Rôles partagés pour la sécurité du système et des données

Français

Échographe Lumify

PHILIPS

Table des matières

1 Introduction..... 5

Informations générales..... 6

2 Contrôle de vulnérabilité de la sécurité des produits Philips Ultrasound..... 7

Stratégie pour une sécurité de défense approfondie..... 7

Environnement réglementaire..... 8

Rôle de Philips dans le partenariat de sécurité des produits..... 8

Rôle des clients dans le partenariat de sécurité des produits..... 10

Problèmes et directives de sécurité..... 11

Exemple de maintien d'informations..... 14

Suppositions sur l'environnement..... 14

Zones d'informations..... 14

Logiciel de protection de sécurité..... 16

Balayage et mises à jour antivirus..... 16

Stockages et archivages..... 17

Procédure de copie de secours..... 17

Plans anti-sinistres..... 18

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

Table des matières

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

1 Introduction

Ce document décrit les dispositifs de sécurité de l'échographe Lumify. Alors que les autres échographes Philips sont livrés avec toutes les fonctionnalités, compte tenu de ce qui est autorisé et disponible pour l'échographe, les dispositifs hôtes Lumify sont acquis, configurés et maintenus par l'établissement de soins ou les utilisateurs.

Ces recommandations sont conçues pour aider les établissements de soins à comprendre comment la sécurité de l'application Lumify Philips et des données des patients peuvent être compromises, et pour mettre en évidence les efforts faits par Philips pour garantir la mise en place de mesures de contrôle permettant d'empêcher de telles infractions à la sécurité.

Pour des informations sur la sécurité des échographes, telles que les communiqués sur la sécurité, la FAQ et les informations sur la vulnérabilité du matériel, consultez le site Web Philips Product Security :

www.philips.com/productsecurity

Pour plus d'informations sur l'échographe Lumify, rendez-vous sur le portail Lumify :

www.philips.com/lumify

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

Philips a pris soin de vérifier l'exactitude de ce document. Toutefois, Philips n'est pas responsable des erreurs ou des omissions qui pourraient apparaître et se réserve le droit de faire toute modification sans préavis sur tout produit mentionné dans ce document afin d'améliorer sa fiabilité, son fonctionnement ou sa conception. Philips peut améliorer ou modifier les produits ou les programmes décrits dans ce document à tout moment.

La copie non autorisée de ce document, en plus de violer le droit d'auteur, pourrait réduire la capacité de Philips à fournir des informations exactes et à jour aux utilisateurs.

Les noms de produit n'appartenant pas à Philips peuvent être des marques déposées de leurs propriétaires respectifs.

Informations générales

Les informations générales suivantes concernent la sécurité du logiciel échographique Philips et des données des patients.

- Les échographes Philips ne permettent pas de conduire des sessions multi-utilisateurs. Ils sont conçus comme des appareils mono-utilisateur. L'accès pour utilisation clinique par l’intermédiaire d’un réseau n’est pas pris en charge.
- Les échographes et ne sont pas des dispositifs de stockage à long terme. Les données persistantes des patients doivent être archivées sur un PACS DICOM, une part de réseau ou un référentiel local.

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

2 Contrôle de vulnérabilité de la sécurité des produits Philips Ultrasound

Philips s'engage à aider tous ses clients à maintenir la confidentialité, l'intégrité et la disponibilité des données des patients, tout en garantissant que leurs échographes continueront à créer et traiter ces informations en toute sécurité. Les échographes peuvent devenir vulnérables aux infractions de sécurité lorsqu'ils sont connectés à un réseau.

Stratégie pour une sécurité de défense approfondie

Au sein de l'établissement de soins, le maintien de la sécurité des données des patients et des produits Philips exige une stratégie de défense en profondeur, complète et à plusieurs niveaux (comprenant les principes, processus et techniques) servant à protéger les informations et les appareils contre toutes menaces externes.

Pour des informations spécifiques sur la sécurité au sein de votre établissement, adressez-vous au personnel en charge de la sûreté des services de sécurité générale et de systèmes d'informations ou aux personnes ayant des responsabilités similaires.

- Responsable principal de la sécurité des informations
- Responsable principal du système d'informations
- Responsable de la sécurité et de la confidentialité HIPAA (uniquement aux États-Unis)
- Responsable de la sécurité

Pour connaître les problèmes généraux de sécurité ou les points vulnérables spécifiques de votre échographe, contactez votre représentant Philips.

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

Environnement réglementaire

Le développement et la fabrication des appareils médicaux sont strictement réglementés, ainsi que la sécurité et la confidentialité des informations des patients à la disposition des fournisseurs de soins médicaux. Cela constitue un défi porté aux fournisseurs de soins et aux fabricants, dans la mesure où ils doivent répondre rapidement aux menaces apportées à la sécurité des données de patients stockées sur les appareils médicaux.

Protection des informations électroniques sur la santé du patient

L'une des valeurs les plus importantes à protéger est l'information médicale du patient. Par exemple, les réglementations suivantes exigent que les informations médicales du patient restent confidentielles, et elles spécifient les mesures de sécurité à prendre pour protéger les informations du patient :

- Health Insurance Portability and Accountability Act (HIPAA) aux États-Unis (www.hhs.gov/ocr/privacy/)
- La directive européenne relative aux appareils médicaux 93/42/CEE
- HPB517 au Japon
- Les parties du programme de stimulation économique (ou HITECH), connu officiellement sous le nom de American Recovery and Reinvestment Act de 2009, relatives au HIPAA aux États-Unis

Rôle de Philips dans le partenariat de sécurité des produits

Philips fonctionne dans le cadre d'une directive globale de sécurité des produits (Product Security Policy) qui régit une conception tournée vers la sécurité de la création des produits, de l'évaluation des risques et des activités de réponse aux accidents pour toute vulnérabilité signalée dans les produits existants. Philips a engagé un processus global de dépistage des problèmes et de niveaux de résolution qui met en évidence les problèmes de sécurité des échographes Philips.

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

Réponse aux problèmes de vulnérabilité

Les groupes d'ingénierie des produits au sein de Philips surveillent continuellement les échographes pour déceler toute nouvelle vulnérabilité, ainsi que celles signalées par des fournisseurs de logiciels de société indépendante et de systèmes d'exploitation, et par des établissements de soins individuels.

Un réseau global de groupes d'intervention spécialisés dans les accidents dus à des problèmes de sécurité des produits rassemble et traite les informations et s'occupe de toute vulnérabilité qui affecte les produits et les solutions Philips. Ces groupes continuent à étendre leur activité pour une protection globale de tous les échographes.

Le but du groupe d'intervention approprié est d'évaluer chaque infraction réelle ou potentielle et de déterminer explicitement le risque, la menace ou la vulnérabilité, et de développer, au besoin, un plan de réponse à la vulnérabilité qui comprend des procédures de qualification et de communication. Ce qui signifie que Philips a l'intention d'informer simultanément les clients des problèmes de vulnérabilité de l'échographe tout en continuant le développement et la réalisation d'efforts de réduction des risques. Pour plus d'informations sur la vulnérabilité des échographes, visitez ce site Web :

www.philips.com/productsecurity

Améliorations de la conception de l'appareil

Philips effectue activement des évaluations internes de la sûreté des produits pour identifier les faiblesses de sécurité potentielles. Les groupes d'ingénierie de Philips possédant ces informations définissent souvent des modifications de configuration et des efforts de reconstruction mécanique, qui permettent à l'échographe de résister aux menaces externes. Les mêmes informations définissent également les spécifications de conception de sécurité pour les nouveaux produits. La directive de sécurité des produits de Philips (Philips Product Security Policy) exige des objectifs de conception avec sécurité pour tous les efforts de création de nouveaux produits.

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

Rôle des clients dans le partenariat de sécurité des produits

AVERTISSEMENT

Des modifications non autorisées effectuées sur votre dispositif Android (« rootage » ou « jailbreaking ») peuvent provoquer un dysfonctionnement de l'échographe qui peut conduire à un mauvais diagnostic.

MISE EN GARDE

Les appareils Android disposent de plusieurs applications disponibles qui peuvent être installées depuis la boutique Google Play. Toutefois, et pour limiter le risque apporté à la sécurité des données des patients, Philips vous recommande de n'installer que des applications provenant de sources fiables et de limiter leur utilisation à vos besoins professionnels.

Comme vous utilisez votre propre appareil avec l'application et les sondes Lumify, il est de votre responsabilité d'assurer que la sécurité de votre appareil et des données du patient satisfont à vos règlements de sécurité et aux exigences réglementaires locaux. Consultez votre service de sécurité informatique médical pour vérifier que votre appareil est fabriqué conformément aux exigences spécifiques de sécurité des informations.

La mise en œuvre pratique des éléments de sécurité technique varie selon le site et peut utiliser un nombre de technologies, comme les pare-feu, un logiciel antivirus, des technologies d’authentification, etc. Comme pour tous les systèmes informatisés, les échographes exigent un niveau de protection généralement fourni par les pare-feu et autres dispositifs de sécurité entre le système médical et tous les systèmes accessibles externes. Le Département des Anciens combattants des États-Unis (United States Department of Veterans Affairs ou VA) a

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

développé une architecture d'isolation très utilisée dans ce but. Ces défenses de périmètres et de réseau sont essentielles aux bonnes pratiques de sécurité. Le Department of Veterans Affairs *Medical Device Isolation Architecture Guide* se trouve sur ce site web :

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

Réponse aux incidents de sécurité du produit et à la détection d'antiprogrammes

Dans le cas d'un incident se rapportant à la sécurité du produit, ou si vous détectez un programme malveillant sur l'échographe, déconnectez immédiatement l'échographe du réseau et signalez le problème à votre service de sécurité informatique médical. Vous pouvez également signaler ce problème par e-mail à- productsecurity@philips.com.

Problèmes et directives de sécurité

Les directives suivantes offrent des exemples concrets de vulnérabilité de l'échographe et des données et des méthodes à utiliser pour les protéger.

REMARQUE

Les outils de gestion centrale des appareils mobiles sont disponibles pour faciliter les recommandations de ce document et les problèmes de déploiement, de configuration et de sécurité. Consultez le service de sécurité informatique médical de votre établissement.

Spécifications relatives à l'appareil

Philips Ultrasound vous recommande de commencer avec un appareil qui est conforme aux spécifications minimales de l'application Lumify, ou les dépassent, ainsi qu'aux besoins de sécurité au sein de votre environnement particulier. L'étape suivante consiste à assurer que les contrôles de sécurité de niveau approprié sont mis en œuvre, de manière à ce qu'ils répondent à vos règlements de sécurité, ainsi qu'à toutes obligations réglementaires locales applicables.

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

Sécurisation renforcée de l'appareil

Comme pour les stratégies de sécurisation renforcée OS utilisées pour les ordinateurs fixes ou portables, la sécurisation renforcée de l'appareil comprend l'identification des fonctions et des applications qui ne sont pas nécessaires et qui se trouvent dans votre appareil, et la désactivation de celles que vous ne devez pas utiliser. Selon l'appareil, cela peut comprendre la désactivation de la possibilité pour ces applications d'avoir une fonction en arrière-plan qui peut affecter la performance de votre appareil lorsque vous utilisez Lumify. La sécurisation renforcée permet de diminuer la surface d'attaque de votre appareil en éliminant les services qui, au fil du temps, peuvent devenir vulnérables.

Cryptage

Le cryptage est une commande clé de sécurité disponible sur la majorité des appareils Android. Il vous aide à assurer que les données stockées sur le système sont protégées et il renforce vos règlements de contrôle d'accès en rendant les données irrécupérables.

Sécurité du réseau

Tous les échographes reliés au réseau doivent être connectés à un réseau local sécurisé qui offre une protection contre les virus informatiques et tout autre code ou circulation dangereuse. Assurez-vous que le réseau local utilise une protection appropriée, comme l’utilisation exclusive de technologies sans fil sécurisées, des pare-feu, des systèmes de détection et de prévention des intrusions et des scanners antivirus.

Contrôle de l’accès physique

Chaque établissement de soins doit limiter l’accès physique aux échographes pour empêcher tout contact accidentel, occasionnel ou délibéré par des personnes non autorisées. Le service de sûreté ou de sécurité de l’établissement peut fournir plus d’informations sur les mesures en place.

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

Position de l'appareil

L’accès visuel non autorisé aux informations protégées peut être limité en plaçant l'appareil de façon à ce qu’il ne puisse pas être vu depuis la porte d’entrée, le couloir et les autres zones de passage. Videz l'écran en vous déconnectant de l'échographe ou en effaçant manuellement l'affichage avant de laisser l'appareil sans surveillance pour une durée quelconque.

Protection des connexions et déconnexions utilisateur

Un mot de passe protège les informations médicales protégées et sauvegardées contre les accès non autorisés, tout en respectant les exigences de sécurité pour s'assurer que le dispositif est opérationnel dès que possible.

Compte tenu de la taille et de la portabilité des tablettes, l'attribution d'un mot de passe ou d'un code est très importante, afin de réduire la possibilité d'exposition des informations personnelles, si l'appareil est déplacé ou volé. Des commandes supplémentaires peuvent être attribuées sur certains appareils, afin d'effacer toutes les données du système si le mot de passe ou le code ne sont pas entrés correctement après un nombre spécifié de saisies. Ces commandes aident à améliorer le modèle standard de commande d'accès et à diminuer la possibilité d'exposer les informations personnelles.

Pour les appareils dotés de la fonction de connexion, un processus de connexion utilisateur consistant, comprenant les noms et mots de passe des utilisateurs, fournit une sécurité excellente à la protection des informations. Dans tous les cas, l'établissement de soins doit contrôler l'accès au système.

Les règles de protection des mots de passe et des connexions comprennent ce qui suit :

- Attribution de mots de passe sophistiqués. C’est la méthode la plus facile et la plus efficace pour assurer la sécurité d’accès. Les mots de passe « forts » comportent au moins huit caractères alphanumériques, en majuscules et en minuscules, des chiffres et des caractères spéciaux tels que « @ » ou « * ». N'utilisez jamais des mots qui se trouvent dans un dictionnaire.
- N’affichez pas et ne partagez pas des noms et mots de passe utilisateur.
- Changez régulièrement de mot de passe.

Apprenez aux utilisateurs à se déconnecter immédiatement après avoir terminé leur travail.

4535 619 14251_A/795 * NOV 2015

Exemple de maintien d’informations

Cet exemple, illustrant comment maintenir la sécurité des informations, utilise un concept de zones de flux d’informations.

Suppositions sur l’environnement

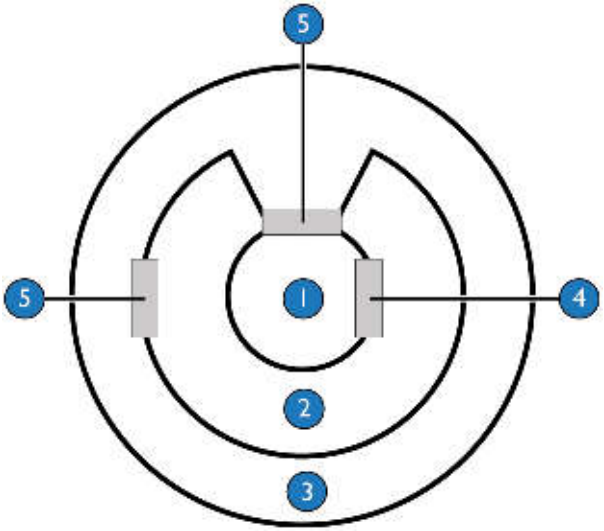
L’échographe dépend de l’établissement de soins pour le maintien d’un environnement sécurisé, avec des mécanismes de protection d’accès au réseau, de codage et de détection des intrusions.

Zones d’informations

Le concept de flux d’informations est généralement incorporé dans les normes de sécurité. Pour visualiser facilement ce concept, il suffit de faire un diagramme de l’établissement de soins divisé en trois zones (voir la figure), chaque zone ayant une priorité et un niveau d’utilisation différents pour les informations. Certains établissements décident de ne pas étendre leurs informations jusqu’à la zone la plus lointaine, parce qu’ils ne peuvent pas garantir sa protection et son intégrité.

4535 619 14251_A/795 * NOV 2015

Philips Healthcare



Solutions de sécurité entre les zones

1	Zone 1 : le service d'échographie
2	Zone 2 : le reste de l'établissement de soins
3	Zone 3 : Internet
4	Pare-feu
5	Pare-feu avec IPSec

Zone 1 : le service d'échographie

La plupart des transferts d'images s'effectuent dans la Zone 1. Les sauvegardes, les copies et les supports contenant des images échographiques doivent être soigneusement gérés par le personnel du service.

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

Zone 2 : le reste de l'établissement de soins

La zone 2 comprend les cliniques en dehors du service qui ont accès à l'échographe et, dans certains cas, Internet. Une autorisation d'accès correcte et une utilisation des journaux d'audit sont extrêmement importantes.

Zone 3 : Internet

La Zone 3 est utilisée pour une mise en réseau avec un fournisseur de stockage cloud conforme à HIPAA.

Sécurité entre les zones

La sécurité entre les zones doit être gérée par des solutions de sécurité informatique standard. Les responsables doivent connaître le niveau attendu de circulation des données pour choisir une solution sûre, mais qui ne bloque pas le flux d'informations. La distribution des images nécessite un réseau à bande passante élevée.

Sécurité à l'intérieur des zones

La sécurité à l'intérieur des zones doit être gérée par une combinaison de solutions de sécurité informatique standard et de la fonction de sécurité de l'échographe.

Logiciel de protection de sécurité

Des mises à jour d'applications Lumify sont fournies régulièrement avec des nouvelles versions disponibles et au moyen du processus Philips Field Change Order.

Balayage et mises à jour antivirus

La meilleure protection contre les virus consiste en l'application, par l'établissement de soins, d'une réglementation efficace de sécurité du réseau.

Les programmes malveillants sont la cause de nombreuses infractions qui font la une de la presse aujourd'hui. Les méthodes traditionnelles de protection contre les programmes malveillants comprennent les antivirus (AV). Philips Ultrasound vous recommande de choisir

4535 619 14251_A/795 * NOV 2015

Philips Healthcare

une option logicielle réputée qui peut répondre à vos besoins de protection contre les programmes malveillants. D'autres mesures peuvent être prises pour limiter la possibilité de programmes malveillants sur vos systèmes. Vous devez notamment veiller à ce que toutes les applications supplémentaires ajoutées à votre appareil proviennent de source réputée. Bien que des applications puissent contenir des programmes malveillants, l'installation uniquement de programmes nécessaires au fonctionnement de votre appareil vous aideront à limiter le risque d'infection ou d'infraction.

Stockages et archivages

MISE EN GARDE

La destination et le mécanisme d'exportation sélectionnés doivent respecter les règlements de votre service de sécurité informatique médical local.

Vous pouvez exporter des images et des examens de l'échographe Lumify vers un DICOM PACS, une part de réseau ou un emplacement d’archivage local. Vous pouvez aussi envoyer les images par e-mail. Les applications d'e-mail prises en charge comprennent Gmail, K-9 Mail, Yahoo, Outlook et Inbox.

Procédure de copie de secours

Les échographes sont conçus pour conserver les informations uniquement si elles sont nécessaires à la production de documentation externe pour des dossiers médicaux (tels que des films, des tracés et des dossiers imprimés). Si une sauvegarde supplémentaire est requise, créez un protocole administratif pour archiver toutes les études cliniques avant leur suppression.

4535 619 14251_A/795 * NOV 2015
Philips Healthcare

Plans anti-sinistres

Vous êtes responsable de l’application d’un plan anti-sinistre qui comprend un stockage régulier et complet des données des patients. Les échographes sont des appareils à stockage intermittent et les données des patients doivent être exportées de l’échographe. Pour plus d’informations sur l'exportation des données du patient, voir les informations utilisateur de votre échographe.

4535 619 14251_A/795 * NOV 2015
Philips Healthcare

Philips Healthcare, une division de Royal Philips

www.philips.com/healthcare

healthcare@philips.com

Adresse du fabricant
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
Pays-Bas

CE 0086

Publié aux États-Unis
4535 619 14251_A/795 * NOV 2015 - fr-FR