(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108135543 A
(43)申请公布日 2018.06.08

(21)申请号 201680059102.8

(22)申请日 2016.09.26

(30)优先权数据
16161496.1 2016.03.22 EP
62/233,612 2015.09.28 US

(85)PCT国际申请进入国家阶段日
2018.03.28

(86)PCT国际申请的申请数据
PCT/EP2016/072848 2016.09.26

(87)PCT国际申请的公布数据
WO2017/055214 EN 2017.04.06

(71)申请人 皇家飞利浦有限公司
地址 荷兰艾恩德霍芬

(72)发明人 J·克罗宁 J·戈盖恩
C·赫法恩斯

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 王英 刘炳胜

(51)Int.Cl.
*A61B 5/145*(2006.01)
*A61B 5/00*(2006.01)
*G06F 19/00*(2018.01)
*H04L 9/08*(2006.01)

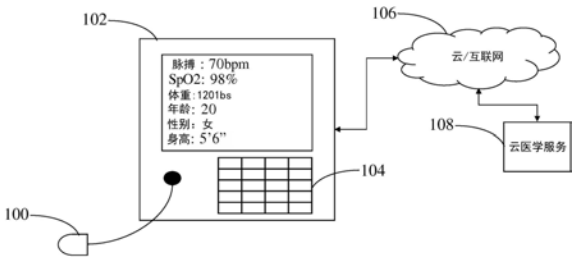
权利要求书3页 说明书4页 附图4页

(54)发明名称

安全的脉搏血氧计、监测器和云连接

(57)摘要

一种用于传输和接收脉搏血氧测定数据的方法，包括：将脉搏血氧计传感器数据传输至脉搏血氧计监测器；由所述脉搏血氧计监测器对所传输的脉搏血氧计数据进行加密；将经加密的数据传输至基于云的医学服务；将所述经加密的数据从所述基于云的医学服务发送回所述脉搏血氧计监测器，所述数据在所述脉搏血氧计监测器被解密和显示；5由所述脉搏血氧计监测器经由通过所述传感器上的随机数触发的随机数生成器来生成随机数，创建针对设备的设备脉搏血氧计监测器的特有的ID；并且针对每个事件通过所述云发送所述特有的ID。




CN 108135543 A

1.一种用于传输和接收患者的脉搏血氧测定数据的方法,所述方法包括:

使用脉搏血氧计来收集所述患者的脉搏数据和$SpO_2$数据;

将所述脉搏数据和所述$SpO_2$数据发送至脉搏血氧测定监测器;

将所述脉搏数据和所述$SpO_2$数据保存到传感器数据库;

基于所述脉搏数据和所述$SpO_2$数据、第一特有的密钥以及设备ID来生成经加密的数据;

将所述经加密的数据、所述第一特有的密钥以及所述设备ID传输至与所述脉搏血氧测定监测器通信的云医学服务器;

对所述经加密的数据进行解密;

分析经解密的数据以生成新的数据;

加密所述新的数据和第二特有的密钥;

将经加密的新的数据和所述第二特有的密钥发送至所述脉搏血氧计监测器;并且

对所述经加密的新的数据进行解密,其中,经解密的新的数据被显示在所述脉搏血氧测定监测器上。

2.根据权利要求1所述的方法,其中,生成所述经加密的数据包括:

访问所述传感器数据库,并且检索针对所述设备ID最新近保存的所述脉搏数据和所述SpO2数据;

对所检索到的脉搏数据和所检索到的SpO2数据进行加密;

使用随机数生成器来访问脉搏血氧计硬件密钥;并且

使用所述脉搏血氧计硬件密钥来创建所述第一特有的密钥。

3.根据权利要求1所述的方法,其中,对所述经加密的新的数据进行解密包括:

检索已知的网络硬件密钥;

使用所述已知的网络硬件密钥对所述经加密的新的数据进行解密;并且

将所述经解密的新的数据保存在接收数据数据库中。

4.根据权利要求1所述的方法,其中,对所述经加密的数据进行解密包括:

访问设备数据库,并且定位针对所述设备ID最新近保存的所述脉搏数据和所述SpO2数据;

检索对应于所述设备ID的脉搏血氧测定硬件密钥;

对所述经加密的数据进行解密;并且

将所述经解密的数据保存在所述传感器数据库中。

5.根据权利要求1所述的方法,其中,生成所述经加密的新的数据包括:

访问网络分析数据库,并且检索针对所述设备ID最新近保存的所述脉搏数据和所述SpO2数据;

对所检索到的脉搏数据和所检索到的SpO2数据进行加密;

使用随机数生成器来访问脉搏血氧计硬件密钥;并且

使用所述脉搏血氧计硬件密钥来创建所述第二特有的密钥。

6.根据权利要求1所述的方法,还包括经由所述云医学服务器使用选自以下中的一个或多个额外的设备来传输和接收保密的医学数据:二氧化碳监测仪、CO-血氧计、动脉血气分析仪、血糖仪、血压监测器,或者其组合。

7.根据权利要求6所述的方法,其中,所述额外的设备被验证以限制对提供给经验证的

医学设备或授权的实体的保密的患者信息的访问。

8.根据权利要求7所述的方法，其中，所述额外的设备是使用来自所述额外的设备的验证代码来验证的。

9.根据权利要求8所述的方法，其中，来自所述脉搏血氧计和所述额外的设备中的每个的数据在被组合之前被单独地加密。

10.根据权利要求8所述的方法，其中，来自所述脉搏血氧计和所述额外的设备中的每个的数据首先被组合，并且随后作为组被加密。

11.根据权利要求1所述的方法，还包括将适合于所述患者的额外的识别符传输至所述云医学服务器。

12.根据权利要求6所述的方法，其中，所述云医学服务器发送对所述脉搏血氧计和所述额外的设备的验证访问的请求。

13.根据权利要求12所述的方法，其中，所述额外的设备中的一个或者所述脉搏血氧计生成验证令牌。

14.一种用于传输和接收脉搏血氧测定数据的方法，所述方法包括：

将脉搏血氧计传感器数据传输至脉搏血氧计监测器；

由所述脉搏血氧计监测器对所传输的脉搏血氧计数据进行加密；

将经加密的数据传输至基于云的医学服务；

将所述经加密的数据从所述基于云的医学服务发送回所述脉搏血氧计监测器，所述数据在所述脉搏血氧计监测器处被解密和显示；

由所述脉搏血氧计监测器经由通过所述传感器上的随机数触发的随机数生成器来生成随机数；

创建针对设备的设备脉搏血氧计监测器的特有的ID；并且

针对每个事件通过所述云发送所述特有的ID。

15.一种用于传输和接收患者的脉搏血氧测定数据的系统，所述系统包括：

脉搏血氧计，所述脉搏血氧计收集所述患者的脉搏数据和$SpO_2$数据；

脉搏血氧测定监测器，所述脉搏血氧测定监测器从所述脉搏血氧计接收所述脉搏数据和所述$SpO_2$数据；

传感器数据库，所述传感器数据库已经在其上保存了所述脉搏数据和所述$SpO_2$数据；以及

脉搏血氧测定处理器，所述脉搏血氧测定处理器执行被存储在存储器中的指令，其中，由所述处理器对所述指令的执行使得：

使用所述脉搏数据和所述$SpO_2$数据、第一特有的密钥以及设备ID来生成经加密的数据；

将所述经加密的数据、所述第一特有的密钥以及所述设备ID传输至被连接到所述脉搏血氧测定监测器的云医学服务器；

对所述经加密的数据进行解密；

分析经解密的数据以生成新的数据；

加密所述新的数据和第二特有的密钥；

将经加密的新的数据和所述第二特有的密钥发送至所述脉搏血氧计监测器；并且

对所述经加密的新的数据进行解密，其中，经解密的新的数据被显示在所述脉搏血氧

测定监测器上。

# 安全的脉搏血氧计、监测器和云连接

## 背景技术

[0001] 脉搏血氧测定是监测和采集患者的氧饱和度(SpO2)水平和灌注指数的有效且无创的方法。其在监测患者的氧合水平重要的许多情况下是非常有用的。例如,脉搏血氧测定在急救护理情况、外科手术、麻醉后护理以及监测新生婴儿的氧合度的过程中是有用的。通常,然而,可能需要将根据对患者进行的医学或健康相关的测量或测试而采集的数据传输至另一设备,诸如传输至健康护理设施内或外部网络服务器的数据库。在这种情况下,将医学数据以安全的方式传输至另一设备以防止对患者的医学数据的未授权的访问是必要的。

## 发明内容

[0002] 脉搏血氧计传感器数据被传送至脉搏血氧计监测器。所述监测器在将所述数据发送至云医学服务器之前对所述数据进行加密。经加密的数据从云医学服务器被发送回所述脉搏血氧计监测器,所述数据在所述脉搏血氧计监测器处被解密和显示。所述脉搏血氧计监测器设备具有由传感器上的随机数触发的随机数生成器,因此,针对该设备的该脉搏血氧计监测器来创建特有的(unique)密钥,其是特有的ID,在此云接收针对每个事件的特有的密钥。

[0003] 为了确保当使用云服务时患者数据保持私人且保密的。脉搏血氧计传感器数据被传送至所述脉搏血氧计监测器。所述监测器在将所述数据发送至云医学服务器之前对所述数据进行加密。所述云医学服务器执行任务,并且然后经加密的数据从所述云医学服务器被发送回所述脉搏血氧计监测器,所述数据在所述脉搏血氧计监测器处被解密和显示以供患者或医务人员使用。

## 附图说明

[0004] 被包括以提供对本发明的进一步理解的随附的附图被并入本文以图示本发明的实施例。连同描述一起,所述附图也用于解释本发明的原理。在附图中:

[0005] 图1示出了根据本发明的优选实施例的系统。

[0006] 图2是图示了根据本发明的示范性实施例的方法的流程图。

[0007] 图3A示出了根据本发明的优选实施例的发送安全软件的流程图。

[0008] 图3B示出了根据本发明的优选实施例的接收安全软件的流程图。

[0009] 图4A示出了根据本发明的优选实施例的网络解密软件的流程图。

[0010] 图4B示出了根据本发明的优选实施例的网络加密软件的流程图。

## 具体实施方式

[0011] 本发明的一些实施例涉及一种用于传输和接收脉搏血氧测定数据的方法,包括:将脉搏血氧计传感器数据传输至脉搏血氧计监测器;由所述脉搏血氧计监测器对所传输的脉搏血氧计数据进行加密;将经加密的数据传输至基于云的医学服务;将所述经加密的数据从所述基于云的医学服务发送回所述脉搏血氧计监测器,所述数据在所述脉搏血氧计监

测器处被解密和显示;由所述脉搏血氧计监测器经由通过所述传感器上的随机数触发的随机数生成器来生成随机数,创建针对设备的设备脉搏血氧计监测器的特有的ID;并且针对每个事件通过所述云发送所述特有的ID。

[0012] 图1示出了根据本发明的优选实施例的系统。脉搏血氧计传感器100被连接到具有键盘104的脉搏血氧计监测器102。脉搏血氧计监测器102经由云或互联网106被连接到基于云的医学服务108。

[0013] 图2是图示了根据本发明的示范性实施例的方法的流程图。所述脉搏血氧计传感器收集脉搏和SpO2数据,并且将所述数据发送至脉搏血氧测定监测器(步骤200)。所述脉搏血氧测定监测器然后接收脉搏数据和SpO2数据,并且将所述数据保存到传感器数据库(步骤202)。然后执行发送安全软件(步骤204),并且所得到的经加密的数据、第一特有的密钥以及设备ID被传输至云医学服务器(步骤206)。所述基于云的医学服务然后接收所述经加密的数据、所述第一特有的密钥以及设备ID(步骤208)。所述基于云的医学服务然后执行网络解密软件(步骤210)。由基于云的医学服务执行动作或分析软件,由此创建新的数据(212)。所述云医学服务器然后执行网络加密软件(步骤214),并且生成经加密的新的数据以及第二特有的密钥。所述基于云的医学服务然后将所述经加密的新的数据以及所述第二特有的密钥发送回所述脉搏血氧计监测器(步骤216)。所述脉搏血氧计监测器接收经加密的数据(步骤218),并且然后执行接收安全软件(步骤220),以对所述经加密的数据进行解密,因此能够在脉搏血氧测定监测器上读取所接收的经加密的新的数据。

[0014] 图3A示出了根据本发明的优选实施例的发送安全软件的流程图。根据该实施例,访问所述传感器数据库,并且检索所述脉搏数据和所述SpO2数据的最新近的条目(步骤300)。所检索的数据然后被加密(步骤302),并且随机数生成器然后访问脉搏血氧计硬件密钥(步骤304)。然后,所述随机数生成器使用所述脉搏血氧计硬件密钥来创建第一特有的密钥(步骤306)。图3B示出了根据本发明的优选实施例的接收安全软件的流程图。在此,第一步骤涉及检索已知的网络硬件密钥(步骤308)。然后使用已知的网络硬件密钥来解密所接收的经加密的数据(步骤310)。然后,经解密的数据被保存在接收数据数据库中(步骤312)。

[0015] 图4A示出了根据本发明的优选实施例的网络解密软件的流程图。在第一步骤中,访问设备数据库,并且定位针对所接收的设备ID的脉搏数据和$SpO_2$数据的匹配条目(步骤400)。然后从所确定的匹配条目检索对应的脉搏血氧测定硬件密钥(步骤402)。接下来,使用所检索到的脉搏血氧测定硬件密钥来解密所接收的经加密的数据(步骤404)。然后,经解密的数据被保存在网络传感器数据库中(步骤406)。

[0016] 图4B示出了根据本发明的优选实施例的网络加密软件的流程图。在此,第一步骤涉及访问网络分析数据库,并且检索针对所接收的设备ID的脉搏数据和SpO2数据的最新近的条目(步骤408)。所述数据然后被加密(步骤410),并且所述随机数生成器访问所述网络硬件密钥(步骤412)。然后,所述随机数生成器使用网络硬件密钥来创建第二特有的密钥(步骤414)。

[0017] 能够由任意数量的类型的设备来传输和接收保密的医学数据。这些设备的范例是用于测量数据以及对患者进行测试的医学设备、以及被连接到这些医学设备的设备,诸如计算机和存储设备。因此,除了脉搏血氧计之外,患者医学数据可以源于二氧化碳监测器、CO-血氧计、动脉血气分析仪、血糖仪和血压监测器或者由其接收。这些设备可以使用不同

的通信协议和格式来传输或接收数据。

[0018] 能够由任意数量的类型的设备来传输和接收保密的医学数据。这些设备的范例是用于测量数据和对患者进行测试的医学设备、以及被连接到这些医学设备的设备，诸如计算机和存储设备。因此，除了脉搏血氧计之外，患者医学数据可以源于二氧化碳监测器、CO-血氧计、动脉血气分析仪、血糖仪和血压监测器或者由其接收。这些设备可以使用不同的通信协议和格式来传输或接收数据。

[0019] 在本发明的优选实施例中，对与基于云的医学服务交换数据的任何设备进行验证，以限制对被提供至经验证的医学设备和授权的实体的保密的患者信息的访问。通过要求验证，能够保护医学数据免于被意外地传播以及被意外的接收者查看。

[0020] 本发明的设备能够使用各种验证手段来进行验证。执行验证的一种方式是需要来自设备的识别代码或验证代码。所述识别代码能够是允许所述设备传输或接收患者信息的任何密钥、数字、代码或识别符。在本发明的一个示范性实施例中，传输或接收患者信息的设备最初从验证实体接收并存储验证代码。响应于针对验证的请求，所述设备将所述验证代码传输至所述验证设备或实体。如果所传输的验证代码不匹配由患者信息的接收者(诸如医学数据服务器、远程患者监测系统或其他设备、互联网、或实体)所存储的代码，则将不接受来自尝试传输所述保密的医学数据的设备的所述患者信息。

[0021] 所述保密的患者信息优选在传输至所述基于云的医学服务之前被加密。如果从不同的设备收集数据，则来自每个设备的数据可以在被组合之前被单独地加密，或者来自不同设备的数据可以首先被组合并且然后作为组被加密。在一些情况下，可能希望仅对从设备或一组设备收集的数据的特定部分进行加密，例如，可能想要仅对与患者有关的敏感信息进行加密以便于数据传输或者减少计算要求。

[0022] 备选地，所述加密过程可以利用医学设备的私人密钥，或者利用预期接收者(诸如基于云的医学服务)的公共密钥，或者利用私人密钥和公共密钥两者。可以使用有线或无线通信系统将所述私人密钥和所述公共密钥传输至基于云的医学服务。在一个实施例中，传输或接收实体可以请求基于云的医学服务的公共密钥被发送至所述传输或接收实体，以实现例如对所接收的经加密的患者医学数据的解密。备选地，充当例如医院服务器与基于云的医学服务之间的媒介的服务器能够从医院服务器向基于云的医学服务重新传输经加密的患者的医学数据，并且反之亦然。

[0023] 例如，如果由医院外面的患者获取诸如脉搏血氧测定数据的医学数据，则将仅需要患者使用先前所描述的加密和验证手段中的任意手段仅将加密的信息传输至基于云的医学服务。除了任何需要的密钥、代码或数字之外，也需要患者传输适合于患者的额外的识别符，诸如患者的姓名、电话号码或社会安全号码。

[0024] 在本发明的实施例中，服务器或网络(诸如基于云的医学服务)生成对验证访问的请求。所述医学数据系统然后向与患者、用户或健康护理提供者相关联的本发明的用户部件发送对验证访问的请求。在接收到对验证访问的请求之后，用户生成验证令牌。

[0025] 所述验证令牌可以包含对应于患者相关的个人信息的文本字符串或数字，诸如电话号码、社会安全号码、帐户号码、或者能够与医学数据服务器中的先前所存储的患者信息进行比较的其他患者识别符。备选地，验证令牌可以由被绘制成数字表示的患者的编码的密码或生物计量数据组成。一旦被生成，出于安全的目的，可以通过在传输至请求实体(诸

如医学数据系统或服务器)之前对所述令牌进行加密、摘要(digest)并且对所述令牌的摘要进行加密、或者密码地散列(hashing)所述令牌来保护所述验证令牌。

[0026] 在本发明的一个实施例中,当生成了验证令牌被时,令牌发送者可以经由例如以下操作来创建对有效性的认证:利用与令牌发起者相关联的私人密钥对所述令牌进行加密;利用与令牌请求者或目标相关联的公共密钥对令牌进行加密;通过诸如散列算法的方法来生成令牌的摘要,并且任选地利用令牌发起者的私人密钥对散列的摘要进行加密,或者提供作为可以与先前所存储的值进行比较的令牌(诸如密码地散列的密码)的至少部分的验证代码。然后,发送经保护的验证令牌,并且当接收者接收所述令牌以及任何加密的或明文的认证数据时,部件可以通过尝试以下操作来确定所述访问是有效的:利用声称的发起者的公共密钥对加密的令牌进行解密;利用声称的发起者的公共密钥对加密的令牌进行解密;利用声称的发起者的公共密钥对加密的摘要进行解密,并且将结果与PIN、令牌、个人识别码、密码、代码的散列值进行比较,或者将针对声称的发起者的密码地散列的密码与已知的预先存储的值进行比较,如果找到匹配,则验证被承认。

[0027] 令牌接收者或核验者然后接收并分析所述验证令牌的有效性。如果验证令牌被确认是可信的,诸如通过将经分析的令牌数据与已知的预先存储的值(诸如患者或患者的健康护理提供者的预先存储的密码或其他患者个人信息)进行比较,那么访问是成功的并且该过程终止。在分析验证令牌或者包含或与令牌相关联的消息,令牌接收者或核验者然后能够决定访问是被允许还是被拒绝,并且可以将该状态传送至验证令牌发送者。此时,所述系统可以重复该过程,允许令牌发起者再次尝试访问。

[0028] 在本发明的优选实施例中,接收针对脉搏血氧计测量的请求。所述系统然后执行诊断测试以查看脉搏血氧计是否不活跃或处于空闲状态。否则意味着设备先前已经被初始化。如果其处于空闲状态,则脉搏血氧计被激活以执行原始信号以及参考或基准测量。所述设备然后可以执行连续测量并且然后用曲线图表示数据,或者所述设备可以获取离散数量的测量样本并且计算样本平均值并且然后传输单个测量结果。

[0029] 其他设备也可以协同脉搏血氧计来使用。例如,CO-血氧计是用于检测缺氧的设备,并且与脉搏血氧计类似地工作。CO-血氧计在若干波长下测量吸收,以区分氧合血红蛋白与碳氧血红蛋白,并且甚至当患者一氧合碳中毒时确定氧合血红蛋白饱和。

[0030] 可以协同本发明的脉搏血氧计使用的另一设备是二氧化碳监测仪,所述二氧化碳监测仪是用于监测呼吸速率和通气的充足性的仪器。其附接到气管导管,并且测量吸入和呼出的空气中的二氧化碳含量。其使用红外光来测量在呼吸期间由二氧化碳分子所吸收的光的量。其检测血流动力学稳定但未病重的患者中的二氧化碳浓度的变化。

[0031] 可以协同本发明的脉搏血氧计使用的又一设备是动脉血气(ABG)分析。这是使用从动脉提取的样本的血液测试。所述测试确定血液的pH、二氧化碳和氧气的分压、以及重碳酸盐水平。许多血气分析仪也将报告乳酸盐、血红蛋白、若干电解质、氧合血红蛋白、碳氧血红蛋白和高铁血红蛋白的浓度。动脉血气分析确定与肺功能相关的血液中的气体交换水平。

[0032] 本发明并不旨在限制于上文所描述的本发明的若干示范性实施例。本领域技术人员可以设想到的其他变型旨在落在本公开之内。

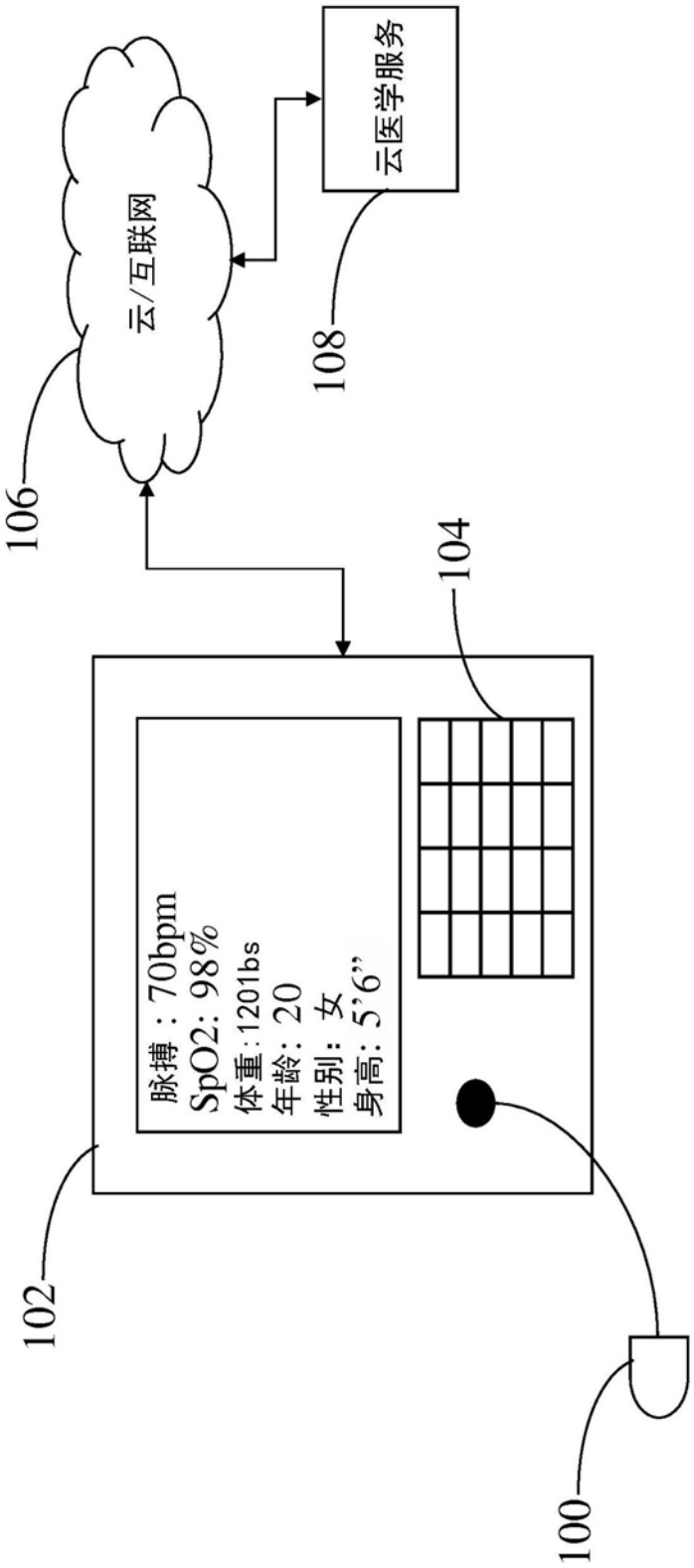

云医学服务
云/互联网
108
106
104
脉搏：70bpm
SpO2: 98%
体重:1201bs
年龄：20
性别：女
身高：5’6”
102
100

图1

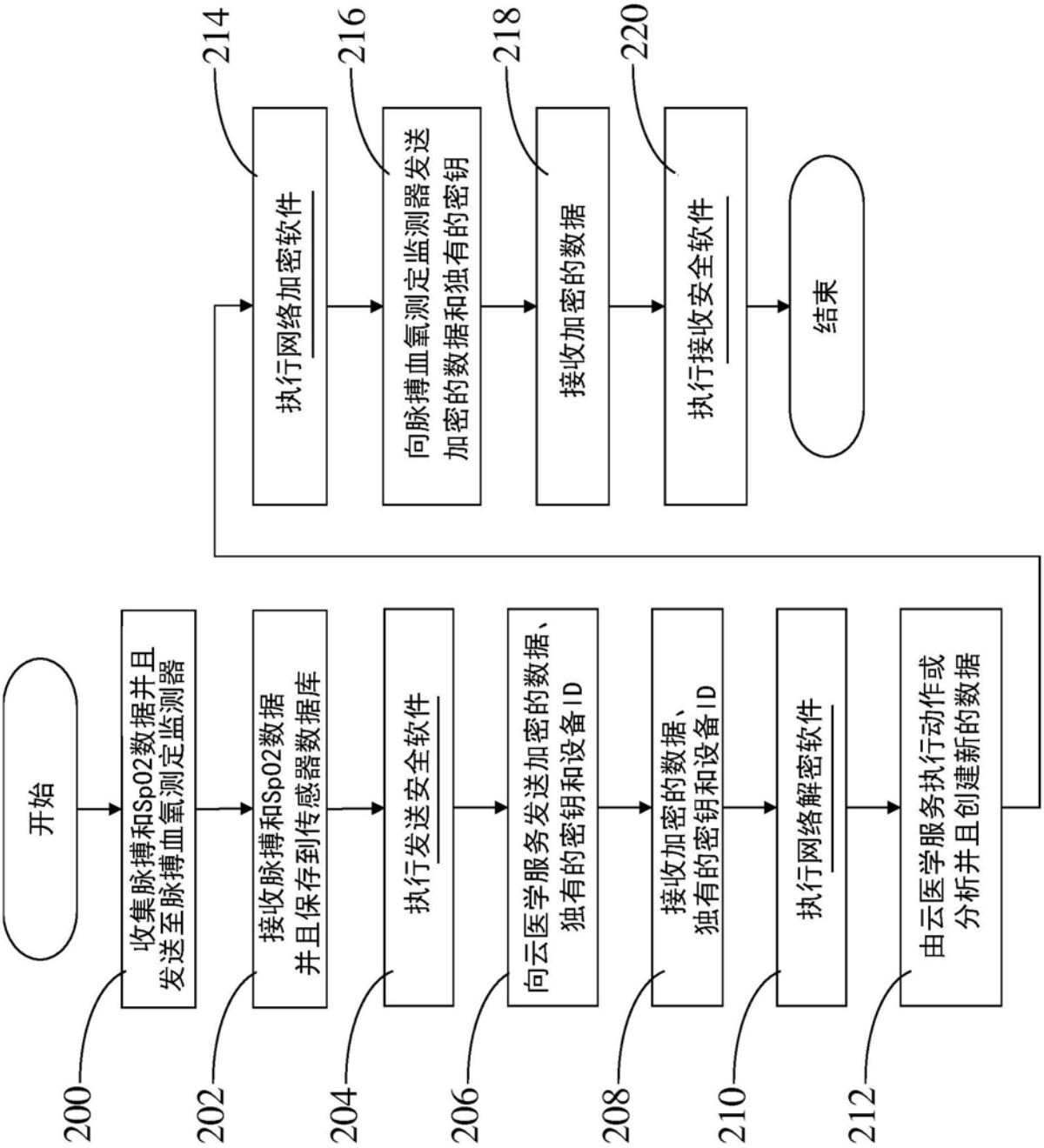

开始
收集脉搏和SpO2数据并且发送至脉搏血氧测定监测器
接收脉搏和SpO2数据并且保存到传感器数据库
执行发送安全软件
向云医学服务发送加密的数据、独有的密钥和设备ID
接收加密的数据、独有的密钥和设备ID
执行网络解密软件
由云医学服务执行动作或分析并且创建新的数据
200
202
204
206
208
210
212
执行网络加密软件
向脉搏血氧测定监测器发送加密的数据和独有的密钥
接收加密的数据
执行接收安全软件
结束
214
216
218
220

图2

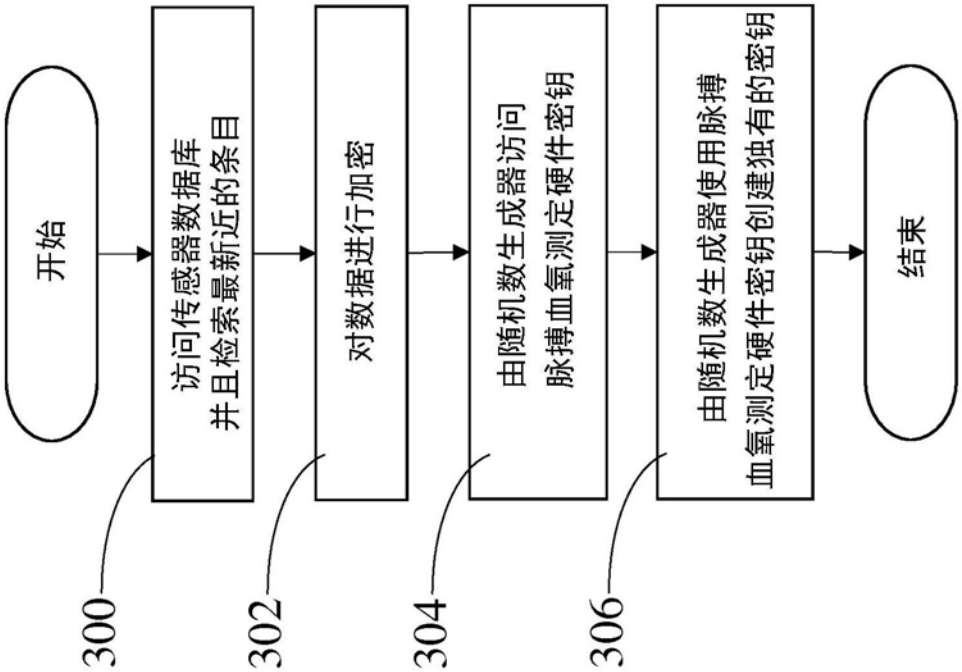

开始
访问传感器数据库
并且检索最新近的条目
对数据进行加密
由随机数生成器访问
脉搏血氧测定硬件密钥
由随机数生成器使用脉搏
血氧测定硬件密钥创建独有的密钥
结束
300
302
304
306

图3A

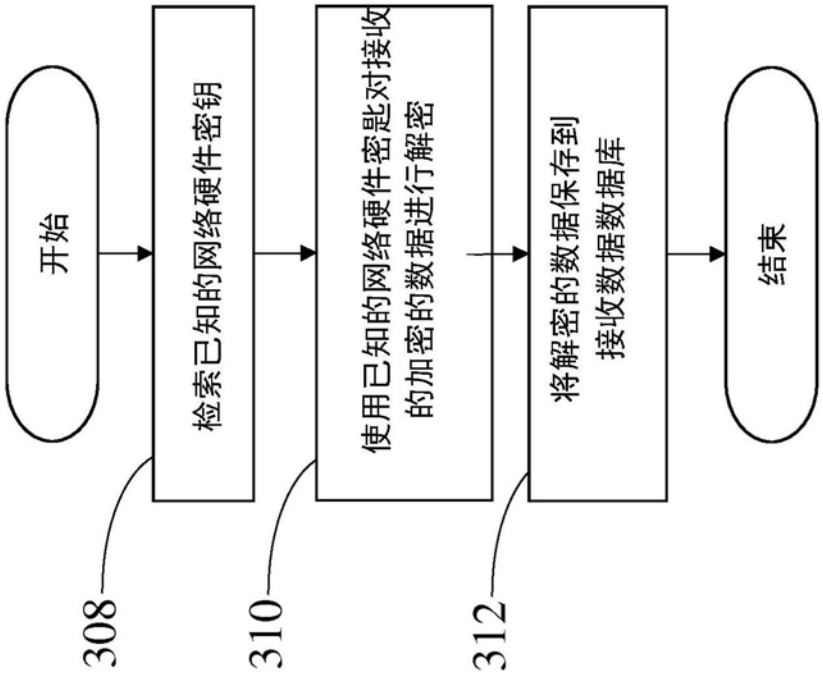

开始
检索已知的网络硬件密钥
使用已知的网络硬件密匙对接收
的加密的数据进行解密
将解密的数据保存到
接收数据数据库
结束
308
310
312

图3B

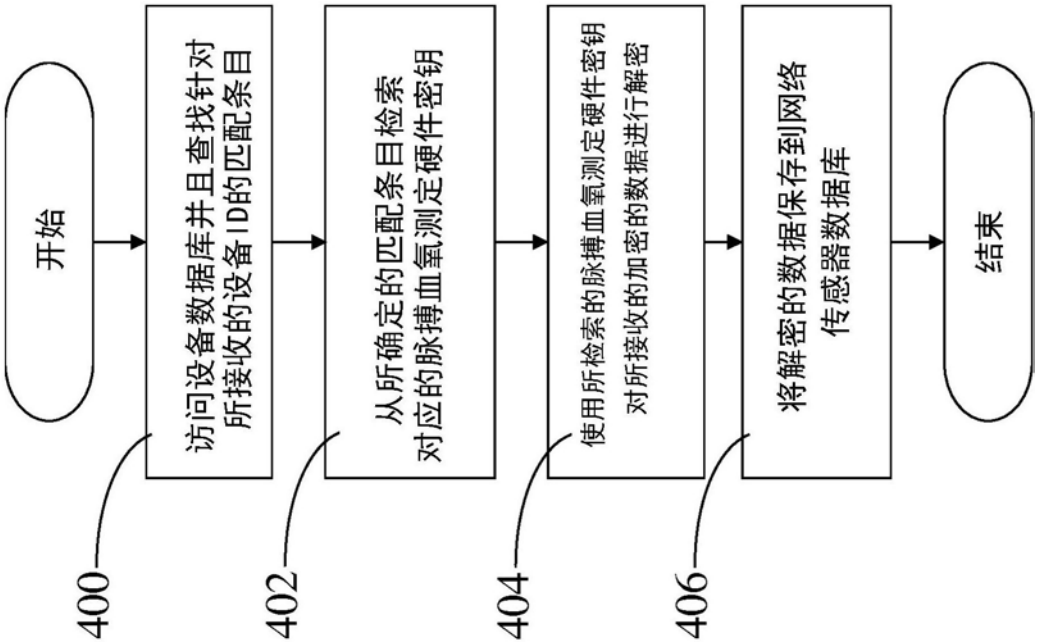

开始
访问设备数据库并且查找针对所接收的设备ID的匹配条目
从所确定的匹配条目检索对应的脉搏血氧测定硬件密钥
使用所检索的脉搏血氧测定硬件密钥对所接收的加密的数据进行解密
将解密的数据保存到网络传感器数据库
结束
400
402
404
406

图4A

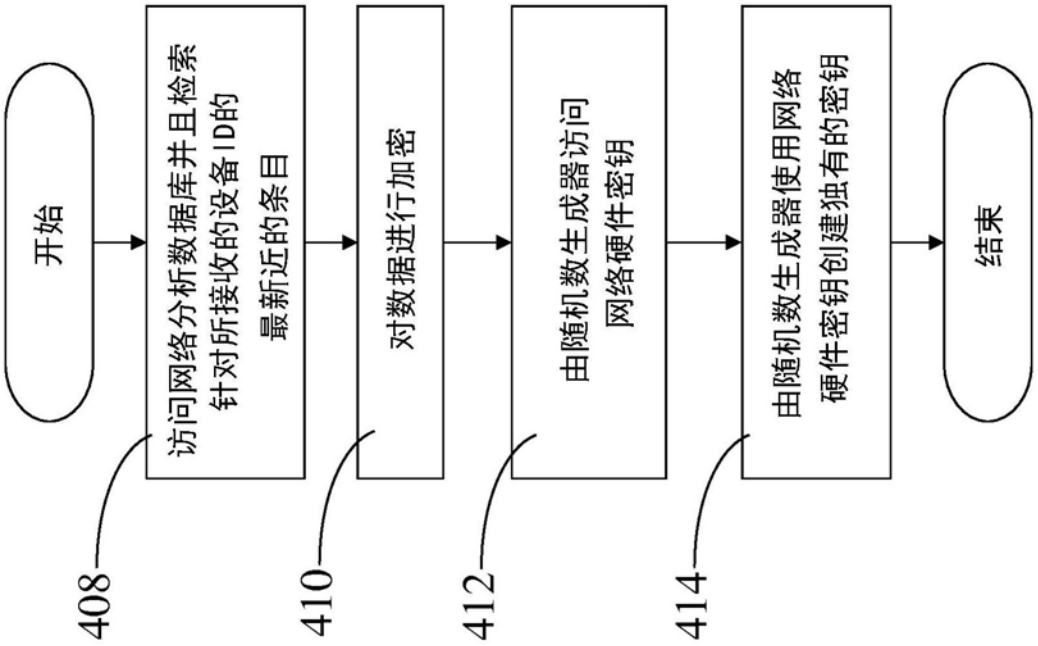

开始
访问网络分析数据库并且检索针对所接收的设备ID的最新近的条目
对数据进行加密
由随机数生成器访问网络硬件密钥
由随机数生成器使用网络硬件密钥创建独有的密钥
结束
408
410
412
414

图4B

| | | | |
|---|---|---|---|
| 专利名称(译) | 安全的脉搏血氧计、监测器和云连接 | | |
| 公开(公告)号 | CN108135543A | 公开(公告)日 | 2018-06-08 |
| 申请号 | CN201680059102.8 | 申请日 | 2016-09-26 |
| [标]申请(专利权)人(译) | 皇家飞利浦电子股份有限公司 | | |
| 申请(专利权)人(译) | 皇家飞利浦有限公司 | | |
| 当前申请(专利权)人(译) | 皇家飞利浦有限公司 | | |
| [标]发明人 | J克罗宁<br>J 戈盖恩<br>C 赫法恩斯 | | |
| 发明人 | J·克罗宁<br>J·戈盖恩<br>C·赫法恩斯 | | |
| IPC分类号 | A61B5/145 A61B5/00 G06F19/00 H04L9/08 | | |
| CPC分类号 | A61B5/0022 A61B5/02438 A61B5/082 A61B5/14532 A61B5/14551 A61B5/4842 A61B2503/045 A61B2505/01 A61B2505/07 A61B5/145 G16H10/60 G16H40/67 G16H70/60 H04L9/0662 H04L9/0894 H04L9/3213 H04L2209/88 A61B5/024 | | |
| 代理人(译) | 王英<br>刘炳胜 | | |
| 优先权 | 2016161496 2016-03-22 EP<br>62/233612 2015-09-28 US | | |
| 外部链接 | Espacenet SIPO | | |


摘要(译)

一种用于传输和接收脉搏血氧测定数据的方法，包括：将脉搏血氧计传感器数据传输至脉搏血氧计监测器；由所述脉搏血氧计监测器对所传输的脉搏血氧计数据进行加密；将经加密的数据传输至基于云的医学服务；将所述经加密的数据从所述基于云的医学服务发送回所述脉搏血氧计监测器，所述数据在所述脉搏血氧计监测器被解密和显示；5由所述脉搏血氧计监测器经由通过所述传感器上的随机数触发的随机数生成器来生成随机数，创建针对设备的设备脉搏血氧计监测器的特有的ID；并且针对每个事件通过所述云发送所述特有的ID。