COMMUNIQUÉ DE PRESSE

Lyon, le 16 octobre 2025

Cybermois : 230 établissements de santé accompagnés et formés par l'ARS ARA et le GCS Sara pour se préparer aux cyber-attaques

A l'occasion du cybermois, l'ARS Auvergne-Rhône-Alpes et le GCS Sara font le point sur la stratégie régionale et les actions de sensibilisation et de formation menées auprès des établissements de santé chaque année. Parmi eux, Calydial, établissement de santé spécialisé dans la prévention de la maladie rénale chronique, de la dialyse, est un des premiers établissements accompagnés dans l'objectif de garantir la sécurité des données de ses 300 patients en dialyse et plus de 2000 patients en maladie rénale chronique. Retour sur les différents programmes et outils utilisés pour se préparer et anticiper ces attaques.

La France est le pays européen le plus touché par les cyber-attaques dans le secteur de la santé[1], 3e secteur le plus touché en France avec 10% d'attaques recensées dans les établissements publics de santé.[2] En région Auvergne-Rhône-Alpes, près de 53 signalements d'incidents de sécurité informatique ont été enregistrés en 2024.

Pour répondre à ces menaces, l'Agence régionale de santé Auvergne-Rhône-Alpes a élaboré une stratégie régionale en matière de cybersécurité dès 2021, en cohérence avec la feuille de route « Ma santé 2022 » et la feuille de route du numérique en santé 2023-2027**. L'objectif : renforcer la sécurité des systèmes d'information, sensibiliser et former les acteurs de santé et du médico-social à ces risques en proposant différents programmes et outils concrets aux établissements.**

Renforcer la sécurité des systèmes d'information hospitaliers avec le programme national CaRE

Lancé au printemps 2024, le programme CaRE (Cybersécurité accélération et résilience des établissements) est un des objectifs prioritaires de la feuille de route du numérique en santé.

Piloté par l'ARS Auvergne-Rhône-Alpes en lien avec les établissements, **ce programme d'appui à la résilience « cyber », financé au niveau national sur des fonds européens de plusieurs millions d'euros, s'étend jusqu'en 2027, avec différents axes d'actions prévus :**

- maîtrise des annuaires recensant les professionnels des établissements et de leurs expositions sur internet,
- stratégie de continuité et de reprise d'activité en cas d'attaques
- gouvernance au sein des établissements pour renforcer leur sécurité numérique

[1] D'après l'ENISA, Agence européenne de la cybersécurité

[2] D'après l'Agence nationale de la sécurité des systèmes d'information

- ressources et mutualisation (former le personnel, recruter des experts en cybersécurité et mutualiser des moyens entre établissements)
- sensibilisation des personnels sur le cadre réglementaire et les bonnes pratiques à adopter.

Un budget de 3,2 millions d'euros[3] dédié à un centre régional de ressources cybersécurité

Créé en mai 2024 par l'ARS Auvergne Rhône-Alpes et le GCS Sara, le Centre régional de ressources cybersécurité (CRRC) accompagne les acteurs de santé régionaux en proposant des services mutualisés : aide à la mise en place du plan de continuité et de reprise d'activité (PCRA), campagnes de sensibilisation du personnel en établissements, tout comme des professionnels de santé libéraux, formations techniques sur la sécurité informatique, assistance en cas d'incident de sécurité, etc.

Une offre complète de services pour se former, anticiper et réagir aux risques cyber

Pour répondre à l'ensemble des besoins des établissements quelles que soient leur taille et leurs activités, le GCS Sara propose une offre complète et adaptée de services qui comprend notamment :

- **La réalisation d'exercices de crise** conduits pour préparer les établissements de la région à tout type d'attaque cyber : **291 exercices de crise** ont été conduits depuis 2023.

- **Des formations-actions dédiées au « Plan de reprise et de continuité d'activité (PCRA). Près de 100 établissements ont été formés par le biais de 30 ateliers pratiques** pour mieux appréhender la démarche de gestion de la continuité des activités essentielles, en situation de crise.

- **Une équipe d'experts accessible toute l'année 24h/24 et 7j/7** qui accompagne les établissements en cas de suspicion ou d'incident avéré de sécurité avec une intervention garantie en moins de 24 heures. **170établissements, tous secteurs confondus bénéficient de ce service dans la région.**

- **Prochainement, un service « Safe zone » d'archivage externalisé de données de santé et administratives actif** en permanence et servant de gisement sécurisé de recours en cas d'indisponibilité du système d'information.

[3] Fonds européens

Calydial, établissement de santé engagé depuis 2022 pour renforcer sa culture de la sécurité numérique

CALYDIAL, établissement de santé rénale, de statut privé non lucratif, propose depuis 2022 à l'ensemble de son personnel un e-learning mensuel, développé par le GCS Sara, permettant de renforcer la culture de sécurité numérique et d'acquérir des cyber-réflexes.

« L'adhésion des professionnels à cette proposition est bonne puisque, selon les mois, le taux de participation varie de 60 à 85%. Les exercices de faux phishing sont également envoyés à fréquence régulière aux salariés. Ils font ensuite l'objet d'un échange en staff, et les salariés piégés sont accompagnés par la RSSI[4] et leur cadre pour apprendre à reconnaître les pièges et à redoubler de vigilance » témoigne **Jean-Pierre Grangier, Directeur des systèmes d'information chez Calydial.**

Calydial a également participé au développement d'un nouveau programme de cybersécurité visant les nouveaux arrivants, afin de les sensibiliser à ces différents enjeux.
Ce programme sera proposé sur toute la région dès la fin de l'année.

Crédit photo : Norbert Lacroix

« L'erreur humaine est la première porte d'entrée pour les pirates : la sensibilisation régulière des salariés participe fortement à renforcer nos défenses face à la cybermenace » ajoute Jean-Pierre Grangier.

D'autre actions sont aussi menées dans le cadre des programmes nationaux (HOP'EN / CaRE), tels que des exercices de crise, qui mettent en situation les professionnels pour qu'ils prennent conscience des risques et acquièrent les bons réflexes en cas d'attaque. Calydial est l'un des 15 lauréats d' « HospiConnect ALPHA », un appel à projets qui permet d'accompagner les structures dans la sécurisation de la chaîne d'identification électronique, en conformité avec le référentiel d'identification électronique (RIE), tout en simplifiant l'expérience utilisateur pour l'accès des professionnels aux services numériques sensibles.

Afin de poursuivre ses actions de sensibilisation auprès des établissements, le GCS Sara organise avec le soutien de l'ARS ARA, une journée régionale Cybersécurité le 22 janvier 2026.

Contacts presse :

ARS Auvergne-Rhône-Alpes – Magali Desongins
Tél. 04 27 86 55 55 - ars-ara-presse@ars.sante.fr

GCS Sara – Sylviane Piedallu
Tél. 04 73 31 87 34 - communication@sante-ara.fr

Calydial - direction@calydial.org

[4] Responsable Sécurité des Systèmes d'information