

CYBERSÉCURITÉ DANS LES PRODUITS SCHILLER

La sécurité des données à travers le continuum des soins

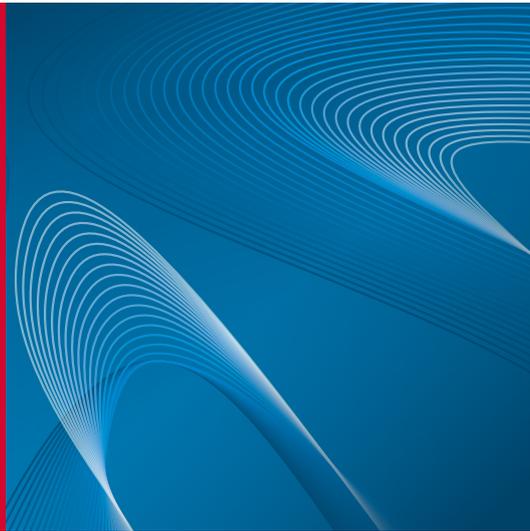


SCHILLER
The Art of Diagnostics

CYBERSÉCURITÉ DANS LES PRODUITS SCHILLER

Les appareils SCHILLER sont cyber-sécurisés grâce à ces fonctionnalités :

- ❖ Commande d'accès basé sur les rôles
- ❖ Caractéristiques d'identification du patient : liste de travail/commandes, code-barres, PDQ
- ❖ Intégration des services d'annuaire via LDAP avec journalisation des audits
- ❖ Transmissions de données cryptées
- ❖ Protocole WiFi WPA2 Enterprise



Les dispositifs d'ECG SCHILLER sont soumis à des tests de pénétration professionnels pour veiller à ce qu'ils soient à l'abri d'attaques malveillantes.

La dernière génération de dispositifs d'ECG de repos SCHILLER est équipée de fonctionnalités de sécurité haut de gamme. Les dispositifs sont soumis à des tests de pénétration professionnels pour garantir une protection contre les cyberattaques. La sécurité est assurée par l'utilisation d'un noyau Linux personnalisé à sécurité renforcée. Cela garantit que les données patients sont protégées de tout accès non autorisé, tout en soutenant le respect des politiques de données informatiques en milieu hospitalier et de la loi RGPD.

DONNÉES PATIENTS PROTÉGÉES CONTRE TOUT UTILISATEUR NON AUTORISÉ

Le niveau de contrôle d'accès peut être configuré entre « aucun » et « avancé ».

- ❖ Les utilisateurs se connectent avec un nom d'utilisateur et un mot de passe personnels.
- ❖ Des rôles peuvent être attribués pour contrôler l'accès aux données patients et les paramètres de configuration.
- ❖ Les comptes utilisateurs sont gérés à distance sur le serveur SCHILLER,

liés aux services d'annuaire avec LDAP via le serveur SCHILLER, ou sur chaque dispositif ECG dans les paramètres.

- ❖ Les utilisateurs sont automatiquement déconnectés après une période d'inactivité spécifiée.
- ❖ Si la gestion des utilisateurs n'est pas active, le dispositif peut toujours être protégé par mot de passe.

DÉPANNAGE FACILE

Le serveur SCHILLER, les applications logicielles cliniques et les dispositifs médicaux disposent de journaux d'audit et de sécurité complets, ce qui garantit l'enregistrement de l'activité de l'utilisateur et des données sur l'appareil.

GARANTIR L'INTÉGRITÉ DES DONNÉES

Il est essentiel d'identifier le patient correctement et facilement. La liste de travail DICOM et les commandes HL7 peuvent être utilisées pour l'identification des patients. La fonction PDQ permet une requête de données du patient rapide et simplifie la routine

quotidienne en milieu hospitalier. Les scanners de codes à barres 1D et 2D sont pris en charge.

Les appareils SCHILLER prennent en charge les champs obligatoires lors de la saisie des données, si nécessaire.

Ces outils aident à réduire considérablement les erreurs démographiques des patients. Le serveur SCHILLER fournit également une vérification de l'intégrité et de la corrélation pour une couche de protection supplémentaire.

ASSURER LA SÉCURITÉ DES DONNÉES

Les données transmises vers et depuis les appareils SCHILLER sont cryptées à l'aide du protocole SSL/TLS.

SCHILLER utilise des protocoles wi-fi sécurisés et standard pour les hôpitaux, comme WPA2 Enterprise, avec authentification basée sur des certificats.

Les données enregistrées peuvent être automatiquement supprimées sur l'appareil une fois la transmission à SEMA et/ou SIH réussie.

COMMANDE D'ACCÈS BASÉE SUR UN RÔLE

Avec un contrôle d'accès utilisateur avancé, SCHILLER s'assure que seul le personnel autorisé peut accéder à un appareil.



Les utilisateurs se connectent avec un nom d'utilisateur et un mot de passe personnels. Les rôles sont attribués aux utilisateurs pour accéder à la mémoire et aux paramètres.



Les comptes utilisateurs sont gérés à distance sur le serveur SCHILLER, liés aux services d'annuaire avec LDAP via le serveur SCHILLER, ou sur chaque dispositif ECG dans les paramètres.



Les utilisateurs sont automatiquement déconnectés après une période d'inactivité spécifiée.

INTÉGRATION LDAP



Les dispositifs médicaux SCHILLER peuvent être intégrés dans le LDAP de l'hôpital (par ex. Active Directory) pour une authentification unique de l'utilisateur.

JOURNALISATION DES AUDITS



Le serveur SCHILLER, les applications logicielles cliniques et les dispositifs médicaux disposent de journaux d'audit et de sécurité complets.



IDENTIFICATION DES PATIENTS

Caractéristiques qui réduisent considérablement les erreurs démographiques des patients et accélèrent les flux de travail :



Liste de travail DICOM et commandes HL7, scanners de codes à barres 1D et 2D.



Prise en charge des champs obligatoires lors de la saisie manuelle des données.



La requête de données patients rapide via PDQ simplifie la routine hospitalière quotidienne.

TRANSMISSION DE DONNÉES SÉCURISÉE



Les données transmises vers et depuis les appareils SCHILLER sont cryptées à l'aide du protocole SSL/TLS.



Des protocoles wi-fi sécurisés sont intégrés, comme WPA2 Enterprise avec authentification basée sur des certificats.



Les données enregistrées peuvent être automatiquement supprimées sur l'appareil une fois la transmission à SEMA et/ou SIH réussie.



Americas
SCHILLER Americas Inc.
 Doral, Florida 33172

North America:
 Phone +1 786 845 06 20
 Fax +1 786 845 06 02
 sales@schilleramericas.com
 www.schilleramericas.com

Latin America & Caribbean
 Phone +1 305 591 11 21
 Fax +1 786 845 06 02
 sales@schilleramericas.com
 www.schilleramericas.com



Asia
SCHILLER Asia-Pacific / Malaysia
 52200 Kuala Lumpur, Malaysia
 Phone +603 6272 3033
 sales@schiller.com.my
 www.schiller-asia.com



Austria
SCHILLER Handelsgesellschaft m.b.H.
 A-4040 Linz
 Phone +43 732 70 99 0
 Fax +43 732 757 000
 sales@schiller.at
 www.schiller.at



China
Alfred Schiller (Beijing) Medical Equipment Co., Ltd.
 100015 Beijing, China
 Phone +86 010 52007020
 Fax +86 010 52007020-8016
 info@schillerchina.com
 www.schillermedical.cn



Croatia
SCHILLER d.o.o.
 10000 Zagreb
 Phone +385 1 309 66 59
 Fax +385 1 309 66 60
 info@schillerzg.hr
 www.schiller.hr



France
SCHILLER Médical
 F-67160 Wissembourg
 Phone +33 3 88 63 36 00
 Fax +33 3 88 63 36 49
 info@schiller.fr
 www.schiller.fr



France (distribution France)
SCHILLER France S.A.S.
 F-77608 Bussy St Georges
 Phone +33 1 64 66 50 00
 Fax +33 1 64 66 50 10
 contact@schillerfrance.fr
 www.schiller-france.com



Germany
SCHILLER Medizintechnik GmbH
 D-85622 Feldkirchen b. München
 Phone +49 89 62 99 81 0
 Fax +49 89 609 50 90
 info@schillermed.de
 www.schillermed.de



India
SCHILLER Healthcare India Pvt. Ltd.
 Mumbai - 400 059, India
 Phone +91 22 6152 3333 / 2920 9141
 Fax +91 22 2920 9142
 sales@schillerindia.com
 www.schillerindia.com



Poland
SCHILLER Poland Sp. z o.o.
 PL-02-729 Warszawa
 Phone +48 22 843 20 89 / +48 22 647 35 90
 Fax +48 22 843 20 89
 schiller@schiller.pl
 www.schiller.pl



Russia & C.I.S.
AO SCHILLER.RU
 119049 Moscow, Russia
 Phone +7 (495) 970 11 33
 mail@schiller.ru
 www.schiller.ru



Serbia
SCHILLER d.o.o.
 11010 Beograd
 Phone +381 11 39 79 508
 Fax +381 11 39 79 518
 info@schiller.rs
 www.schiller.rs



Slovenia
SCHILLER d.o.o.
 2310 Slovenska Bistrica
 Phone +386 2 843 00 56
 Fax +386 2 843 00 57
 info@schiller.si
 www.schiller.si



Spain
SCHILLER ESPAÑA, S.A.
 ES-28232 Las Rozas/Madrid
 Phone +34 91 713 01 76
 Fax +34 91 355 79 33
 schiller@schiller.es
 www.schiller.es



Switzerland
SCHILLER-Reomed AG
 CH-8912 Obfelden
 Phone +41 44 744 30 00
 Fax +41 44 740 37 10
 sales@schiller-reomed.ch
 www.schiller-reomed.ch



Turkey
SCHILLER TÜRKIYE
 Okmeydani-Sisli - Istanbul
 Phone +90 212 210 8681 (pbx)
 Fax +90 212 210 8684
 info@schiller.com.tr
 www.schiller-turkiye.com



United Kingdom
SCHILLER UK Ltd.
 Anstruther, Fife KY10 3H
 Phone +44 16 190 72 565
 sales@schilleruk.com
 www.schilleruk.com

La disponibilité de l'appareil est assujettie à l'approbation des autorités de réglementation locales.

