**us-blockchain-opportunities-for-health-care**

国家卫生信息技术协调员办公室发布了“全国共享互操作性路线图”，其中定义了全国互操作性所需的关键政策和技术组件，包括（1）无处不在，安全网络基础设施，（2）所有参与者的可验证身份和认证， （3）访问电子健康信息授权的一致性表示等几项要求。 然而，目前的技术并不能完全满足这些要求，因为它们面临与安全性，隐私性和全面生态系统互操作性有关的限制。

目前的卫生保健记录状况由于缺乏通用的体系结构和标准而脱节并且被窃取，这些架构和标准将允许系统中的利益相关者之间安全地传递敏感信息。卫生保健提供者在每次提供医疗服务时跟踪和更新患者的常见临床数据集。该信息包括标准数据，例如患者的性别和出生日期，以及根据提供的特定服务的独特信息，例如所执行的程序，护理计划和其他注释。传统上，这些信息是在一个单一的组织内或一个确定的医疗保健利益相关者网络的数据库中进行跟踪。每次执行服务时，通过医疗机构来自患者的这种信息流不需要在个人组织层面停止。相反，卫生保健组织可以采取一个更多的步骤，并将每个患者互动中存在的一组标准化信息引导到全国性的块链交易层。该事务层的表面信息将包含不受保护的健康信息（PHI）或个人身份信息（PII）的信息;相反，选择和非个人身份的人口统计和服务提供的信息可以使医疗保健组织和研究机构能够访问一个广泛和数据丰富的信息集。存储在块链上的信息可以通过块链私钥机制通用于特定个体，使患者能够更加无缝地与医疗机构共享信息。在块链上部署一个事务层可以帮助完成ONC HIT的互操作性目标，同时创建一个无信任和协作的信息共享生态系统，以提供新的见解，提高国家医疗体系的效率和公民的健康。

面向块链互操作性

作为事务层，块链可以存储两种类型的信息：（1）直接存储在块链上的“On-chain”数据，或者（2）存储在作为指针的块链上的链接的“Off-chain”数据存储在单独的传统数据库中的信息。将医疗信息直接存储在块状链上，确保信息完全受到块状属性的保护，并且可以立即被视为有权访问该链的用户;同时，存储大量数据文件会降低块处理速度，并为系统扩展带来潜在的挑战。相比之下，加密的链接的大小是最小的，一旦被激活

具有正确私钥的用户访问该块并跟随加密的链接

包含信息的单独位置。作为示例，块链不能直接存储诸如x射线或MRI图像的抽象数据类型：这种类型的数据将需要链接到单独的位置。因此，考虑如何存储数据的组织应仔细评估技术和机密性限制。

创建互操作性需要无摩擦的提交和访问来查看数据。因此，块链可以用作组织使用一个安全系统提交和共享数据的事务层。这将是最有效的一个具体的集合

的标准化数据直接存储在块上，以便立即获得许可访问，并在需要时补充脱链数据链接。

标准化数据集可以包括诸如人口统计学（性别，出生日期，其他数据），病史（免疫接种，手术）和所提供的服务（生命体征，服务执行和其他数据）等信息。随着现场的成熟，需要进一步的评估和指导，以确定每个数据类型应在哪里和如何存储。

一旦建立了一套标准化的医疗保健信息，就可以在智能合同中创建具体的数据字段，以采用处理和存储块上信息的规则，以及在块链存储之前规定所需的批准。每当患者互动发生时，医疗保健机构都会将信息传递给智能合同，合同的参数将验证有效信息是否已提交。作为示例，智能合同可以规定所有字段需要在块链存储之前提供，或者特定字段必须包含特定数据类型（例如数字）才能有效。一旦智能合同确认已经提交了正确的数据字段，它将将事务引导到块状存储。

块链增强数据完整性和病人数字身份

可互操作的块链可以增强数据完整性，同时更好地保护患者的数字身份。 2015年，由于黑客/ IT事件8起，医疗保健记录数据泄露达1.12亿。 2016年，估计有三分之一的医疗保健受益人将成为数据泄露的受害者。密码公共/私人密钥访问，工作证明和分布式数据的块链固有属性为医疗保健信息创建了一个新的完整级别。

连接到块链网络的每个参与者具有秘密私钥和作为公开可见标识符的公钥。该对被加密地链接，使得可以使用私钥在一个方向上进行识别。因此，必须具有私钥以解锁参与者的身份，以揭示块链中的哪些信息与其配置文件相关。因此，块链公钥/私钥加密方案创建身份许可层，以允许患者与特定医疗保健共享不同的身份属性

根据需要在卫生保健生态系统内部组织，减少由所有方面存储PII引起的漏洞，并允许患者或提供者引入数据访问时间限制。

此外，单个患者私钥的潜在黑客攻击可能会限制潜在的不利影响，因为黑客需要单独攻击每个用户以获得唯一的私钥来访问可识别的有价值信息。在无处不在的周边防火墙破坏和ransomware的时代，异步加密的过程保护了跨组织或组织内的病人身份。

另外，与块状链接相关的所有医疗保健机构都可以保留自己的保健分类帐的更新副本 - 因此 - 如果要修改历史块，则需要51％的网络参与者批准更改，如需要更新该块的每一个副本以反映更改。

此功能可提高安全性，并可帮助限制恶意活动的风险，因为更改会立即广播到网络，而分布式分类帐提供防止恶意攻击的保护副本。

块链技术为医疗保健提供了许多机会; 然而，今天还不完全成熟，也不是立即适用的灵丹妙药。 在全国各地的组织采用卫生保健块状况之前，必须解决好几种技术，组织和行为上的经济学挑战。

可扩展性限制：事务量与可用计算能力之间的权衡

Blockchain框架表明组织可以推出无权或许可的块链技术实现。无限制的块链是有吸引力的，因为它们允许更广泛的访问，允许开放式创新，并在整个网络中挖掘出更大的计算能力。同时，现有的无权的块链，如Ethereum或Bitcoin，面临交易量限制。今天，比特币块链每秒处理大约7笔交易，但是有超过1000万用户和20万日交易10。现场许多人都在呼吁技术进步，以便加快处理时间。

许多块链接可以加快交易处理时间，但是由于网络参与减少，它们可能会面临计算能力的限制。理论上，HHS可以提供​​处理所有块链交易所需的计算能力，一个被许可的网络选择参与者;然而，这将导致HHS作为块链的相对拥有者，并且可以排除真正分散的系统的价值。全国范围内的大量医疗保健参与者，将使系统不仅可以更加互操作，而且还可以使其更加安全。

数据标准化和范围

除了评估无权和许可的块链之外，组织还应考虑在块链中或在块链上存储哪些信息。对于存储在块链上的保健信息，最直接的关注​​是存储在块链上的信息的大小。将数据自由提交给块链，如医生笔记，可能会造成不必要的大量事务

尺寸可能会对块链的性能产生不利影响。然而，块链仍然可以通过具体和限制的数据集合来进行有效的操作，例如人口统计信息，病史和提供服务的代码。

为了标准化存储在块链上的数据并管理性能，组织应该在框架上进行对齐，以定义可以提交的数据，大小和格式。在某些情况下，技术API可以连接和解除连接存储和广播的信息，以压缩数据大小。最后，参与者可以将块链私有化，限制只对注册和有效组织的访问。

采纳和激励参与

块级成功需要两级激励。在技​​术层面上，必须存在互连的计算机网络（节点），以便在提交事务时提供创建块所需的计算能力。在无权许可的情况下，以隐式货币形式出现的货币激励措施鼓励个人将其计算能力借给网络。对于获得批准的块链，可以通过财务激励或访问块链数据来促进参与，以交换处理交易。

除了积极开展技术工作的激励之外，还可能需要进一步的支持来鼓励组织采用技术并参与共享网络。虽然一些组织已经在测试技术来在内部验证和跟踪医疗记录和索赔，但是当共享网络上的用户数量增加时，块链接将更加强大。类似于医疗保险和医疗补助服务中心（CMS）的有意义使用计划11，其激励供应商转向电子病历，可以增加收养并促进全国性的块状健康交换。

监管考虑

卫生保健决策者应考虑与行业的深入合作，以便在现有监管框架和新的行政政策目标的范围内了解和促进生态系统的增长。注意事项可能包括拥有记录所有权（以及所有权何时改变）的块链的分布式存储性质的含义，以及如何使用块链进行访问授权。

HHS通过HIPAA隐私规则，制定了保护个人医疗记录隐私的国家标准。该规则规定了保护个人健康信息隐私的条件，并设定了无需患者授权即可使用和披露的限制和条件。由于这些条件，块链解决方案可以通过将身份，PII和PHI分离并加密成可以通过基于KSI层次结构的块链接访问的分离实体来解决HIPAA隐私规则。如互操作性部分所述，患者可以根据需要与卫生保健生态系统共享不同的身份属性。同时，存储在块状链上的高级别人口信息的类型需要仔细考虑;这种人口统计信息与位置数据配对的理论可以理论上允许特定个体的三角测量。例如，与人口稠密的城市中心相比，在农村地区识别具有罕见健康状况的个体的潜力可能更大。这些担忧可能通过获得批准的块链来部分调解。尽管如此，随着块链实验的进步，这些问题需要仔细考虑。

**11-74-ablockchainforhealthcare**

分布式区块链包含健康记录、文档或图像数据存储和数据吞吐量影响的局限性。如果模仿比特币区块链, 分布式网络中每个成员的卫生保健区块链的一个副本每个健康记录每一个人在美国,这并不实用的数据存储的角度来看。因为健康数据是动态的和广泛的,复制所有健康记录每一个成员在网络带宽密集型的,浪费在网络上资源和对数据吞吐量问题。

我们提出健康区块链中包含的信息将是一个索引,所有的列表用户的健康记录和健康数据。索引类似于图书馆卡片目录。的卡片目录包含关于这本书的元数据和一个位置可以找到这本书。健康区块链会以同样的方式工作。块将包含一个事务用户的唯一标识符,一个加密有关的健康记录和一个时间戳的时候事务被创建。提高数据访问效率,事务将包含类型的数据包含在促进健康记录和其他元数据经常使用的查询(可以添加元数据标签)。健康区块链将包含一个完整的索引所有医疗数据的历史,包括正式的医疗记录从移动应用程序和可穿戴传感器健康数据,并将遵循一个独立的个体用户终其一生。

当一个卫生保健提供者创建一个医疗记录(处方、实验室测试、病理结果, MRI)将创建数字签名验证文档的真实性或图像。的健康数据加密和数据发送到湖用于存储。每一次信息保存到湖一个指针指向的数据区块链以及健康记录登记用户的唯一标识符。病人健康数据添加到他的通知区块链。病人能够以相同的方式添加健康数据与数字从群签名和加密

用户将会获得他的数据和控制他的数据如何被共享。的用户分配一组访问权限和指定谁可以查询和写入数据他的区块链。移动仪表板应用程序将允许用户看到谁了权限访问他的区块链。用户还可以查看他们的审计日志访问他的区块链,包括时间和数据的访问。相同的仪表板将允许用户和撤销访问权限给任何个人谁有一个独特的标识符。

用户可以设置具体的,关于谁有权访问的详细交易, 规定时间内的特定类型的数据访问和可访问。在任何给定的时间用户可以改变的一组权限。访问控制策略也将安全地存储在块链中，并且只允许用户更改它们。 这提供了透明度的环境，并允许用户对收集的数据以及如何共享数据做出所有决定。

根据这一模式，用户可以对其数据进行单一的控制，并授权访问具体的医疗保健提供者和/或医疗机构进行疾病治疗和预防的沟通和协作。 块分散结合数字签名交易的性质确保对手不能像用户一样构成网络，也不会损坏网络，因为这意味着对手伪造数字签名或获得对网络资源大部分的控制。 类似地，对手将无法从共享的公共账簿中学习任何东西，因为只有散列的指针和加密的信息将包含在交易中