系统与数据安全的共同责任

简体中文

Lumify 超声诊断系统

PHILIPS

目录

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

目录

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

1 简介

本文档将讨论有关 Lumify 超声诊断系统的安全性。如果其他 Philips 超声诊断系统作为完整系统交付，且有系统授权和可用性限制，Lumify 主机设备就应该由医疗机构或个人进行采购、配置和维护。

这些准则旨在帮助医疗机构了解哪些情况会危害 Philips Lumify 应用和患者数据的安全性，并重点介绍 Philips 为避免安全漏洞所作的努力。

有关超声诊断系统安全资源（如安全公告、常见问题解答和漏洞信息），请访问 Philips 产品安全网站：

www.philips.com/productsecurity

有关 Lumify 超声诊断系统的信息，请访问 Lumify 门户网站：

www.philips.com/lumify

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

常规信息

下面的常规信息适用于 Philips 超声软件和患者数据的安全性。

- Philips 超声诊断系统不支持多用户会话操作。它们被设计成单用户设备。不支持通过网络用于临床。
- 超声诊断系统不是长期存储设备。永久性患者数据必须存档到 DICOM PACS、网络共享或本地存储库上。

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

2 有关 Philips 超声产品的安全漏洞控制

Philips 致力于帮助所有用户保持患者数据的保密性、完整性和有效性，确保用户的超声诊断系统能够连续不断的使此类信息的生成与管理绝对安全。当超声诊断系统连接到网络时，可能会存在安全漏洞。

深层防御安全策略

医疗机构对患者数据和 Philips 产品的安全维护需采用深层防御安全策略，这是一个全方位、多层次的安全策略（包括策略、过程和技术），可防止信息和仪器系统受到内部和外部的威胁。

有关贵机构安全方面的特殊信息，请咨询以下部门或承担类似责任部门的安全专家：

- 首席信息安全官
- 首席信息官
- HIPAA（健康保险流通及责任法案）隐私或安全官（美国）
- 安全官

要了解常规安全问题或超声诊断系统的特定漏洞，请联系 Philips 代表。

制度背景

医疗设备的研发及制造方面的管制非常严格，而医疗服务供应商持有的患者信息的安全性及隐私的管制同样严格。这为医疗保健产品提供商和制造商针对医疗设备上所存储患者数据的新威胁采取快速响应带来了挑战。

患者健康电子信息的保护

应采取安全措施保护的最重要资产之一就是患者健康信息。例如，以下法令要求对患者的健康信息加以保密，并且对保护患者信息应采取的安全措施作出相关规定：

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

- 美国健康保险流通与责任法案（Health Insurance Portability and Accountability Act，HIPAA）（www.hhs.gov/ocr/privacy/）
- 欧洲医疗设备指令（European Medical Device Directive）93/42/EEC
- 日本的 HPB517
- 美国联邦经济刺激法案（正式名称为 2009 年美国恢复和再投资法案）中与 HIPAA 相关的部分（或称为 HITECH）

产品安全合作中 Philips 的责任

Philips 运作过程依据于一个全球产品安全策略，该策略控制着产品创新、风险评估和现有产品安全漏洞事件应变活动的安全设计。Philips 已建立了全球问题跟踪和升级处理流程，随时掌控涉及 Philips 诊断系统的安全问题。

安全漏洞的应变

Philips 产品工程设计小组对诊断系统的新安全漏洞实施连续监控，包括第三方软件和操作系统厂商所识别的漏洞，以及各个医疗机构所报告的漏洞。

一个全球网络应变小组专门负责产品安全事件的信息收集和管理，并解决影响 Philips 产品和解决方案的漏洞。这些应变小组将他们的活动范围不断扩大，涵盖了全球所有诊断系统。

相应的应变小组的目标是明确估计风险、威胁或漏洞以评估每个实际存在的和潜在的安全隐患，并根据需要开发包括鉴定和沟通程序在内的漏洞应变计划。这意味着 Philips 要在开发和布置风险降低措施的同时将诊断系统所存在的漏洞通知客户。有关诊断系统漏洞的更多信息，请访问以下网站：

www.philips.com/productsecurity

设计改进

Philips 积极实施产品内部安全评估以发现潜在的安全漏洞。利用这些信息，Philips 工程设计小组常常通过更改配置和重新设计来加固系统，以应对外来威胁。这些信息同时也提高了新产品的安全设计要求。Philips 产品安全策略要求将安全设计目标作为所有新产品创新工作的一部分。

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

产品安全合作中客户的责任

警告

对 Android 设备进行未经授权更改（“刷机”或“破解”）可能会引起超声诊断系统故障，从而导致误诊。

小心

Android 设备可通过 Google Play Store 安装多种应用。但是，为了将患者数据安全性的风险降低到最低，Philips 建议您仅安装来自受信任来源的应用并根据业务需要限制其使用。

由于您将自有设备与 Lumify 应用和探头结合使用，因此，您有责任确保设备与患者数据的安全性，以符合您当地的安全政策和法规要求。请咨询您的医疗 IT 安全部门，确保已根据信息安全的特定要求配置您的设备。

技术性安全要素的实际执行会因地点的不同而有所不同，而且可能需使用多种技术，包括防火墙、病毒扫描软件、身份验证技术等等。由于超声诊断系统是基于计算机的系统，因此一般需要用防火墙和其他安全设备，在此医疗系统与任何外部可访问的系统间构建保护层级。美国退伍军人事务部为此研发了一种使用广泛的隔离体系结构。这种防线和网络防卫是良好的安全惯例的一个基本要素。*《退伍军人事务部医疗设备隔离体系结构指南》*位于此网站上：

http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=7236

对产品安全事件和恶意软件检测的响应

如果发生产品安全事件，或在系统上检测到恶意软件，请立即断开系统网络，并向医疗 IT 安全部门报告此事件。或者，发送电子邮件至 productsecurity@philips.com 报告该事件。

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

安全问题与准则

下列准则包括具体的系统和数据漏洞实例及实施保护的方法。

备注

我们提供的移动设备集中管理工具可以帮助简化本文档中的准则，并且有助于简化部署、配置和安全问题。请咨询您机构的医疗 IT 安全部门。

设备要求

Philips Ultrasound 建议使用符合或超过 Lumify 应用最低要求及特定环境安全需求的设备。下一步是确保以符合当地安全政策及所有适用法规要求的方式，实施相应级别的安全控制措施。

设备加固

与台式机或笔记本电脑上使用的操作系统加固原理类似，设备加固涉及标识设备内包含的所有非必要功能和应用以及禁用不需要使用的功能或应用。根据设备情况，这可能包括禁用执行后台功能的应用，在使用 Lumify 时这些后台功能可能会影响设备的性能。设备加固可以消除随着时间推移可能会造成安全漏洞的服务，从而缩小设备的攻击面。

加密

大多数 Android 设备上采用的主要安全措施是加密。通过显示不可恢复的数据，加密有助于确保存储在系统上的数据得到保护并提高访问控制策略的强度。

网络安全

所有网络超声诊断系统必须连接到安全的局域网上，该局域网须提供防御计算机病毒和其他有害代码或通信阻塞的保护措施。确保局域网配备适当的保护措施，如仅使用安全的无线技术、防火墙、入侵检测和防护系统，以及漏洞扫描程序。

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

物理访问控制

每家医疗机构都应采取切实措施限制他人接近超声诊断系统，以防止个人未经授权意外、偶然或蓄意接触诊断系统。医疗机构的安全部门可以提供有关适当措施的详细信息。

设备位置

设备的放置位置应避免能从门口、走廊和其他通道看到，这样可以减少受保护信息在未经授权的情况下被人看到的几率。不管离开设备多长时间，都应在离开之前通过退出系统以显示空白屏幕或者手动清屏。

用户登录和退出保护

使用密码可以保护已保存的受保护健康信息（PHI），避免未经授权的访问，同时也能满足安全要求，使设备能够尽快投入使用。

考虑到平板电脑设备的大小和便携性，设置密码对于降低因系统放置错误或被盗造成的个人信息暴露风险非常重要。对于某些设备，可能采取了其他附加措施，在错误输入密码超过指定次数之后擦除设备中的所有数据。这些控制措施可以帮助增强标准的访问控制模式，并且有助于降低个人信息暴露的风险。

对于具有登录功能的设备，通过一个可靠的包括用户名和密码在内的用户登录进程，对信息提供良好的安全保护。在所有情况下，医疗保健机构必须控制对系统的访问。

保护性登录和密码惯例包括：

- 使用强密码。这是增强安全性最简单、最有效的方法。强密码由至少八个字母数字、混合大小写字母和特殊字符（例如“@”或“*”）构成。切勿使用可在字典中找到的字词。
- 切勿将用户名和密码告诉他人。
- 定期更改密码。

训练系统操作员，让他们在完成工作后立即退出系统。

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

信息维护实例

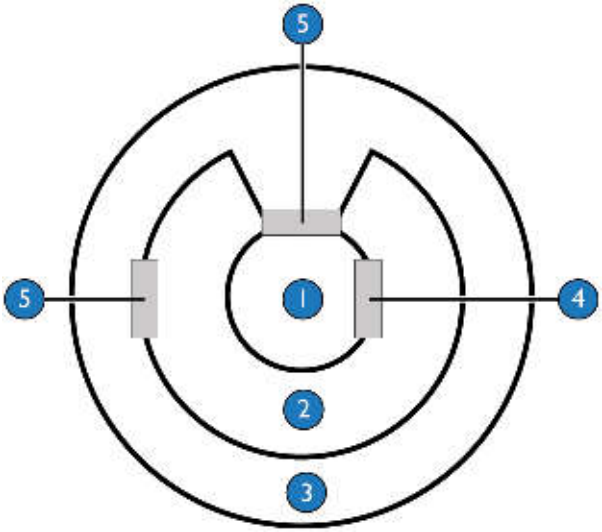
此信息安全维护实例采用信息流区域模型。

环境假设

超声诊断系统需医疗机构采用网络访问、加密和入侵检测等保护机制维持环境安全。

信息区域

此信息流模型通常涵盖在安全标准内。直观表示此模型的简单方法是，将医疗机构图示划分为三个区域（请参阅图示），每个区域对信息使用有不同的优先权和级别。有些医疗机构因不能保证其保护措施和完整性，决定不让信息扩散到最外层区域。



各区域之间的安全解决方案

1	区域 1：超声部门
2	区域 2：医疗机构的其他科室

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

3	区域 3：互联网
4	防火墙
5	采用 IPSec 的防火墙

区域 1：超声部门

绝大部分图像传输是在区域 1 内进行的。包含超声图像的备份、副本和介质必须由科室职员妥善保管。

区域 2：医疗机构的其他科室

某些情况下，区域 2 包括科室以外有权访问诊断系统和互联网的门诊部。正确的访问授权和审计跟踪极为重要。

区域 3：互联网

区域 3 用于连接到符合 HIPAA 的云存储提供商。

区域间的安全

区域间安全应由 IT 安全标准解决方案管理。管理人员必须知道数据流量的预期级别，从而选择安全的解决方案，但不要成为数据流的瓶颈。图像分发需要高带宽网络。

区域内的安全

区域内的安全应由 IT 标准安全解决方案和超声诊断系统的安全功能共同管理。

安全保护软件

通过定期发布新版本和 Philips 现场变更控制流程，提供 Lumify 应用更新。

防病毒扫描和更新

最好的防病毒措施是由医疗机构建立有效的网络安全策略。

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

恶意软件是导致那些占据头条新闻的许多漏洞的主要原因。传统的恶意软件防护方法包括防病毒 (AV)。Philips Ultrasound 建议选择能够满足您的恶意软件防护需求且享有声誉的软件包。此外，还可以采取其他措施降低系统出现恶意软件的潜在风险。这包括确保添加到设备的所有其他应用均来自可靠来源。虽然应用中可能包括恶意软件，但是，仅安装设备功能所需的应用有助于降低入侵或出现漏洞的风险。

备份和存档

小心

所选输出目标设备和机制必须符合当地的医疗 IT 安全政策。

您可以将 Lumify 超声诊断系统中的检查和图像输出到 DICOM PACS、网络共享或本地存储库。您还可以通过电子邮件发送图像。受支持的电子邮件应用包括 Gmail、K-9 Mail、Yahoo、Outlook 和 Inbox。

备份过程

超声诊断系统只适合保留必要的信息，用来生成医疗记录所需的外部文档（例如胶片、描记和打印的记录）。如果需要附加备份，请制定一个管理协议，以便在删除之前存档所有临床检查数据。

灾难恢复计划

确保有灾难恢复计划，包括进行定期的完整患者数据备份是使用者的责任。超声诊断系统是间歇性的存储设备；患者数据必须从超声诊断系统上输出。有关输出患者数据的更多信息，请参见超声诊断系统用户信息。

4535 619 14241_A/795 * NOV 2015

Philips Healthcare

Philips Healthcare 是 Royal Philips 的子公司

www.philips.com/healthcare
healthcare@philips.com

制造商地址.
Philips Ultrasound, Inc.
22100 Bothell Everett Hwy
Bothell, WA 98021-8431
USA

EC REP
Philips Medical Systems Nederland B.V.
Veenpluis 4-6
5684 PC Best
The Netherlands

CE 0086

发表于美国
4535 619 14241_A/795 * NOV 2015 - zh-CN