决方案很可能涉及法律、社会规范和技术支持的某种组合;但它们可能需要数年时间才能解决,而且我们很可能最终会在不同的文化中得到不同的解决方案。例如,东亚国家容忍了更具侵入性的监视,并且在大流行中遭受的死亡人数要少得多,至少到目前为止是这样。这会改变其他地方的态度吗?

进一步阅读

关于分区模式安全的文献是分散的:大多数公共领域的论文都在 NCSC/NISSC 和 ACSAC 会议的会议记录中,而 Amoroso [47] 和 Gollmann [779] 涵盖了网格和中国墙的基础知识楷模。有关 2009 年英国在健康、社会关怀和教育方面的隐私失败调查,请参阅“数据库状态”[102]。有关 NHS 国家 IT 计划的案例研究,请参阅 [379],有关英国议会公共账户委员会后来关于总成本的报告,请参阅 [1559]。对于 BMA 模型,请参阅政策本身 [58]、奥克兰版本 [59]、关于该政策的会议记录 [63] 以及 Hastings 关于试点系统的论文 [535、536]。有关美国医疗隐私的国家研究委员会研究,请参阅 [1412]; [1191] 还有一份关于在研究中使用去识别化数据的 HHS 报告。但是有关医疗隐私问题的最新消息的最佳来源是相关游说团体的网站:英国的 medConfidential 和美国的 Patient Privacy Rights。