Ruoli condivisi per la protezione di sistemi e dati

Italiano

Sistema per ecografia Lumify

PHILIPS

Sommario

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

Sommario

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

1 Introduzione

Questo documento affronta le questioni di sicurezza relative ai sistemi per ecografia Lumify. Qualora gli altri sistemi per ecografia Philips vengano forniti come sistemi completi, con eventuali limiti in termini di autorizzazioni e disponibilità per il sistema, l'acquisto, la configurazione e la manutenzione dei computer host Lumify sono a carico della struttura sanitaria o del singolo individuo.

Le presenti linee guida sono state redatte per informare le strutture sanitarie sul modo in cui la sicurezza dei dati dei pazienti e dell'app Lumify Philips possono essere compromessi e per illustrare le misure adottate da Philips per proteggere tali dati e impedire violazioni della sicurezza.

Per accedere alle risorse relative alla sicurezza del sistema per ecografia, come bollettini sulla sicurezza, FAQ e informazioni sulla vulnerabilità del prodotto, visitare il sito Web Philips Product Security, all'indirizzo:

www.philips.com/productsecurity

Per ulteriori informazioni sul sistema per ecografia Lumify, visitare il portale Lumify:

www.philips.com/lumify

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

Philips ha adottato le opportune misure per garantire la precisione del presente documento. Tuttavia Philips declina qualsiasi responsabilità per eventuali errori od omissioni e si riserva il diritto di apportare modifiche senza preavviso a qualsiasi prodotto ivi menzionato, al fine di migliorarne l'affidabilità, la funzione o il disegno. Philips può apportare miglioramenti o modifiche ai prodotti o ai programmi illustrati nel documento in qualsiasi momento.

La copia non autorizzata del presente documento, oltre alla violazione del copyright, potrebbe ridurre la capacità di Philips di fornire agli utenti informazioni accurate e aggiornate.

I nomi di prodotti non di Philips possono essere marchi commerciali di proprietà dei rispettivi detentori.

Informazioni generali

Le seguenti informazioni generali riguardano la sicurezza dei dati dei pazienti e del software dei sistemi per ecografia Philips.

- I sistemi per ecografia Philips non supportano la modalità multiutente. Sono progettati per essere utilizzati come dispositivi per un singolo utente. L'accesso all'utilizzo clinico in rete non è supportato.
- I sistemi per ecografia non sono dispositivi di archiviazione a lungo termine. I dati permanenti dei pazienti devono essere archiviati in un DICOM PACS, condivisi in rete o salvati in un archivio locale.

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

2 Controllo delle vulnerabilità dei prodotti per ecografia Philips

Philips si impegna ad aiutare tutti i clienti a preservare la riservatezza, l'integrità e la disponibilità dei dati dei pazienti e a garantire che i propri sistemi per ecografia siano in grado di generare e gestire tali informazioni in modo sicuro. I sistemi per ecografia possono divenire vulnerabili ed essere soggetti a violazioni se sono collegati a una rete.

Strategia di protezione a più livelli

All'interno di una struttura sanitaria, la gestione della sicurezza dei dati dei pazienti e dei prodotti Philips richiede l'adozione di una strategia di protezione a più livelli, completa e composta da elementi diversificati (che includono criteri, procedure e tecnologie), per proteggere i dati e i sistemi da minacce interne ed esterne.

Per informazioni specifiche sulla protezione all'interno della struttura, rivolgersi agli specialisti dei reparti indicati di seguito o di reparti equivalenti con responsabilità analoghe:

- Responsabile della protezione dei dati
- Responsabile del dipartimento IT
- Responsabile della riservatezza o della sicurezza HIPAA (negli Stati Uniti)
- Responsabile della sicurezza

Per informazioni di carattere generale sulla protezione o su vulnerabilità specifiche del sistema per ecografia in uso, rivolgersi al rappresentante dell'assistenza Philips.

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

Panorama normativo

Lo sviluppo e la produzione di apparecchi medicali sono soggetti a rigorose normative, analogamente alla protezione e alla riservatezza dei dati dei pazienti gestiti dai fornitori di servizi sanitari. Tanto i fornitori di servizi sanitari quanto i produttori sono pertanto chiamati a individuare rapidamente delle contromisure alle nuove minacce che mettono a rischio la sicurezza dei dati dei pazienti memorizzati nelle apparecchiature medicali.

Protezione dei dati sanitari dei pazienti in formato elettronico

Una delle risorse più importanti che è necessario proteggere con misure adeguate è rappresentata dai dati sanitari dei pazienti. Le seguenti disposizioni, ad esempio, stabiliscono l'obbligo di riservatezza dei dati sanitari dei pazienti e indicano le misure di protezione da utilizzare per la salvaguardia di tali dati:

- la normativa HIPAA (Health Insurance Portability and Accountability Act) negli Stati Uniti (www.hhs.gov/ocr/privacy/);
- la direttiva 93/42/CEE dell'Unione Europea sui dispositivi medici;
- la normativa HPB517 in Giappone;
- le parti correlate all'HIPAA della normativa HITECH (federal economic-stimulus act) statunitense, chiamata ufficialmente American Recovery and Reinvestment Act del 2009.

Partnership per la protezione dei prodotti: il ruolo di Philips

Philips ha adottato un criterio globale di protezione dei prodotti in base al quale la sicurezza dei prodotti viene progettata nella fase di creazione, nella valutazione dei rischi e nelle attività di risposta agli incidenti per le vulnerabilità identificate nei prodotti esistenti. Philips ha implementato una procedura globale di identificazione e gestione che assicura la visibilità dei problemi legati alla sicurezza relativi ai sistemi Philips.

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

Risposta alle vulnerabilità

I team interni Philips incaricati della progettazione dei prodotti tengono costantemente sotto controllo le nuove vulnerabilità per la sicurezza dei sistemi, incluse le vulnerabilità identificate da altri produttori di software e di sistemi operativi e quelle segnalate dalle singole strutture sanitarie.

Una rete globale di team specializzati studia il metodo di risposta agli incidenti relativi alla sicurezza dei prodotti, gestisce le informazioni e risolve le vulnerabilità riguardanti i prodotti e le soluzioni Philips. Questi team specializzati estendono sempre più le proprie attività allo scopo di garantire la copertura globale di tutti i sistemi.

L'obiettivo di ciascun team è esaminare le singole violazioni, effettive o potenziali, della protezione con una chiara valutazione dei rischi, delle minacce e delle vulnerabilità, come pure sviluppare, in base alle necessità, un piano di risposta che includa procedure di certificazione e comunicazione. Con questa strategia, Philips intende informare i clienti delle vulnerabilità dei sistemi e, contemporaneamente, sviluppare e implementare misure di riduzione dei rischi. Per ulteriori informazioni sulle vulnerabilità del sistema, visitare il sito Web:

www.philips.com/productsecurity

Progettazione più efficace

Philips esegue valutazioni interne sulla sicurezza dei prodotti allo scopo di identificare le potenziali vulnerabilità. Grazie a tali informazioni, i team di progettazione Philips studiano modifiche alle configurazioni e nuove progettazioni in grado di aumentare il livello di protezione dei sistemi contro le minacce esterne. Le stesse informazioni vengono utilizzate per definire i requisiti di protezione nella progettazione dei nuovi prodotti. La politica di Philips per la protezione dei prodotti include obiettivi di design di sicurezza in tutte le attività di sviluppo di nuovi prodotti.

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

Partnership per la protezione dei prodotti: il ruolo dei clienti

AVVERTENZA

Le modifiche non autorizzate al dispositivo Android ("rooting" o "jailbreaking") possono causare il malfunzionamento del sistema con conseguenti diagnosi errate.

ATTENZIONE

I dispositivi Android possono avere applicazioni scaricabili tramite Google Play Store. Tuttavia, per ridurre il rischio di compromissione della sicurezza dei dati paziente, Philips consiglia di installare le applicazioni solo da fonti certe e di limitarne l'utilizzo alle sole esigenze lavorative.

Poiché il proprio dispositivo viene utilizzato con app e trasduttori Lumify, è responsabilità dell'utente garantire che la sicurezza del dispositivo e la protezione dei dati dei pazienti siano conformi ai protocolli di sicurezza locali e ai requisiti normativi. Consultare il reparto di sicurezza IT della propria struttura sanitaria per verificare che il dispositivo sia configurato in conformità ai requisiti specifici relativi alla protezione dei dati.

L'implementazione pratica degli elementi tecnici per la protezione varia da caso a caso e può impiegare tecnologie diverse, ad esempio firewall, software antivirus, tecniche di autenticazione e così via. Come accade per tutti i sistemi informatici, i sistemi per ecografia richiedono il livello di protezione generalmente fornito da firewall e altri dispositivi di protezione installati tra il sistema medico e qualsiasi sistema accessibile dall'esterno. A questo proposito, il Dipartimento degli Affari dei Veterani degli Stati Uniti ha sviluppato un'architettura di isolamento ampiamente utilizzata nel settore. Le difese perimetrali e della rete

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

rappresentano un elemento essenziale di efficaci pratiche di sicurezza. La guida all'architettura di isolamento delle apparecchiature del Dipartimento degli Affari dei Veterani degli Stati Uniti (*Medical Device Isolation Architecture Guide*) è disponibile sul sito Web all'indirizzo:

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

Risposta ad incidenti sulla sicurezza del prodotto e alla rilevazione di malware

Nell'eventualità di incidenti correlati alla sicurezza del prodotto o se si rilevano malware (programmi nocivi) nel sistema, scollegare immediatamente il sistema dalla rete e segnalare l'incidente al reparto di sicurezza IT della propria struttura sanitaria. In alternativa, segnalare l'incidente inviando un'e-mail all'indirizzo productsecurity@philips.com.

Problemi e linee guida relativi alla sicurezza

Le linee guida riportate di seguito forniscono esempi pratici di vulnerabilità di sistemi e dati e illustrano i metodi per aumentare il livello di protezione.

NOTA

Gli strumenti per la gestione centralizzata dei dispositivi mobili sono disponibili come supporto per la semplificazione delle linee guida in questo documento e per facilitare la soluzione di problemi di implementazione, configurazione e sicurezza. Consultare il reparto di sicurezza IT della propria struttura sanitaria.

Requisiti del dispositivo

Philips Ultrasound consiglia di utilizzare un dispositivo con requisiti corrispondenti o superiori a quelli richiesti dall'app Lumify e che soddisfi le esigenze di sicurezza all'interno dell'ambiente di lavoro specifico. Il passo successivo è garantire i livelli appropriati dei controlli di sicurezza, in modo da rispettare la conformità ai protocolli di sicurezza locali e ai requisiti normativi.

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

Consolidamento dei dispositivi

Così come accade per le strategie di consolidamento dei sistemi operativi utilizzate su computer desktop e portatili, il consolidamento dei dispositivi comporta l'identificazione di tutte le funzioni e applicazioni non necessarie incluse nel dispositivo e la successiva disattivazione. A seconda del dispositivo, l'operazione potrebbe includere la disattivazione della funzionalità di background delle applicazioni che potrebbe compromettere le prestazioni del dispositivo durante l'utilizzo di Lumify. Il consolidamento del dispositivo riduce l'esposizione del dispositivo agli attacchi e l'eliminazione dei servizi che potrebbero diventare vulnerabili nel tempo.

Cifratura

Un controllo di sicurezza fondamentale disponibile nella maggior parte dei dispositivi Android è la cifratura che aiuta a garantire la protezione dei dati archiviati e accresce la solidità delle norme di controllo degli accessi rendendo i dati non recuperabili.

Protezione della rete

Tutti i sistemi per ecografia in rete devono essere collegati a una LAN (Local Area Network) protetta, in grado di assicurare una protezione adeguata da virus e altro codice o traffico dannoso. Verificare che la rete LAN sfrutti strumenti di protezione efficaci, ad esempio uso esclusivo di tecnologie wireless protette, firewall, sistemi di rilevamento e prevenzione delle intrusioni e delle vulnerabilità.

Controllo dell'accesso fisico

Sarebbe opportuno che ciascuna struttura sanitaria limitasse l'accesso fisico ai sistemi per ecografia per impedirne l'uso accidentale, casuale o deliberato da parte di persone non autorizzate. Il reparto della struttura addetto alla sicurezza è in grado di fornire maggiori informazioni sulle misure in vigore.

Posizione del dispositivo

L'accesso visivo non autorizzato a informazioni protette può essere limitato posizionando il dispositivo in modo da evitare che sia visibile da porte aperte, corridoi e altre aree ad accesso pubblico. Avviare la cancellazione del contenuto dello schermo uscendo dal sistema o eliminando la schermata manualmente prima di lasciare il dispositivo incustodito.

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

Protezioni di accesso e scollegamento utente

Le informazioni sanitarie protette (PHI) salvate sono protette tramite password contro l'accesso non autorizzato mentre vengono contemporaneamente rispettati i requisiti di sicurezza per rendere operativo il dispositivo al più presto possibile.

Considerate le dimensioni e la portabilità dei dispositivi tablet, l'implementazione di una password o di un passcode è fondamentale per ridurre il potenziale di esposizione delle informazioni personali in caso di spostamento non autorizzato o di furto del sistema. Con alcuni dispositivi, è possibile implementare controlli aggiuntivi per rimuovere tutti i dati dal dispositivo in caso di inserimento errato della password o del passcode dopo un numero di volte specificato. Questi controlli consentono di migliorare il modello di controllo di accesso standard e di ridurre il potenziale di esposizione delle informazioni personali.

Per i dispositivi dotati di funzionalità per l'accesso è necessario definire una procedura di accesso coerente, in cui vengano utilizzati nomi utente e password, tale da garantire un'adeguata protezione dei dati. In ogni caso, l'accesso al sistema deve essere controllato dalla struttura sanitaria.

Le procedure di protezione in cui si utilizzano nomi utente e password includono le seguenti misure:

- Implementazione di password sicure. Si tratta del metodo più semplice ed efficace per aumentare il livello di protezione. Le password sicure sono costituite da almeno otto caratteri alfanumerici e contengono lettere sia minuscole che maiuscole, numeri e caratteri speciali, ad esempio "@" o "*". Non utilizzare parole rintracciabili in un dizionario.
- Non inviare o condividere nomi utente e password.
- Modificare periodicamente le password.

Addestrare gli operatori del sistema a scollegarsi immediatamente dopo aver portato a termine il lavoro.

Esempio di gestione delle informazioni

L'esempio riportato di seguito illustra la modalità di utilizzo di un modello a zone del flusso di informazioni per la protezione dei dati.

4535 619 14231_A/795 * NOV 2015

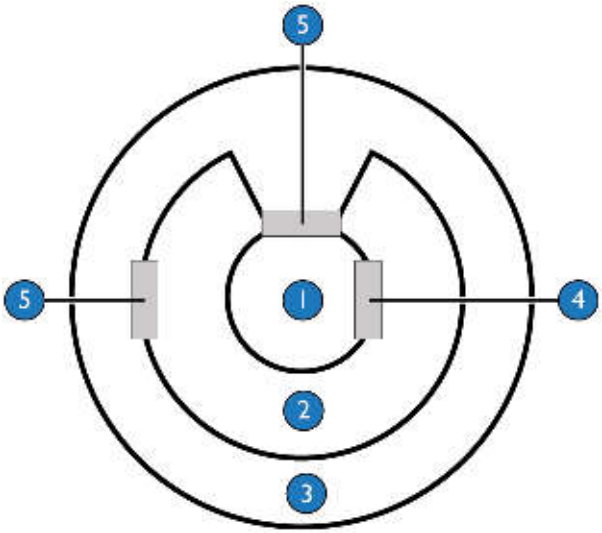
Philips Healthcare

Requisiti dell’ambiente

Le strutture sanitarie che utilizzano il sistema per ecografia sono responsabili dell’implementazione di un ambiente protetto, dotato di tecniche di protezione per l’accesso alla rete, la crittografia e il rilevamento delle intrusioni.

Zone delle informazioni

Il modello del flusso di informazioni è generalmente integrato negli standard di protezione. Un modo efficace per visualizzare questo modello è rappresentare schematicamente la struttura sanitaria suddividendola in tre zone (vedere la figura) e assegnando a ciascuna zona priorità e livelli diversi di utilizzo dei dati. Alcune strutture decidono di non estendere i propri dati nella zona più distante in quanto non sono in grado di garantirne la protezione e l’integrità.



Soluzioni di protezione tra le zone

1	Zona 1: reparto di ecografia
2	Zona 2: parte restante della struttura sanitaria
3	Zona 3: Internet

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

4	Firewall
5	Firewall con IPSec

Zona 1: reparto di ecografia

La maggior parte del trasferimento di immagini viene eseguita nella Zona 1. I backup, le copie e i supporti delle immagini delle ecografie devono essere gestiti dal personale del reparto con la massima attenzione.

Zona 2: parte restante della struttura sanitaria

La Zona 2 include le cliniche esterne al reparto che possono accedere al sistema e, in alcuni casi, a Internet. Un'apposita autorizzazione per l'accesso e l'utilizzo degli itinerari di controllo è di importanza fondamentale.

Zona 3: Internet

La zona 3 viene utilizzata per la connettività a un provider di memoria cloud conforme all'HIPAA.

Protezione tra le zone

La protezione tra le diverse zone deve essere gestita in base a soluzioni standard per la sicurezza dei sistemi informatici. I responsabili devono conoscere il livello previsto di traffico dei dati e scegliere una soluzione sicura ma che non rallenti il flusso delle informazioni. Per la distribuzione delle immagini è richiesta una rete a elevata larghezza di banda.

Protezione all'interno delle zone

La protezione all'interno delle zone deve essere gestita attraverso una combinazione di soluzioni standard per la protezione dei sistemi informatici e di funzioni di protezione del sistema per ecografia.

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

Software di protezione

Gli aggiornamenti dell'app Lumify sono forniti tramite rilasci regolari e il processo di Ordine di modifica sul campo Philips.

Software antivirus e aggiornamenti

La difesa più efficace contro i virus per qualsiasi struttura sanitaria consiste nell'implementare una funzionale politica di protezione della rete.

Oggi, il malware è responsabile di molte violazioni alla sicurezza. I metodi tradizionali di protezione dal malware sono gli antivirus (AV). Philips Ultrasound consiglia di scegliere un pacchetto software valido che permetta di soddisfare le esigenze di protezione da malware. Per limitare i rischio di attacchi malware ai propri sistemi, è possibile intraprendere azioni ulteriori. Ad esempio, è necessario avere la garanzia che qualunque applicazione aggiuntiva installata sul proprio dispositivo abbia una provenienza sicura. Sebbene le applicazioni possano contenere malware, l'installazione delle sole applicazioni necessarie sul proprio dispositivo limiterà il rischio di infezioni o violazioni.

Backup e archivi

ATTENZIONE

La destinazione di esportazione e il meccanismo selezionati devono essere conformi alle norme di sicurezza IT della propria struttura sanitaria.

È possibile esportare esami e immagini dal sistema per ecografia Lumify a un DICOM PACS, una condivisione di rete o un archivio locale. È inoltre possibile inviare immagini tramite e-mail. Le applicazioni di posta elettronica supportate includono Gmail, K-9 Mail, Yahoo, Outlook e Inbox.

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

Procedura di backup

I sistemi per ecografia sono destinati a conservare le informazioni solo come necessario per produrre la documentazione esterna per i record medici (ad esempio, pellicole, tracce e record stampati). Se è necessario backup aggiuntivo, stabilire un protocollo di amministrazione per archiviare tutti gli studi clinici prima dell'eliminazione.

Piani di ripristino

È responsabilità dell'utente garantire l'esistenza di piani di ripristino che includano procedure di backup dati paziente completi e a cadenza regolare. I sistemi per ecografia sono dispositivi di memorizzazione temporanei; i dati paziente devono essere esportati dal sistema per ecografia. Per ulteriori informazioni sull'esportazione dei dati del paziente, vedere il materiale informativo per l'utente del sistema per ecografia.

4535 619 14231_A/795 * NOV 2015

Philips Healthcare

Philips Healthcare fa parte del gruppo Royal Philips

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

Indirizzo produttore
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

Pubblicato in USA
4535 619 14231_A/795 * NOV 2015 - it-IT