RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Agence Régionale de Santé Bourgogne-Franche-Comté

Emetteur DIS / Département e-santé	**Relevé de décisions** **Comité stratégique e-santé** **Renforcer la résilience numérique du système de santé** **-** **Réunion du 15.04.2026**	Date : 07/05/2026
Destinataires : Tout public		PJ : Support de la réunion

Emargement

29 participants :

LIGIER Lucie	ARS BFC
DUBOUDIN Cédric	ARS BFC
LE RHUN Bertrand	ARS BFC
JOURNOT-PAGNY Julie	ARS BFC
LANTELME Tom	ARS BFC
TAN Ivan	ARS BFC
CARVALHO Emmanuelle	ARS BFC
LOUIS Pascal	URPS Pharmaciens
PERRAULT Bruno	GRADeS BFC
GRIVELET Etienne	GRADeS BFC
AMALRIC Sarah	CHU Dijon
YEME Pierre-Guillaume	FHP
DEFRAIN Lydie	URPS Infirmiers
VACHON Lilian	DCGDR / CPAM Côte d'Or
SERRE Catherine	URIPOSS
PERROT Faustine	FEHAP
ROBISSON Floriane	Représentante de usagers
NARGAUD Francis	URPS Masseurs-kinésithérapeutes
HENRY Géraldine	NEXEM
CHAPPAZ Romain	URPS Infirmiers
DORMEYER Sonia	Déléguée régionale adjointe – FHF BFC
PICARD Matthieu	Directeur Adjoint - URPS ML
VADOT Thomas	CHI de Haute-Comté
ORY Vincent	CHI de Haute-Comté
BENSASSI Dalila	URPS Pharmacien
LUIGI Emmanuel	CHU Besançon
GRAVERON Arnaud	CHU Besançon
COUHERT Michel	Mutualité Comtoise
GREUSARD Mathilde	CPTS Entre Doubs et Jura

1. Éléments de cadrage stratégique

Le comité stratégique e-santé s'est réuni afin d'aborder les priorités régionales 2026 en matière de santé numérique, avec un focus particulier sur la résilience numérique du système de santé en cas de crise cyber.

2. Priorités stratégies ARS BFC 2026

Les orientations prioritaires pour 2026 ont été rappelées par Madame LIGIER, Directrice Générale Adjointe :

- Santé mentale
- Santé des enfants
- Territorialisation de l'action de l'ARS ;

Le numérique est réaffirmé comme un levier transversal au service des politiques publiques, des parcours et des coopérations territoriales.

Concernant la territorialisation, il est précisé qu'il ne s'agit pas d'une réorganisation structurelle de l'ARS mais d'un renforcement de la proximité territoriale, de l'analyse des besoins et des coopérations locales.

3. Renforcer la résilience numérique du système de santé

Constats et enjeux régionaux

Le comité partage le constat d'une montée forte du risque cyber dans l'ensemble du système de santé, touchant les établissements sanitaires, les professionnels de ville et le secteur médico-social.

Le programme national de renforcement de la cybersécurité des établissements de santé (CaRE) est présenté, avec une déclinaison régionale portée par l'ARS et le GRADeS. Les travaux engagés portent notamment sur la sécurisation des accès, la continuité et reprise d'activité, les accès distants et la gouvernance cyber.

Les échanges mettent en évidence la nécessité d'élargir progressivement ces démarches au secteur médico-social, dont le niveau de maturité cyber demeure très hétérogène.

Retour sur la cyberattaque du CHI Haute Comté

L'attaque subie en octobre a affecté simultanément les applications métiers, les moyens de communication, certaines fonctions administratives ainsi que l'organisation quotidienne des soins. Les intervenants insistent sur les effets en cascade générés par l'interconnexion croissante des établissements et de leurs partenaires. Les impacts ont concerné non seulement l'établissement touché, mais également les laboratoires, l'imagerie et les partenaires territoriaux.

La gestion de crise a mis en évidence l'importance des plans de continuité et de reprise d'activité (PCRA) et des exercices préparatoires. Plusieurs enseignements opérationnels sont

partagés :

- La nécessité de cloisonner les réseaux ;
- L'importance de la détection précoce ;
- Le besoin d'une supervision continue des infrastructures ;
- La préparation régionale coordonnée à la reprise d'activité.

Les échanges soulignent également l'impact humain majeur d'une telle crise. Enfin, le retour à la normale est présenté comme particulièrement long et mobilisateur, avec des conséquences durables sur l'activité des établissements.

Retour d'expérience d'une cyberattaque en secteur libéral

Le retour d'expérience relatif à l'attaque du logiciel métier Weda met en lumière la vulnérabilité des cabinets libéraux face aux incidents cyber.

L'interruption d'accès aux dossiers patients a fortement désorganisé l'activité médicale quotidienne : difficultés d'accès aux antécédents, perturbation des prescriptions, impossibilité de consulter certains résultats médicaux et ralentissement important des consultations.

Les dispositifs de continuité d'activité demeurent encore peu développés en médecine de ville, notamment en l'absence de solutions alternatives de fonctionnement en mode dégradé. Les échanges mettent également en avant les conséquences économiques et organisationnelles pour les professionnels concernés, ainsi que les interrogations des patients relatives à la confidentialité de leurs données de santé.

La nécessité de développer des solutions minimales de continuité d'activité adaptées aux professionnels libéraux est identifiée comme un enjeu prioritaire.

Perspectives du comité

Les échanges conduisent à un consensus sur la nécessité de structurer un RETEX régional approfondi afin de capitaliser sur les enseignements des incidents récents, à engager lors du premier COPIL Cybersécurité à venir.

Plusieurs thématiques sont identifiées comme prioritaires :

- Les modalités de détection et d'alerte ;
- Les dispositifs de reprise d'activité ;
- La mobilisation des ressources humaines en situation de crise ;
- Les impacts financiers et organisationnels ;
- Les modalités de communication avec les professionnels et les usagers.

Le comité souligne également l'intérêt de construire un socle régional minimal de préparation cyber, comprenant des référentiels communs, des outils de gestion de crise et une meilleure visibilité du niveau de préparation des structures.

4. Téléexpertise en dermatologique : modèle de centres ressources

Le comité souligne la montée en puissance du modèle régional de téléexpertise, en particulier

en dermatologie, présenté comme une organisation désormais mature et reconnue au niveau national.

Les échanges mettent en avant une amélioration significative de l'accès à l'avis spécialisé, avec des délais de réponse majoritairement inférieurs à 24 heures et une réduction importante des consultations présentielles non nécessaires.

Les participants soulignent également les effets positifs observés sur la fluidité des parcours, la montée en compétence des professionnels de premier recours et le renforcement des coopérations territoriales. L'activité poursuit sa progression, avec environ 13 000 téléexpertises réalisées en dermatologie et une forte croissance constatée en 2025.

Le comité rappelle toutefois que la pérennité du modèle repose sur une organisation régionale structurée et sur des financements complémentaires au droit commun, nécessaires au maintien des centres ressources.

Les travaux d'extension se poursuivent dans plusieurs spécialités, notamment en cardiologie, neurologie, rhumatologie, hématologie et santé mentale. Cette dernière est identifiée comme une priorité régionale pour les prochains développements.

9. Conclusion

Les dates des prochaines séances du COSTRA e-santé sont définies et communiquées aux membres, qui sont invités à remonter les sujets qu'ils aimeraient aborder.

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Agence Régionale de Santé Bourgogne-Franche-Comté

Renforcer la résilience numérique du système de santé

Lucie LIGIER, Directrice Générale Adjointe
Cédric DUBOUDIN, Directeur de l'Innovation et de la Stratégie
Bertrand LE RHUN, Responsable du département e-santé

Direction de l'Innovation et de la Stratégie
Agence Régionale de Santé Bourgogne Franche-Comté

Priorités 2026 de l'Agence Régionale de Santé Bourgogne-Franche-Comté

Lucie LIGIER

Focus : la résilience numérique du système de santé régional face au risque cyber

Tom LANTELME, Vincent ORY, Dr Mathilde GREUSARD

Qu'est-ce que la cybersécurité ?

Protéger les systèmes informatiques (réseaux, serveurs, postes)

Sécuriser les données sensibles (patients, clients, entreprise)

Garantir la continuité d'activité

Confidentialité → éviter les accès non autorisés

Intégrité → garantir que les données ne sont pas altérées

Disponibilité → assurer que les services restent accessibles

Prévenir, détecter et réagir aux cyberattaques

AVANT

Prévention & Préparation

- Audit & cartographie du SI
- Plan de Continuité (PCA/PRA)
- Procédures papier de secours
- Exercices de crise (simulation)
- Formation anti-phishing
- Sauvegardes hors ligne (3-2-1)

PENDANT

Réponse à Incident

- Isolation du SI compromise
- Activation cellule de crise
- Mode dégradé
- Alerte ARS, ANSSI
- Investigation forensique
- Maintien des soins critiques

APRÈS

Remédiation & Retour REX

- Reconstruction sécurisée du SI
- Déploiement postes assainis
- Renforcement sécurité (MFA…)
- Analyse de la compromission
- RETEX complet avec équipes
- Mise à jour PCA / PRA
- Plan d'amélioration continue

Contexte et risques actuels

- Contexte géopolitique : risque accrue dans un contexte d'instabilité mondial
- Secteur de la santé particulièrement sensible :
  - manque de prise en compte de l'aspect cyber
  - sensibilité des données de santé
  - processus de prise en charge massivement numérisé.

Chiffres clés : En **2024**, **749 incidents** ont été **déclarés au niveau national**

- Attaques majeures en 2025 : WEDA, CEGEDIM, **CHI HC de Pontarlier**
- Politique volontariste de l'état qui se traduit par l'existence du programme de financement CaRE

Cybersécurité : programme national CaRe

Objectif : Prévenir les cyberattaques et renforcer la résilience des SI pour assurer la continuité des soins

Budget : 750 M€ d'ici 2027, dont 250 M€ jusqu'en 2025

Acteurs régionaux : Au niveau régional, les ARS et les GRADeS sont les relais opérationnels du programme Santé France

4 domaines d'action : Annuaires techniques (D1) · Continuité/reprise d'activité (D2) · Accès distants (D3) · Gouvernance (D4)

Cybersécurité en BFC : travaux 2025-2026

→ **Organisation d'un RETEX approfondi** du CHI HC permettant d'inventorier l'ensemble des impacts informatiques, techniques, administratifs et de prise en charge et d'engager la réflexion pour répondre, à un niveau régional, à des futures problématiques similaires.

- Pilotage du programme **CARE Domaine 2 :** 100 % des GHT et 85% des ES privés s'engagent en BFC

- Programmation de **l'exercice régional de crise cybersécurité 2026** : le scénario intégrera la mise en place d'une CRAPS dans le cadre d'une attaque d'un établissement pivot de GHT.

CRRC : Centre Régional de Ressources Cybersécurité (portage GRADeS BFC)
- actions de sensibilisations et formations techniques : près de **28 000 utilisateurs sensibilisés**,
- accompagnement des établissements dans la mise en œuvre des Plans de Continuité et de Reprise d'Activité,
- prestations spécifiques dédiées aux ESMS : 41 diagnostics de maturité SI et 19 exercices de crise

ReSIST – Assurer la continuité des soins en cas de problème informatique (panne ou attaque)
-> Dispositif régional de remise en fonctionnement express : sauvegardes externes et prêts de matériels

La résilience numérique hospitalière doit être pensée à l'échelle régionale

M. Vincent ORY,

Directeur des Affaires Générales et Coopérations Finances et Performances,

M. Thomas VADOT,

Responsable de la sécurité des systèmes d'information,

La crise nous à appris qu'un établissement de santé n'est plus un système isolé, mais un maillon critique d'un ensemble territorial interconnecté.

Recommandation issue de la crise : raisonner « écosystème » et non « site isolé ».

La résilience numérique hospitalière doit être pensée à l'échelle régionale

Un établissement interconnecté

Un établissement comme le nôtre héberge, échange ou partage des services numériques avec d'autres structures de santé : dossiers patients, messageries, fonctions de biologie ou autres applicatifs critiques. Il n'est plus un système isolé.

Une menace territoriale

Dans ce contexte, une attaque cyber ne menace pas uniquement le fonctionnement interne de l'établissement touché ; elle peut désorganiser plusieurs acteurs du territoire en même temps, avec des effets immédiats sur la continuité des soins.

Une chaîne numérique territoriale

La crise a montré que la continuité des soins dépend désormais d'une chaîne numérique territoriale associant établissements, partenaires, laboratoires, imagerie, hébergeurs, tutelles et acteurs d'appui spécialisés.

Une recommandation claire

La première recommandation que nous tirons de cette situation est donc claire : la cybersécurité hospitalière doit être conçue comme un enjeu de résilience régionale, et non comme une problématique strictement locale.

Une cyberattaque sur un établissement pivot produit des effets en cascade

La crise nous à appris qu'une compromission du cœur du SI peut rapidement dépasser le périmètre technique initial et devenir une crise territoriale.

Mécanismes d'amplification

Dans le cas d'une attaque réussie, l'atteinte aux fonctions d'administration du SI, à la virtualisation et aux sauvegardes peut entraîner une interruption massive et prolongée des services numériques critiques.

Les interdépendances techniques, les services mutualisés, les liens de confiance entre environnements et le stockage partagé sont autant de facteurs susceptibles d'amplifier la propagation de l'impact.

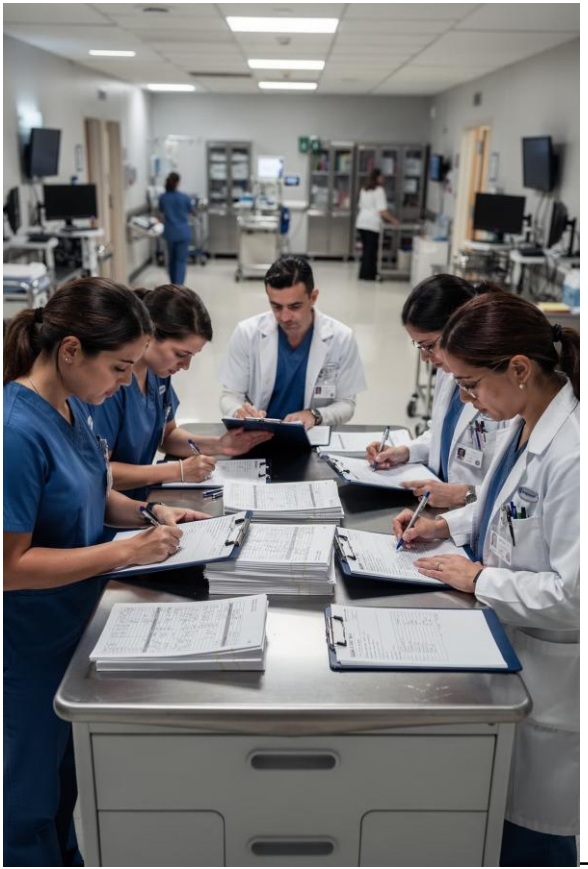
Point de fragilité systémique

La crise a montré qu'un établissement pivot peut devenir un point de fragilité systémique pour les structures qui dépendent de ses ressources, de ses échanges ou de ses hébergements. Une seule compromission peut ainsi paralyser un réseau entier de soins.

Recommandation opérationnelle

La recommandation opérationnelle qui en découle est de réduire au maximum les effets domino, par une architecture cloisonnée, une gouvernance explicite des dépendances et une séparation nette des environnements.

Recommandation issue de la crise : empêcher qu'une compromission locale devienne une crise régionale.



La continuité des soins en mode dégradé

La résilience ne se mesure pas seulement par la vitesse de redémarrage du SI, mais par la capacité à continuer de soigner en sécurité malgré la rupture numérique.

Impact immédiat

Perte simultanée de l'accès aux prescriptions, aux résultats, aux antécédents, aux circuits administratifs, aux plannings et aux communications, ainsi que de la téléphonie IP, mais persistance heureuse des lignes analogiques cuivre.

Risques associés

Charge mentale accrue, circuits allongés, retranscription manuelle et exposition plus élevée au risque d'erreur.

Exigence opérationnelle

Chaque métier, service et établissement doit disposer de procédures dégradées formalisées, testées et appropriées.

Recommandation issue de la crise : pas de résilience numérique sans continuité métier réellement opérationnelle.

Des impacts humains concrets sur les organisations

Doublement des tâches

Retranscriptions manuelles, validations papier, reconstitution des dossiers et multiplication des appels téléphoniques ou fax.

Services en surcharge

Biologie, pharmacie, secrétariats, archives et unités de soins : heures supplémentaires, besoins de renforts, difficultés à tenir le rythme dans la durée.

Fatigue et stress

Fatigue des équipes, des métiers déstabilisés et la nécessité d'évaluer la charge en soins au regard de la traçabilité papier.

La résilience numérique repose sur quatre exigences structurantes

La crise nous à appris qu'une posture résiliente repose sur le cloisonnement, la détection, la capacité de reprise et la coordination.

1. Cloisonner

Renforcer la segmentation réseau, séparer strictement les environnements hébergeur/hébergés, réduire les liens de confiance et sécuriser tous les accès distants par MFA, bastion et filtrage renforcé.

2. Détecter plus tôt

La crise a confirmé la nécessité d'une supervision centralisée, d'un EDR, d'un SOC et d'un SIEM capables d'identifier précocement les comportements anormaux et de documenter les incidents.

3. Reconstruire sainement

Les opérations de remédiation doivent permettre de repartir d'une chaîne d'administration saine, de sauvegardes vérifiées et d'un environnement de reprise maîtrisé — un "cœur de confiance" préservé.

4. Coordonner et Communiquer

La réponse à une crise majeure suppose une articulation forte entre équipes internes, direction, partenaires territoriaux, expertise cyber spécialisée et capacités d'appui logistique à l'échelle du territoire.

Recommandation issue de la crise : segmenter, détecter, reconstruire sainement et coordonner à l'échelle du territoire.

Nos priorités de résilience pour le système régional de santé

La crise nous à appris que l'objectif n'est pas le risque zéro, mais la réduction de l'exposition, la limitation de l'impact et l'accélération de la reprise.

→ Sécuriser le socle commun

Généraliser l'authentification forte, durcir les accès à privilèges, renforcer l'administration sécurisée et améliorer la traçabilité des actions sensibles sur l'ensemble du périmètre territorial.

→ Repenser les architectures mutualisées

Limiter les interdépendances excessives, sanctuariser les sauvegardes, isoler les fonctions critiques et éviter les zones de confiance trop larges qui constituent des vecteurs d'amplification en cas d'attaque.

→ Organiser une capacité régionale de reprise

Mettre en place des solutions externalisées ou territorialisées permettant un redémarrage minimal et rapide des applications critiques en cas d'attaque majeure, avec des niveaux de service définis et testés.

→ Renforcer les moyens de crise

Communication de secours, achats d'urgence, stock de matériel mobilisable, exercices réguliers, acculturation des métiers et culture partagée de cybersécurité à l'échelle de l'ensemble des acteurs du territoire.

La résilience numérique n'est pas un sujet technique isolé, mais une condition de continuité, de sécurité et de souveraineté des soins à l'échelle régionale. Protéger le système d'information, c'est protéger la capacité du territoire à soigner.

Les impacts d'une attaque cyber

Témoignages

Docteur Mathilde GREUSARD,

Médecin Généraliste
Vice-Présidente de la CPTS entre Doubs et Jura

Impactée par les cyberattaques du CHI HC et de WEDA.
Impliquée dans les initiatives d'entraide entre professionnels de santé pour reconstituer les dossiers patients perdus.

Les impacts d'une cyberattaque

Principaux impacts d'une cyberattaque

Prise en charge patients

- Surcharge des équipes dans une période de tension
- Plannings reconstruits à la main
- Soignants qui travaillent de mémoire sur papier, avec très peu de matériel informatique
- Difficulté à consulter l'historique patient
- Résultats de biologie compliqués à exploiter
- Inventaire des pharmacies manuel des stocks

Systèmes d'information

- La téléphonie interne s'arrête avec le SI, obligation d'utiliser les téléphones personnels
- Complexité à joindre un médecin, un labo, le SAMU
- Coordination entre services : transmissions orales massive
- Gestion de la crise avec le CERT, L'ANSSI, le GRADeS et l'ARS
- Mutualisation de moyens : mise à disposition de matériel de secours, logique de prêt en situation de crise par le GRADeS

Organisation administrative

- Les nouveaux patients peuvent être réorientés vers d'autres hôpitaux
- Consultations programmées annulées ou déplacées dans certains cas
- Commandes fournisseurs bloquées
- Pertes de facturations importantes
- La reconstruction du SI est longue, complexe et coûteuse
- Soutient de 2 millions d'euros de l'ARS

Situation de résilience

Préparation des structures (PCRA / SDSI)

Quelles sont les principales difficultés rencontrées pour renforcer la préparation des structures ?

Situation de résilience

Préparation des structures (PCRA / SDSI)

PCRA (Plan de Continuité et de Reprise d'Activité) : définir les procédures dégradées en cas d'attaque — qui fait quoi, comment maintenir les soins sans SI.

SDSI (Schéma Directeur des Systèmes d'Information) : fixer la trajectoire de sécurisation du SI sur plusieurs années.

Les difficultés sont principalement organisationnelles et culturelles

Organisationnelles & culturelles

- Priorisation minoritaire face aux enjeux de production de soins
- Besoin d'une meilleure coordination entre métiers et DSI
- Difficulté à maintenir les plans à jour dans le temps

Techniques & opérationnelles

- Vision incomplète du SI et des éléments externes
- Difficulté à identifier les activités critiques
- Plans PCRA / SDSI souvent théoriques et peu opérationnels
- Manque de ressources (temps, budget, compétences)

Situation de résilience

Sensibilisation des acteurs

Quelles actions collectives pourraient être renforcées dans les établissements et au niveau régional ?

Situation de résilience

Sensibilisation des acteurs

Axe prioritaire

- Eviter les erreurs humaines (phishing, mots de passe faibles, négligences)
- Toucher tous les professionnels : médecins, administratifs, personnels de soin…

Actions collectives

- Mutualisation des ressources et référents cyber entre établissements
- Partage de retours d'expérience entre structures
- Animation d'une communauté régionale des RSSI
- Impulsion de l'ARS dans la coordination régionale

Actions à renforcer

- Formations systématique et régulières pour tous les personnels
- Simulations de phishing pour tester les réflexes
- Exercices de crise cyber (type Cyberexercice ANSSI) pour tester les plans PCRA
- Intégration de la cyber dans l'accueil des nouveaux arrivants

Situation de résilience

Stratégie et gouvernance

La cyber est-elle aujourd'hui suffisamment portée au niveau stratégique dans les établissements, la ville et les institutions ?

Situation de résilience

Stratégie et gouvernance

Constat actuel :

- La cyber reste souvent portée par la DSI seule, sans remontée au niveau stratégique
- Peu présente dans les instances : Direction, CME, Conseil de surveillance
- En ville et dans les institutions (CPTS, GHT, EHPAD…) la prise de conscience est encore plus faible
- Exigences HAS pas toujours traduites en actions concrètes

Risque de décisions structurantes prises sans vision cyber

Ce qu'il faut viser :

↳ Inscrire la cyber à l'agenda des instances de gouvernance
↳ Nommer un référent cyber au CODIR des établissements
↳ Intégrer les enjeux cyber dans le projet d'établissement

Création du COPIL Cybersécurité

Première instance en juin 2026

Modèle de centres de ressources

Ivan TAN

Publication : Téléexpertise dermatologique en Bourgogne-Franche-Comté : leviers et défis

Objectif : capitaliser sur l'expérience de la téléexpertise dermatologique en Bourgogne–Franche-Comté pour en diffuser les bonnes pratiques

Principaux enseignements

- La téléexpertise apporte une réponse concrète aux tensions d'accès aux soins dermatologiques dans une région particulièrement sous-dotée et rurale.
- Le déploiement régional constitue un succès quantitatif.
- Le maillage territorial autour des centres de ressources et l'usage de la plateforme Telmi permettent d'inscrire la téléexpertise dans un parcours de soins structuré, coordonné et de proximité.

Publication : Téléexpertise dermatologique en Bourgogne-Franche-Comté : leviers et défis

Principaux enseignements (suite)

- La téléexpertise améliore l'accès à l'avis spécialisé, accélère le tri des situations, limite les déplacements inutiles et contribue à réduire les inégalités territoriales.
- En 2024, les 13 220 téléexpertises dermatologiques réalisées représentent un volume équivalent à plus de 6 ETP de dermatologues s'il avait dû être absorbé en présentiel.
- Le dispositif favorise également la montée en compétence des médecins de ville et renforce l'articulation ville-hôpital.
- Sa pérennité suppose cependant des ressources médicales et administratives adaptées, la consolidation des financements ARS (bonus/territoire) et une évolution du cadre réglementaire, notamment sur les questions de facturation et d'identitovigilance.

Conclusions des assises de la télésanté

4 grands enjeux

- Renforcer la place de la télésanté dans le **suivi et le parcours des patients et** notamment **la téléexpertise**
  - Déploiement massif pour les médecins généralistes
  - Mobilisation des hôpitaux, CHU et spécialistes libéraux pour y répondre
  - Accès à l'expertise spécialisée dans chaque Maison France Santé
- Déployer la télésanté au bénéfice des **publics prioritaires** (personnes sans médecin traitant, territoires sous-denses, personnes dépendantes ou en situation de handicap, patients isolés ou ne pouvant se déplacer, personnes détenues)
  - Téléconsultation assistée dans les ESMS notamment en Ehpad
  - Annuaire des bornes de téléconsultation
  - Dérogations ciblées au seuil de 20 % de téléconsultations
  - Exclusion du seuil de 20 % pour toutes les téléconsultations assistées par un PS

Conclusions des assises de la télésanté

4 grands enjeux (suite)

- Améliorer la **qualité des soins** et **limiter les éventuelles dérives**
  - Encadrement renforcé des télécabines (déclaration aux ARS/recommandations HAS, ..)
- Développer les **compétences** des professionnels de santé en matière de **télémédecine**

Une feuille de route nationale en construction

et des projets régionaux déjà alignés avec les perspectives nationales.

Notre modèle de centres de ressources

Dans les grandes lignes

Un contexte régional avec une **forte dynamique en téléexpertise** :

- Entre 2024 et 2025 : Activité + 42 % / Nb de requérants : + 55% / Nb experts : + 14%
- Sur le 1er trimestre 2026 : Activité + 48 % / Nb de requérants : + 31%

Des **centres de ressources opérationnels sur toute la BFC** :

- 4 en dermatologie : Activité + 43% entre 2024 et 2025, + 56 % T1 2026/T1 2025
- 5 en hématologie : Démarrage avril 2025
- 3 en rhumatologie : CHU Dijon, Chalon et GH70
- D'autres spécialités à venir : centres de ressources en santé mentale et en neurologie

QUESTIONS / REPONSES

Conclusion

Relevés de décisions à votre disposition

Création d'un espace où retrouver les sur le site internet externe.

Consultable ici : [Instance stratégiques e-santé | Agence régionale de santé Bourgogne-Franche-Comté]

Prochains COSTRA e-santé

- Prochain COSTRA le **mardi 25 juin de 14h à 16h**

- Autre date à venir :
  - Mardi 20 octobre de 14h à 16h