



Mesdames, Messieurs,

La **numérisation** peut apporter un **soulagement sur le plan administratif**, mais elle comporte aussi **certains risques**. Compte tenu du **caractère sensible des données dans le système de santé, la protection des données** y joue un rôle central. Dans cette newsletter, nous vous présentons les moyens qui vous permettront de **saisir les opportunités** et de relever les défis. Selon la devise: «Une numérisation en toute sécurité!»

Salutations sécurisées
Votre équipe HIN



Signer numériquement avec l'identité HIN: rien de plus simple et pourquoi cela vaut la peine

Avec HIN Sign, vous signez les documents directement sur l'ordinateur et gardez ainsi la force probante de votre documentation électronique. Avec l'exemple de Pulse Medica, nous montrons la facilité avec laquelle la signature numérique fonctionne directement à partir du logiciel de cabinet.

[En savoir plus](#)

Les données particulièrement sensibles et leur traitement: entretien avec Adrian Lobsiger

Les professionnels de la santé sont-ils autorisés à stocker les données des patients dans un cloud? L'envoi d'une photo d'un dossier de traitement est-il conforme à la protection des données? Et quelles conséquences peuvent avoir les violations de la protection des données? Adrian Lobsiger, Préposé fédéral à la protection des données et à la transparence, nous renseigne.



[Lire l'entretien](#)



Les e-mails HIN sont-ils toujours envoyés de manière conforme à la protection des données?

Lorsque des e-mails sont échangés entre deux adresses e-mail HIN, ceux-ci sont automatiquement envoyés de manière conforme à la protection des données. Mais parfois, des informations doivent aussi être envoyées à des patients ou à des collègues spécialistes sans raccordement HIN. Découvrez ce à quoi vous devez veiller dans un tel cas.

[En savoir plus](#)



Félicitations aux gagnants de notre concours anniversaire!

En 2020, HIN a bloqué une moyenne de 252 000 spams ou virus par jour! Félicitations aux gagnants qui ont répondu correctement à la question de notre concours. Nous leur souhaitons beaucoup de plaisir avec les prix remportés.

Le NCSC met en garde contre les attaques visant le système de santé

Le Centre national pour la cybersécurité (NCSC) met en garde: le système de santé fait de plus en plus l'objet de cyberattaques, souvent sous la forme de rançongiciels (appelés également ransomware). Certains groupes criminels se sont spécialisés dans l'attaque de cibles plus petites telles que les cabinets médicaux. En coopération avec le NCSC, HIN vous demande de redoubler de vigilance.



[Voici comment vous protéger \(blog HIN\)](#)
[Article sur les rançongiciels \(site Web du NCSC\)](#)



«La numérisation peut permettre aux prestataires de service de disposer de davantage de temps pour leurs patients»

Le système de santé suisse fait pâle figure en matière de numérisation en comparaison internationale, c'est ce que révèle le Digital Health Report 2021/22. Quelles en sont les raisons? Et comment faire progresser la numérisation? HIN s'est entretenue sur le sujet avec le professeur Alfred Angerer, auteur du rapport et chef de l'unité de gestion des soins de santé à la ZHAW.

[Vers l'entretien](#)

Avantages du DEP pour les professionnels de la santé

Plus la population et les professionnels de la santé s'affilieront au DEP, plus le réseau sera dense et plus il y aura d'avantages pour tout le monde. En collaboration avec eHealth Suisse, nous avons publié une série d'articles soulignant les avantages du dossier électronique du patient (DEP) pour les professionnels de la santé sous différents angles.



[Vers la série d'articles](#)

Événements

Formations Awareness HIN

HIN propose des formations Awareness consacrées à la «sécurité informatique» ou à la «protection des données» pour des groupes et des participants individuels. Au cours de ces formations, vous découvrirez les mesures de sécurité importantes et les outils nécessaires pour protéger de manière optimale votre cabinet dans le domaine numérique.

Prochaines dates:

- 15.12.2021 / de 17h30 à 19h00 / module Sécurité informatique (allemand)
- 08.02.2022 / de 17h30 à 19h00 / module Sécurité informatique (allemand)
- 17.02.2022 / de 15h30 à 17h00 / module Sécurité informatique (français)
- 03.03.2022 / de 15h30 à 17h00 / module Sécurité informatique (allemand)
- 10.03.2022 / de 15h30 à 17h00 / module Protection des données (allemand)
- 07.04.2022 / de 15h30 à 17h00 / module Sécurité informatique (allemand)
- 12.04.2022 / de 17h30 à 19h00 / module Sécurité informatique (français)

[Détails et inscription](#)

Formations Awareness avec nos partenaires

- 17.02.2022 / Présentation à la pharmaDavos - en collaboration avec IFAK Data (allemand) - [Détails et inscription](#)
- 18.02.2022 / SBAP Workshop - Indépendant en tant que psychologue (allemand) - [Détails et inscription](#)
- 17.03.2022 / Physioswiss (allemand) - [Détails et inscription](#)

Vous prévoyez un congrès, une conférence ou une formation continue en interne sur la protection des données et la sécurité de l'information? HIN se fera un plaisir de vous mettre à votre disposition un orateur spécialisé en sécurité informatique et en sensibilisation. [Contactez-nous!](#)

Nouveaux raccordements

De plus en plus d'organisations et d'institutions communiquent de manière sécurisée via HIN. Par exemple, [la maison de repos Seeblick](#), [CONTACT](#), [Fondation Aide Addiction](#), [le Hof Rickenbach](#) et [JDMT Medical Services AG](#).



Avez-vous des questions ou besoin de notre aide? Vous pouvez joindre le support HIN du lundi au vendredi de 8h00 à 18h00 au numéro de téléphone [0848 830 741](tel:0848830741) ou par e-mail à infosr@hin.ch.

Health Info Net SA | Avenue des Sciences 13 | 1400 Yverdon-les-Bains | www.hin.ch/fr | infosr@hin.ch | [0848 830 741](tel:0848830741)