(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104335209 B
(45)授权公告日 2019.05.10

(21)申请号 201380026992.9
(22)申请日 2013.05.08
(65)同一申请的已公布的文献号
申请公布号 CN 104335209 A
(43)申请公布日 2015.02.04
(30)优先权数据
13/530,185 2012.06.22 US
(85)PCT国际申请进入国家阶段日
2014.11.24
(86)PCT国际申请的申请数据
PCT/US2013/040065 2013.05.08
(87)PCT国际申请的公布数据
WO2013/191813 EN 2013.12.27
(73)专利权人 甲骨文国际公司
地址 美国加利福尼亚
(72)发明人 V·K·皮莱
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 陈新
(51)Int.Cl.
G16H 10/60(2018.01)
(56)对比文件
US 2005/0236474 A1,2005.10.27,
US 2005/0236474 A1,2005.10.27,
US 2004/0215981 A1,2004.10.28,
US 6463417 B1,2002.10.08,
US 2008/0010254 A1,2008.01.10,
EP 2426617 A1,2012.03.07,
审查员 杨静

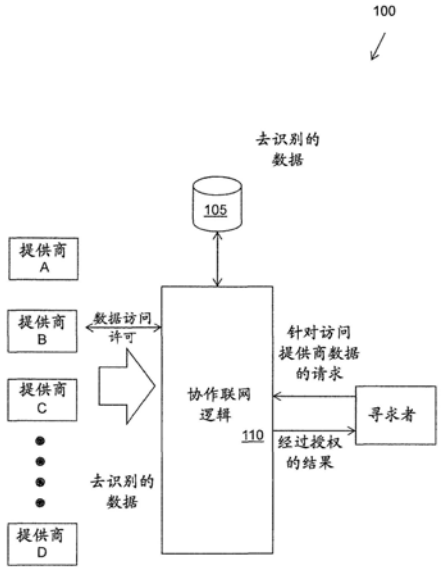
权利要求书3页 说明书10页 附图9页

(54)发明名称

协作联网工具

(57)摘要

本发明描述了各种系统、方法和相关联的其他实施例。在一个实施例中，一种方法包括从提供商接收描述患者的去识别的数据。所述方法包括：允许经过提供商授权的寻求者对数据存储库中的去识别的数据进行选择性的访问。



CN 104335209 B

1.一种计算机实现的装置,包括:

用于对从提供商设备接收的电子去识别的记录进行存储的构件,所述电子去识别的记录被存储在数据存储库中,其中每个去识别的记录包括描述对象的特性而不标识该对象的去识别的数据,其中所述去识别的记录包括用于掩蔽所述去识别的记录的部分的第一层级掩蔽标识符;

用于将第二层级掩蔽标识符指派给所述去识别的数据并且生成将所述第二层级掩蔽标识符映射到所述第一层级掩蔽标识符的映射的构件;

用于从寻求者设备接收对访问包括多个去识别的记录的去识别的数据的请求的构件;

用于确定去识别的数据的提供商设备是否授权寻求者设备访问去识别的数据的构件;

用于在寻求者设备被授权时,从寻求者设备接收一条或多条选择标准的构件;

用于访问存储去识别的数据的数据存储库的构件;

用于识别出具有满足所述一条或多条选择标准的数据存储库中的去识别的记录的对象的构件;

用于向寻求者设备返回所识别出的对象的计数而不返回去识别的记录的构件,以及

用于响应于经由来自寻求者设备的因特网通信而接收到标识对象的掩蔽标识符以及对关于所述对象的信息的请求而访问所述映射的构件,

其中用于访问的构件访问所述第二层级掩蔽标识符到所述第一层级掩蔽标识符的映射,以将所述掩蔽标识符翻译为由提供商指派给所述对象的第一层级掩蔽标识符;以及

用于使用因特网通信将所述请求和所述第一层级掩蔽标识符传送给所述提供商设备,而不将所述第二层级掩蔽标识符传送给所述提供商设备的构件,

其中所述第一层级掩蔽标识符和所述第二层级掩蔽标识符不会造成在所述寻求者设备和所述提供商设备之间从计算机在所述因特网通信中交换关于所述对象的标识信息。

2.根据权利要求1所述的计算机实现的装置,其中,用于确定寻求者设备是否被授权的构件包括用于从寻求者设备接收口令并且把所述口令与来自提供商的口令进行比较的构件。

3.根据权利要求1所述的计算机实现的装置,还包括:

用于通过以下操作创建去识别的记录的构件,针对每个去识别的记录:

从提供商接收包括由提供商指派给对象的第一层级掩蔽标识符的记录,其中提供商保持第一层级掩蔽标识符与唯一识别所述对象的对象标识符之间的第一映射,并且进一步地,其中所述记录不包括所述对象标识符;

将第二层级掩蔽标识符指派给所述对象;

保持第一层级掩蔽标识符到第二层级掩蔽标识符的第二映射;

从所述记录中去除第一层级掩蔽标识符;以及

将第二层级掩蔽标识符添加到所述记录以创建去识别的记录;

用于从寻求者设备接收第二层级掩蔽标识符的构件;

用于访问第二映射以将第二层级掩蔽标识符映射到第一层级掩蔽标识符的构件;

用于将第一层级掩蔽标识符提供给提供商的构件。

4.一种计算系统,包括:

处理器;以及

数据存储库，其对与多个对象相关联的电子去识别的记录进行存储，其中每个去识别的记录包括描述对象的特性而不标识该对象的去识别的数据，其中所述去识别的记录包括用于掩蔽所述去识别的记录的部分的第一层级掩蔽标识符；

其中所述处理器被配置为(i)将第二层级掩蔽标识符指派给所述去识别的数据，以及(ii)生成将所述第二层级掩蔽标识符映射到所述第一层级掩蔽标识符的映射；

协议验证逻辑，其被配置成使所述处理器：

经由来自寻求者设备的因特网通信接收用于选择去识别的记录的一条或多条选择标准；

访问数据存储库并且搜索满足所述一条或多条标准的去识别的记录；

对具有满足所述一条或多条选择标准的去识别的记录的多个对象进行计数；

经由因特网通信向寻求者设备返回其去识别的记录满足所述一条或多条选择标准的多个对象的计数而不返回去识别的记录；以及

招募逻辑，其被配置为使得处理器中介提供商设备与寻求者设备之间的通信，以保护数据通信，其中响应于经由来自寻求者设备的因特网通信接收到(i)作为标识对象的第二层级掩蔽标识符的所请求的掩蔽标识符，以及(ii)对关于所述对象的信息的请求，所述招募逻辑被配置成使所述处理器：

使用所述映射将所述第二层级掩蔽标识符翻译为由提供商设备指派给所述对象的第一层级掩蔽标识符；以及

经由因特网通信将所述请求和所述第一层级掩蔽标识符传送给所述提供商设备，而不将所述第二层级掩蔽标识符传送给所述提供商设备，

其中在所述寻求者设备和所述提供商设备之间在所述因特网通信中不交换关于所述对象的标识信息。

5.根据权利要求4所述的计算系统，其中提供商设备具有对识别与去识别的记录相关联的信息的监管，所述系统还包括数据和协作管理逻辑，所述数据和协作管理逻辑被配置成使所述处理器：

通过接收来自寻求者设备的口令并且把所述口令与来自提供商设备的口令进行比较来确定寻求者设备是否有权访问去识别的数据；以及

当来自寻求者设备的口令与来自提供商设备的口令不匹配时，拒绝对于数据存储库的访问。

6.根据权利要求5所述的计算系统，其中，所述招募逻辑还被配置成使所述处理器：

通过以下操作创建去识别的记录，针对每个去识别的记录：

从提供商设备接收包括由提供商设备指派给对象的第一层级掩蔽标识符的记录，其中提供商设备保持第一层级掩蔽标识符与唯一识别所述对象的对象标识符之间的第一映射，并且进一步地，其中所述记录不包括所述对象标识符；

将第二层级掩蔽标识符指派给所述对象；

保持第一层级掩蔽标识符到第二层级掩蔽标识符的第二映射；

从所述记录中去除第一层级掩蔽标识符；

将第二层级掩蔽标识符添加到所述记录以创建去识别的记录；

从寻求者设备接收第二层级掩蔽标识符；

访问第二映射以将第二层级掩蔽标识符映射到第一层级掩蔽标识符;以及

将第一层级掩蔽标识符提供给所述提供商设备。

7.一种计算机实现的方法,所述方法包括:

对从提供商设备接收的电子去识别的记录进行存储,所述电子去识别的记录被存储在数据存储库中,其中每个去识别的记录包括描述对象的特性而不标识该对象的去识别的数据,其中所述去识别的数据记录包括用于掩蔽所述去识别的记录的部分的第一层级掩蔽标识符;

将第二层级掩蔽标识符指派给所述去识别的数据并且生成将所述第二层级掩蔽标识符映射到所述第一层级掩蔽标识符的映射;

从寻求者设备接收对访问包括多个去识别的记录的去识别的数据的请求;

确定去识别的数据的提供商设备是否授权寻求者设备访问去识别的数据;

在寻求者设备被授权时,从寻求者设备接收一条或多条选择标准;

访问存储去识别的数据的数据存储库;

识别出具有满足所述一条或多条选择标准的数据存储库中的去识别的记录的对象;

向寻求者设备返回所识别出的对象的计数而不返回去识别的记录,以及

响应于经由来自所述寻求者设备的因特网通信接收到标识对象的掩蔽标识符以及对关于所述对象的信息的请求:

(a)访问所述第二层级掩蔽标识符到所述第一层级掩蔽标识符的映射,以将所述掩蔽标识符翻译为由提供商指派给所述对象的第一层级掩蔽标识符;以及

(b)经由因特网通信将所述请求和所述第一层级掩蔽标识符从计算机传送给所述提供商设备,而不将所述第二层级掩蔽标识符传送给所述提供商设备,

其中所述第一层级掩蔽标识符和所述第二层级掩蔽标识符不会造成在所述寻求者设备和所述提供商设备之间从计算机在所述因特网通信中交换关于所述对象的标识信息。

8.根据权利要求7所述的计算机实现的方法,其中,确定寻求者设备是否被授权包括从寻求者设备接收口令并且把所述口令与来自提供商的口令进行比较。

9.根据权利要求7所述的计算机实现的方法,还包括:

通过以下操作创建去识别的记录,针对每个去识别的记录:

从提供商接收包括由提供商指派给对象的第一层级掩蔽标识符的记录,其中提供商保持第一层级掩蔽标识符与唯一标识所述对象的对象标识符之间的第一映射,并且进一步地,其中所述记录不包括所述对象标识符;

将第二层级掩蔽标识符指派给所述对象;

保持第一层级掩蔽标识符到第二层级掩蔽标识符的第二映射;

从所述记录中去除第一层级掩蔽标识符;以及

将第二层级掩蔽标识符添加到所述记录以创建去识别的记录;

从寻求者设备接收第二层级掩蔽标识符;

访问第二映射以将第二层级掩蔽标识符映射到第一层级掩蔽标识符;以及

将第一层级掩蔽标识符提供给提供商。

协作联网工具

[0001] 相关申请的交叉引用

[0002] 本专利公开内容要求2012年6月22日提交的序列号为13/530,185的美国实用新型申请的权益,通过引用的方式将其全文合并在此。

背景技术

[0003] 在生命科学产品的发展中所面对的一项主要挑战是针对高质量临床信息的访问,以便理解执行临床研究的可行性以及对于临床研究招募患者。由于患者隐私法律的存在以及由于健康护理提供商缺少进行协作的诱因,从而大大限制了针对患者临床记录的访问。在许多事例中,医生充当实施研究的生命科学企业(制药/生物科技以及医疗器械公司)之间的中间人,以便找到满足研究的包含/排除要求的患者。这样就把将会受益于最新的临床研究的可能患者的总集限制到与所述生命科学企业有联系的医生的患者。这也意味着对于临床试验的患者的招募常常是通过口头方式进行的。

[0004] 为了促进生命科学产品公司与健康护理提供商之间的协作,一些公司充当中介,其从健康护理提供商购买去识别(de-identified)的临床数据并且将所述数据销售给生命科学产品公司。提供商常常不愿意将其患者数据销售给这些中介公司,因为这样做会失去对其数据的控制,而所述数据是对其非常有价值的资产。此外,中介公司所拥有的数据仅仅是销售时的患者数据的快照,这意味着其很快就会过期。

发明内容

[0005] 在一个实施例中,提供一种存储计算机可执行指令的非瞬时性计算机可读介质,所述计算机可执行指令在由计算机执行时使得所述计算机实施促进协作联网的方法。所述方法包括:从提供商接收描述给定对象的去识别的数据,其中所述去识别的数据包括由提供商指派给所述给定对象的第一层级掩蔽标识符。所述方法还包括:将去识别的数据存储在数据存储库中,并且拒绝由未经提供商授权的寻求者访问所述去识别的数据。

[0006] 在一个实施例中,所述指令还包括:在把去识别的数据存储在数据存储库中之前从去识别的数据去除第一层级掩蔽标识符;将第二层级掩蔽标识符指派给去识别的数据;以及保持第一层级掩蔽标识符到第二层级掩蔽标识符的映射以用于未来的处理。

[0007] 在一个实施例中,所述方法包括:确定提供商是否授权访问去识别的数据包括从寻求者接收口令以及把所述口令与来自提供商的口令进行比较。

[0008] 在一个实施例中,所述指令还包括:当寻求者被授权访问时,允许在数据存储库中查询去识别的数据,以便向查询返回满足查询标准的对象的计数而不返回去识别的数据。

[0009] 在一个实施例中,所述指令还包括:通过选择预定的去识别的数据属性数值对所接收到的数据进行筛选;以及将所选择的数据属性数值存储在数据存储库中而不存储不对应于预定数据属性数值的去识别的数据。

[0010] 在一个实施例中,提供一种存储计算机可执行指令的非瞬时性计算机可读介质,所述计算机可执行指令在由计算机执行时使得所述计算机实施促进协作联网的方法。所述

方法包括：从寻求者接收针对访问去识别的数据的请求，以及确定去识别的数据的提供商是否授权所述寻求者访问去识别的数据。所述方法还包括：当寻求者被授权时，从寻求者接收一条或多条选择标准；访问存储与多个对象相关联的去识别的数据的数据存储库，并且识别出与数据存储库中的满足所述标准的去识别的数据相关联的对象。所述方法包括：向寻求者返回所识别出的对象的计数，从而不向寻求者返回去识别的数据。

[0011] 在一个实施例中，确定寻求者是否被授权包括从寻求者接收口令，并且包括把所述口令与来自提供商的口令进行比较。

[0012] 在一个实施例中，所述指令还包括：从寻求者接收唯一地标识对象的第二层级掩蔽标识符。所述方法包括：将第二层级掩蔽标识符映射到第一层级掩蔽标识符并且将第一层级掩蔽标识符提供给提供商。

[0013] 在一个实施例中，提供一种实施协作联网的计算系统。所述计算系统包括协作联网工具逻辑。所述联网工具逻辑包括数据和协作管理逻辑，其被配置成从提供商接收描述给定对象的去识别的数据；并且将第二层级掩蔽标识符和去识别的数据存储在数据存储库中。所述协作联网工具被配置成拒绝由未经提供商授权的寻求者访问所述去识别的数据。

[0014] 在一个实施例中，提供一种实施协作联网的计算系统。所述计算系统包括协议验证逻辑，其被配置成：从寻求者接收一条或多条选择标准；访问存储与多个对象相关联的去识别的数据的数据存储库；以及识别出对应于满足所述标准的对象的数据存储库中的去识别的数据。所述协议验证逻辑还被配置成向寻求者返回满足所述选择标准的对象的计数，从而不响应于接收到选择标准而返回去识别的数据。

附图说明

[0015] 被合并在说明书中并且构成说明书的一部分的附图示出了本公开内容的各种系统、方法和其他实施例。应当认识到，附图中示出的元件边界(例如方框、方框组或其他形状)代表所述边界的一个实施例。本领域技术人员将认识到，在一些实施例中，一个元件可以被设计成多个元件，或者多个元件可以被设计成一个元件。在一些实施例中，被显示为另一个元件的内部组件的元件可以被实施为外部组件，反之亦然。此外，各个元件可能不是按比例绘制的。

[0016] 图1示出了与协作联网工具相关联的系统的一个实施例。

[0017] 图2示出了与协作联网工具相关联的系统的另一个实施例。

[0018] 图3示出了与协作联网工具相关联的系统的一个实施例。

[0019] 图4示出了与协作联网工具相关联的系统的另一个实施例。

[0020] 图5示出了与协作联网工具相关联的系统的另一个实施例。

[0021] 图6示出了与协作联网工具相关联的方法的一个实施例。

[0022] 图7示出了与协作联网工具相关联的方法的另一个实施例。

[0023] 图8示出了与协作联网工具相关联的方法的另一个实施例。

[0024] 图9示出了示例性系统和方法以及等效方案可以操作在其中的计算系统的一个实施例。

具体实施方式

[0025] 过去不存在允许健康护理机构以有意义的方式与生命科学公司安全地共享信息(例如临床数据)以进行二次利用(比如开发新的疗法)同时保护其患者的隐私并且保持信息的价值的工具或模型。生命科学公司与健康护理机构之间的这一临床信息共享在许多方面可以是有价值的。在本说明书中,使用临床数据来找到参加临床试验的患者将是焦点所在。但是这里所描述的协作联网工具可以被采用来出于许多目的共享信息。临床数据可以对于生命科学公司有用的其中一些方式是对于研究协议的建模和可行性分析,找到参加临床研究的理想候选人,促进市场上的药物的临床研究、销售、安全性监督,护理管理,比较效果研究等等。

[0026] 简单地知道满足特定协议或标准的患者的计数对于生命科学公司常常可能是非常有价值的。这一信息可以帮助生命科学公司修改其标准,从而使得所述标准款反到足以包括足够数目的患者。满足描述某种病症的标准的患者数目可以被用来识别出对应于治疗所述病症的药物的潜在市场。通过在各个提供商处知道满足所述标准的患者数目可以帮助生命科学公司选择临床试验的位置。这里所描述的协作联网工具允许通过保密的方式共享患者计数,并且同时保护患者的身份以及所述信息对于健康护理提供商的价值。

[0027] 临床研究是医疗产品(例如医疗器械或药品)开发的一个重要部分。在临床研究中,"协议"包括描述所述研究感兴趣的患者的身体特性的所选择的包含和排除标准。举例来说,包含标准可以规定患者具有特定疾病或病症,排除标准则可以规定患者不可高于特定年龄。找到满足协议标准的足够数目的患者常常被证明是一项障碍。为了高效地实施临床试验,必须找到可以与少量试验现场的其中之一进行交互的足够数目的患者。

[0028] 过去,识别临床研究现场和招募患者的过程相当耗时。在将这些过程流水线化的努力中,成立了合同研究组织(CRO)。CRO是由生命科学企业签订合同来实施医疗产品开发的各个方面(包括临床研究)的服务组织。即使对于CRO所享有的规模效益,对于验证协议、确定针对患者的适当的包含/排除标准、招收研究现场以及招募患者仍然需要大量时间。等到实施了整个过程时,为了进行研究所招募的其中一些患者常常由于其状况的改变而不再适合。

[0029] 这里描述了提供协作联网工具的系统和方法,所述协作联网工具托管来自多家提供商(例如健康护理提供商)的关于患者的去识别的纵向信息(例如在一段时间内收集的临床数据)。所述协作联网工具在提供商的授权下为寻求者(例如医疗产品公司、CRO)提供对于该信息的访问。因此,订购所述协作联网工具并且经过其数据由所述工具托管的提供商授权的寻求者可以访问所述数据,以便验证协议(例如检查所述标准涵盖适当数目的患者)以及/或者识别出满足一条或多条标准的患者。所述协作联网工具充当去识别的数据的托管者而不包括可以被用来识别患者的关于患者的数据(例如姓名、地址、治疗医生、具体地理细节),所述去识别的数据描述通常是协议标准的对象的患者特性(例如诊断、年龄、性别、当前治疗)。可以为提供商给出许可对其数据的访问的机会,从而允许提供商保持对于其敏感的并且有价值的患者数据的所有权。

[0030] 寻求者可以在由协作联网工具托管的去识别的数据商实施查询,以便确定提供商是否具有满足协议标准的足够数目的患者。这样就允许寻求者寻求与具有满足所述协议的足够患者的提供商的协作关系。该协作还可以通过协作联网工具来实施,正如后面将更加

详细地描述的那样。

[0031] 出于本说明书的目的，由协作联网工具托管的数据是关于处在健康护理提供商的医疗治疗下的患者的临床数据。所述协作联网工具可以被用来托管任何类型的数据，其中数据对象(例如患者)的身份将保持保密。举例来说，其数据可以由协作联网工具保密地托管的对象包括可以被招募以进行雇佣的专业人士、寻求相亲服务的人等等。在更宽泛的意义上，所述对象可以不是人，而可以是其数据可以由希望提供对于该数据的受控访问的提供商所有的任何实体。

[0032] 虽然隐私限制阻碍了将电子医疗记录广泛用于临床数据的二次利用，所述协作联网工具允许健康护理提供商将来自电子医疗记录的去识别的临床数据存储“在云中”(例如由协作联网工具控制的数据库/数据仓库)。这样就创建了一个广大的患者总集，从而使得决策制定者能够基于高质量临床数据做出准确的决定，从而大大加快研究的执行速度。去识别的数据的提供商同样受益，这是因为通过将患者的去识别的临床数据提供给协作联网工具，所述提供商使其患者能够接触到最新的医疗研究。

[0033] 参照图1，其中示出了与被用来托管对应于患者的临床数据的协作联网工具110相关联的系统100的一个实施例。在其他实施例中，协作联网工具110按照这里所描述的方式托管关于其他对象的数据。系统100包括被配置成存储去识别的数据(例如在一个实施例中是临床数据)的数据存储库105。出于本说明书的目的，所述数据描述处于健康护理提供商的治疗下的患者。所述数据包括描述对象的各个方面的对象数据(例如患者的电子医疗记录(EMR))的所选部分，而不会损害对象身份的保密性。针对所述数据的访问由协作联网工具110控制。图3提供了关于数据被存储在数据存储库105中的方式的附加细节。

[0034] 协作联网工具逻辑110控制对于数据存储库105中的去识别的数据的访问。举例来说，可以对来自每一家提供商的数据单独进行口令保护，从而使得协作联网工具110在没有提供商口令的情况下阻止寻求者对于数据的访问。协作联网工具逻辑110接收来自多家数据提供商(例如健康护理提供商)的去识别的数据。所述去识别的数据被存储在数据存储库105中。协作联网工具逻辑110被配置成为经过授权的寻求者(例如寻求验证协议或者针对临床试验招募患者的实体)提供规定类型的访问。在一个实施例中，协作联网工具逻辑110对来自寻求者的针对查询给定提供商的数据的请求进行处理。如果寻求者被授权访问所述提供商的数据(例如具有特定于所述提供商的口令)，则协作联网工具逻辑110允许寻求者查询所述(多家)提供商的数据。

[0035] 通过这种方式，协作联网工具逻辑110保护患者保密性，并且允许数据提供商保持对其数据的控制(例如通过为寻求者提供口令)，同时为寻求者提供对于临床数据的较大总集的访问。协作联网工具逻辑110还可以包括计费特征，其针对在数据存储库105中保持其数据的提供商以及访问数据的寻求者进行收费。

[0036] 在一个实施例中，协作联网工具逻辑110和数据存储库105被提供“在云中”。在该实施例中，数据存储库105与提供商和寻求者的物理位置分开，并且由提供商和寻求者经由因特网访问。提供商和寻求者可以订购协作联网服务，其通过协作联网工具逻辑110准许对于数据存储库105中的数据的访问。数据存储库105可以是根据由提供商建立的准则保持的专用的HIPAA认证的数据库。

[0037] 图2示出了包括协作联网工具逻辑210和去识别的数据存储库105的协作联网系统

200的一个示例性实施例。协作联网工具逻辑210包括数据和协作管理逻辑220、协议验证逻辑230和招募者逻辑240。数据和协作管理逻辑220被配置成将数据保持在数据存储库105中。数据存储库105中的数据被去识别。保持在数据存储库105中的数据可以是源自EMR、临床数据、实验室数据、药房数据以及调度表数据。在将所述数据发送到协作联网工具逻辑210之前，提供商去除所有患者个人可识别信息(基于HIPAA规章)，并且为每一位患者的数据指派唯一的第一层级掩蔽标识符。提供商保持第一层级掩蔽标识符到其原始患者标识符的映射。当数据到达数据和协作管理逻辑220时，所述数据和协作管理逻辑220为数据指派第二层级掩蔽标识符。数据和协作管理逻辑220保持第二层级掩蔽标识符到第一层级掩蔽标识符的映射。通过这种方式，数据被掩蔽两次以保护患者隐私。除了患者标识符之外，医师和治疗位置标识符也可以被掩蔽。

[0038] 除了掩蔽的层级之外，可以采取其他措施来对数据进行去识别。举例来说，只有患者数据的所选属性被存储在数据存储库105中。包含医师评注(physician note)的临床数据列不可被存储在数据存储库105中，以便确保评注中的标识细节不会被无意地存储在数据存储库105中。还可以采取由HIPAA或其他认证实体规定的其他安全性措施。对应于所选属性的数据数值可以被转换到预定格式(例如标准医疗术语)以便于查询。

[0039] 提供商还可以能够基于针对临床试验参与的不同的同意程度来对患者加标签。因此，一些患者可能同意给出血液和组织样本，而不同意签订临床试验的合同。可以对招收在研究中的患者加标签，从而使其不会同时被多于一项研究接洽招募。加标签有助于提供商通过其处于卫生系统内的任何地方的治疗医师高效地招募患者，并且为寻求者提供有价值的服务。

[0040] 图3示出了数据存储库105的一个实施例。数据存储库105中的数据通过提供商划分，从而使得来自不同提供商的数据不会被混合并且无法被其他提供商访问。在一个实施例中，对应于每一家提供商的数据被存储在物理上分开的专用数据库中。提供商继续“拥有”其数据，并且可以为之给出许可针对数据存储库105中的该提供商的数据的每一个访问事例的机会。举例来说，每一个提供商数据库可以通过一个口令来保护。提供商可以通过为寻求者给出口令来授权寻求者访问其数据库。在请求数据时，寻求者默认地仅接收患者计数而没有单项(l ine item)细节。

[0041] 来自提供商的传入数据由适配器310处理，其被配置成由特定提供商的EMR系统使用。适配器310选择将被存储在数据存储库105中的属性，并且应用格式化规则从容将提供商的特定格式翻译成数据存储库105的共同格式。正如前面对于双层掩蔽所描述的那样，适配器310用针对数据的第二层级掩蔽标识符替换由提供商指派的第一层级掩蔽标识符。为了保持数据存储库105是最新的，提供商可以周期性地向数据存储库推送去识别的临床数据。当然，推送数据的频度越高，数据存储库105被保持的当前程度就越高。在一个实施例中，数据被每日推送。

[0042] 图3中示出的数据存储库105的实施例允许提供商保持对于其患者的EMR数据的所有权(例如通过对其数据进行口令保护)，并且规定去识别的临床数据可以被使用的方式。由于使得所述数据可用于许多寻求者，因此提供商对于其患者获得针对许多可能的临床研究的曝光，从而提升了提供商在患者当中的声望。此外，提供商能够出于其自身的目的以预定格式访问存储在数据存储库105中的数据，从而可能节省了保持其自身的数据存储库的

成本。

[0043] 回到图2，协议验证逻辑230应对来自寻求者的协议验证查询。寻求者订购提供用于对数据存储库105进行查询的基于云的服务。协议验证逻辑230被配置成处理所选提供商的数据上的协议验证查询。协议验证查询规定描述寻求者感兴趣的患者(例如对于临床试验的可能候选)的一条或多条包含/排除标准。协作联网工具210例如通过使用口令关于所选提供商确认对于寻求者的授权。如果寻求者对于提供商被授权，则协议验证逻辑返回满足所述标准的患者的计数。

[0044] 取代向寻求者返回临床数据，协作联网工具逻辑110对于每一个提供商标识符返回满足所述标准的患者计数。没有响应于协议验证查询而提供“行层级”信息。通过评估该信息，寻求者可以很容易识别出哪些提供商具有适合于其临床研究的患者，以及每一家提供商正在治疗多少患者。这样就允许寻求者寻求与所识别出的提供商的协作关系以便选择特定患者。在这一过程中的任何阶段寻求者都不具有关于患者是谁的任何知识，这是因为所述数据是去识别的。只有提供商处的经过授权的人员才能够识别出患者。

[0045] 图4示出了关于如何由协议验证逻辑230的一个实施例处理协议验证查询的一个实例。开始时，寻求者订购协作联网服务并且发起研究，以便找到处于指定提供商治疗下的患者以参与到临床研究中。由于在对寻求者准许访问(口令)时，协议验证逻辑的所有处理都可以由提供商许可，因此内部审查委员会(IRB)许可并不必要。如果寻求者已被提供商授权，则协议验证逻辑230允许寻求者查询提供商的数据。

[0046] 如果提供商授权由寻求者进行查询，则提供商使用协作联网工具来准许寻求者访问数据，从而许可协议验证逻辑对数据的访问。寻求者输入具有对应于临床研究的包含/排除标准的协议验证查询。协议验证逻辑230访问数据存储库105中的提供商的去识别的临床数据。所述查询返回满足所述标准的患者的计数。寻求者随后审查该信息，并且决定是否在临床研究中与所述提供商协作。

[0047] 回到图2，招募逻辑240被配置成在保护患者保密性的同时促进寻求者与提供商之间的协作。在一个实施例中，招募逻辑240中介寻求者与提供商之间的通信，这是通过把对应于在来自寻求者的通信中所涉及的患者的第二标识符翻译成可由提供商辨识的第一标识符来实现的。

[0048] 图5示出了在寻求者与提供商的协作期间如何有招募逻辑240的一个实施例处理数据以便实施临床研究。回顾图4，寻求者具有对应于满足协议验证查询的包含/排除标准的患者的第二层级掩蔽标识符的列表。为了开始与所选提供商的协作关系，可能需要IRB许可。所述患者列表(其由协作联网工具逻辑指派的第二标识符标识)被发送到招募逻辑240。招募逻辑用第一层级掩蔽标识符替换第二层级掩蔽标识符，并且将所述列表传送到提供商。在提供商处的IRB许可之后，提供商可以向寻求者提供关于所选患者的附加信息。

[0049] 寻求者使用所述信息来选择用于进行研究的患者，并且向招募逻辑240传送所选患者的列表以及针对IRB许可的请求。招募逻辑用第一层级掩蔽标识符替换列表中的第二层级掩蔽标识符，并且将所述列表提供给提供商以用于IRB许可。提供商选择研究者(将对患者施加所述协议的医师或护士)。寻求者将协议和教育材料上传到招募逻辑240，并且为研究者设立针对这些材料的访问特权。对于现有的和新的患者发起涉及所述协议的告警，并且通过所述告警向研究者通知协议中的改变。在临床研究期间，由研究者访问协议和教

育材料，以便确定如何治疗各个患者以及记录试验结果。招募逻辑240继续对于寻求者通过第二标识符并且对于提供商通过第一标识符来识别患者，从而保持患者的保密性。一旦对于临床试验招募了患者，就可以对于预定时间段为数据存储库(未示出)中的所述患者的临床数据加标签，从而表明所述患者的数据不应当被作为结果返回给任何其他协议验证查询。

[0050] 图6概括了与协作联网工具相关联的方法600的一个实施例。在610处，所述方法包括：从提供商接收描述给定对象(例如患者)的去识别的数据。所述去识别的数据包括由提供商指派给所述给定对象的第一层级掩蔽标识符。在620处，所述方法包括：将第二层级掩蔽标识符关联到所述数据。在630处，所述方法包括：将去识别的数据存储在数据存储库中。在640处，所述方法包括：阻止未经授权的寻求者访问所述数据。在一个实施例中，阻止访问是通过在允许访问提供商的数据之前要求提供商指定的口令来实施的。

[0051] 所述方法还可以包括处理协议验证查询。协议验证查询包括协议的包含/排除标准。响应于协议验证查询，返回其去识别的数据满足查询选择标准的对象的计数而不是去识别的数据本身。这意味着并不响应于数据存储库上的协议验证查询返回去识别的数据。

[0052] 在一些实施例中，所述方法还包括：在把去识别的数据存储在数据存储库中之前从去识别的数据中去除第一层级掩蔽标识符。所述方法向去识别的数据指派第二层级掩蔽标识符，并且将第二层级掩蔽标识符与去识别的数据一起存储在数据存储库中。保持第一层级掩蔽标识符到第二层级掩蔽标识符的映射以用于未来的处理。

[0053] 在一个实施例中，方法600包括：从寻求者接收第二层级掩蔽标识符。与所识别出的患者相关联的第一层级掩蔽标识符被提供给数据的提供商。

[0054] 在一个实施例中，方法600包括：通过选择预定的去识别的数据属性数值对所接收到的数据进行筛选，以及将所选择的数据属性数值存储在数据存储库中而不存储不对应于预定数据属性数值的去识别的数据。

[0055] 图7概括了与协作联网工具相关联的方法700的一个实施例。在710处，所述方法包括：从提供商接收描述给定对象(例如患者)的去识别的数据。所述去识别的数据包括由提供商指派给所述给定对象的第一层级掩蔽标识符。在720处，所述方法包括：将相应的第二层级掩蔽标识符与去识别的数据相关联。在730处，所述方法包括：将去识别的数据存储在数据存储库中。在740处，所述方法包括：允许数据存储库中的去识别的数据上的协议验证查询。协议验证查询包括协议的包含/排除标准。响应于协议验证查询，返回其数据(例如临床数据)满足查询选择标准的对象的计数而不是所述对象的数据。这意味着并不响应于数据存储库上的协议验证查询返回去识别的数据。

[0056] 图8示出了与协作联网相关联的方法800的一个实施例。在810处，所述方法包括：确认寻求者能够访问所选择的提供商的数据。举例来说，所述方法可以包括：在继续之前确定口令的有效性。在820处，所述方法包括：从寻求者接收规定一条或多条选择标准(例如包含/排除标准)的协议验证查询。在830处，所述方法包括：访问存储与多个对象相关联的数据的数据存储库。所述方法包括：在840处，识别出数据存储库中的满足所述标准的对象。在850处，所述方法包括：向寻求者返回具有满足所述标准的数据的对象的计数。

[0057] 在一些实施例中，方法800允许寻求者与提供商之间的协作。为此，所述方法包括：从寻求者接收所选择的第二层级掩蔽标识符。所述方法包括：取回相应的第一层级掩蔽标

识符，并且向提供商提供第一层级掩蔽标识符。通过这种方式，所述方法允许寻求者和提供商在不交换任何标识数据的情况下关于特定患者进行通信。

[0058] 一般计算机实施例

[0059] 图9示出了这里所描述的示例性系统和方法以及等效方案可以操作在其中的示例性计算设备。所述示例性计算设备可以是计算机900，其包括适于通过总线909连接的处理器902、存储器904以及输入/输出端口910。在一个实例中，计算机900可以包括协作联网工具930，其被配置成按照促进数据提供商与对象寻求者之间的协作的方式存储去识别的数据，并且同时保持对象的保密性以及数据提供商对于数据的所有权。在不同的实例中，工具930可以通过硬件、存储有指令的非瞬时性计算机可读介质、固件和/或其组合来实施。虽然工具930被图示为附着到总线908的硬件组件，但是应当认识到，在一个实例中，工具930可以被实施在处理器902中。

[0060] 在一个实施例中，协作联网工具930是用于按照促进数据提供商与对象寻求者之间的协作的方式存储去识别的数据并且同时保持对象的保密性以及数据提供商对于数据的所有权的装置(例如硬件、非瞬时性计算机可读介质、固件)。

[0061] 所述装置例如可以被实施为ASIC，其被编程来支持在去识别的数据上进行查询。所述装置还可以被实施为所存储的计算机可执行指令，其作为数据916被呈现给计算机900，所述数据916被临时存储在存储器904中并且随后由处理器902执行。

[0062] 作为对于计算机900的示例性配置的一般描述，处理器902可以是多种处理器，其中包括双微处理器以及其他多处理器架构。存储器904可以包括易失性存储器和/或非易失性存储器。非易失性存储器例如可以包括ROM、PROM等等。易失性存储器例如可以包括RAM、SRAM、DRAM等等。

[0063] 盘906可以适于例如经由输入/输出接口(例如卡、设备)918和输入/输出端口910连接到计算机900。盘906例如可以是磁盘驱动器、固态盘驱动器、软盘驱动器、带驱动器、Zip驱动器、闪存卡、记忆棒等等。此外，盘906可以是CD-ROM驱动器、CD-R驱动器、CD-RW驱动器、DVD ROM等等。存储器904例如可以存储进程914和/或数据916。盘906和/或存储器904可以存储控制并且分配计算机900的资源的操作系统。

[0064] 总线908可以是单一内部总线互连架构以及/或者其他总线或网状架构。虽然示出了单一总线，但是应当认识到，计算机900可以利用其他总线(例如PCIE、1394、USB、以太网)与多种设备、逻辑和外设进行通信。总线908可以是多种类型，其中例如包括存储器总线、存储器控制器、外围总线、外部总线、纵横开关(crossbar switch)以及/或者局部总线。

[0065] 计算机900可以经由i/o接口918和输入/输出端口910与输入/输出设备进行交互。输入/输出设备例如可以是键盘、麦克风、指示和选择设备、摄影机、视频卡、显示器、盘906、网络设备920等等。输入/输出端口910例如可以包括串行端口、并行端口以及USB端口。

[0066] 计算机900可以操作在网络环境中，因此可以经由i/o接口918和/或i/o端口910连接到网络设备920。通过网络设备920，计算机900可以与网络进行交互。通过网络，计算机900可以在逻辑上连接到远程计算机。计算机900可以与之进行交互的网络包括(但不限于)LAN、WAN以及其他网络。

[0067] 在另一个实施例中，所描述的方法和/或其等效方案可以利用计算机可读指令来实施。因此，在一个实施例中，利用所存储的计算机可执行指令来配置非瞬时性计算机可读

介质，所述计算机可执行指令在由机器(例如处理器、计算机等等)执行时使得所述机器(和/或相关联的组件)实施在图6-8中描述的方法。

[0068] 虽然为了解释简单起见将附图中所示的方法示出并且描述为一系列方框，但是应当认识到，所述方法不受限于方框的顺序，这是因为一些方框可以按照不同于所示出并描述的顺序发生以及/或者与其他方框同时发生。此外，可以使用少于所示出的所有方框来实施一种示例性方法。各个方框可以被组合或分离成多个组成部分。此外，附加的和/或替换的方法可以采用未示出的附加方框。

[0069] 后面包括这里所采用的所选术语的定义。所述定义包括落在术语的范围内并且可以被用于实施的组件的各种实例和/或形式。所述实例并不意图做出限制。单数和复数形式的术语都可以落在所述定义内。

[0070] 在提到“一个实施例”、“某一实施例”、“一个实例”、“某一实例”等等时，其表明所描述的(多个)实施例或(多个)实例可以包括特定特征、结构、特性、属性、元素或限制，但是并非每一个实施例或实例都必须包括该特定特征、结构、特性、属性、元素或限制。此外，对于短语“在一个实施例中”的重复使用并不一定是指相同的实施例，但是其可以是指相同的实施例。

[0071] ASIC:专用集成电路。

[0072] CD:紧致盘。

[0073] CD-R:CD可记录。

[0074] CD-RW:CD可重写。

[0075] DVD:数字通用盘和/或数字视频盘。

[0076] HTTP:超文本传输协议。

[0077] LAN:局域网。

[0078] PCI:外围组件互连。

[0079] PCIE:PCI express。

[0080] RAM:随机存取存储器。

[0081] DRAM:动态RAM。

[0082] SRAM:同步RAM。

[0083] ROM:只读存储器。

[0084] PROM:可编程ROM。

[0085] EPROM:可擦写PROM。

[0086] EEPROM:电可擦写PROM。

[0087] SQL:结构化查询语言。

[0088] OQL:对象查询语言。

[0089] USB:通用串行总线。

[0090] XML:可扩展标记语言。

[0091] WAN:广域网。

[0092] 这里所使用的“计算机可读介质”指的是存储指令和/或数据的非瞬时性介质。计算机可读介质可以采取多种形式，其中包括(但不限于)非易失性介质和易失性介质。非易失性介质例如可以包括光盘、磁盘等等。易失性介质例如可以包括半导体存储器、动态存储

器等等。计算机可读介质的常见形式可以包括(但不限于)软盘、柔性盘、硬盘、磁带、其他磁性介质、ASIC、CD、其他光学介质、RAM、ROM、存储器芯片或卡、记忆棒以及计算机、处理器或其他电子设备可以从中进行读取的其他介质。

[0093] 在一些实例中,“数据库”被用来指代表。在其他实例中,“数据库”可以被用来指代表的集合。在其他实例中,“数据库”可以指代数据存储库的集合以及用于访问和/或操纵这些数据存储库的方法。

[0094] 这里使用的“数据存储库”指代可以在非瞬时性计算机可读介质上存储数据的物理和/或逻辑实体。数据存储库例如可以是数据库、表、文件、列表、队列、堆栈、存储器、寄存器等等。在不同的实例中,数据存储库可以驻留在一个逻辑和/或物理实体中,并且/或者可以分布在两个或更多逻辑和/或物理实体之间。

[0095] 这里使用的“逻辑”包括(但不限于)硬件、固件、存储指令的非瞬时性计算机可读介质、在机器上执行的指令以及/或者前述每一项的组合,其用来实施(多项)功能或(多个)动作,并且/或者导致来自另一个逻辑、方法和/或系统的功能或动作。逻辑可以包括微处理器、离散逻辑(例如ASIC)、模拟电路、数字电路、已编程逻辑设备、包含指令的存储器设备等等。逻辑可以包括一个或多个门、门的组合或者其他电路组件。在描述多个逻辑时,有可能将所述多个逻辑合并到一个物理逻辑中。类似地,在描述单一逻辑时,有可能将该单一逻辑分布在多个物理逻辑之间。

[0096] 这里使用的“查询”指的是促进收集和处理信息的语义构造。可以通过数据库查询语言(例如SQL)、OQL、自然语言等等来制定查询。

[0097] 这里使用的“用户”包括(但不限于)一个或多个人、计算机或其他设备或者其组合。

[0098] 虽然前面通过描述实例说明了示例性系统、方法等等,并且以可观的细节描述了所述实例,但是申请人并不意图将所附权利要求书的范围约束或者以任何方式限制到这样的细节。为了描述这里所描述的系统、方法等等,当然不可能描述每一种可以设想到的组件或方法组合。因此,本公开内容不限于所示出和描述的具体细节、代表性设备和说明性实例。因此,本申请意图涵盖落在所附权利要求书的范围内的各种改动、修改和变型。

[0099] 就在说明书或权利要求书中采用的术语“包含”而言,其意图是包含性的并且类似于作为关联词采用在权利要求中时的术语“包括”。

[0100] 就使用在说明书或权利要求书中的术语“或者”而言(例如A或者B),其意图表示“A或者B或者全部二者”。当申请人意图表明“仅有A或者B但是并非全部二者”,则将会使用短语“仅有A或者B但是并非全部二者”。因此,这里使用的术语“或者”是包含性而非排他性的用途。参见Bryan A.Garner的“A Dict ionary of Modern Legal Usage 624”(第2版,1995年)。

[0101] 就这里所使用的短语“A、B和C的其中一项或多项”而言(例如被配置成存储A、B和C的其中一项或多项的数据存储库),其意图传达以下可能性的集合:A、B、C、AB、AC、BC和/或ABC(例如数据存储库可以仅存储A、仅存储B、仅存储C、存储A和B、存储A和C、存储B和C以及/或者存储A和B和C)。其不意图要求其中一个A、其中一个B和其中一个C。当申请人意图表明“至少其中一个A、至少其中一个B和至少其中一个C”时,则将会使用短语“至少其中一个A、至少其中一个B和至少其中一个C”。

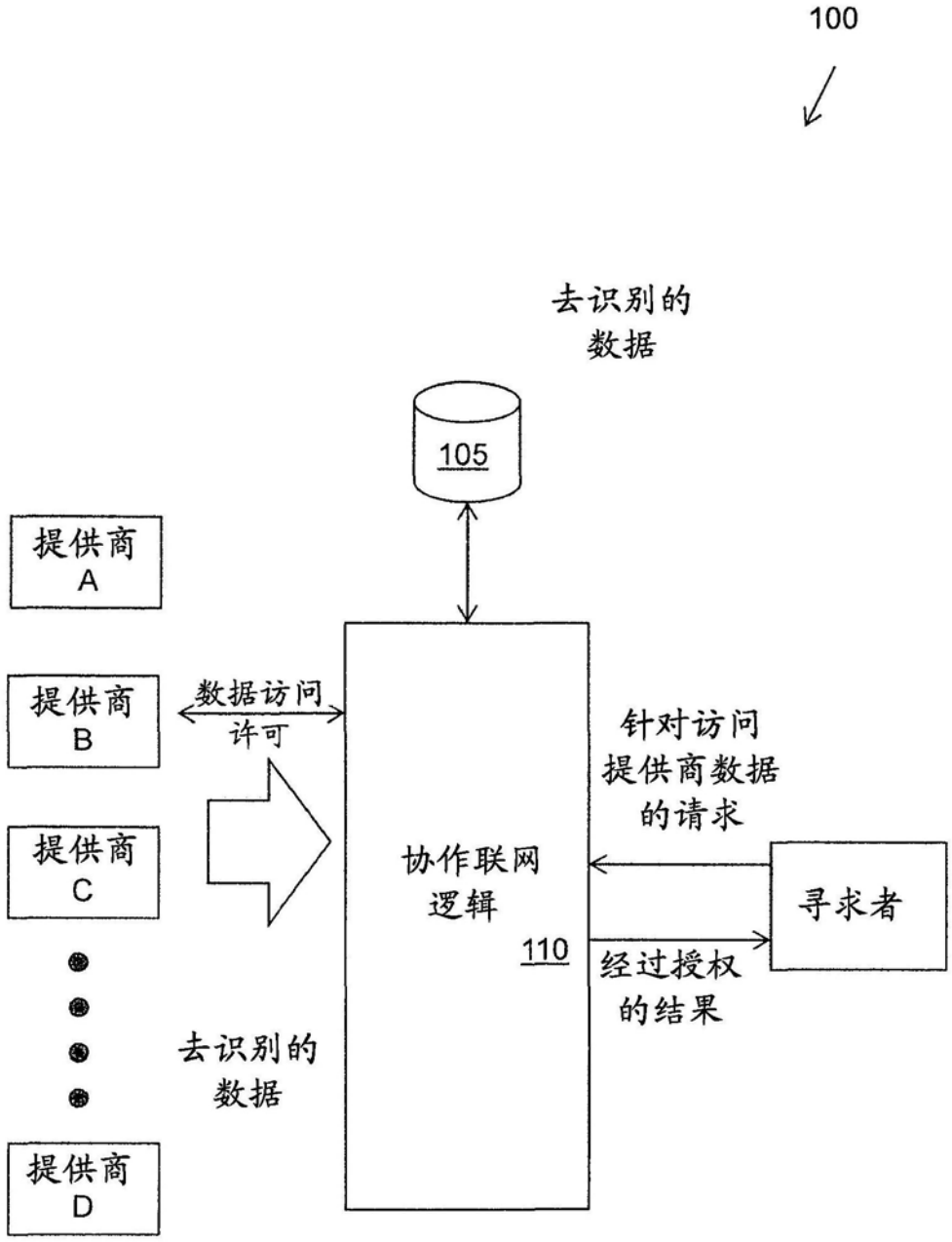

100
去识别的
数据
105
提供商
A
提供商
B
提供商
C
提供商
D
数据访问
许可
协作联网
逻辑
110
针对访问
提供商数据
的请求
寻求者
经过授权
的结果
去识别的
数据

图1

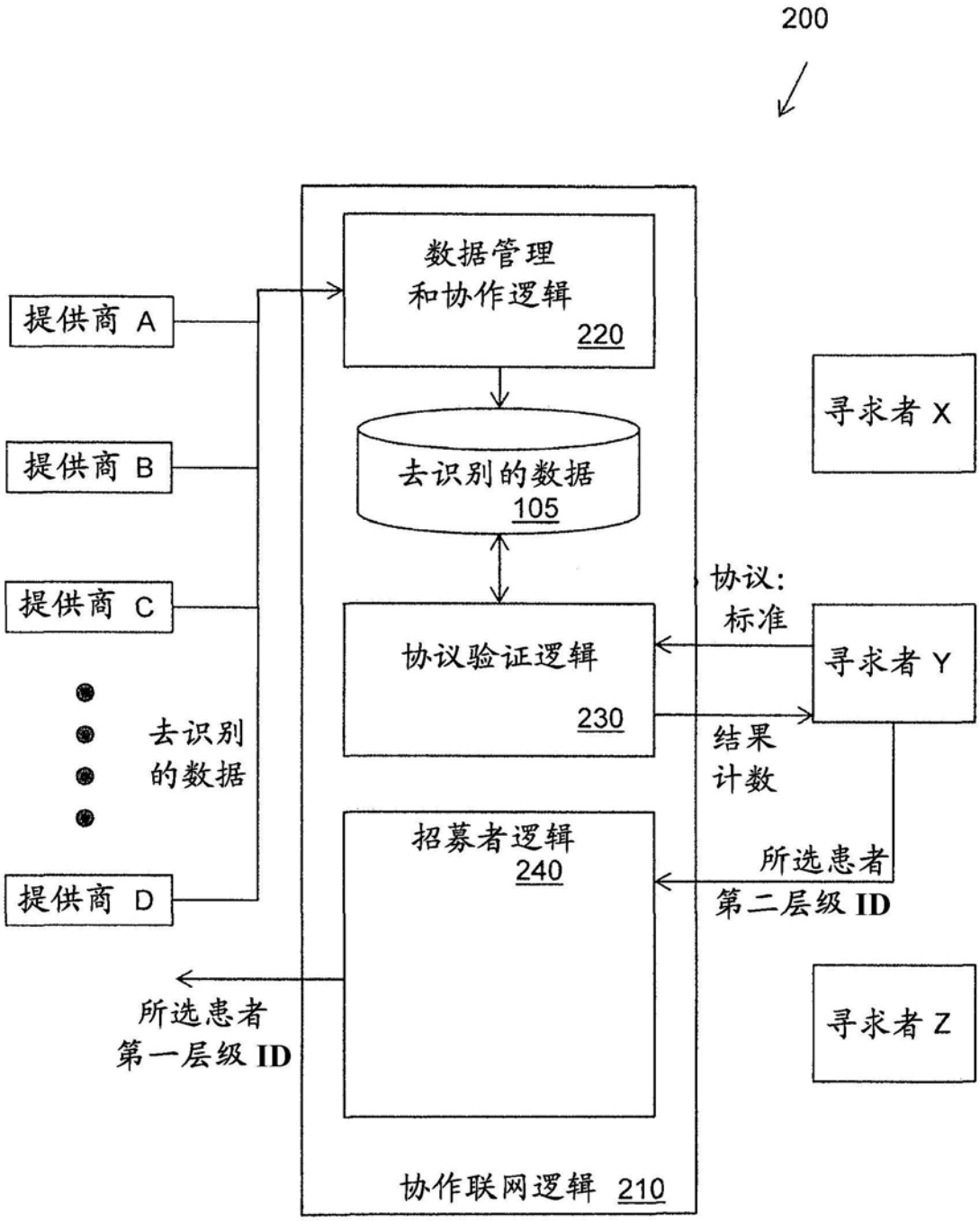

200
数据管理
和协作逻辑
220
提供商 A
提供商 B
提供商 C
提供商 D
去识别
的数据
去识别的数据
105
协议验证逻辑
230
协议:
标准
结果
计数
寻求者 X
寻求者 Y
寻求者 Z
招募者逻辑
240
所选患者
第二层级 ID
所选患者
第一层级 ID
协作联网逻辑 210

图2

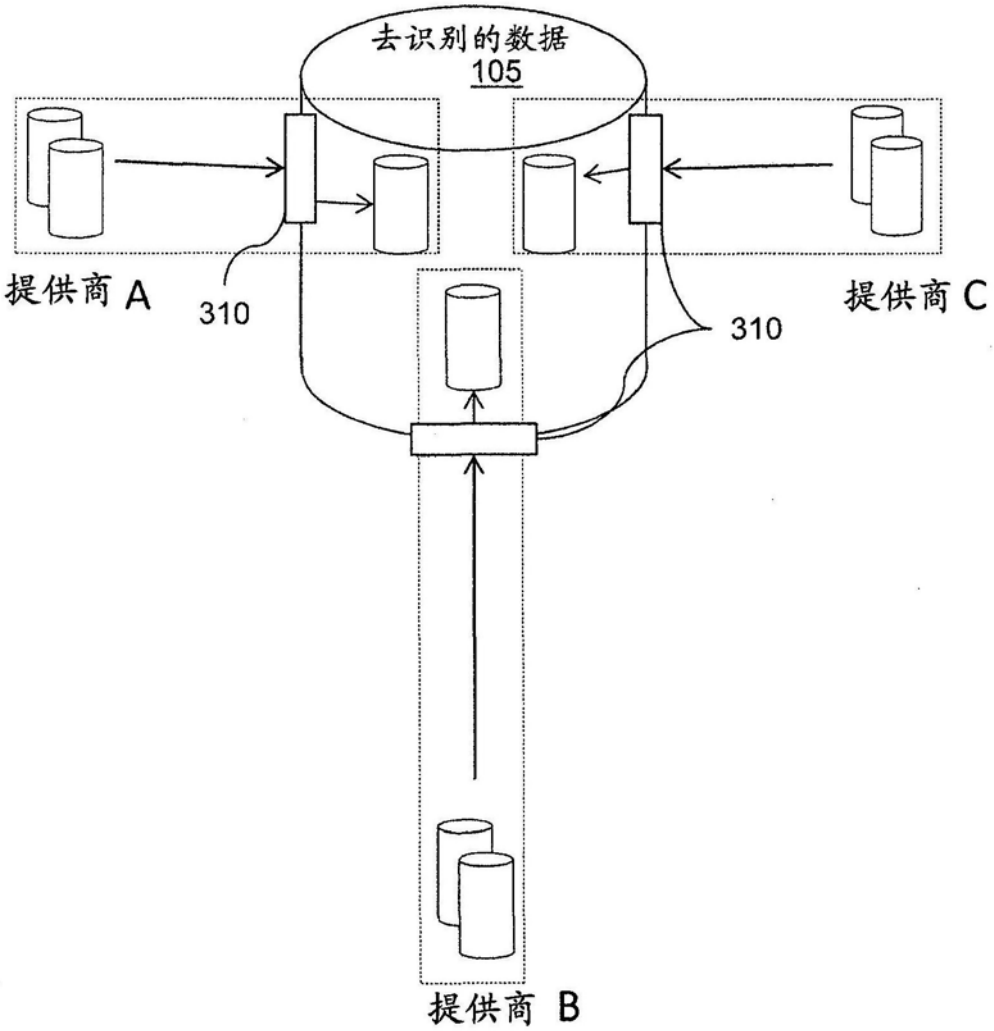


图3

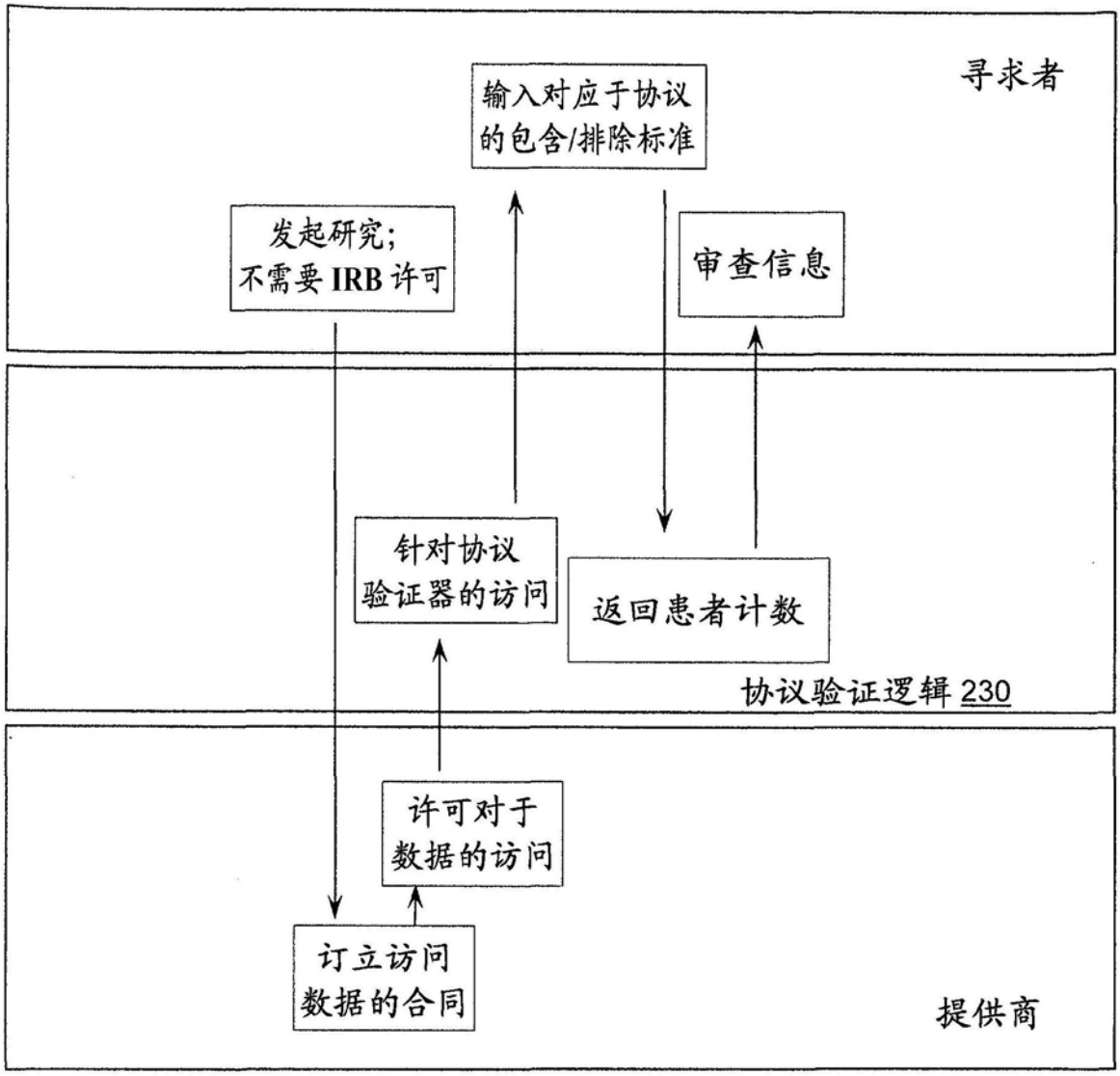

寻求者
输入对应于协议的包含/排除标准
发起研究；不需要 IRB 许可
审查信息
针对协议验证器的访问
返回患者计数
协议验证逻辑 230
许可对于数据的访问
订立访问数据的合同
提供商

图4

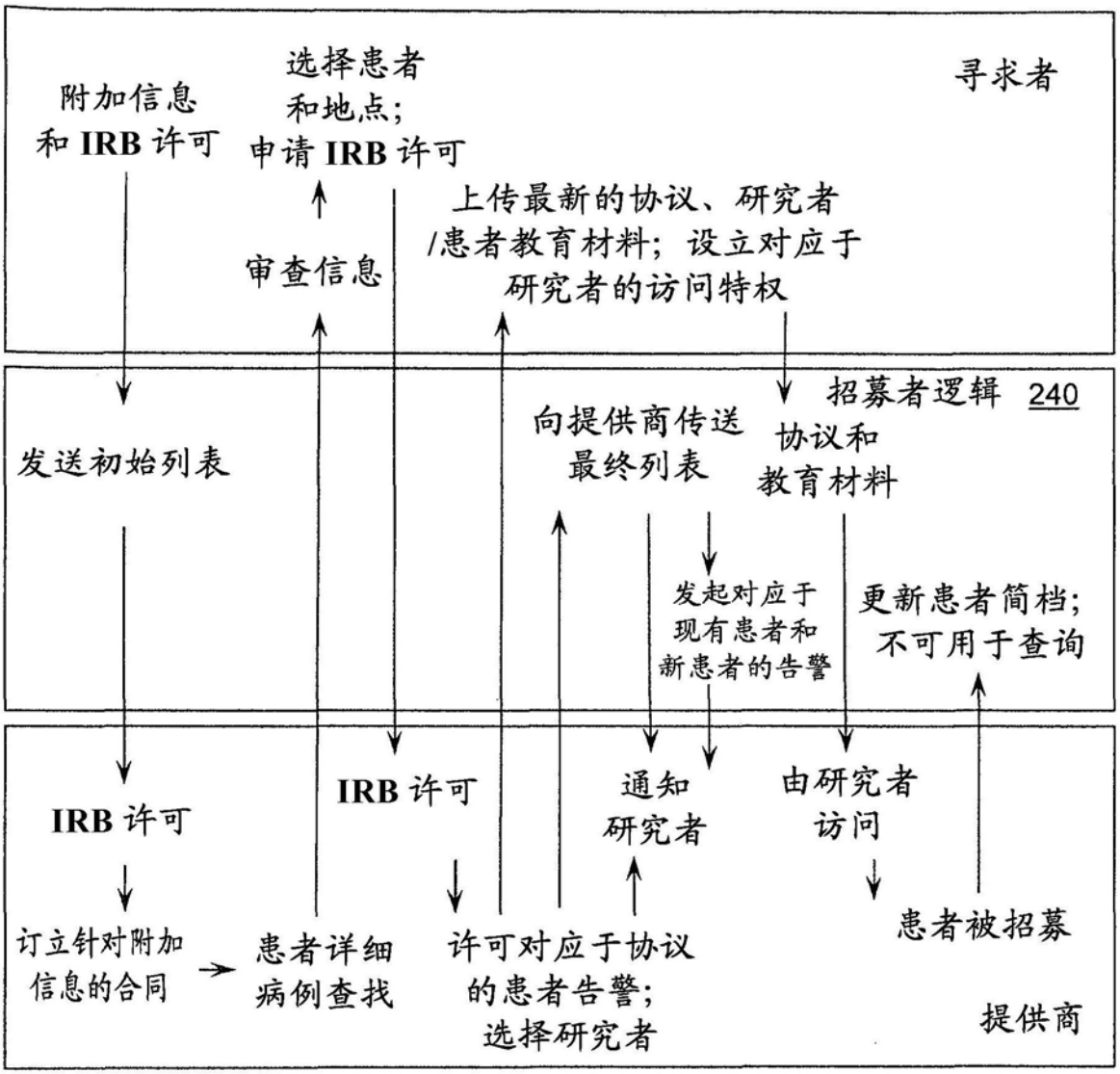

寻求者
附加信息
和 IRB 许可
选择患者
和地点;
申请 IRB 许可
审查信息
上传最新的协议、研究者
/患者教育材料; 设立对应于
研究者的访问特权
招募者逻辑 240
发送初始列表
向提供商传送
最终列表
协议和
教育材料
发起对应于
现有患者和
新患者的告警
更新患者简档;
不可用于查询
IRB 许可
IRB 许可
通知
研究者
由研究者
访问
订立针对附加
信息的合同
患者详细
病例查找
许可对应于协议
的患者告警;
选择研究者
患者被招募
提供商

图5

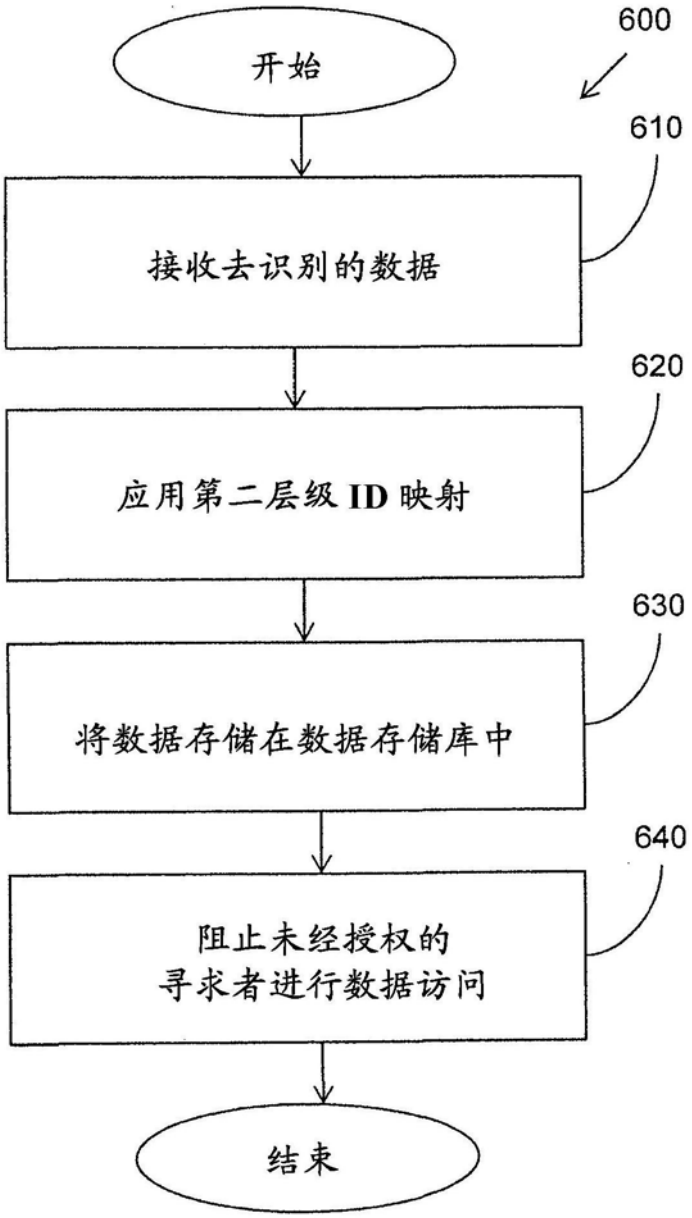

600
开始
610
接收去识别的数据
620
应用第二层级 ID 映射
630
将数据存储在数据存储库中
640
阻止未经授权的
寻求者进行数据访问
结束

图6

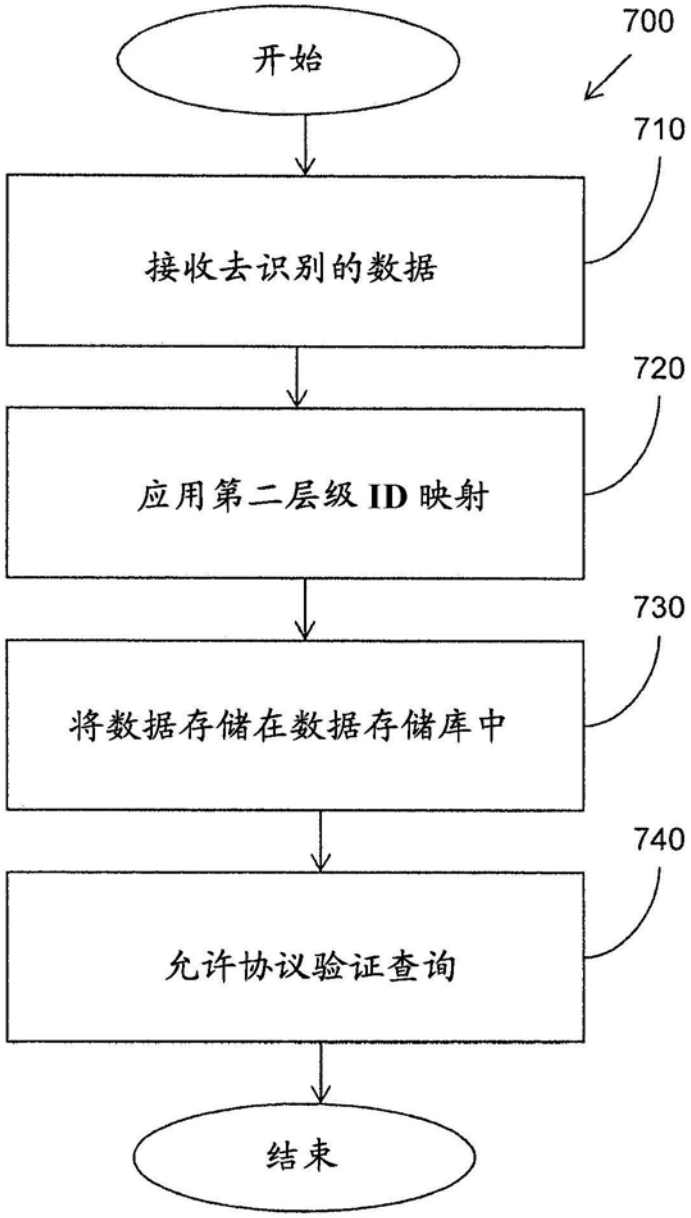

开始
700
710
接收去识别的数据
720
应用第二层级 ID 映射
730
将数据存储在数据存储库中
740
允许协议验证查询
结束

图7

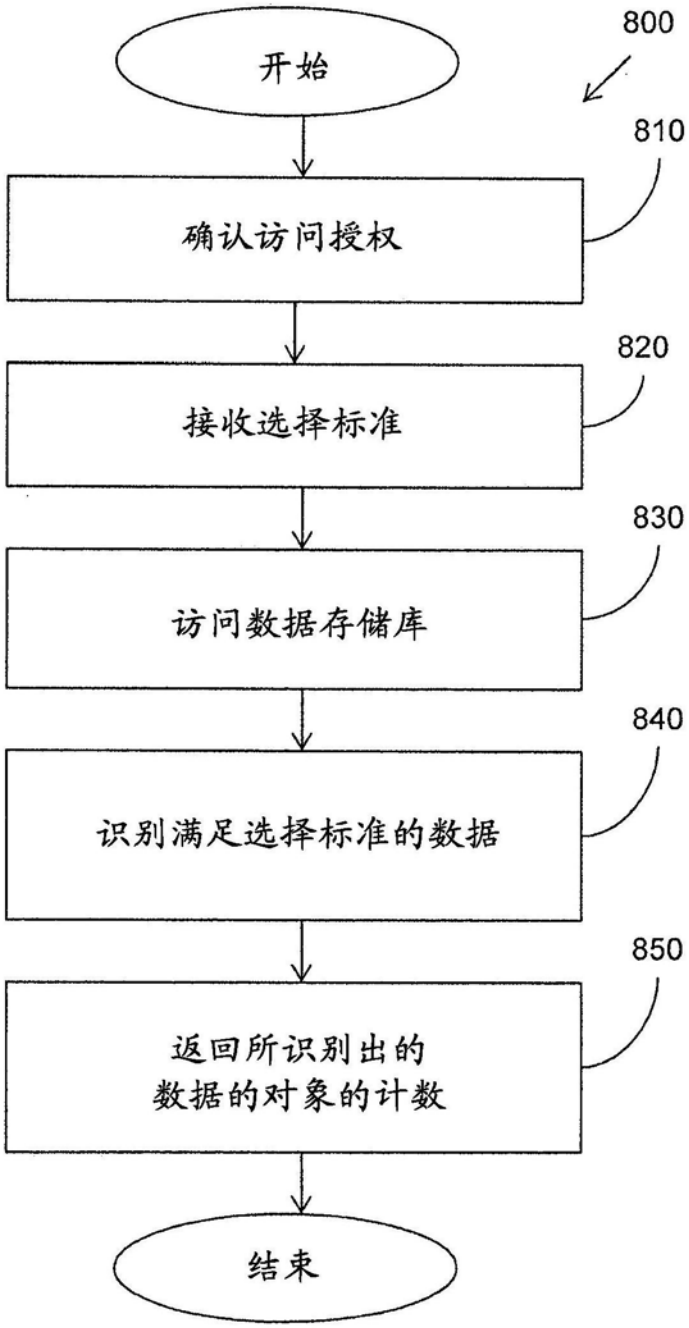

800
开始
810
确认访问授权
820
接收选择标准
830
访问数据存储库
840
识别满足选择标准的数据
850
返回所识别出的
数据的对象的计数
结束

图8

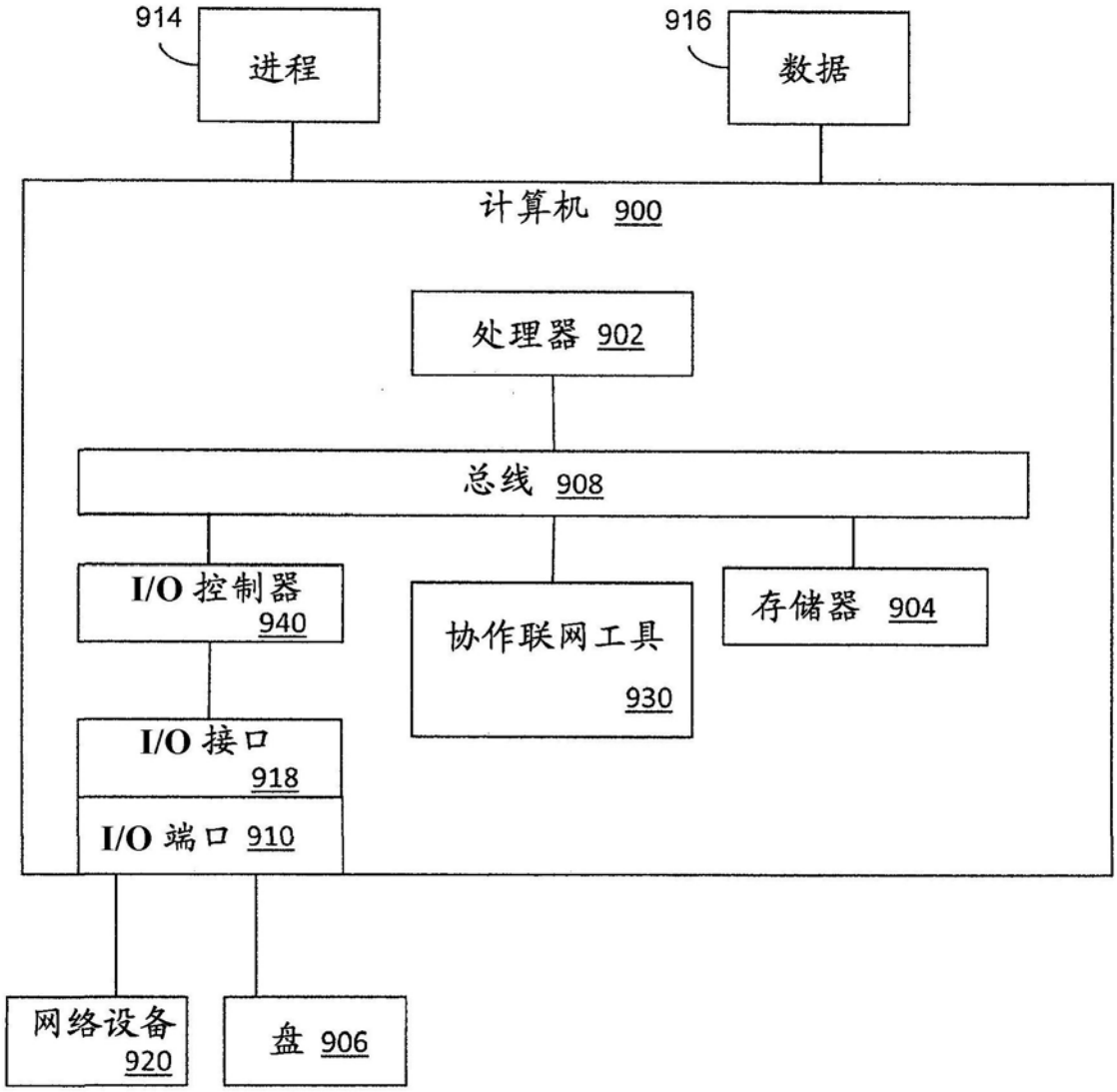

914
进程
916
数据
计算机 900
处理器 902
总线 908
I/O 控制器 940
协作联网工具 930
存储器 904
I/O 接口 918
I/O 端口 910
网络设备 920
盘 906

图9