



Κοινοί Ρόλοι για την
Ασφάλεια Συστήματος
και Δεδομένων

Ελληνικά

Σύστημα Υπερήχων Lumify

PHILIPS

Περιεχόμενα

1	Εισαγωγή.....	5
	Γενικές Πληροφορίες	6
2	Έλεγχος Ευπάθειας Ασφάλειας στα Προϊόντα Philips.....	7
	Στρατηγική για Άμυνα και Ασφάλεια σε Βάθος	7
	Ρυθμιστικό Περιβάλλον	8
	Ο Ρόλος της Philips στη Συνεργασία για την Ασφάλεια των Προϊόντων	8
	Ο Ρόλος των Πελατών στη Συνεργασία για την Ασφάλεια των Προϊόντων	9
	Θέματα και Οδηγίες Ασφάλειας	10
	Πληροφορίες-Παράδειγμα Συντήρησης	13
	Υποθέσεις Σχετικά με το Περιβάλλον.....	13
	Ζώνες Πληροφοριών	13
	Λογισμικό Προστασίας Ασφαλείας.....	15
	Ανίχνευση Ιών και Ενημερώσεις	15
	Αντίγραφα Ασφαλείας και Αρχεία	16
	Διαδικασία Δημιουργίας Αντιγράφων Ασφαλείας.....	16
	Σχέδια Αποκατάστασης Καταστροφής	16

4535 619 41961_A/795 * FEB 2018

Philips

1 Εισαγωγή

Στο έγγραφο αυτό εξετάζεται η ασφάλεια του Συστήματος Υπερήχων Lumify. Η Philips παρέχει διαφορετικές επιλογές διαμόρφωσης για το Σύστημα Υπερήχων Lumify, συμπεριλαμβανομένης της Bring Your Own Device (Φέρε τη Δική Σου Συσκευή) (BYOD). Ενώ άλλα συστήματα υπερήχων Philips παρέχονται ως ολοκληρωμένα συστήματα, με περιορισμούς σε ότι είναι εγκεκριμένο και διαθέσιμο για το σύστημα, οι κεντρικές συσκευές Lumify μπορούν να αποκτηθούν, διαμορφωθούν και συντηρηθούν από τον οργανισμό υπηρεσιών υγείας ή από ιδιώτες.

Οι επιλέξιμοι πελάτες μπορούν να επιλέξουν μια «πακεταρισμένη» έκδοση του προϊόντος, που πωλείται ως πλήρες σύστημα (υλικό και λογισμικό). Τόσο στις BYOD όσο και στις «πακεταρισμένες» εκδόσεις, η συσκευή πρέπει να διαμορφωθεί και να συντηρηθεί από οργανισμό υπηρεσιών υγείας ή από ιδιώτη.

Οι οδηγίες αυτές έχουν σχεδιαστεί για να συμβάλλουν ώστε οι οργανισμοί υπηρεσιών υγείας να κατανοήσουν τον τρόπο με τον οποίο μπορεί να παραβιαστεί η ασφάλεια της εφαρμογής Lumify της Philips και των δεδομένων ασθενούς, καθώς και για να τονίσουν τις προσπάθειες της Philips ώστε να διασφαλίσει ότι υπάρχουν οι αναγκαίες προστασίες που θα συμβάλλουν στην αποφυγή παραβιάσεων ασφαλείας.

Για τους πόρους ασφαλείας του συστήματος υπερήχων, όπως ενημερωτικά δελτία ασφαλείας, συνήθεις ερωτήσεις και πληροφορίες ευπάθειας, βλ. την ιστοσελίδα Ασφάλειας Προϊόντων της Philips:

www.philips.com/productsecurity

Για πληροφορίες σχετικά με το Σύστημα Υπερήχων Lumify, επισκεφθείτε την πύλη Lumify:

www.philips.com/lumify

Δεν επιτρέπεται η αναπαραγωγή, αντιγραφή μέρους ή του συνόλου, η προσαρμογή, η τροποποίηση, η δημοσιοποίηση του παρόντος εγγράφου και των ψηφιακών μέσων και πληροφοριών της Philips, που αποτελούν πνευματική ιδιοκτησία και εμπιστευτικές πληροφορίες της Philips χωρίς προηγούμενη γραπτή έγκριση από το Νομικό Τμήμα της Philips. Το έγγραφο αυτό ή τα ψηφιακά μέσα προορίζονται για χρήση είτε από πελάτες, στους οποίους παραχωρείται κατόπιν άδειας ως τμήμα της αγοράς του εξοπλισμού Philips, ή έτσι ώστε να πληρούνται οι ρυθμιστικές δεσμεύσεις που απαιτούνται από τον οργανισμό FDA υπό τον κανονισμό 21 CFR 1020.30 (και τυχόν τροποποιήσεις αυτού) και άλλες τοπικές κανονιστικές απαιτήσεις. Η χρήση του παρόντος από μη εξουσιοδοτημένα άτομα απαγορεύεται αυστηρά.

Η Philips παρέχει το έγγραφο αυτό χωρίς κανενός είδους εγγύηση, σιωπηρή ή ρητή, συμπεριλαμβανομένων, χωρίς όμως να περιορίζεται σε αυτές, των σιωπηρών εγγυήσεων εμπορευσιμότητας και καταλληλότητας για συγκεκριμένο σκοπό.

Η Philips έχει μεριμνήσει για τη διασφάλιση της ακρίβειας αυτού του εγγράφου. Παρόλα αυτά, η Philips δεν είναι υπεύθυνη για σφάλματα ή παραλείψεις και διατηρεί το δικαίωμα να κάνει αλλαγές χωρίς άλλη προειδοποίηση σε οποιοδήποτε προϊόν που αναφέρεται στο παρόν ώστε να βελτιώσει την αξιοπιστία, τη λειτουργία ή τη σχεδίασή του. Η Philips μπορεί να προβεί σε βελτιώσεις ή αλλαγές στα προϊόντα ή στα προγράμματα που περιγράφονται στο παρόν έγγραφο ανά πάσα στιγμή.

Η Philips δεν παρέχει στον χρήστη ή σε οποιοδήποτε άλλο μέρος εξουσία αντιπροσώπευσης ή εγγύηση όσον αφορά την καταλληλότητα του παρόντος εγγράφου για κάθε ειδική χρήση ή όσον αφορά την καταλληλότητά του να παράγει ένα συγκεκριμένο αποτέλεσμα. Το δικαίωμα του χρήστη να αξιώσει αποζημίωση για ζημιές που προκλήθηκαν από σφάλμα ή αμέλεια εκ μέρους της Philips περιορίζεται στο ποσό που καταβλήθηκε από το χρήστη στην Philips για την παροχή αυτού του εγγράφου. Η Philips δεν ευθύνεται σε καμία περίπτωση για ειδικές, παράπλευρες, τυχαίες, άμεσες, έμμεσες ή περαιτέρω ζημιές, απώλειες, κόστη, χρεώσεις, απαιτήσεις ή αξιώσεις για απολεσθέντα κέρδη, δεδομένα, τέλη ή δαπάνες οποιασδήποτε φύσης ή είδους.

Η μη εξουσιοδοτημένη αντιγραφή του παρόντος εγγράφου, εκτός του ότι παραβιάζει τα πνευματικά δικαιώματα, ενδέχεται να μειώσει την ικανότητα της Philips να παρέχει ακριβείς και επίκαιρες πληροφορίες στους χρήστες.

Τα ονόματα των προϊόντων που δεν είναι Philips ("non-Philips products") μπορεί να είναι εμπορικά σήματα των ιδιοκτητών τους.

Γενικές Πληροφορίες

Οι ακόλουθες γενικές πληροφορίες ισχύουν για την ασφάλεια του λογισμικού υπερήχων της Philips και των δεδομένων ασθενούς.

- Τα συστήματα υπερήχων της Philips δεν υποστηρίζουν λειτουργίες συνεδρίας πολλαπλών χρηστών. Έχουν σχεδιαστεί ως συσκευές ενός χρήστη. Δεν υποστηρίζεται η πρόσβαση κλινικής χρήσης μέσω δικτύου.
- Τα συστήματα υπερήχων δεν αποτελούν συσκευές μακροπρόθεσμης αποθήκευσης. Τα μόνιμα δεδομένα ασθενούς πρέπει να αρχειοθετούνται σε DICOM PACS, σε κοινόχρηστο δίκτυο ή σε τοπικό κατάλογο.

2 Έλεγχος Ευπάθειας Ασφάλειας στα Προϊόντα της Philips

Η Philips είναι αφοσιωμένη στο να συμβάλει ώστε να διατηρηθεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων ασθενούς για όλους τους πελάτες, ενώ διασφαλίζει ότι τα συστήματα υπερήχων θα εξακολουθήσουν να δημιουργούν και να διαχειρίζονται πληροφορίες με πλήρη ασφάλεια. Τα συστήματα υπερήχων όταν είναι συνδεδεμένα σε δίκτυο μπορεί να καταστούν ευάλωτα σε παραβιάσεις ασφαλείας.

Στρατηγική για Άμυνα και Ασφάλεια σε Βάθος

Εντός του οργανισμού υπηρεσιών υγείας, κατά τη διατήρηση της ασφάλειας των δεδομένων ασθενούς και των προϊόντων Philips απαιτείται στρατηγική για άμυνα και ασφάλεια σε βάθος, η οποία θα είναι ευρεία και πολυδιάστατη (που θα συμπεριλαμβάνει, πολιτικές, διαδικασίες και τεχνολογίες) για την προστασία των πληροφοριών και των συστημάτων από εσωτερικές και εξωτερικές απειλές.

Για ειδικές πληροφορίες σχετικά με την ασφάλεια εντός του οργανισμού σας, συμβουλευθείτε τους ειδικούς ασφαλείας στα ακόλουθα γραφεία ή με εκείνους με παρόμοιες αρμοδιότητες:

- Υπεύθυνος Ασφαλείας Πληροφοριών
- Υπεύθυνος Πληροφοριών
- Υπεύθυνος Ιδιωτικότητας ή Ασφάλειας HIPAA (στις Η.Π.Α.)
- Υπεύθυνος Ασφαλείας

Για να ενημερωθείτε σχετικά με γενικά ζητήματα ασφαλείας ή ειδικές ευπάθειες του συστήματος υπερήχων σας, επικοινωνήστε με τον αντιπρόσωπό σας της Philips.

Ρυθμιστικό Περιβάλλον

Η ανάπτυξη και κατασκευή ιατρικών συσκευών υπόκειται σε αυστηρές ρυθμίσεις, όπως η ασφάλεια και η ιδιωτικότητα των πληροφοριών ασθενούς που έχουν στην κατοχή τους οι πάροχοι υπηρεσιών υγείας. Αυτό δημιουργεί προκλήσεις τόσο για τους παρόχους υπηρεσιών υγείας όσο και για τους κατασκευαστές, ώστε να ανταποκρίνονται γρήγορα στις νέες απειλές κατά της ασφάλειας των δεδομένων ασθενούς που είναι αποθηκευμένα σε ιατροτεχνολογικές συσκευές.

Προστασία των Ηλεκτρονικών Πληροφοριών για την Υγεία του Ασθενούς

Ένα από τα σημαντικότερα στοιχεία που πρέπει να προστατευθούν με μέτρα ασφαλείας είναι οι πληροφορίες υγείας του ασθενούς. Ως παράδειγμα, οι ακόλουθοι κανονισμοί απαιτούν οι πληροφορίες υγείας του ασθενούς να παραμείνουν εμπιστευτικές και ορίζουν μέτρα ασφαλείας για την προστασία των πληροφοριών ασθενούς:

- Νόμος περί Φορητότητας και Λογοδοσίας για την ασφάλιση Υγείας (HIPAA), Η.Π.Α. (www.hhs.gov/ocr/privacy/)
- Ευρωπαϊκή Οδηγία για Ιατροτεχνολογικά Προϊόντα 93/42/ΕΟΚ
- HPB517 Ιαπωνίας
- Τμήματα του ομοσπονδιακού νόμου των Η.Π.Α. για την ανάκαμψη της οικονομίας που σχετίζονται με την HIPAA (ή HITECH), επίσημα γνωστά ως Αμερικανική Πράξη Ανάκαμψης και Επανεπένδυσης του 2009.

Ο Ρόλος της Philips στη Συνεργασία για την Ασφάλεια των Προϊόντων

Η Philips λειτουργεί σύμφωνα με την παγκόσμια Πολιτική Ασφάλειας των Προϊόντων που διέπει τη δημιουργία προϊόντων με σχεδιασμό ασφαλείας, την αξιολόγηση κινδύνου και τις ενέργειες αντιμετώπισης συμβάντων για ευπάθειες που διαπιστώνονται σε υπάρχοντα προϊόντα. Η Philips έχει θέσει σε εφαρμογή μια παγκόσμια διαδικασία εντοπισμού και κλιμάκωσης προβλημάτων, που παρέχει προβολή σε θέματα ασφαλείας που σχετίζονται με τα συστήματα Philips.

Αντιμετώπιση Ευπαθειών

Ομάδες σχεδιασμού προϊόντων εντός της Philips πραγματοποιούν συνεχείς ελέγχους για τον εντοπισμό νέων ευπαθειών ασφαλείας στα συστήματά μας, συμπεριλαμβανομένων εκείνων που προσδιορίζονται από λογισμικό τρίτων μερών και από προμηθευτές λειτουργικών συστημάτων, καθώς και εκείνων που αναφέρονται από μεμονωμένους οργανισμούς υπηρεσιών υγείας.

Ένα παγκόσμιο δίκτυο ομάδων αντιμετώπισης που αφοσιώνεται σε περιστατικά που σχετίζονται με την ασφάλεια των προϊόντων, συλλέγει και διαχειρίζεται πληροφορίες και αντιμετωπίζει τις ευπάθειες που επηρεάζουν προϊόντα και λύσεις της Philips. Οι ομάδες αντιμετώπισης εξακολουθούν να επεκτείνουν τις δραστηριότητες τους στην καθολική κάλυψη όλων των συστημάτων.

Ο στόχος είναι η εκτίμηση από την κατάλληλη ομάδα αντιμετώπισης κάθε πραγματικής και πιθανής παραβίασης ασφάλειας, με σαφή αξιολόγηση της επικινδυνότητας, της απειλής ή της ευπάθειας, καθώς και η ανάπτυξη, όπως απαιτείται, σχεδίου αντιμετώπισης των ευπαθειών, που περιλαμβάνει διαδικασίες αναγνώρισης και επικοινωνίας. Αυτό σημαίνει ότι η Philips προτίθεται να ενημερώσει ταυτόχρονα τους πελάτες όσον αφορά τις ευπάθειες του συστήματος, ενώ προχωρά στην ανάπτυξη και εγκατάσταση τεχνικών μετριασμού του κινδύνου. Για περισσότερες πληροφορίες σχετικά με τις ευπάθειες των συστημάτων, βλ. την ιστοσελίδα:

www.philips.com/productsecurity

Βελτιώσεις Σχεδιασμού

Η Philips διεξάγει ενεργά εσωτερικές αξιολογήσεις ασφάλειας των προϊόντων, για να προσδιορίσει πιθανές αδυναμίες όσον αφορά την ασφάλεια. Με τις πληροφορίες αυτές, οι ομάδες σχεδιασμού της Philips καθορίζουν συχνά αλλαγές στη διαμόρφωση και οριοθετούν προσπάθειες επανασχεδιασμού που θα ενισχύσουν το σύστημα έναντι εξωτερικών απειλών. Οι ίδιες πληροφορίες καθοδηγούν τις απαιτήσεις σχεδιασμού ασφαλείας για τα νέα προϊόντα. Η Πολιτική Ασφάλειας Προϊόντων της Philips απαιτεί στόχους σχεδιασμού ασφαλείας, ως μέρος του συνόλου των προσπαθειών δημιουργίας νέων προϊόντων.

Ο Ρόλος των Πελατών στη Συνεργασία για την Ασφάλεια των Προϊόντων



ΠΡΟΕΙΔΟΠΟΙΗΣΗ

Μη εξουσιοδοτημένες τροποποιήσεις στη συσκευή σας Android "rooting" (δημιουργία λογαριασμού υπερχρήστη) ή "jailbreaking" (κατάργηση περιορισμών) ενδέχεται να προκαλέσει δυσλειτουργία του συστήματος υπερήχων, η οποία μπορεί να οδηγήσει σε εσφαλμένη διάγνωση.

**ΠΡΟΣΟΧΗ**

Οι συσκευές Android διαθέτουν πολλές εφαρμογές για εγκατάσταση μέσω του καταστήματος Google Play. Ωστόσο, για ελαχιστοποίηση του κινδύνου αναφορικά με την ασφάλεια των δεδομένων ασθενούς, η Philips συνιστά την εγκατάσταση εφαρμογών μόνο αξιόπιστης προέλευσης, καθώς και τον περιορισμό της χρήσης τους μόνο για επιχειρηματικές ανάγκες.

Είστε υπεύθυνοι για τη διασφάλιση της ασφάλειας της συσκευής σας και των δεδομένων ασθενούς, ώστε να πληρούνται οι τοπικές πολιτικές ασφαλείας και οι ρυθμιστικές απαιτήσεις. Επικοινωνήστε με το τμήμα Ασφάλειας των Πληροφοριακών Συστημάτων Υγειονομικής Περίθαλψης, για να βεβαιωθείτε ότι το προφίλ ασφαλείας της συσκευής σας είναι διαμορφωμένο σύμφωνα με τις ειδικές απαιτήσεις σας για την ασφάλεια των πληροφοριών.

Η πρακτική εφαρμογή τεχνικών στοιχείων ασφαλείας ποικίλλει ανά τοποθεσία και μπορεί να περιλαμβάνει διάφορες τεχνολογίες μεταξύ των οποίων, τείχη προστασίας, λογισμικό ανίχνευσης ιών, τεχνολογίες ελέγχου ταυτότητας, και ούτω καθεξής. Όπως με κάθε σύστημα που βασίζεται σε ηλεκτρονικό υπολογιστή, τα συστήματα υπερήχων απαιτούν το επίπεδο προστασίας που κατά κανόνα παρέχεται από τα τείχη προστασίας και από άλλες συσκευές ασφαλείας μεταξύ του ιατρικού συστήματος και οποιουδήποτε εξωτερικά προσβάσιμου συστήματος. Το Τμήμα Υποθέσεων Βετεράνων των Η.Π.Α. έχει αναπτύξει για αυτόν τον σκοπό μια αρχιτεκτονική απομόνωσης που χρησιμοποιείται ευρέως. Τέτοιες περιμετρικές άμυνες και άμυνες δικτύου αποτελούν ουσιαστικό στοιχείο των ορθών πρακτικών ασφαλείας. Ο Οδηγός της Αρχιτεκτονικής Απομόνωσης Ιατροτεχνολογικών συσκευών του Τμήματος Υποθέσεων Βετεράνων διατίθεται στην ιστοσελίδα:

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

Ανταπόκριση σε Περιστατικά Ασφάλειας Προϊόντων και στον Εντοπισμό Λογισμικού Κακόβουλης Λειτουργίας

Σε περίπτωση περιστατικού που σχετίζεται με την ασφάλεια προϊόντος ή εφόσον εντοπίσετε λογισμικό κακόβουλης λειτουργίας (κακόβουλο λογισμικό) στο σύστημα, αποσυνδέστε αμέσως το σύστημα από το δίκτυο και αναφέρετε το περιστατικό στο τμήμα Ασφάλειας των Πληροφοριακών Συστημάτων Υγειονομικής Περίθαλψης. Εναλλακτικά, αναφέρετε το περιστατικό με αποστολή ηλεκτρονικής αλληλογραφίας (e-mail) στην ηλεκτρονική διεύθυνση:

productsecurity@philips.com

Θέματα και Οδηγίες Ασφάλειας

Οι ακόλουθες οδηγίες παρέχουν συγκεκριμένα παραδείγματα ευπαθειών συστήματος και δεδομένων, καθώς και μεθόδους προστασίας.

ΣΗΜΕΙΩΣΗ

Για διευκόλυνση όσον αφορά τις οδηγίες σε αυτό το έγγραφο καθώς και παροχή βοήθειας για να μετριαστούν τα ζητήματα που προκύπτουν αναφορικά με την ανάπτυξη, τη διαμόρφωση και την ασφάλεια, διατίθενται εργαλεία για κεντρική διαχείριση των κινητών συσκευών. Συμβουλευθείτε το τμήμα ασφάλειας των πληροφοριακών συστημάτων υγειονομικής περίθαλψης του οργανισμού σας.

Απαιτήσεις Συσκευής

Η Philips συνιστά να ξεκινήσετε με μια διαμόρφωση συσκευής που να πληροί ή να υπερβαίνει τις ελάχιστες απαιτήσεις της εφαρμογής Lumify, καθώς και τις ανάγκες για ασφάλεια εντός του συγκεκριμένου περιβάλλοντός σας. Το επόμενο βήμα είναι να διασφαλιστεί ότι θα εφαρμοστεί το κατάλληλο επίπεδο ελέγχων ασφαλείας, κατά τρόπο που θα πληροί τις πολιτικές ασφαλείας τις περιοχής σας, καθώς και τις ισχύουσες κανονιστικές υποχρεώσεις.

Θωράκιση Συσκευής

Παρομοίως σε γενικές γραμμές με τις στρατηγικές θωράκισης OS που χρησιμοποιούνται σε υπολογιστές και φορητούς υπολογιστές, η θωράκιση συσκευής περιλαμβάνει την αναγνώριση όλων των απαραίτητων λειτουργιών και εφαρμογών που περιλαμβάνονται στη συσκευή σας και την απενεργοποίηση όλων εκείνων των λειτουργιών ή εφαρμογών που δεν χρειάζονται. Ανάλογα με τη συσκευή, η διαδικασία αυτή μπορεί να περιλαμβάνει επίσης απενεργοποίηση της ικανότητας των εφαρμογών να εκτελούν λειτουργίες υποβάθρου που ενδέχεται να επηρεάσουν την απόδοση της συσκευής σας ενώ χρησιμοποιείται η εφαρμογή Lumify. Η θωράκιση συσκευής μειώνει την ευάλωτη σε επιθέσεις περιοχή της συσκευής σας, εξαλείφοντας τις υπηρεσίες που ενδέχεται να καταστούν ευπαθείς με την πάροδο του χρόνου.

Κρυπτογράφηση

Ένας βασικό στοιχείο ελέγχου της ασφάλειας που διατίθεται στις περισσότερες συσκευές Android είναι η κρυπτογράφηση. Η κρυπτογράφηση συμβάλλει στη διασφάλιση της προστασίας των δεδομένων που αποθηκεύονται στο σύστημα και αυξάνει την ισχύ των πολιτικών ελέγχου πρόσβασης, καθιστώντας τα δεδομένα μη ανακτήσιμα.

Ασφάλεια Δικτύου

Κάθε σύστημα υπερήχων δικτύου πρέπει να είναι συνδεδεμένο σε ασφαλές τοπικό δίκτυο, που να παρέχει προστασία έναντι ιών των υπολογιστών και άλλων επιζήμιων κωδικών ή επιζήμιας κυκλοφορίας. Βεβαιωθείτε ότι το τοπικό δίκτυο χρησιμοποιεί κατάλληλη προστασία, όπως η αποκλειστική χρήση ασύρματων τεχνολογιών ασφαλείας, τειχών προστασίας, συστημάτων εντοπισμού εισβολής ή συστημάτων πρόληψης, καθώς και σαρωτών ευπαθειών.

Έλεγχος Φυσικής Πρόσβασης

Κάθε οργανισμός υπηρεσιών υγείας θα πρέπει να περιορίζει τη φυσική πρόσβαση στα συστήματα υπερήχων, για την αποφυγή ακούσιας, τυχαίας ή εκούσιας πρόσβασης από μη εξουσιοδοτημένα άτομα. Το γραφείο ασφαλείας του οργανισμού μπορεί να παρέχει περισσότερες πληροφορίες αναφορικά με τα μέτρα τα οποία εφαρμόζονται.

Τοποθέτηση της Συσκευής

Η μη εξουσιοδοτημένη οπτική πρόσβαση σε προστατευμένες πληροφορίες μπορεί να ελαχιστοποιηθεί με την τοποθέτηση της συσκευής έτσι ώστε να αποτρέπεται η θέασή της από πόρτες, διαδρόμους και άλλες περιοχές κυκλοφορίας. Προετοιμάστε την κενή οθόνη με αποσύνδεση από το σύστημα ή με χειροκίνητη απαλοιφή εμφάνισης της οθόνης προτού αφήσετε τη συσκευή χωρίς επίβλεψη για οποιοδήποτε χρονικό διάστημα.

Προστασίες Σύνδεσης και Αποσύνδεσης Χρήστη

Ένας κωδικός πρόσβασης παρέχει προστασία στις αποθηκευμένες προστατευμένες πληροφορίες υγείας (PHI) από μη εξουσιοδοτημένη πρόσβαση, ενώ πληρούνται οι απαιτήσεις ασφαλείας ώστε η συσκευή να τεθεί σε λειτουργία το συντομότερο δυνατόν.

Λαμβάνοντας υπόψη το μέγεθος και τη δυνατότητα μεταφοράς των φορητών συσκευών tablet, είναι σημαντική η εφαρμογή κωδικού πρόσβασης, ώστε να μειωθούν οι πιθανότητες έκθεσης προσωπικών πληροφοριών αν το σύστημα χαθεί ή κλαπεί. Σε κάποιες συσκευές, δύνανται να εφαρμοστούν πρόσθετα στοιχεία ελέγχου, για σβήσιμο από τη συσκευή όλων των δεδομένων, αν ο κωδικός πρόσβασης εισάγεται λάθος για έναν καθορισμένο αριθμό επαναλήψεων. Αυτά τα στοιχεία ελέγχου συμβάλλουν στην ενίσχυση του πρότυπου μοντέλου ελέγχου πρόσβασης και επίσης συμβάλλουν στη μείωση των πιθανοτήτων έκθεσης των προσωπικών πληροφοριών.

Για συσκευές με δυνατότητες σύνδεσης, μια σταθερή διαδικασία σύνδεσης χρήστη, που περιλαμβάνει ονόματα χρηστών και κωδικούς πρόσβασης, παρέχει καλή ασφάλεια όσον αφορά την προστασία των πληροφοριών. Σε κάθε περίπτωση, ένας οργανισμός υπηρεσιών υγείας πρέπει να ελέγχει την πρόσβαση στο σύστημα.

Στις πρακτικές σύνδεσης και κωδικού πρόσβασης ασφαλείας περιλαμβάνονται τα εξής:

- Εφαρμογή ισχυρών κωδικών πρόσβασης. Αυτή είναι η ευκολότερη και πιο αποτελεσματική μέθοδος για αύξηση της ασφάλειας. Οι ισχυροί κωδικοί πρόσβασης αποτελούνται από τουλάχιστον οκτώ αλφαριθμητικούς, πεζούς ή κεφαλαίους χαρακτήρες και ειδικούς χαρακτήρες, για παράδειγμα «@» ή «*». Μην χρησιμοποιείτε ποτέ λέξεις που μπορεί να βρει κανείς σε ένα λεξικό.
- Ποτέ να μην δημοσιεύετε ή κοινοποιείτε ονόματα χρηστών και κωδικούς πρόσβασης.
- Αλλάζετε περιοδικά τους κωδικούς πρόσβασης.

Εκπαιδεύστε τους χειριστές του συστήματος να αποσυνδέονται από το σύστημα αμέσως μετά την ολοκλήρωση της εργασίας τους.

Πληροφορίες-Παράδειγμα Συντήρησης

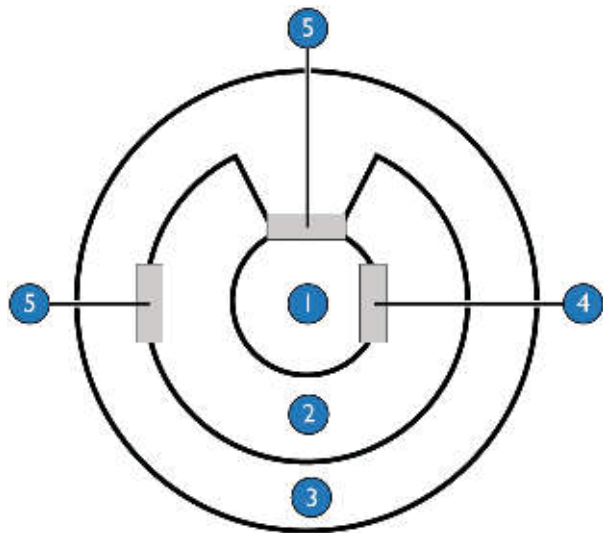
Αυτό το παράδειγμα τρόπου διατήρησης της ασφάλειας των πληροφοριών χρησιμοποιεί μοντέλο ζώνης ροής πληροφοριών.

Υποθέσεις Σχετικά με το Περιβάλλον

Το σύστημα υπερήχων βασίζεται στον οργανισμό υπηρεσιών υγείας για τη διατήρηση ενός ασφαλούς περιβάλλοντος, με μηχανισμούς προστασίας όσον αφορά την πρόσβαση στο δίκτυο, την κρυπτογράφηση και τον εντοπισμό εισβολών.

Ζώνες Πληροφοριών

Το μοντέλο ροής πληροφοριών ενσωματώνεται ευρέως στα πρότυπα ασφαλείας. Ένας εύκολος τρόπος απεικόνισης αυτού του μοντέλου είναι ο σχεδιασμός του οργανισμού υπηρεσιών υγείας με τη μορφή διαγράμματος χωρισμένου σε τρεις ζώνες (βλ. εικόνα), με κάθε ζώνη να έχει διαφορετική προτεραιότητα και επίπεδο χρήσης όσον αφορά τις πληροφορίες. Κάποιοι οργανισμοί αποφασίζουν να μην επεκτείνουν τις πληροφορίες τους στην τελευταία ζώνη, επειδή δεν μπορούν να παρέχουν εγγυήσεις όσον αφορά την προστασία και την ακεραιότητά τους.



Λύσεις ασφαλείας μεταξύ των ζωνών

1	Ζώνη 1: Το τμήμα υπερήχων
2	Ζώνη 2: Ο υπόλοιπος οργανισμός υπηρεσιών υγείας
3	Ζώνη 3: Το διαδίκτυο (internet)
4	Τείχος προστασίας
5	Τείχος προστασίας με IPSec

Ζώνη 1: Το Τμήμα Υπερήχων

Ο μεγαλύτερος όγκος μεταφοράς εικόνων εκτελείται εντός της Ζώνης 1. Η διαχείριση των αντιγράφων ασφαλείας, των αντιγραφών και των μέσων που περιέχουν εικόνες υπερήχων πρέπει να εκτελείται με προσοχή από το προσωπικό του τμήματος.

Ζώνη 2: Ο Υπόλοιπος Οργανισμός Υπηρεσιών Υγείας

Η Ζώνη 2 περιλαμβάνει κλινικές εκτός του τμήματος, που έχουν πρόσβαση στο σύστημα και, σε κάποιες περιπτώσεις, στο διαδίκτυο (internet). Η κατάλληλη εξουσιοδότηση για πρόσβαση και χρήση των ιχνών ελέγχου είναι εξαιρετικά σημαντική.

Ζώνη 3: Το Διαδίκτυο (Internet)

Η ζώνη 3 χρησιμοποιείται για συνδεσιμότητα σε συμμορφούμενη με την HIPAA υπηρεσία παροχής χώρου αποθήκευσης στο νέφος.

Ασφάλεια Μεταξύ των Ζωνών

Ο χειρισμός της ασφάλειας μεταξύ των ζωνών πρέπει να γίνεται με πρότυπες λύσεις ασφαλείας των πληροφοριακών συστημάτων. Οι υπεύθυνοι θα πρέπει να γνωρίζουν το αναμενόμενο επίπεδο κυκλοφορίας δεδομένων, για να επιλέξουν μια λύση ασφαλή, που όμως δεν θα προκαλεί συμφόρηση στη ροή των πληροφοριών. Για τη διανομή εικόνων απαιτείται δίκτυο υψηλού εύρους ζώνης.

Ασφάλεια Εντός των Ζωνών

Η διαχείριση της ασφάλειας εντός των ζωνών πρέπει να γίνεται με συνδυασμό πρότυπων λύσεων πληροφοριακών συστημάτων και των λειτουργιών ασφαλείας του συστήματος υπερήχων.

Λογισμικό Προστασίας της Ασφάλειας

Οι ενημερώσεις της εφαρμογής Lumify παρέχονται μέσα από τακτικές κυκλοφορίες και μέσω της διαδικασίας Παραγγελίας Αλλαγής Πεδίου της Philips.

Σάρωση Προστασίας από Ιούς και Ενημερώσεις

Η καλύτερη προστασία κατά των ιών είναι ο οργανισμός υπηρεσιών υγείας να καθιερώσει μια αποτελεσματική πολιτική ασφαλείας του δικτύου.

Τα λογισμικά κακόβουλης λειτουργίας ευθύνονται για ένα μεγάλο μέρος των παραβιάσεων που στις μέρες μας βλέπουμε στα πρωτοσέλιδα. Οι παραδοσιακές μέθοδοι προστασίας από λογισμικό κακόβουλης λειτουργίας περιλαμβάνουν λογισμικό Προστασίας από ιούς (AV). Η Philips συνιστά την επιλογή ενός αξιόπιστου πακέτου λογισμικού που θα μπορεί να καλύψει τις ανάγκες προστασίας από λογισμικό κακόβουλης λειτουργίας. Πρόσθετα βήματα μπορούν να ληφθούν για τον περιορισμό της πιθανότητας να επηρεαστούν τα συστήματά σας από κάποιο λογισμικό κακόβουλης λειτουργίας. Τα βήματα αυτά περιλαμβάνουν τη διασφάλιση ότι τυχόν πρόσθετες εφαρμογές που έχουν προστεθεί στη συσκευή σας είναι αξιόπιστης προέλευσης. Επειδή οι εφαρμογές ενδέχεται να περιλαμβάνουν λογισμικό κακόβουλης λειτουργίας, η εγκατάσταση μόνο των εφαρμογών που είναι απαραίτητες για τη λειτουργία της συσκευής σας θα συμβάλλει στον περιορισμό του κινδύνου προσβολής ή παραβίασης.

Αντίγραφα Ασφαλείας και Αρχεία



ΠΡΟΣΟΧΗ

Τόσο ο επιλεγμένος προορισμός, όσο και ο μηχανισμός εξαγωγής πρέπει να συμφωνούν με τις τοπικές πολιτικές ασφαλείας των πληροφοριακών συστημάτων υγείας.

Μπορείτε να εξάγετε εξετάσεις και εικόνες από το σύστημα υπερήχων Lumify σε DICOM PACS, σε κοινόχρηστο δίκτυο ή σε τοπικό κατάλογο. Μπορείτε επίσης να αποστέλλετε εικόνες με ηλεκτρονική αλληλογραφία e-mail.

Διαδικασία Δημιουργίας Αντιγράφων Ασφαλείας

Τα συστήματα υπερήχων έχουν σχεδιαστεί για να διατηρούν μόνο τις πληροφορίες που είναι αναγκαίες για τη δημιουργία εξωτερικών εγγράφων για ιατρικά αρχεία (όπως φιλμ, ίχνη και εκτυπωμένα αρχεία). Αν απαιτούνται πρόσθετα αντίγραφα ασφαλείας, καθιερώστε ένα πρωτόκολλο διαχείρισης για την αρχειοθέτηση όλων των κλινικών μελετών, πριν τη διαγραφή.

Σχέδια Αποκατάστασης Καταστροφής

Είστε υπεύθυνοι για την εξασφάλιση ενός σχεδίου αποκατάστασης της καταστροφής, που θα περιλαμβάνει τακτικά και πλήρη αντίγραφα ασφαλείας δεδομένων ασθενούς. Τα συστήματα υπερήχων δεν αποτελούν συσκευές μακροπρόθεσμης αποθήκευσης. Τα δεδομένα ασθενούς πρέπει να εξαγονται από το σύστημα υπερήχων. Για περισσότερες πληροφορίες σχετικά με την εξαγωγή δεδομένων ασθενούς, βλ. τις πληροφορίες χρήστη του δικού σας συστήματος υπερήχων.

www.philips.com/healthcare



Philips Ultrasound, Inc.
22100 Bothell Everett Hwy
Bothell, WA 98021-8431
USA



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



© 2018 Koninklijke Philips N.V.

Με επιφύλαξη κάθε δικαιώματος. Απαγορεύεται η αναπαραγωγή ή μετάδοση ολόκληρου ή μέρους του παρόντος σε οποιαδήποτε μορφή ή με οποιονδήποτε τρόπο, ηλεκτρικό, μηχανικό ή άλλο, χωρίς τη γραπτή συγκατάθεση του κατόχου των δικαιωμάτων.

4535 619 41961_A/795 * FEB 2018