(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 104063667 B
(45)授权公告日 2018.09.25

(21)申请号 201410106473.X
(22)申请日 2014.03.21
(65)同一申请的已公布的文献号
申请公布号 CN 104063667 A
(43)申请公布日 2014.09.24
(30)优先权数据
13160595.8 2013.03.22 EP
(73)专利权人 霍夫曼-拉罗奇有限公司
地址 瑞士巴塞尔
(72)发明人 A.克纳菲尔
(74)专利代理机构 北京坤瑞律师事务所 11494
代理人 封新琴
(51)Int.Cl.
G06F 21/62(2013.01)
G06F 12/14(2006.01)
(56)对比文件
US 2003145222 A1,2003.07.31,
CN 101673249 A,2010.03.17,
CN 101690102 A,2010.03.31,
CN 202679426 U,2013.01.16,
CN 101911090 A,2010.12.08,
US 2012060008 A1,2012.03.08,
审查员 郭瑞

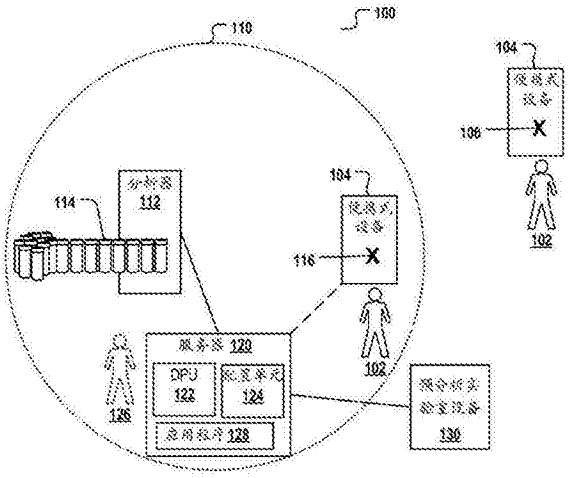
权利要求书3页 说明书10页 附图5页

(54)发明名称

确保敏感数据不可访问的方法和系统

(57)摘要

本公开涉及一种帮助确保尤其包括患者数据的敏感数据不被未授权人员访问的方法和分析系统。所公开的方法和系统有助于防止存储在便携式设备中的敏感数据与便携式设备一起传输至安全范围外的场所。通过确定是否便携式设备位于所述安全范围外并且如果确定便携式设备位于所述安全范围外，则自动删除存储在所述便携式设备中的敏感数据，所公开的方法和系统有助于防止敏感数据对未授权人员公开。



CN 104063667 B

1.一种用于确保存储在便携式设备的存储介质中的敏感数据不被未授权人员访问的方法,所述敏感数据包括患者数据,所述方法包括:

所述便携式设备确定其当前位置;

所述便携式设备确定其当前位置是否处于围绕分析系统的分析器的预定安全范围内;以及

在所述当前位置被确定为处于所述安全范围外的情况下,所述便携式设备自动删除所述存储介质中的所述敏感数据,

其中根据一个或多个规则执行所述删除,所述规则中的至少一个包括基于用户的删除原则,所述方法进一步包括:

所述便携式设备接收用户标识符;以及

执行所述规则,从而将所述用户标识符、所确定的当前位置和所述安全范围作为输入,其中,在所述当前位置被确定为处于所述安全范围外的情况下,基于用户执行所述删除,从而删除的敏感数据的量和/或种类取决于所述用户标识符。

2.根据权利要求1所述的方法,其中,删除所述存储介质中的所述敏感数据包括:

通过格式化所述存储介质或格式化包含所述敏感数据的分区来删除所述敏感数据;或

通过移除所述敏感数据的指示符同时使所述敏感数据保持不变来删除所述敏感数据;或

通过移除所述敏感数据的指示符并且使用自动生成的数据模式重写所述敏感数据来删除所述敏感数据;或

更改或删除解密以加密形式存储在所述存储介质中的所述敏感数据所需的解密密钥。

3.根据权利要求1或2所述的方法,还包括:

所述便携式设备从数据源请求所述敏感数据,其中仅当所述便携式设备的当前位置在提交请求的时刻处于所述安全范围内时,所述便携式设备才请求所述敏感数据,并且所述数据源是预分析实验室设备、分析实验室设备、后置分析实验室设备或实验室信息系统;以及

通过所述便携式设备从所述数据源接收所请求的敏感数据。

4.根据权利要求1或2所述的方法,所述删除包括:

评估包含所述敏感数据的数据集合,并且可选地删除所述敏感数据,同时在所述存储介质上保留所述数据集合中的其余部分。

5.根据权利要求1或2所述的方法,所述删除包括:

在所述存储介质中存储将要删除的所述敏感数据的数据记录的标识符,使得当在将来通过所述便携式设备确定所述便携式设备的当前位置处于所述安全范围内时,能够恢复被删除的数据记录。

6.根据权利要求1或2所述的方法,其中:

所述便携式设备向用户显示实验室设备操作数据;

所述便携式设备基于所述实验室设备操作数据,接收用户经由用户接口输入的控制输入数据;以及

仅在其当前位置处于所述安全范围内的情况下,所述便携式设备根据所输入的控制输入数据向实验室设备提交控制命令。

7.根据权利要求1或2所述的方法，还包括：

当前处于所述安全范围内的所述便携式设备自动确定所述便携式设备和所述安全范围的边界之间的当前距离小于距离阈值；以及

响应于所述确定，经由所述便携式设备的用户接口向用户输出通知，所述通知指示用户将要离开安全范围，并且在用户离开安全范围的情况下，所述敏感数据将被删除。

8.根据权利要求1或2所述的方法，其中，所述便携式设备还对任意以下事件执行所述敏感数据的删除：

当所述便携式设备关机时；

当发生用户从所述便携式设备注销的事件时；

当在所述便携式设备上执行的、实施前述权利要求中任一项所述的方法的应用程序停止时；

当发生用户从所述应用程序注销的事件时；

当收到与所述便携式设备进行交互的用户所触发的删除命令时；以及

当所述便携式设备收到处于所述安全范围内的数据处理系统所提交的删除命令时。

9.根据权利要求1或2所述的方法，其中，不断重复所述当前位置的确定和所述敏感数据是否要被删除的决定。

10.根据权利要求1或2所述的方法，其中，所述确定所述便携式设备的当前位置是否处于所述安全范围内包括：

所述便携式设备访问存储在所述存储介质中或存储在另外的可操作地耦合到所述便携式设备的存储设备中的地理数据，所述地理数据包括指定所述安全范围的位置坐标；以及

确定所确定的当前位置的当前地理坐标是否处于所述安全范围的位置坐标内。

11.根据权利要求1或2所述的方法，其中，所述确定是否要删除所述敏感数据和所述数据删除可通过在所述便携式设备上执行的第一应用程序来实施，所述第一应用程序与数据处理设备上执行的第二应用程序可互操作，所述第一应用程序和所述第二应用程序交互地使用户能够执行以下步骤中的一个或多个：

分析存储在所述便携式设备的存储介质中的敏感数据；和/或

经由所述便携式设备的接口来编辑或删除存储在所述便携式设备的存储介质中的敏感数据的各个数据记录，其中，任何对所述数据记录的修改均被自动传播到中央存储介质并且与存储在中央存储介质中的敏感数据的副本同步；和/或

控制实验室设备以经由所述第一应用程序的图形用户界面，基于呈现给用户的敏感数据，来停止、启动或重新安排患者样本的预分析处理、分析处理或后置分析处理；和/或

监测实验室设备对患者样本执行预分析处理、分析处理或后置分析处理。

12.根据权利要求11所述的方法，其中，以依靠用户标识符或作用标识符和所确定的当前位置的方式来执行所述确定是否要删除敏感数据、所述数据删除、所述监测和/或控制，其中所述依靠可通过由所述第一应用程序执行的规则来实现。

13.根据权利要求1所述的方法，其中，在所述便携式设备处于所述预定安全范围内的同时，将存储在所述便携式设备的存储介质中的敏感数据不断与服务器的另一存储介质同步，从而使得所述便携式设备上的修改的敏感数据能够存储在所述服务器的另一存储介质

中，以便已离开了所述预定安全范围但具有相应权限的用户能够访问修改后的敏感数据。

14.一种包括指令的计算机可读存储介质，当所述指令由便携式设备的处理器执行时，使得所述处理器执行上述权利要求中任何一项所述的方法。

15.一种确保敏感数据不被未授权人员访问的分析系统，所述敏感数据至少包括患者数据，所述分析系统包括至少一个用于分析生物样本的分析器，所述分析系统还包括便携式设备，所述便携式设备包括：

处理器；

其中包含所述敏感数据的存储介质；和

定位装置，可操作用于确定所述便携式设备的当前位置；

应用程序的计算机可解释指令，当所述处理器执行所述指令时，导致所述应用程序执行包括下面步骤的一种方法：

触发所述便携式设备的当前位置的确定；以及

在所述当前位置被确定为处于至少一个分析器周围的安全范围外的情况下，所述便携式设备自动删除所述存储介质中的所述敏感数据，

其中根据一个或多个规则执行所述删除，所述规则中的至少一个包括基于用户的删除原则，所述方法进一步包括：

所述便携式设备接收用户标识符；以及

执行所述规则，从而将所述用户标识符、所确定的当前位置和所述安全范围作为输入，其中，在所述当前位置被确定为处于所述安全范围外的情况下，基于用户执行所述删除，从而删除的敏感数据的量和/或种类取决于所述用户标识符。

16.根据权利要求15所述的分析系统，还包括样本处理系统，其中至少部分敏感数据从所述至少一个分析器收集，所述样本处理系统包括：

数据处理单元，所述数据处理单元处于所述安全范围内且可操作用于经由网络将收集的敏感数据转发到所述便携式设备的所述应用程序；以及

配置单元，用于允许第一用户或第二用户指定所述安全范围的位置坐标和/或配置用户特定的和/或位置特定的规则，以便确定如何执行所述删除。

确保敏感数据不可访问的方法和系统

技术领域

[0001] 本发明涉及生物样本分析系统领域，且更具体地，涉及保护敏感患者数据免受未授权访问的分析系统。

背景技术

[0002] 必须防止对例如由分析系统所产生的、具有已分析的患者生物样本的生物医学测量数据的敏感数据的未授权访问。越来越多的实验人员使用如笔记本电脑、平板电脑和智能手机的便携式处理设备来分析敏感数据和/或管理、监测和控制实验室设备或其他实验室相关的项目和任务。便携式设备可在实验室内不同房间中使用，但亦可被携带出实验室建筑和公司或学校场地，例如在很多情况下便携式设备不仅在工作过程中使用，而且在家中自用。例如当一实验室工作人员乘坐公共交通设施上下班时，这存在便携设备丢失或被盗的风险。因此，对于未授权的第三方，存储在所述便携式设备中的敏感数据变得可访问。

[0003] 具有对于便携式设备的硬件的访问权、且具有特定知识和足够时间的人员能够容易地绕过便携式设备上的如基于密码授权的锁定机制的数据保护措施，。而如基于加密密钥的锁定机制的更安全的锁定机制，可能需要复杂的密钥管理，在使用中往往不切实际。

[0004] US20110191862描述了一种基于请求发送方的位置来限制对所请求数据的访问的系统和方法。所描述的系统和方法要求请求-响应系统被启动和运行。在便携式设备丢失或被盗，以及未授权人员已占有其中包括需要被保护的数据的硬件设备的情况下，所描述的系统和方法不能提供任何保护。

[0005] US7912455B2公开了一种对已在存储清除机制注册的应用程序进行数据保护的方法和系统。注册的应用程序可从存储清除机制接收待处理的存储清除操作的通知。在接收到通知时，注册的应用程序可释放存储或断开存储链接从而实现数据删除。

发明内容

[0006] 本发明的目的在于提供一种用于保护存储在便携式设备中的敏感患者数据的改进的分析系统和方法。该目的由独立权利要求的特征来解决。在从属权利要求中给出了本发明的优选实施例。除非另有说明，否则本发明的实施例可自由地相互组合。

[0007] 本文中所用的“用户”是由唯一地指派给用户的用户ID来表示和识别的一个人。用户可在程序逻辑(program logic)处登记，所述程序逻辑是实验室的IT基础构造的一部分。

[0008] 本文中所用的“生物样本”或“样本”是在实验室分析过程中或预分析处理和后置分析处理中所用的一些生物材料，如血、尿、唾液、组织切片等。

[0009] 本文中所用的术语“分析器”或“分析实验室设备”包括任何能够导致生物样本与试剂发生反应而获得测量值的设备或设备组件。分析器可操作用于通过各种化学、生物、物理、光学或其他技术程序来确定样本的参数值或其组分。分析器可用于测量样本或至少一种分析物的参数，并返回所得到的测量值。由分析器返回的可能分析结果的列表包括但不限于样本中分析物的浓度、表明样本中分析物的存在的数字结果(是或否)(对应浓度高于

可检测浓度)、光学参数,DNA或RNA序列、和从蛋白质或代谢产物的质谱分析获得的数据和各种物理或化学参数。如本文所用的术语“分析器”还包括显微镜和任何其他类型的可操作用于从样本中获得指示某一生理、生化、或诊断相关特征的数据的实验室设备。

[0010] “预分析实验室设备”是可操作用于对一个或多个生物样本执行一个或多个预分析处理步骤,从而为一个或多个后续的分析测试制备样本的实验室设备。预分析处理步骤可以是,例如,离心步骤、封盖、开盖、或重新封盖工序,等分(aliquotation)步骤,将缓冲剂添加至样本的步骤等等。

[0011] “后置分析实验室设备”是可操作以自动地处理和/或存储一个或多个后置分析的生物样本的实验室设备。后置分析处理步骤可包括重新封盖步骤、从分析器卸载样本的步骤或将样本输送至存储单元或用于收集生物废物的单元的步骤。

[0012] 本文中所用的“分析系统”包括一个或多个分析器。此外,它可以包括一个或多个预分析实验室设备和/或后置分析实验室设备。分析系统可包括一个或多个控制单元,可操作用于监视和/或控制分析器和/或预分析实验室设备和/或后置分析实验室设备的性能。控制单元可操作用于评估和/或处理收集的分析数据,控制样本到分析器和/或从分析器的加载、存储和/或卸载,初始化分析系统的分析操作或硬件操作或软件操作,以便制备用于分析的样本、样本管或试剂等等。一个或多个控制单元可被实现为或包括安装在一个或多个便携式设备上的应用程序,其中便携式设备不论其当前位置均被认为是分析系统的一部分。

[0013] 本文中所用术语“敏感数据”包括通过其能够识别患者的患者数据。患者数据可包括患者姓名、生日、地址或部分地址、和/或患者标识符(如社会安全号码或医疗保险号码、患者的医疗记录标识符、电子邮件地址或其他独特标识符)。此外,敏感数据可包括医疗和/或技术数据,例如与患者相关的实验室设备操作数据和/或测量数据。测量数据可通过处理患者的生物样本来获得。测量数据同样可以是图像数据,如X-射线图像或NMR图像,染色的组织切片的图像等等。敏感数据可进一步包括测量值,但也可包括先前或目前的诊断和治疗信息、患者地址信息、患者ID等等。实验室设备操作数据指示实验室设备的类型、运行状态和/或性能。例如,实验室设备操作数据可包括每次处理的样本的号码,错误统计和指示分析质量的参数。实验室设备操作数据可以指示实验室设备的试剂或消耗品是否用完了或实验室设备由于技术错误而停滞。

[0014] “规则”是计算机可解释的指令的集合,指令包括至少一个动作,并包括一个或多个条件,其中至少一个动作的执行取决于关于一个或多个输入值对一个或多个条件的评估。执行规则意味着基于输入值来评估条件和基于评估结果来执行至少一个动作。

[0015] 本文中所用的“便携式设备”是可被人便携的任何数据处理设备。例如,便携式设备可以是笔记本、平板电脑、移动电话,尤其是智能电话等等。

[0016] 术语“生物样本”包括来源于人类或其它任何生物体的任何种类的组织或体液。特别地,生物样本可以是全血、血清、血浆、尿液、脑脊髓液、或唾液样本或其任何衍生物。

[0017] “安全范围”是一个地理和/或空间区域,其范围存储在便携式设备的存储介质中或便携式设备可访问的存储介质中,在数据安全性方面,其被认为是受保护的区域。安全范围包围分析系统的分析器,并且包括分析器周围的预定义区域。由安全范围所限定的区域可具有任何形状或大小,并且取决于分析器的实施例和位置,其可具有精确定义或粗略定

义的范围。取决于实施例，安全范围可被指定为一个有预定义的圆心和半径的圆、一个或多个建筑物的组群、建筑物内的一个或多个房间等等。特别地，安全范围可以是围绕实验室、大学、医院等的建筑物的区域。例如，可以通过GPS坐标或发送信号(例如发送信号通过位于分析器内的设备或靠近分析器的设备来发送)的范围来定义安全范围，其中，所述便携式设备丢失信号指示已超出安全范围。或者，安全范围可以由提供指示已超出安全范围的信号到便携式设备的发射器来限定。这样的发射器可以是处于围绕分析器的一个或多个房间中的发射器，从而当离开分析器的附近时一个携带便携式设备的人必须通过发射器。

[0018] 在一方面，本发明涉及一种用于确保存储在便携式设备的存储介质中的敏感数据不被未授权人员访问的方法。敏感数据包括患者数据。便携式设备确定其当前位置，并确定其当前位置是否处于预定安全范围内。定义预定义的安全参数使得安全范围围绕分析系统的分析器。如果确定当前位置处于安全范围外，则便携式设备自动删除存储介质中的敏感数据。

[0019] 上述特征可确保万一便携式设备丢失或被盗并移至安全范围外，基于定位的触发机构能主动删除存储介质中的敏感数据，从而排除能够接触到硬件设备的未授权用户破解不足的保护措施、并访问敏感数据的可能性。

[0020] 取决于实施例，当前位置可以是地理位置(Geoposition)，例如GPS(地理定位服务)坐标。同样地，当前位置可以是相对于给定地图的基本元素或相对于坐标系的任何种类的设备位置指示符。当前位置也可以是房间号码和/或建筑物号码、部门或实验室的标识符等等。

[0021] 根据实施例，所述方法进一步包括：分析器分析患者的一种或多种生物样本，从而生成分析测量数据。分析测量数据经由网络从分析器传送到便携式设备。便携式设备关联患者的敏感数据来存储分析测量数据，其中的生物样本取自患者，而患者由包含在敏感数据中的患者数据确定。便携式设备的用户可评估患者的分析测量数据，并且使用评估以提交命令，命令用于监测和/或控制从便携式设备到分析系统的进一步的预分析样本处理步骤、分析样本处理步骤或后置分析样本处理步骤。

[0022] 根据一些实施例，根据一个或多个规则来执行删除。规则可存储在，例如，便携式设备的存储设备上，或者可存储在中央服务器上，且必要时动态地从服务器检索。规则中的至少一个包括基于用户的删除原则。便携式设备接收用户标识符。例如，当用户登录到便携式设备或登录到便携式设备上运行的应用程序并执行上述方法时，可接收到标识符，在此也称为“用户ID”。便携式设备执行规则，从而将用户标识符、所确定的当前位置和安全范围作为输入。用户ID可用于选择某些用户特定的规则。在当前位置被确定为处于安全范围外的情况下，基于用户执行删除，从而删除的敏感数据的量和/或种类取决于用户标识符。例如可以通过编译的程序代码或程序脚本的形式来实施规则。规则可被实现为在便携式设备上执行的应用程序的一部分。

[0023] 根据一些实施例，每个用户都分配了一个角色和对应的角色ID。至少部分规则是角色特定的，并实施角色特定的删除政策。根据实施例，按照ASTM标准(American Society for Testing and Materials)E1986-09和/或ISO标准，例如ISO/TS22600-1:2006，ISO/TS22600-2:2006，ISO/DIS22600-2，ISO/TS22600-3:2009和ISO/DIS22600-3来实施角色和相应的规则。

[0024] 根据一些实施例，便携式设备的存储介质为非易失性存储介质。这样可具有的优点是，在发生电源故障期间，假如便携式设备没有移出安全范围外，数据可以很容易地从非易失性存储介质恢复。

[0025] 根据其它实施例，存储介质为易失性存储介质。敏感数据永远不会保存到非易失性存储介质中。这样可进一步提高安全性，并加快删除敏感数据的过程。

[0026] 根据更进一步的实施例，存储介质包括易失性存储介质和非易失性存储介质，其中分别存储有敏感数据或部分敏感数据。删除敏感数据包括从易失性存储介质中删除敏感数据和从非易失性存储介质中删除敏感数据。对这两种存储介质的删除策略可以不同。根据实施例，易失性存储介质是便携式设备的主存储器，而非易失性存储介质是硬盘，例如电磁存储设备。

[0027] 根据一些实施例，从存储介质中删除敏感数据包括：

[0028] 通过格式化存储介质或格式化包含敏感数据的分区来删除敏感数据；这可对于特别节省的删除过程提供；或

[0029] 通过移除敏感数据的指示符同时使敏感数据保持不变来删除敏感数据；这可对于特别快速的删除过程提供；或

[0030] 通过移除敏感数据的指示符并且使用自动生成的数据模式重写敏感数据来删除敏感数据；自动生成的数据模式可以是，例如，随机数据模式；这可在执行一次或多次重写后对于特别节省的删除过程提供，可能仍包含在原先存储的敏感数据的物理存储块中的任何信息将被删除；或

[0031] 更改或删除解密以加密形式存储在存储介质中的敏感数据所需的解密密钥。这可对于快速和安全的数据删除方式提供。

[0032] 在一些实施例中，可以组合多个删除策略，例如可删除解密密钥以及可另外格式化存储介质。

[0033] 根据一些实施例，便携式设备从数据源请求敏感数据。数据源可以是实验室设备，例如，数据源是预分析实验室设备、分析实验室设备、后置分析实验室设备或实验室信息系统(LIS，Laboratory Information System)。仅当其当前位置在提交请求的那一刻就处于安全范围内时，便携式设备才请求敏感数据。然后，便携式设备从数据源接收所请求的敏感数据。便携式设备处于安全范围内来接收数据的要求可增加安全性，因为确保了数据传输也在安全区域中执行。

[0034] 实验室设备或主持LIS的服务器可处于安全范围外或安全范围内，并且可包括使能便携式设备能够与实验室设备进行数据交换的接口。此外，或者可选地，实验室设备和实验室信息系统LIS可从便携式设备接收数据管理命令、设备管理命令和/或控制命令。

[0035] 敏感数据或部分敏感数据，例如测量数据，可首先从收集数据的实验室设备传送至数据处理设备，数据处理设备通常是作为实验室信息系统LIS的一部分的计算机。数据处理设备可充当用于多个其他计算机和/或实验室的实验室设备的信息枢纽，和/或充当用于接收定向到实验室设备的控制命令的通用接口。数据处理设备可收集测量数据，监测从实验室设备接收的数据和/或状态信息。可通过网络，例如实验室内联网，执行传送，或者可通过便携数据载体，例如U盘，执行传送。数据处理设备可将数据作为敏感数据发送至安全范围内的请求便携式设备。附加地或者可选地，数据处理设备可接收控制命令，向便携式设备

请求进一步的敏感数据等等，并且使用接收到的命令来控制数据处理操作和/或控制实验室设备的操作。

[0036] 根据一些实施例，删除包括评估包含敏感数据的数据集合。删除可包括可选地删除敏感数据，同时在存储介质上保留数据集中的其余部分(例如，不能识别相应患者的患者病历标识符、与实验室设备和试剂相关的标识符和统计数据、警示消息等等)。此外，或可选地，该方法可包括存储或继续存储存储介质中的将要删除的敏感数据的数据记录标识符。存储或继续存储以下面的方式执行：使得当在将来通过便携式设备确定便携式设备的当前位置处于安全范围内时，被删除的数据记录能够恢复。该方法还可包括便携式设备确定其当前位置再次处于安全范围内，并且基于未删除的记录标记符恢复被删除的数据记录。可通过从便携式设备到用作数据源的数据处理设备，例如实验室信息系统LIS的数据库服务器，发送包含记录标识符的请求，并经由记录标识符从数据源检索各个记录，来恢复数据记录。这有利于各数据记录的重建，并且可在便携式设备上不留下任何敏感数据的前提下加速数据记录的重新加载。

[0037] 在其它实施例中，删除可包括删除一个数据集合中的所有数据，或者存在恢复被删除的数据的可能，或者不存在恢复被删除的数据的可能。

[0038] 根据一些实施例，便携式设备向用户显示实验室设备操作数据，并接收用户通过用户接口输入的控制输入数据。用户接口可以是键盘、麦克风、触摸屏等等。基于所显示的实验室设备操作数据来输入控制输入数据当接收到输入数据时，仅在其当前位置处于安全范围内的情况下，便携式设备根据所输入的控制输入数据向实验室设备提交控制命令。

[0039] 根据一些实施例，基于用户在便携式设备上的一些操作，便携式设备继续交互地请求和从数据源接收进一步的敏感数据。交互式请求-响应操作可由数据源托管的服务器程序和便携式设备上运行的客户端程序来执行。当便携式设备的当前位置被确定为处于安全范围内时，便携式设备的应用程序就在存储介质中存储所接收的敏感数据。当确定当前位置处于安全范围外时，应用程序将删除敏感数据。

[0040] 根据一些实施例，当携带便携式设备的用户正接近安全范围的边界，例如当一个工作日结束离开实验室时，目前处于安全范围内的便携式设备可自动确定便携式设备和安全范围的边界之间的当前距离小于距离阈值。响应于确定，便携式设备经由便携式设备的用户接口向用户输出通知。通知指示用户将要离开安全范围，此情况下，敏感数据将被删除。因此，在用户正通过便携式设备使用敏感数据工作并将要意外地离开安全范围的情况下，用户可以立即停止运动。这样可以防止由于意外踏出安全范围而导致的数据丢失。接口可以是图形界面、声接口等等。

[0041] 根据一些实施例，便携式设备还对任一以下事件执行敏感数据的删除：当便携式设备关机时；当发生用户从便携式设备注销的事件时；当在便携式设备上执行的、实施前述实施例任一的方法的应用程序停止时；当发生用户从应用程序注销的事件时；当收到与便携式设备进行交互的用户所触发的删除命令时；以及当便携式设备收到处于安全范围内的数据处理系统所提交的删除命令时。

[0042] 根据实施例，当前位置的确定和敏感数据是否要被删除的决定不断重复，例如在固定的时间间隔。此外，基于位置的删除可在接收到用户操作时执行，例如点击按键，以及沿着任何便携式设备的轴的加速等等。

[0043] 根据一些实施例，确定便携式设备的当前位置是否处于安全范围内包括：便携式设备访问存储在存储介质中或存储在另外的可操作地耦合到便携式设备的存储设备中的地理数据。地理数据包括指定安全范围的位置坐标，如GPS数据，一个或多个房间的ID和/或建筑物的ID等等；然后，便携式设备确定所确定的便携式设备的当前位置的当前理坐标是否处于安全范围的位置坐标内。根据一些实施例，位置坐标指定的安全范围可以被用户编辑或操作，例如通过图形用户界面，以方便安全范围的边界的重新定义。

[0044] 确定是否要删除敏感数据和数据删除可通过在便携式设备上执行的第一应用程序来实施。便携式设备可以是移动电话，而应用程序可以是一个所谓的“应用”。应用可被实现为本地应用，其中数据从未存储或高速缓存到便携式设备的存储介质中，除非执行应用的显式存储功能。可替代地，应用被实现为经由网络执行数据处理设备上运行的第二应用程序所提供的网络应用的网络浏览器。数据处理设备可以是一台中央服务器或多个实验室设备之一。通常，浏览器会缓存所有接收到的数据，当执行敏感数据的删除时，缓存即被清空。

[0045] 第一应用程序与数据处理设备上执行的第二应用程序可互操作。数据处理设备可处于安全范围内或安全范围外。

[0046] 第一应用程序和第二应用程序交互地使用户能够执行以下步骤中的一个或多个：

[0047] 分析存储在便携式设备的存储介质中的敏感数据；和/或

[0048] 经由便携式设备的接口来编辑或删除存储在便携式设备的存储介质中的敏感数据的各个数据记录；任何对数据记录的修改均被自动传播到中央存储介质并且与存储在中央存储介质中的敏感数据的副本同步；中央存储介质可以是实验室信息系统LIS的一部分，并且便携式设备可远程访问中央存储介质；和/或

[0049] 控制实验室设备以经由第一应用程序的图形用户界面，基于呈现给用户的敏感数据，来停止、启动或重新安排患者样本的预分析处理、分析处理或后置分析处理；和/或

[0050] 监测实验室设备对患者样本执行预分析处理、分析处理或后置分析处理。

[0051] 托管第二应用程序的数据处理设备可以是实验室信息系统LIS的计算机、实验室设备的处理器、设备控制计算机等等。数据处理设备也可作为或可包括提供敏感数据到便携式设备的数据源。数据处理设备可包括或可操作地耦合到中央存储介质。

[0052] 根据一些实施例，以依靠用户标识符和依靠所确定的当前位置的方式来执行确定是否要删除敏感数据、数据删除、监测和/或控制，其中依靠可通过由第一应用程序执行的规则来实现。

[0053] 在另一个方面，本发明涉及包括指令的计算机可读存储介质，当指令由便携式设备的处理器执行时，其促使处理器执行上述实施例中任何一个的方法。

[0054] 在另一个方面，本发明涉及一种分析系统，系统确保敏感数据不被未授权人员访问。敏感数据至少包括患者数据。分析系统包括至少一个用于分析生物样本的分析器和便携式设备。便携式设备包括处理器和其中包含敏感数据的存储介质。便携式设备还包括定位装置，可操作用于确定便携式设备的当前位置。定位装置设备可被实现为GPS传感器、本地定位系统(Local Positioning System,LPS)模块等等。便携式设备还包括应用程序的计算机可解释指令，当处理器执行指令时，使得应用程序执行包括下面步骤的一种方法：触发便携式设备的当前位置的确定；以及在当前位置被确定为处于安全范围外的情况下，便携

式设备自动删除存储介质中的敏感数据。

[0055] 取决于实施例，分析器可处于安全范围的中心或安全范围内的任何其它区域。

[0056] 根据一些实施方例，定位装置是由便携式设备的制造商提供的定位服务。例如，便携式设备可以是移动电话，而定位服务可由移动电话的制造商提供为内置硬件功能。

[0057] 根据一些实施例，分析系统进一步包括一个或多个附加的样本处理实验室设备，例如预分析实验室设备和/或后置分析实验室设备。附加的样本处理实验室设备可处于安全范围内或安全范围外。所述附加的实验室设备可被用于收集来自患者生物样本的附加敏感数据，并从分析系统发送敏感数据到便携式设备。附加收集的敏感数据可以是测量数据。

[0058] 样本处理系统还可包括：

[0059] 数据处理单元，可操作用于经由网络将收集的敏感数据转发到便携式设备的应用程序；根据一些实施例，数据处理单元可以是分析器的一部分或附加的实验室设备，从而使得分析器或附加实验室设备可用作数据源和直接将敏感数据转发到便携式设备；

[0060] 配置单元，用于允许第一用户或第二用户指定安全范围的位置坐标和/或配置用户特定的和/或位置特定的规则，以便确定如何执行删除。配置单元可以是便携式设备的一部分，和/或可经由网络连接到便携式设备的数据处理设备主持。

[0061] 可有实验室的操作员远程地或由便携式设备的用户经由便携式设备的接口执行配置。配置可要求用户或操作者在LIS和/或在便携式设备上运行的应用程序授权。优选地，如果便携式设备位于安全范围外，则通过便携式设备禁止经由便携式设备的接口的配置。

附图说明

[0062] 下面通过参考附图仅以示例方式更详细地解释本发明的实施例，其中：

[0063] 图1示出了包括便携式设备、服务器、分析器和其他实验室设备的分析系统；

[0064] 图2为便携式设备的框图；

[0065] 图3为由便携式设备执行的方法的流程图；

[0066] 图4示出了相互对接的两个应用程序的方框图；

[0067] 图5描述了移动至安全区外的便携式设备；以及

[0068] 图6描述了所述移动的过程图。

具体实施方式

[0069] 图1示出了分布式分析系统100，分析系统用于确保存储在用户102的便携式设备104的存储介质中的敏感数据不被未授权人员访问。通过当用户102离开安全范围110时便携式设备从其存储介质中自动删除敏感数据来确保存储在用户102的便携式设备104的存储介质中的敏感数据不被未授权人员访问。安全范围在此被视为地理区域，在安全范围内存储在便携式设备上的敏感数据被认为是安全的。

[0070] 系统包括具有数据处理单元122和配置单元124的服务器120。服务器还包括应用程序128，应用程序128与便携式设备上运行的应用程序相对接。操作员126可使用配置单元来配置一些规则，所述规则存储在服务器中或便携式设备中，且用于执行数据删除。

[0071] 系统100还包括分析器112，所述分析器112可操作来分析一个或多个患者的某些生物样本114。分析器收集的测量数据被传送到服务器。生物样本可已被预分析实验室设备

130准备好以便分析，所述预分析实验室设备130还可向到服务器120发送一些患者相关数据。服务器可从处于安全范围内（如分析器）或安全范围外（如预分析实验室设备）的一个或多个实验室设备收集敏感数据。然后，服务器可将收集的敏感数据传送至便携式设备104，以便使得例如护士或其他医疗专业人员或技术人员的用户102能够评估敏感数据和/或监视或控制正在进行的预分析、分析或后置分析样本处理。数据传输可经由移动电话连接来执行。服务器120或者用作数据源的任何实验室设备优先驻留在安全范围110内或在另一个保护区域内，以自始保护敏感数据。在其它实施例中，用作数据源的一个或多个实验室设备可直接与便携式设备连接。

[0072] 在两个不同的位置116、106描述携带便携式设备104的用户102。当便携式设备通过其定位单元确定其当前位置116处于安全范围110内时，将敏感数据从服务器传送到便携式设备，以便至少暂时在便携式设备的存储介质中存储敏感数据，以使得用户102能够评估敏感数据。当便携式设备确定其当前位置106处于安全范围外时，便携式设备自动删除存储在其存储介质中的敏感数据。

[0073] 图2示出了便携式设备104及其组件的框图。便携式设备包括用于确定其当前位置的定位单元218（此处为GPS传感器）。便携式设备包括处理器204和主存储器206。已由用户102输入到便携式设备的敏感数据210和/或已接收到的来自服务器120的敏感数据210被存储在主存储器中。此外，所描述的便携式设备的实施例包括包含敏感数据210或其部分的副本的非易失性存储介质208。存储介质208也可包括一些规则212，所述规则212用于在定位单元218确定便携式设备处于安全范围外的情况下，删除主存储器和/或非易失性存储介质208中的敏感数据210。配置模块214使得用户能够经由便携式设备104的用户接口来配置存储在便携式设备中的规则和/或安全范围的边界。附加地或可选地，规则和/或安全范围的边界可由分析系统的操作员126远程配置。

[0074] 应用程序216可操作来执行用于基于从定位单元218接收的输入来删除敏感数据的规则。应用程序216可以能够从用户102接收用户标识符，以便将用户ID作为输入提供至规则212，并以用户特定的方式执行规则。例如，某些用户可被认为是特别值得信赖的和可靠的，在此情况下，数据删除可被限制至敏感数据的特定的敏感子集。

[0075] 图3示出了根据实施例的由便携式设备执行的用于确保在便携式设备104的存储介质206、208中存储的敏感数据不被未授权人员访问的方法的流程图。在步骤302中，便携式设备确定其当前位置。在步骤304中，便携式设备确定其当前位置处于围绕分析系统的分析器的预定安全范围内。确定可通过例如由便携式设备的当前位置与指定安全范围的位置坐标的集合进行比较来完成。位置坐标的集合可具有地理地图的形式。在便携式设备的当前位置已被确定为处于安全范围外的情况下，在步骤306中，便携式设备，例如通过执行一些规则212，删除存储介质中的敏感数据。

[0076] 图4示出了根据另一实施例，服务器120和便携式设备104的一些部件。应用程序216包括接口408.b，所述接口408.b用于从由服务器120运行的服务器应用程序128接收敏感数据，所述服务器120包括对应的接口408.a。应用程序216和128可交互操作用于从用作数据源的服务器传送敏感数据到便携式设备。因此，应用程序128可用作服务器应用程序，而应用程序216可用作相应的客户端应用程序。如在图6中更详细地描述的，两个应用程序都可交换请求和各个响应。

[0077] 图5示出了单个便携式设备104位于三个不同位置，即在安全范围110内，在安全范围110边界上，以及在安全范围110外。便携式设备包括定位服务502形式的定位单元，所述定位服务502可被应用程序216调用以便于确定便携式设备的当前位置。在接收到应用程序216的调用时，定位服务执行定位模块218并将当前位置返回到应用程序216。应用程序216有权访问预定义的和优选地可配置的指定安全范围110的边界的位置坐标的集合。位置坐标可被存储在便携式设备的内部存储介质中或便携式设备可访问的外部存储介质中。通过比较当前位置与安全范围的所述位置坐标，应用程序216将确定其目前正处于安全范围内，敏感数据210可存储或继续存储在存储介质504中，而没有任何安全风险。存储介质504可以是易失性存储介质或非易失性存储介质或两者的组合。

[0078] 箭头508指示便携式设备的用户接近安全范围的边界。应用程序216可定期调用定位服务502，如每一秒。通过比较便携式设备的当前位置和安全范围的位置坐标，应用程序可确定便携式设备是否小于预定义的、可配置的距离安全范围边界的最小距离。这种情况下，应用程序216向用户102输出通知512，如果用户继续接近安全范围的边界，存储介质504的敏感数据210将被删除。例如，安全范围可以是围绕医疗机构内的一地理点的圆形区域，且具有200米的半径。最小距离可以是20米。因此，可以防止因用户意外踏出安全范围而导致的敏感数据的意外删除。如果用户有意要离开安全范围，则其可完成数据分析并向在安全范围内的处理设备上运行的并与便携式设备中的应用程序216对接的应用程序128提交评估结果或控制命令。如箭头510所示，当用户离开安全范围时，应用程序216删除敏感数据。在位于“安全范围外”的位置时，存储介质504不再包含敏感数据210。

[0079] 图6描述了可在用户在安全范围110外携带便携式设备时执行的，服务器120和便携式设备104交换一些请求和各个响应的过程图。在开始时，服务器120的操作员可远程配置规则和/或指定安全范围的位置坐标。包括配置数据的相应消息602被从服务器102传送至便携式设备104。配置数据用于配置可由便携式设备的应用程序216访问的、在存储介质中存储的安全范围的位置坐标。

[0080] 然后，处于安全范围内的便携式设备的客户端应用程序216向服务器提交数据请求604，并接收包含在相应响应606中的一些敏感数据210。所接收的敏感数据可被用户102处理和评估。在步骤610中，所接收的和/或经处理的敏感数据被存储在便携式设备的存储介质504上。可定期调用定位服务502。只要在用户和便携式设备处于安全范围内，在通过便携式设备和用户来处理和/或评估敏感数据的同时，可在便携式设备和服务器之间交换附加的数据请求604和相应响应。此外，还可存在响应于用户操作由便携式设备向服务器提交的某些控制命令，以便通过实验室设备来控制生物样本的处理。另外或可替代地，便携式设备可直接或经由服务器120从一个或多个实验室设备或分析器接收监测信息。

[0081] 在便携式设备的客户端应用程序216确定用户将要离开安全范围的情况下，在步骤612中，向用户输出通知，以确保敏感数据不被误删除，且防止评估结果由于离开安全范围之前未能被及时提交到服务器120而可能会丢失。通知可以是声学信号、显示的警告消息等等。

[0082] 然后，在便携式设备确定其当前位置处于安全范围外的情况下，在步骤614中，便携式设备(更具体地，它的应用程序216)删除存储在便携式设备的存储介质504中的敏感数据。最后，在步骤616中，可通知用户敏感数据已被删除。附加地或可选地，在步骤618中，消

息被从便携式设备发送到服务器，以便于通知服务器敏感数据已被删除。

[0083] 根据一些实施例，服务器内或可操作地耦合到服务器的存储介质402还包括敏感数据，并且在便携式设备上评估和修改的敏感数据和存储介质402中的敏感数据的同步经由在后台执行的自动请求响应循环来执行。因此，存储介质402上的敏感数据不断与存储在便携式设备的存储介质中的可由用户修改的敏感数据进行同步。在用户已离开了安全范围并具有相应权限的情况下，在步骤622中，用户可以直接经由网络连接624访问存储在存储介质402中的敏感数据。

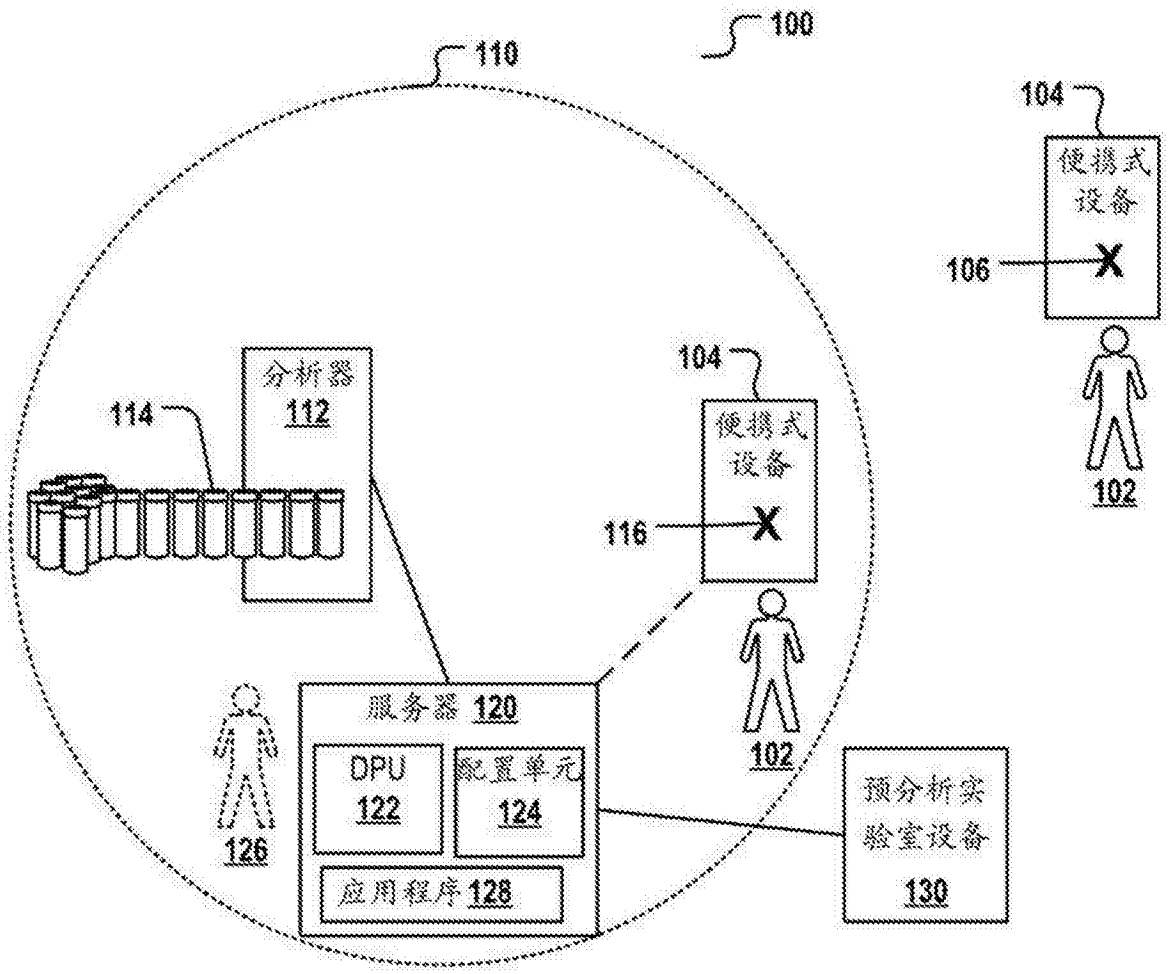

100
110
104
便携式设备
106
102
分析器
112
114
104
便携式设备
116
102
服务器 120
DPU
122
配置单元
124
应用程序 128
126
预分析实验室设备
130

图1

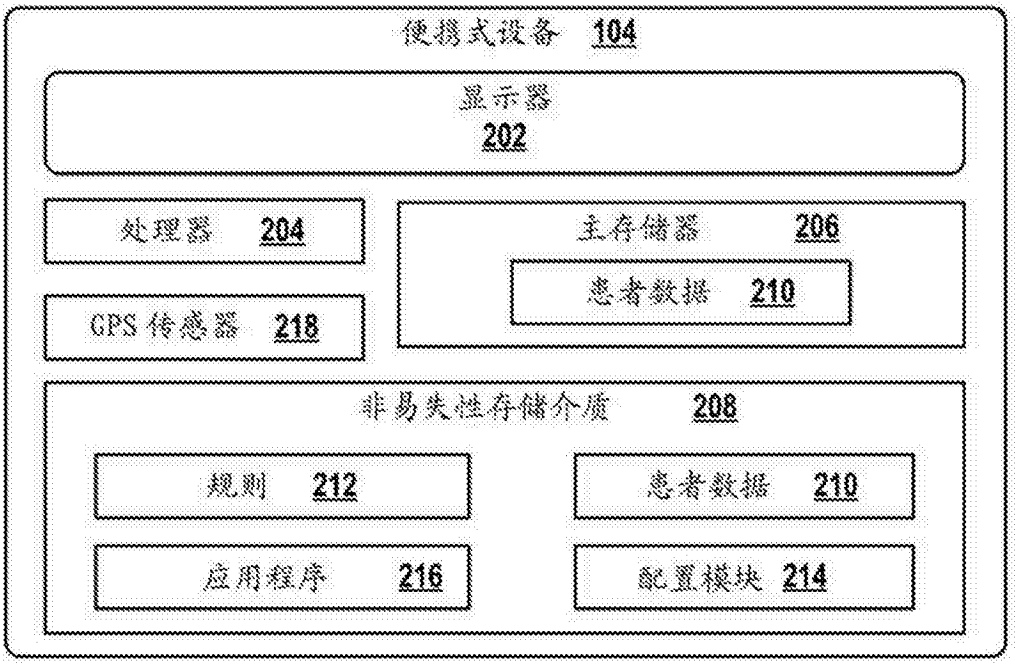

便携式设备 104
显示器
202
处理器 204
主存储器 206
患者数据 210
GPS 传感器 218
非易失性存储介质 208
规则 212
患者数据 210
应用程序 216
配置模块 214

图2

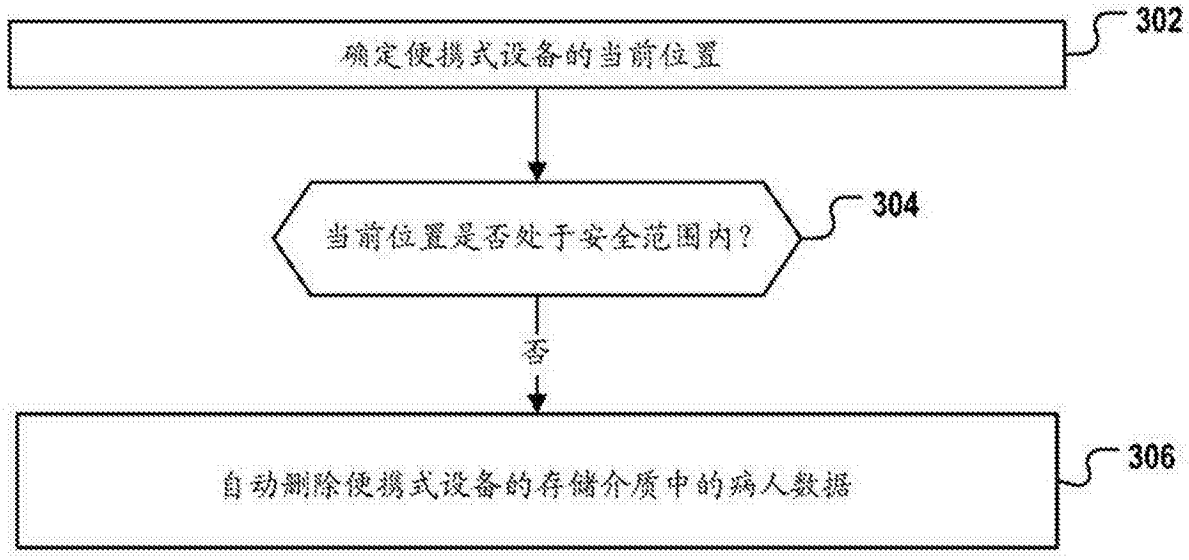

确定便携式设备的当前位置
302
当前位置是否处于安全范围内?
304
否
自动删除便携式设备的存储介质中的病人数据
306

图3

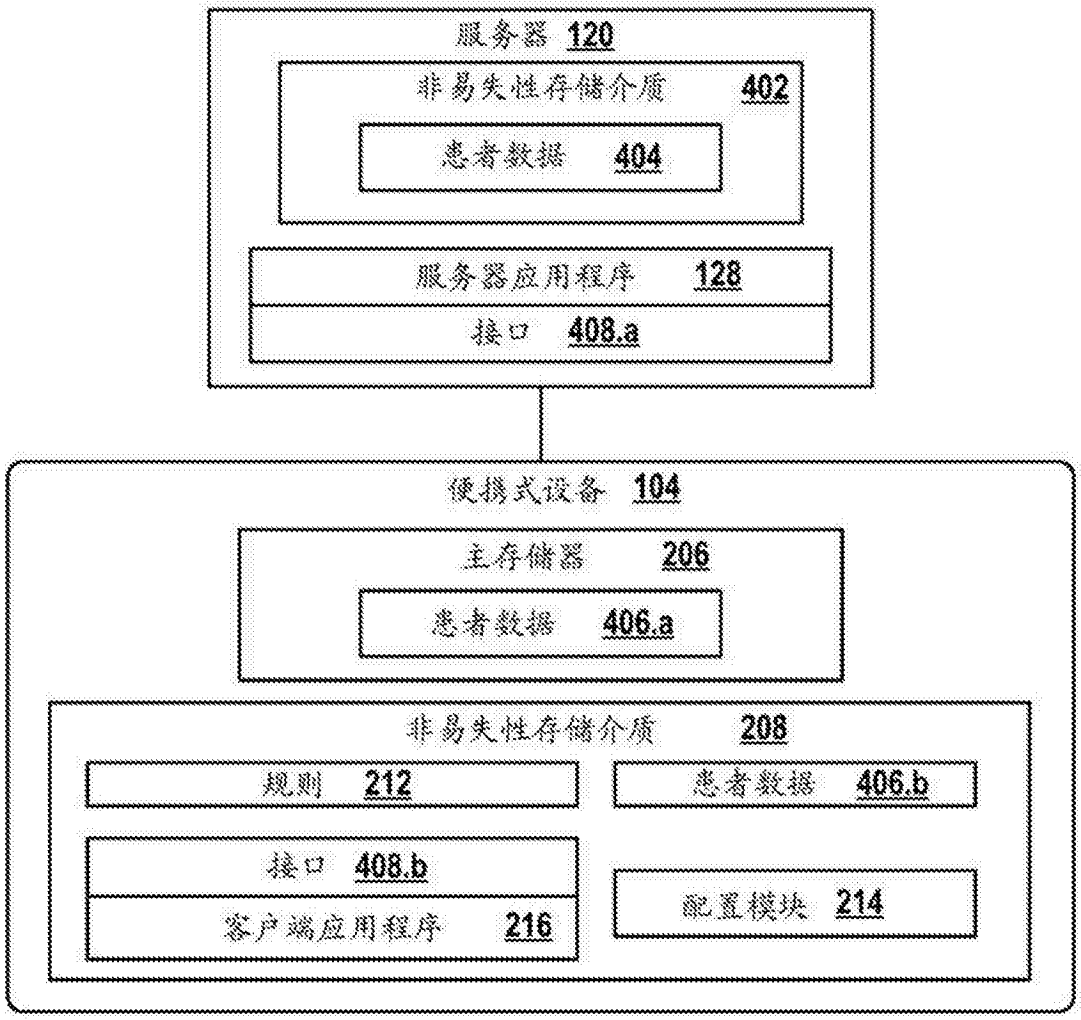

服务器 120
非易失性存储介质 402
患者数据 404
服务器应用程序 128
接口 408.a
便携式设备 104
主存储器 206
患者数据 406.a
非易失性存储介质 208
规则 212
患者数据 406.b
接口 408.b
客户端应用程序 216
配置模块 214

图4

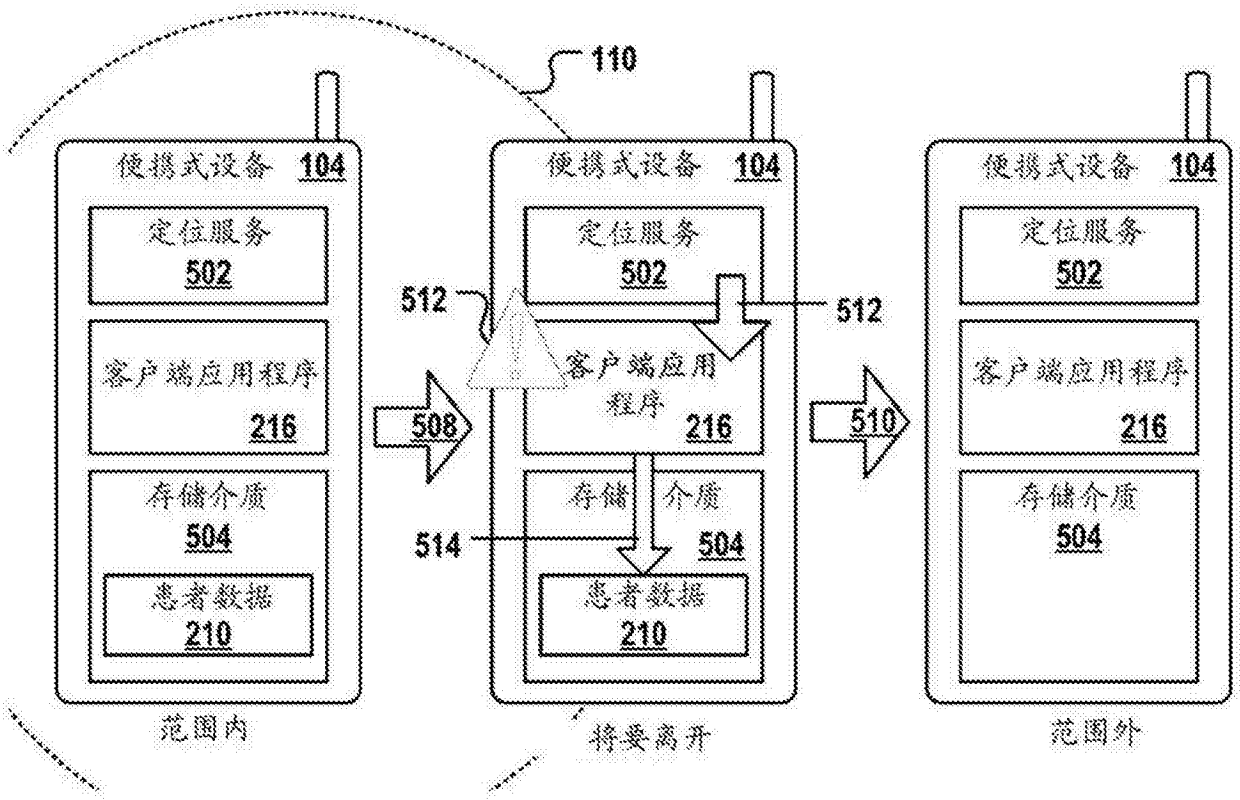

110
便携式设备 104
定位服务
502
客户端应用程序
216
存储介质
504
患者数据
210
范围内
512
508
便携式设备 104
定位服务
502
客户端应用程序
216
存储介质
504
514
患者数据
210
将要离开
512
510
便携式设备 104
定位服务
502
客户端应用程序
216
存储介质
504
范围外

图5

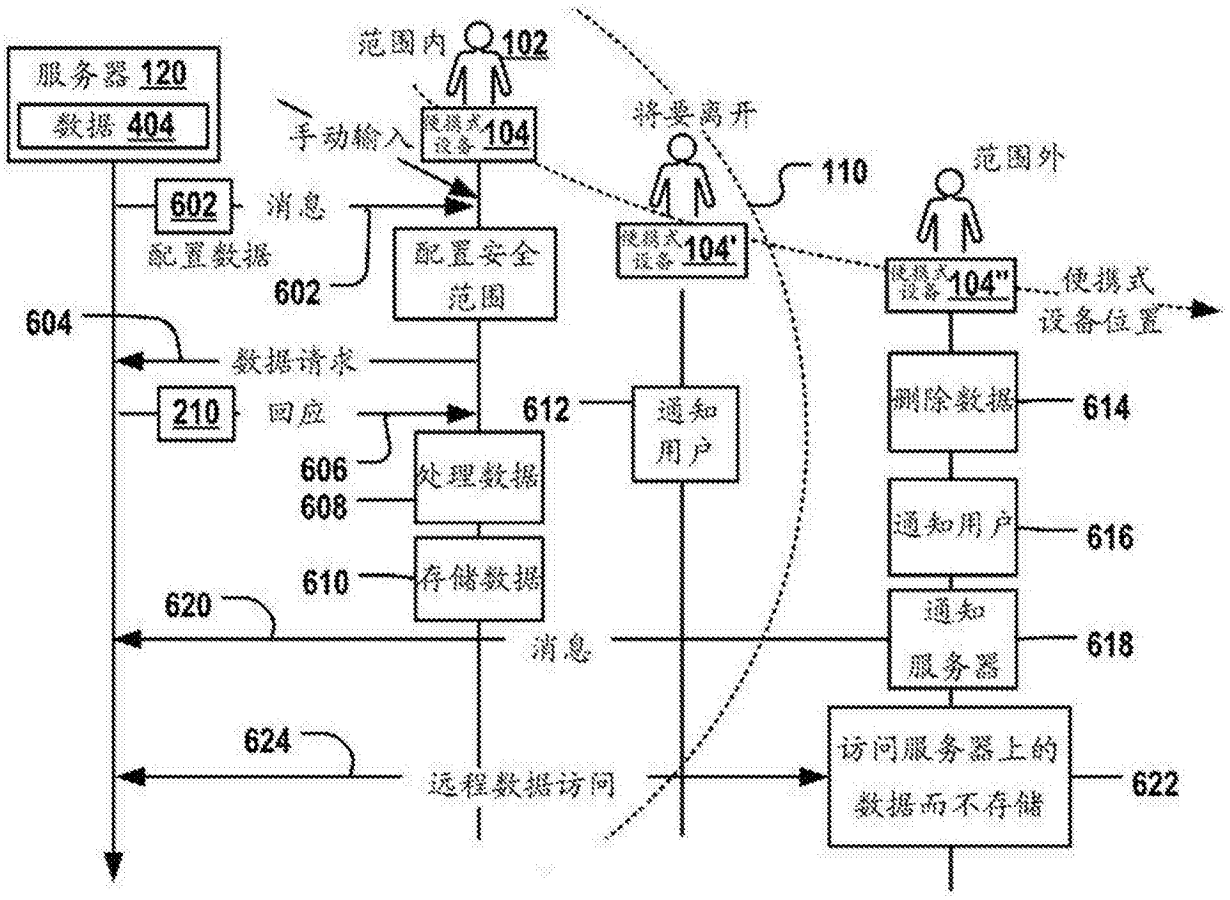

服务器 120
数据 404
范围内
102
手动输入
104
将要离开
110
范围外
602
消息
配置数据
602
配置安全范围
104'
104"
便携式设备位置
604
数据请求
210
回应
612
通知用户
删除数据
614
606
处理数据
608
610
存储数据
通知用户
616
620
消息
通知服务器
618
624
远程数据访问
访问服务器上的数据而不存储
622

图6