NEWSLETTER 3C

PROTECTION DES DONNÉES ET CYBERSÉCURITÉE

CONTACT 3C NORD

VEYRAT Cyrielle
Coordinatrice 3C
04 50 82 27 80
cyveyrat@ch-alpes-leman.fr

Accès site Internet 3C

CENTRE DE COORDINATION EN CANCEROLOGIE HAUTE-SAVOIE NORD

QU'EST-CE QUE LE RGPD ?

Le RGPD (Règlement Général sur la Protection des Données) encadre juridiquement depuis le 25 mai 2018 la collecte et le traitement des données personnelles sur le territoire de l'Union Européenne. Les professionnels de santé en cancérologie sont amenés à traiter, collecter et échanger des données personnelles de patients, notamment des données de santé.

QU'EST-CE QUE LA CYBERSÉCURITÉ ?

La cybersécurité recouvre l'ensemble des moyens, des mesures ou pratiques concourant à assurer l'échange et le stockage de l'information de manière sécurisée et conforme à la réglementation en vigueur.

QU'EST-CE QUE L'IDENTITOVIGILANCE ?

L'identitovigilance est l'ensemble des mesures mises en œuvre pour fiabiliser l'identification de l'usager afin de sécuriser ses données de santé, à toutes les étapes de sa prise en charge.

La bonne identification du patient constitue le premier acte d'un processus qui se prolonge tout au long de sa prise en charge par les différents professionnels de santé impliqués, quels que soient la spécialité, le secteur d'activité et les modalités d'accompagnement

L'identification d'un usager est capitale pour la qualité et la sécurité de sa prise en charge. Pour répondre à cet enjeu, l'utilisation de l'Identité Nationale de Santé (INS) est obligatoire depuis le 1er janvier 2021.

Plus d'infos, *cliquez ici !*

POURQUOI EST-CE IMPORTANT ?

Le professionnel de santé doit avoir conscience que les informations qu'il manipule et qu'il utilise au quotidien peuvent représenter un intérêt pour une tierce partie (entreprise à but lucratif, puissance étrangère) ou des tiers malveillants (hackers).

Chaque professionnel de santé à son niveau doit connaître le degré de sensibilité des informations qu'il traite, qu'elles soient d'ordre économique, fiscal ou en lien avec la santé des patients.

"La sécurité est l'affaire de tous !"

POURQUOI UNE NEWSLETTER ?

- Sensibiliser et informer sur les enjeux RGPD et la cybersécurité.
- Communiquer sur les outils sécurisés disponibles pour les professionnels de santé.
- Relayer et rappeler les bonnes pratiques RGPD.
- Informer des actualités sur le territoire (projets, outils, formations, événements,...).

ENQUÊTE 3C “PRATIQUES ET CONNAISSANCES RGPD SUR LE 74 NORD”

En 2024, le 3C 74 Nord a mené une enquête auprès des professionnels en cancérologie du territoire sur leurs pratiques et connaissances RGPD dans le but de réaliser un état des lieux et proposer des actions d’amélioration.

Tous les professionnels de santé en cancérologie de la ville et de l’hôpital du 74 Nord étaient concernés : médecins, IDE, Cadres de santé, personnels administratifs, pharmaciens, paramédicaux, ..

Découvrez les résultats : cliquez ici !

CYBER RÉFLEXES

Se protéger sur Internet

1 DES MOTS DE PASSE SOLIDES ET DIFFÉRENTS POUR CHAQUE COMPTE TU CHOISIRAS

Un mot de passe c'est comme une clé propre à chaque porte, elle te protège de l'intrusion. Si tu te fais voler un mot de passe que tu utilises pour différents sites web ou applications, ils pourront tous être piratés !

BONNES PRATIQUES

- Utiliser des mots de passe suffisamment longs, complexes et surtout différents pour chaque compte.
- Les garder secrets et privilégier un gestionnaire de mots de passe sécurisé pour les conserver.

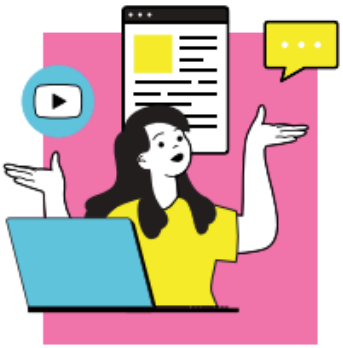
2 LES MISES À JOUR DE TES APPAREILS SANS TARDER TU FERAS

Les failles de sécurité de tes logiciels, applications et matériels sont comme des portes laissées ouvertes pour les pirates. Ils peuvent les utiliser pour accéder à tes données personnelles ou les voler.

BONNES PRATIQUES

- Faire les mises à jour des logiciels, applications et appareils, dès qu'elles te sont proposées pour corriger leurs failles de sécurité.
- Activer les options de mises à jour automatiques chaque fois que c'est possible.

3 EN LIGNE, LE MOINS POSSIBLE SUR TON IDENTITÉ TU DIRAS

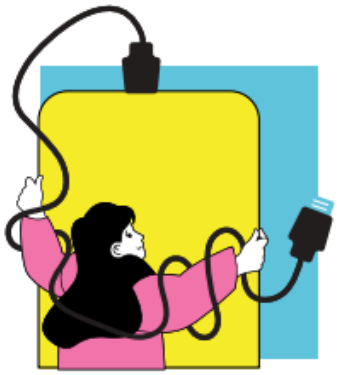


Publier et partager tes données personnelles sur Internet (nom, prénom, adresse mail, photos, vidéos, vocaux…) peut les exposer à une utilisation malveillante.

BONNES PRATIQUES

- Éviter de divulguer tes données personnelles et celles de tes connaissances.
- Vérifier les paramètres de confidentialité de tes comptes pour définir ce qui peut être visible par les autres.

4 EN LIEU SÛR, UNE COPIE DE TES DONNÉES TU CONSERVERAS



Copier tes données, c'est les sauvegarder pour éviter de les perdre en cas de piratage, de vol, de panne ou de casse de tes appareils.

BONNE PRATIQUE

- Penser à faire régulièrement des sauvegardes de tes données sur un autre support (clé USB, disque externe, *cloud*...) pour pouvoir les retrouver en cas de problème.

5 DES MESSAGES INATTENDUS ET ALARMANTS TOUJOURS TU TE MÉFIERAS

L'hameçonnage ou *phishing*, ce sont des messages (courriels, SMS, réseaux sociaux) ou appels d'escrocs qui se font passer pour un organisme familier (banque, administration…). Ces arnaques visent à te voler des informations personnelles et bancaires, te faire télécharger un virus ou directement t'escroquer.

BONNES PRATIQUES

- Toujours te méfier et ne pas te précipiter pour cliquer ou répondre.
- Vérifier toujours l'information par toi-même, en te connectant à ton compte sur le service concerné.

6 LES CONTENUS PIRATÉS OU NON OFFICIELS TU ÉVITERAS

Des virus qui peuvent pirater tes appareils ou tes comptes sont souvent présents dans les logiciels ou jeux piratés, les extensions de triche de jeux vidéo, les sites de *streaming* illégaux...

BONNES PRATIQUES

- Ne pas télécharger des contenus illégaux ni des solutions non officielles.
- Installer uniquement des applications depuis les sites ou magasins officiels des éditeurs.

Plus d'infos : cliquez ici !

L'ANS : AGENCE DU NUMÉRIQUE EN SANTÉ

L'Agence du Numérique en Santé contribue à l'amélioration du système de santé aux côtés de tous les acteurs, privés comme publics, professionnels ou usagers, grâce à la transformation numérique.

Les actions et réalisations

À travers un ensemble d'initiatives et de projets d'envergure, l'Agence du Numérique en Santé s'engage à fournir un cadre réglementaire robuste, à promouvoir des services numériques performants et à garantir l'accessibilité des soins de santé pour tous.

Messageries MSSanté

Il s'agit d'un ensemble de messageries sécurisées au sein d'un espace de confiance destiné aux professionnels, établissements habilités et patients. L'ANS en qualité de gestionnaire de l'espace MSSanté propose plusieurs offres afin d'aiguiller au mieux vers la MSSanté qui convient aux professionnels de santé et aux usagers.

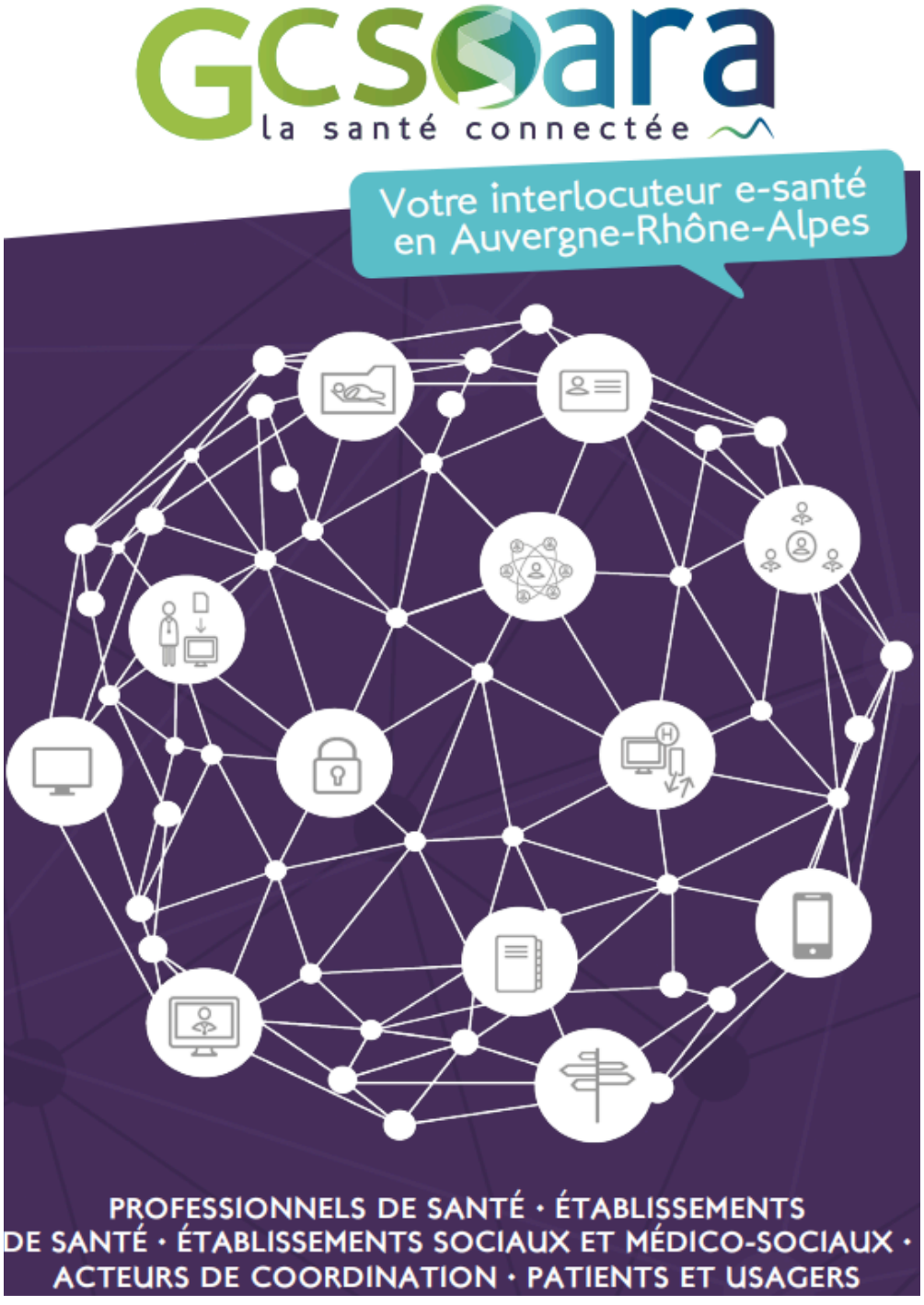
Plus d'infos, cliquez ici!

LE GCS SARA, VOTRE EXPERT RÉGIONAL EN E-SANTÉ

Le Groupement de Coopération Sanitaire Système d'Information Santé en Auvergne-Rhône-Alpes (GCS Sara), est l'expert opérationnel clé au service des projets de e-santé.

Le GCS conçoit et développe depuis plusieurs années des outils numériques sécurisés et innovants, pour répondre aux besoins des professionnels et s'adapter à l'évolution du système de santé.

Plus d'infos, cliquez ici!



Notre offre de SERVICES

Nous mettons à disposition des acteurs de santé d'Auvergne-Rhône-Alpes un **bouquet de services numériques innovants, sécurisés et interopérables**.

Nos services phares

MonSisra

Échanges en toute sécurité entre professionnels de santé et accès aux services régionaux.

MesPatients

Suivi, organisation et partage de l'évolution du parcours des usagers et évaluation de son activité.

Téléexpertise

Demandes d'avis sécurisés permettant de centraliser et coter les actes de façon simplifiée.

ViaTrajectoire

Aide à l'orientation et à l'admission de patients ou usagers vers les structures sanitaires et médico-sociales.

d'infos sur :
www.sante-ara.fr/services

Nos PROJETS

Nous accompagnons la **mise en œuvre des stratégies nationales** et des **initiatives régionales.**

Nos projets phares

Sécurité Numérique

Accompagnement en cybersécurité des structures sanitaires et médico-sociales.

Mon espace santé

Accompagnement des initiatives régionales en faveur de l'usage de Mon espace santé.

Parcours spécifiques

Suivi coordonné de parcours protocolisés (ETP, obésité pédiatrique, ...).

CPTS

Accompagnement à la coordination des professionnels de santé de ville et des acteurs sanitaires, sociaux et médico-sociaux d'un territoire.

d'infos sur :
www.sante-ara.fr/projets

Plus d'infos, cliquez ici!

MON SISRA, MESSAGERIE PROFESSIONNELLE 100% SÉCURISÉE !

MonSisra

certifiée MS Santé

Messagerie sécurisée de santé

A la disposition des professionnels du sanitaire, du médico-social et du social, MonSisra permet l'**échange de données de santé** entre utilisateurs de messageries sécurisées, quelles qu'elles soient :

- **Communiquez en instantané**, en mode tchat
- **Adressez des courriers** ou des **photos**
- Gagnez du temps avec l'**intégration automatique des documents** dans le dossier patient de votre logiciel
- Transmettez facilement les contenus de votre choix grâce à l'**imprimante virtuelle**
- Trouvez facilement vos correspondants dans l'**annuaire**
- **Transmettez vos courriers à vos patients** vers la messagerie citoyenne Mon espace santé
- **Déléguez votre compte** à un secrétariat ou un confrère

Outil de télémédecine gratuit

- Réalisez des **demandes d'expertises** ou rendez des avis
- Réalisez des **téléconsultations** par visioconférence

Portail d'accès aux applications de e-santé

Accédez simplement aux autres services e-santé déployés dans la région, en toute sécurité et sans codes d'accès à ressaisir :

Téléconsultation, Annuaire des professionnels de santé, ViaTrajectoire, MesPatients, ROR, ...

Plus d'infos et ressources

Plus d'infos, cliquez ici!

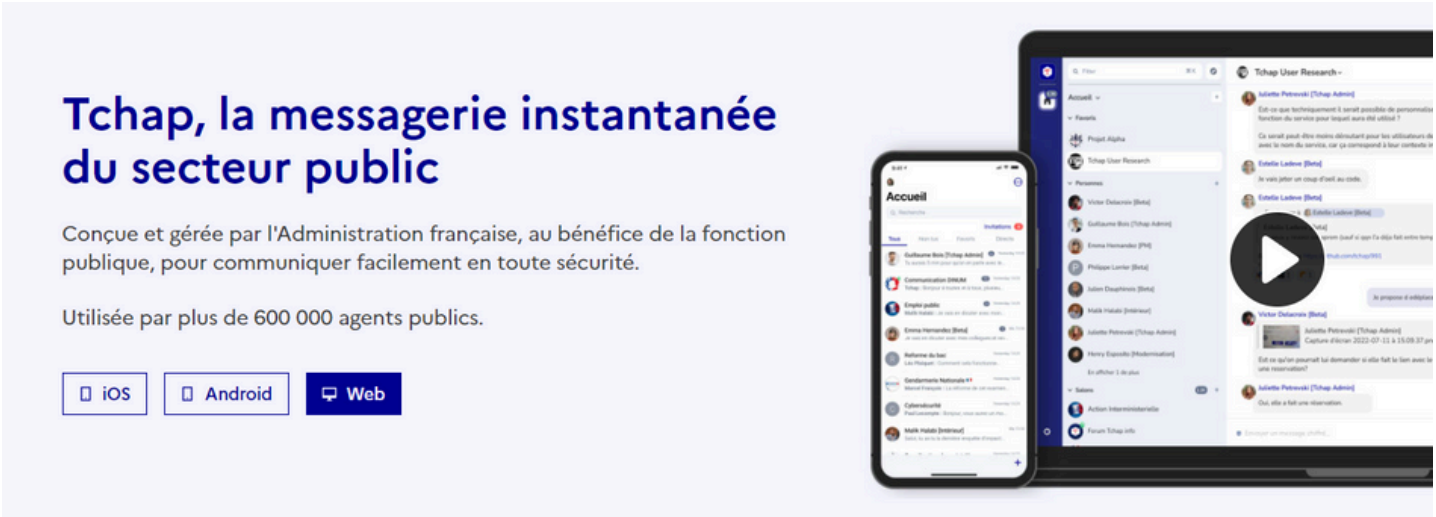
POUR VOS ÉCHANGES PROFESSIONNELS, N'UTILISEZ PLUS "WHATSAPP" MAIS "TCHAP" !

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Tchap
La messagerie instantanée du secteur public

Tchap est une messagerie instantanée spécialement conçue pour les agents du secteur public. Cet outil sécurisé, souverain est opéré par l'État (DINUM) et garantit la confidentialité totale des échanges professionnels. Il est hébergé dans le "cloud" du ministère de l'Intérieur, offrant ainsi une sécurité optimale, et une maitrise publique de son opération.

En 2024, Tchap compte plus de 200 000 utilisateurs actifs mensuels issus de diverses entités publiques, dont l'administration centrale, l'Assemblée Nationale, le Sénat et les services déconcentrés de l'État. Chaque mois, plus de 4 millions de messages sont échangés via cette plateforme sécurisée. l'Outil Tchap est également adopté par de nombreuses collectivités territoriales et leurs élus.



Plus d'infos, cliquez ici!

PROCHAINES FORMATIONS :

- Webinaires de formations 2025 du GCS Sara sur la messagerie sécurisée MonSisra, sur l'identitovigilance, sur la cybersécurité,... : **cliquez ici !**
- Webinaire ANS sur l'identitovigilance, ***cliquez ici !***
- Topo cybersécurité lors de la journée des soignants en cancérologie du 74, le 8 avril 2025 au CHAL, ***cliquez ici !***
- MOOC "SecNumacadémie" pour former le plus grand nombre de citoyens à la sécurité du numérique, ***cliquez ici !***

CONTACTS UTILES

ACCOMPAGNEMENT PROJETS GCS SARA :

Alicia COTTIN

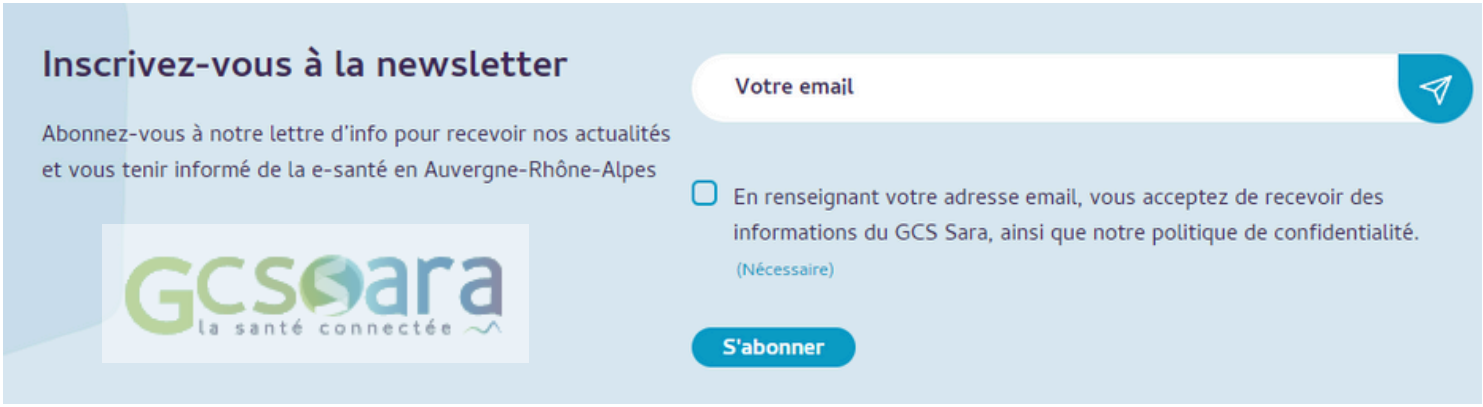
Animatrice territoriale Haute-Savoie

alicia.cottin@sante-ara.fr

ASSISTANCE GCS SARA :

assistance@sante-ara.fr

POUR ALLER PLUS LOIN...



Inscription newsletter GCS Sara, cliquez ici!