Servicios compartidos para seguridad del sistema y de los datos

Español

Sistema de ultrasonido Lumify

PHILIPS

Contenido

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

1 Introducción

Este documento aborda temas de seguridad en el sistema de ultrasonido Lumify. Mientras que otros sistemas de ultrasonido Philips se suministran como sistemas completos, con restricciones sobre qué funciones están autorizadas y disponibles para los mismos, es el centro sanitario o son personas individuales quienes se hallan a cargo de adquirir, configurar y mantener los dispositivos host de Lumify.

Estas directrices se han diseñado para ayudar a que los centros sanitarios comprendan cómo se puede poner en peligro la seguridad tanto de la aplicación Lumify de Philips como de los datos de paciente, y enfatizar los esfuerzos de Philips para cerciorarse de que estén correctamente puestas las salvaguardas que ayudarán a la prevención de brechas en la seguridad.

Si desea acceder a recursos de seguridad relacionados con sistemas de ultrasonido, tales como boletines de seguridad, preguntas frecuentes e información sobre vulnerabilidades, consulte el sitio web de seguridad de los productos Philips:

www.philips.com/productsecurity

Para obtener información sobre el sistema de ultrasonido Lumify, visite el portal de Lumify:

www.philips.com/lumify

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

Philips ha procurado garantizar la exactitud de este documento. Sin embargo, Philips no se hace legalmente responsable de los posibles errores u omisiones y se reserva el derecho a introducir cambios sin previo aviso a cualquiera de los productos aquí mencionados para mejorar su fiabilidad, funcionamiento o diseño. En cualquier momento, Philips puede introducir mejoras o cambios en los productos o programas descritos en este documento.

La copia no autorizada de este documento, además de violar las leyes de copyright, podría reducir la capacidad de Philips para proporcionar información exacta y actual a los usuarios.

Los nombres de productos que no pertenecen a Philips pueden ser marcas comerciales de sus respectivos titulares de derecho.

Información general

La siguiente información general se aplica al software de ultrasonido de Philips y a los datos de paciente.

- Los sistemas de ultrasonido Philips no son compatibles con el funcionamiento en sesiones multiusuario. Se han diseñado como dispositivos monousuario. No se permite el acceso para uso clínico a través de una red.
- Los sistemas de ultrasonido no son dispositivos para el almacenamiento a largo plazo. Los datos permanentes de los pacientes deben archivarse en un servidor DICOM PACS, en un recurso compartido de red o en un repositorio local.

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

2 Control de las vulnerabilidades en la seguridad de los productos de Philips Ultrasound

El objetivo de Philips es ayudar a todos los clientes a proteger la confidencialidad, integridad y disponibilidad de los datos de los pacientes a la vez que garantizar que los sistemas de ultrasonido sigan generando y administrando esta información con total seguridad. Los sistemas de ultrasonido pueden quedar vulnerables a brechas de seguridad al conectarse a una red.

Estrategia para una protección exhaustiva de la seguridad

En un centro sanitario, garantizar la seguridad de los datos de los pacientes y de los productos Philips requiere una estrategia de protección exhaustiva a varios niveles (entre los que se incluyen las políticas, los procesos y las tecnologías) para preservar la información y los sistemas de amenazas tantos internas como externas.

Si desea obtener información específica sobre la seguridad en su centro, consulte a los especialistas en seguridad de los siguientes departamentos o al personal con responsabilidades similares:

- Responsable principal de seguridad de la información
- Director del departamento de tecnologia de la información
- Responsable de cumplir con la seguridad o privacidad según las normas de HIPAA (ley de transferibilidad y responsabilidad de seguros médicos, en los Estados Unidos)
- Responsable de seguridad

Si desea obtener información sobre los problemas de seguridad en general o sobre vulnerabilidades concretas del sistema de ultrasonido, póngase en contacto con el representante de Philips.

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

Entorno reglamentario

Tanto el desarrollo y fabricación de los dispositivos médicos como la seguridad y privacidad de la información sobre pacientes que manipulan los profesionales sanitarios se hallan regulados de forma estricta. Esto supone una serie de retos para los profesionales sanitarios y los fabricantes, dado que deben responder de inmediato a cualquier nueva amenaza para la seguridad de los datos de paciente almacenados en los dispositivos médicos.

Protección de la información médica en formato electrónico

Uno de los activos más importantes que es necesario proteger con medidas de seguridad es la información médica de los pacientes. Por ejemplo, las siguientes regulaciones gubernamentales requieren que se proteja la confidencialidad de la información médica de los pacientes y especifican medidas de seguridad para resguardar la información de éstos:

- Ley de transferibilidad y responsabilidad de seguros médicos (Health Insurance Portability and Accountability Act, más conocida por su sigla HIPAA), en los Estados Unidos (www.hhs.gov/ocr/privacy/)
- Directiva europea sobre dispositivos médicos 93/42/CEE
- Norma HPB517 en Japón
- Partes relacionadas con HIPAA de la ley de estímulo económico federal de los EE. UU. (o la ley HITECH), conocida anteriormente como la ley de recuperación y reinversión americana de 2009

Función de Philips en la asociación para la seguridad de los productos

Philips opera conforme a una política de seguridad de productos global que regula el diseño orientado a la seguridad en la creación de productos, la evaluación de riesgos y las actividades de respuesta frente a incidentes por vulnerabilidades identificadas en los productos. Philips ha establecido un proceso de seguimiento de problemas y consultas global para aumentar la visibilidad de los problemas de seguridad en los sistemas Philips.

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

Respuesta a vulnerabilidades

Los ingenieros de productos de Philips controlan continuamente las vulnerabilidades de los sistemas, entre las que se incluyen las identificadas por los proveedores de software y sistemas operativos de otros fabricantes y las comunicadas por los centros sanitarios.

Una red global de equipos de respuesta dedicada a los incidentes de seguridad de los productos recopila y gestiona la información además de resolver las vulnerabilidades que afectan a los productos y soluciones Philips. Los equipos de respuesta siguen ampliando sus actividades con el fin de ofrecer una cobertura global para todos los sistemas.

El objetivo del equipo de respuesta es evaluar cada brecha actual y potencial a la seguridad mediante una valoración explícita del riesgo, la amenaza o la vulnerabilidad y desarrollar, según sea necesario, un plan de respuesta a las vulnerabilidades que incluya procedimientos de calificación y comunicación. Esto significa que el objetivo de Philips es informar a los clientes de las vulnerabilidades del sistema a la vez que desarrolla e implementa funciones para reducir el riesgo. Encontrará más información sobre las vulnerabilidades del sistema en este sitio web:

www.philips.com/productsecurity

Mejoras del diseño

Philips realiza evaluaciones exhaustivas de la seguridad de los productos para identificar las posibles vulnerabilidades. Con esta información, los equipos de ingenieros de Philips suelen definir una serie de cambios en la configuración y técnicos que protegen el sistema frente a las amenazas externas. Dicha información proporciona además los requisitos de diseño de seguridad necesarios para los nuevos productos. La política de seguridad de productos de Philips requiere un conjunto de objetivos de diseño orientado a la seguridad como parte de todo el proceso de creación de nuevos productos.

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

Función de los clientes en la asociación para la seguridad de los productos

ADVERTENCIA

Las modificaciones no autorizadas en su dispositivo Android ("rooting" [rootear] o "jailbreaking" [destrabar]) pueden provocar una avería en el sistema de ultrasonido, de la cual tal vez resulte un diagnóstico erróneo.

PRECAUCIÓN

En Google Play Store se dispone de muchas aplicaciones que se pueden instalar en los dispositivos Android. Sin embargo, a fin de minimizar el riesgo para la seguridad de los datos de paciente, Philips recomienda instalar sólo aplicaciones provenientes de fuentes de confianza y que su uso se limite a las necesidades del negocio.

Debido a que usted utiliza su propio dispositivo con la aplicación Lumify y los transductores, le corresponde garantizar la seguridad tanto de su dispositivo como de los datos de paciente para cumplir con las políticas de seguridad y los requisitos reglamentarios locales. Consulte con su departamento de seguridad tecnológica de la información de atención médica para cerciorarse de que su dispositivo esté implementado de acuerdo con los requisitos de seguridad de la información específicos de su institución.

La implementación práctica de elementos de seguridad técnicos varía en función de la ubicación y puede requerir diversas tecnologías como, por ejemplo, cortafuegos, software de detección de virus, tecnologías de autenticación, etc. Al igual que ocurre con otros sistemas informáticos, los sistemas de ultrasonido requieren el nivel de protección que suelen ofrecer los cortafuegos y otros dispositivos de seguridad entre el sistema médico y los sistemas a los que se puede acceder externamente. Para esta finalidad, el Departamento de Asuntos de Veteranos de los Estados Unidos desarrolló una arquitectura de aislamiento que se utiliza ampliamente.

4535 619 14271_A/795 * NOV 2015
Philips Healthcare

Dicha protección del perímetro y de la red es esencial para unas prácticas correctas en materia de seguridad. El documento *Department of Veterans Affairs Medical Device Isolation Architecture Guide* (Guía a la arquitectura de aislamiento de dispositivos médicos del Departamento de Veteranos) puede leerse en este sitio web:

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

Respuesta a incidentes de seguridad de los productos y detección de malware

En caso de un incidente de seguridad de los productos o si detecta malware (software malicioso) en el sistema, desconecte inmediatamente el sistema de la red e informe sobre el incidente a su departamento de seguridad tecnológica de la información de atención médica. Otra alternativa es informar acerca del incidente enviando un correo electrónico a productsecurity@philips.com.

Problemas y directrices de seguridad

Las siguientes directrices ofrecen ejemplos concretos de vulnerabilidades del sistema y los datos además de métodos para proporcionar protección.

NOTA

Se dispone de herramientas para la gestión central de dispositivos móviles a fin de ayudar a facilitar las directrices contenidas en este documento y a aliviar problemas relacionados con la implementación, configuración y seguridad. Consulte con el departamento de seguridad tecnológica de la información de atención médica de su institución.

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

Requisitos del dispositivo

Philips Ultrasound recomienda empezar con un dispositivo que cumpla con o supere los requisitos mínimos de la aplicación Lumify así como las necesidades de seguridad dentro del entorno específico. El siguiente paso es asegurar que se implemente el nivel adecuado de controles de seguridad de manera que éstos cumplan con las políticas de seguridad así como con toda obligación reglamentaria aplicable.

"Hardening" (protección) del dispositivo

El hardening del dispositivo, que es similar a las estrategias de hardening del sistema operativo utilizadas en equipos informáticos de escritorio o portátiles, implica identificar todas las funciones y aplicaciones no necesarias incluidas en su dispositivo e inhabilitar dichas funciones o aplicaciones que no se requieren para los propósitos de su institución. Dependiendo del dispositivo, esto podría incluir inhabilitar la capacidad de las aplicaciones de realizar funciones en segundo plano que podrían afectar al rendimiento de su dispositivo mientras se encuentre en uso Lumify. El hardening del dispositivo reduce la superficie de ataque de su dispositivo eliminando los servicios que puedan volverse vulnerables con el tiempo.

Cifrado

El cifrado es un control de seguridad clave disponible en la mayoría de los dispositivos Android. El cifrado ayuda a garantizar que los datos almacenados en el sistema estén protegidos, y aumenta el fortalecimiento de sus políticas de control de acceso al impedir que los datos sean recuperables.

Seguridad de la red

Todos los sistemas de ultrasonido en red se deben conectar a una red de área local segura que ofrezca protección frente a los virus informáticos y otros códigos o tráfico que puedan dañar el quipo. Asegúrese de que la red de área local utilice la protección adecuada, como, por ejemplo, emplear solamente tecnologías inalámbricas seguras, servidores de seguridad, sistemas de detección y prevención de intrusiones y detectores de vulnerabilidades.

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

Control de acceso físico al área

Todos los centros sanitarios deben restringir el acceso físico a los sistemas de ultrasonido para evitar el contacto accidental, casual o deliberado de personas no autorizadas. El departamento de seguridad del centro puede ofrecer más información sobre las medidas establecidas.

Ubicación del dispositivo

El acceso visual no autorizado a la información protegida se puede minimizar mediante la ubicación del dispositivo de modo que no se pueda ver desde las entradas, los pasillos y otras áreas de tránsito. Inicie el blanqueo de pantalla dando por finalizada su sesión con el sistema o borrando manualmente la visualización antes de dejar el dispositivo desatendido por cualquier lapso de tiempo.

Protecciones de inicio y cierre de sesión de usuario

Una contraseña protege la información médica protegida (PHI, por sus siglas en inglés) contra el acceso no autorizado, a la vez que cumple los requisitos de seguridad para que el dispositivo se pueda utilizar lo antes posible.

Tomando en cuenta el tamaño y la transportabilidad de los dispositivos de tableta, la implementación de una contraseña o un código de acceso es fundamental para reducir la posibilidad de que la información del sistema quede expuesta si el sistema se extravía o es robado. Con algunos dispositivos, pueden implementarse controles adicionales para eliminar todos los datos del dispositivo en caso de que se introduzca incorrectamente la contraseña o el código de acceso una cierta cantidad de veces. Dichos controles ayudan a mejorar el modelo de control de acceso estándar y a reducir la posibilidad de que quede expuesta información personal.

Para los dispositivos con funciones de inicio de sesión, un proceso sistemático de inicio de sesión de usuario que incluya nombres de usuario y contraseñas ofrece un nivel de seguridad adecuado para proteger la información. En todos los casos, corresponde al centro sanitario la responsabilidad de controlar el acceso al sistema.

Las prácticas de inicio de sesión y contraseña incluyen lo siguiente:

4535 619 14271_A/795 * NOV 2015
Philips Healthcare

- Implemente contraseñas seguras. Es el método más sencillo y eficaz para aumentar la seguridad. Las contraseñas seguras constan como mínimo de ocho caracteres alfanuméricos, caracteres en mayúsculas y minúsculas, y caracteres especiales como “@” o “*”. Nunca utilice palabras que pueden encontrarse en un diccionario.
- No envíe ni comparta los nombres de usuario y las contraseñas.
- Cambie las contraseñas periódicamente.

Instruya a los usuarios del sistema para que cierren la sesión inmediatamente después de finalizar su trabajo.

Ejemplo de mantenimiento de la información

Este ejemplo sobre cómo proteger la seguridad de la información utiliza un modelo de zona para el flujo de información.

Suposiciones sobre el entorno

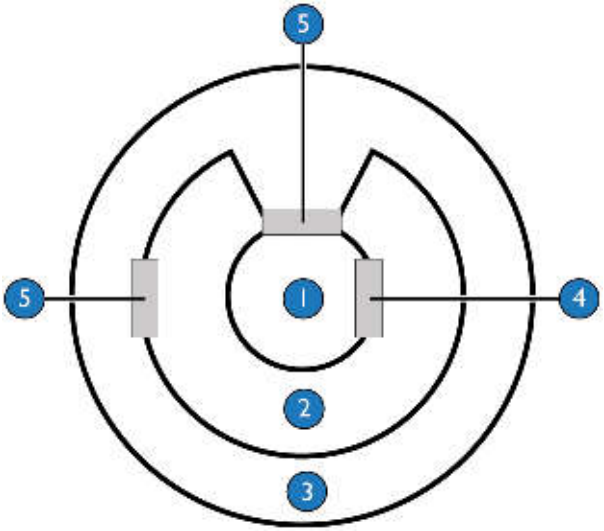
El sistema de ultrasonido depende del centro sanitario por lo que respecta al mantenimiento de un entorno seguro mediante una serie de mecanismos de protección para el acceso a la red, cifrado y detección de intrusiones.

Zonas de información

El modelo de flujo de información suele incluirse en los estándares de seguridad. Una forma sencilla de visualizar este modelo consiste en trazar un plano del centro sanitario dividido en tres zonas (consulte la figura), cada una de las cuales tendrá una prioridad y nivel distintos por lo que respecta al uso de la información. Algunos centros optan por no llevar la información hasta la zona más alejada debido a que no pueden garantizar su protección e integridad.

4535 619 14271_A/795 * NOV 2015

Philips Healthcare



Soluciones de seguridad entre zonas

1	Zona 1: Departamento de sistemas de ultrasonido
2	Zona 2: Resto del centro sanitario
3	Zona 3: Internet
4	Servidor de seguridad
5	Servidor de seguridad con IPSec

Zona 1: Departamento de sistemas de ultrasonido

La mayor parte de la transferencia de imágenes se realiza en la Zona 1. El personal del departamento debe gestionar con cuidado las copias, las copias de seguridad y los soportes que contienen imágenes ecográficas.

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

Zona 2: Resto del centro sanitario

La Zona 2 incluye a personal externo al departamento que tiene acceso al sistema y, en algunos casos, a Internet. Una autorización adecuada para el acceso y uso de las pistas de auditoría es de vital importancia.

Zona 3: Internet

La Zona 3 se utiliza para la conexión a un proveedor de almacenamiento en la nube, que cumpla con la ley HIPAA.

Seguridad entre zonas

La seguridad entre zonas se debe gestionar mediante soluciones de seguridad de TI. Los administradores deben tener en cuenta el nivel previsto de tráfico de datos para elegir una solución segura sin que actúe como cuello de botella en el flujo de información. La distribución de imágenes requiere una red con un ancho de banda alto.

Seguridad en las zonas

La seguridad en las zonas se debe gestionar mediante una combinación de soluciones de seguridad de TI estándar y las funciones de seguridad del sistema de ultrasonido.

Software de protección de seguridad

Se proporcionan actualizaciones a la aplicación Lumify mediante versiones regulares y el proceso de Philips para solicitud de modificación del producto en campo (FCO, por sus siglas en inglés).

Exploración antivirus y actualizaciones

La mejor protección contra virus consiste en que el centro sanitario establezca una política eficaz de seguridad de red.

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

El malware es responsable de muchas de las brechas que actualmente ocupan los titulares. Entre los métodos tradicionales de protección contra malware se incluye el antivirus (AV). Philips Ultrasound recomienda elegir un paquete de software reconocido que sea capaz de satisfacer sus necesidades de protección contra malware. Pueden tomarse pasos adicionales para limitar la posibilidad de la aparición de malware en sus sistemas. Esto incluye asegurar que toda aplicación que se añada a su dispositivo provenga de una fuente de confianza. Si bien existen aplicaciones que pueden incluir malware, instalar sólo aplicaciones necesarias para la funcionalidad de su dispositivo ayudará a limitar el riesgo de infección o brechas.

Copias de seguridad y archivos permanentes

PRECAUCIÓN

El destino de exportación y mecanismo elegidos deben cumplir con las políticas de seguridad tecnológica de la información de atención médica locales.

Se pueden exportar exámenes e imágenes desde el sistema de ultrasonido Lumify a un servidor DICOM PACS, a un recurso compartido de red o a un repositorio local. También se pueden enviar imágenes en mensajes de correo electrónico. Entre las aplicaciones de correo electrónico compatibles se incluyen Gmail, K-9 Mail, Yahoo, Outlook e Inbox.

Procedimiento de copias de seguridad

Los sistemas de ultrasonido se han diseñado para conservar la información sólo en la medida de lo necesario para producir documentación externa en función de registros médicos (como películas, trazados y registros impresos). Si se requiere un sistema adicional de copias de seguridad, establezca un protocolo administrativo para archivar todos los estudios clínicos antes de ser eliminados.

4535 619 14271_A/795 * NOV 2015
Philips Healthcare

Planes de recuperación de desastres

Corresponde al usuario asegurar la implementación de un plan de recuperación de desastres que incluya la realización periódica y completa de copias de seguridad de datos de paciente. Los sistemas de ultrasonido son dispositivos de almacenamiento temporal; los datos de paciente se deben exportar desde dichos sistemas. Encontrará más información sobre cómo exportar datos de paciente en la información para el usuario del sistema de ultrasonido.

4535 619 14271_A/795 * NOV 2015

Philips Healthcare

Philips Healthcare forma parte de Royal Philips

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

Dirección de fabricación
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
Países Bajos

CE 0086

Publicado en EE.UU.
4535 619 14271_A/795 * NOV 2015 - es-ES