IL Y A 1 AN : LA CYBER ATTAQUE !

- *Gilles CALMES - Directeur du Centre Hospitalier Sud Francilien et du Centre Hospitalier d'Arpajon*
- *Patrice GARCIA – Directeur du Système d'Information*

«Les 3 800 professionnels de santé du CHSF seront encore plus riches et plus performants après la gestion de cette crise majeure»


Centre Hospitalier
ud Francilien
Centre Hospitalier Sud Francilien (CHSF)

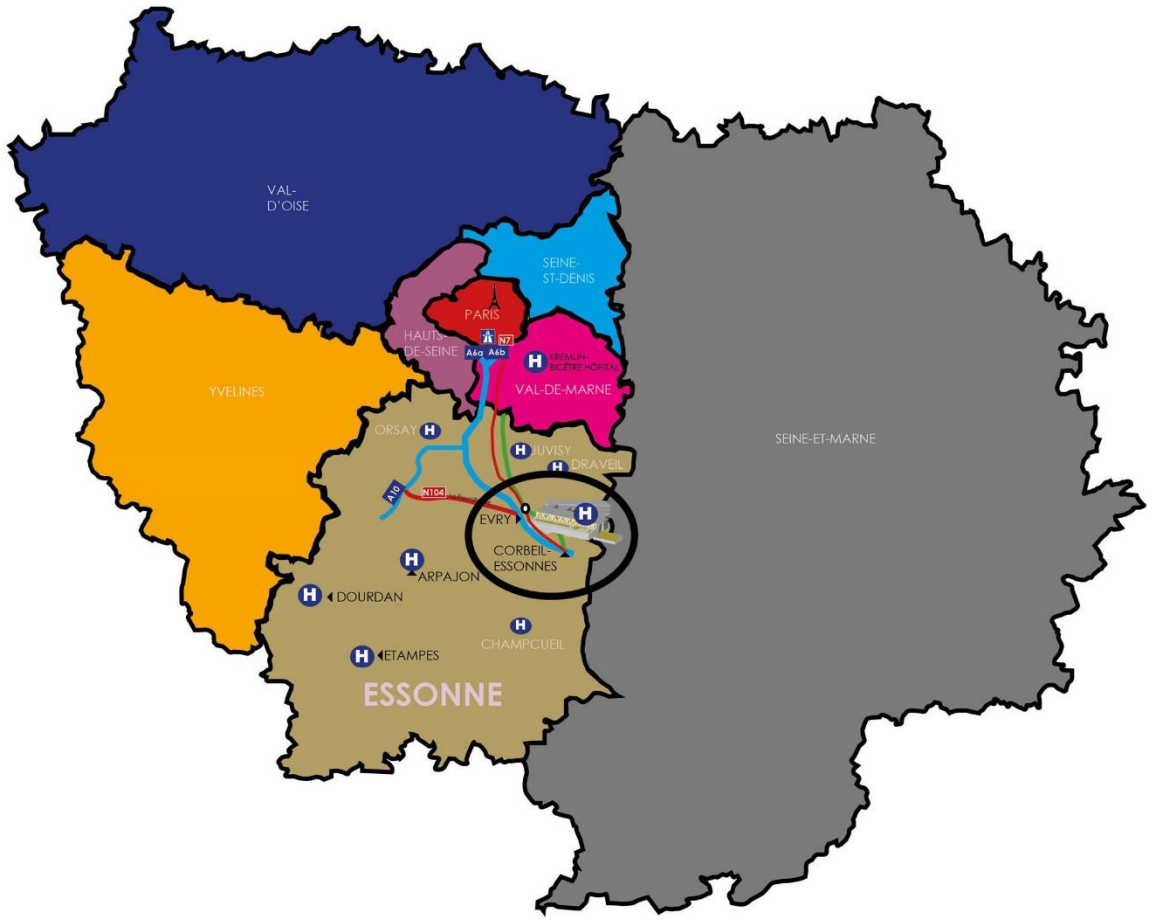
Territoire de santé
900 000 habitants

1 200 lits et places

Médecine Chirurgie Obstétrique

3 800 agents

400 M€ de budget de fonctionnement



Etablissement de recours & référent

Disciplines où le Centre Hospitalier est référent du territoire

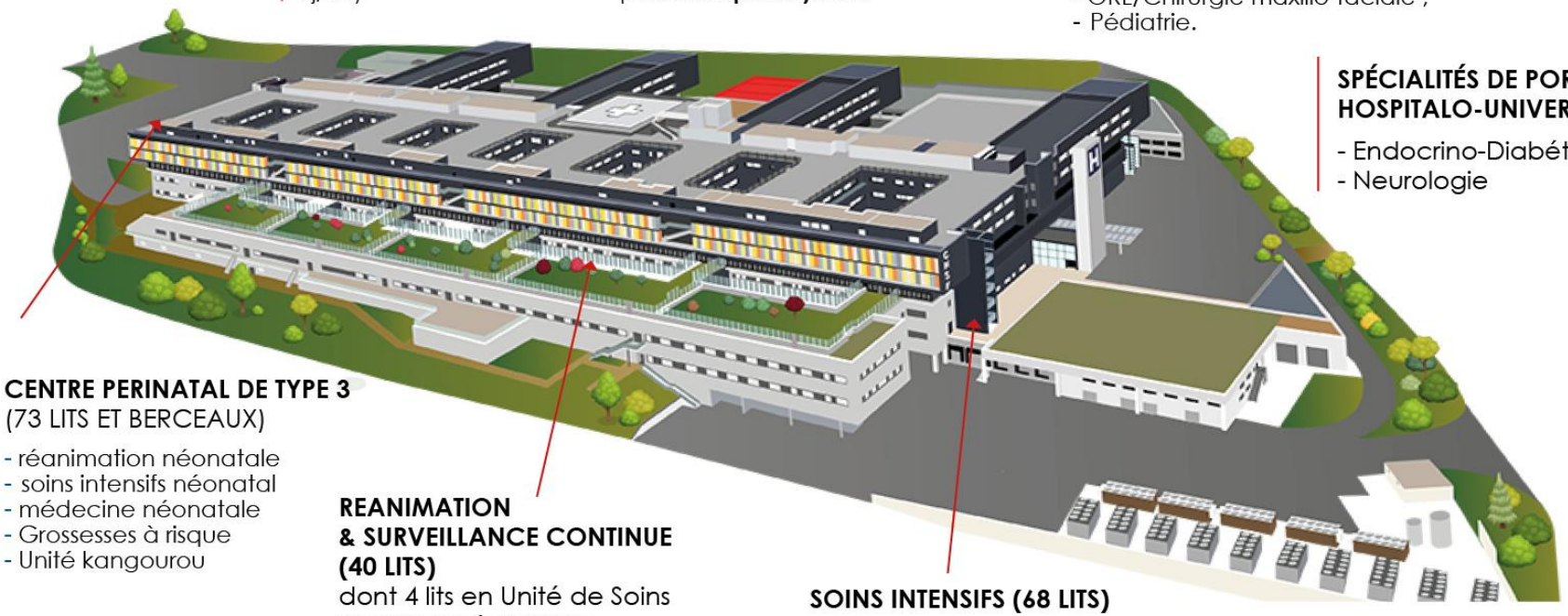
SPÉCIALITÉS DE RECOURS

- **Centre de Coordination en Cancérologie** (8 parcours rapides)
- **Centre de Procréaltion Médicalement Assistée**
- **Chirurgie** (Ophtalmologie, Urologie avec une premanence des soins 24h/24 et 7j/7...)
- Accrédité en **Hématologie** *« Hémopathies tous types »*
-- **Néphrologie-Dialyse** (prise en charge totale des patients atteints de maladies rénales)
- Centre de compétences pour la **Drépanocytose**...

URGENCES
300 passages/jour en moyenne

Accueil 24h/24

- Accident Vasculaire Cérébral/ Accident Ischémique Transitoire en phase aiguë ;
- Coronarographie et Angioplasties ;
- Chirurgie digestive,viscérale, vasculaire ;
- Chirurgie orthopédique et traumatologique ;
- Endoscopies digestives ;
- Gynécologie-obstétrique ;
- Imagerie ;
- Radiologie interventionnelle ;
- Néonatalogie ;
- ORL/Chirurgie maxillo-faciale ;
- Pédiatrie.



SPÉCIALITÉS DE PORTÉE HOSPITALO-UNIVERSITAIRE

- Endocrino-Diabétologie
- Neurologie

CENTRE PERINATAL DE TYPE 3
(73 LITS ET BERCEAUX)

- réanimation néonatale
- soins intensifs néonatal
- médecine néonatale
- Grossesses à risque
- Unité kangourou

REANIMATION & SURVEILLANCE CONTINUE (40 LITS)
dont 4 lits en Unité de Soins Continus pédiatrique

SOINS INTENSIFS (68 LITS)

- Néonataux
Neuro-vasculaire
- Cardiologie
- Hématologie

Equipements autorisés et installés

Imagerie médicale

- 1 mammographe numérique
- 2 scanners de dernière génération
- 2 IRM (1,5 et 3 Tesla)
- 6 salles de radiologie
- 3 salles d'échographie

Biologie médicale

- **1 laboratoire de biologie médicale** (biochimie, hématologie, bactériologie-microbiologie clinique) *avec double chaine analytique automatisée*
- **1 laboratoire d'hygiène hospitalière** (environnement, épidémiologie, lait maternel)
- **Seul centre public d'Anatomie et de Cytologie Pathologiques (ACP) de l'Essonne.**

Médecine nucléaire

- 1 TEP-scan
- 2 gamma-caméras (couplées à un scanner)

Bloc opératoire

- **1 bloc lourd** de 11 salles d'opération (dont 6 salles de chirurgie, une salle dédiée aux urgences chirurgicales, une salle de radiologie interventionnelle, une salle de rythmologie, 2 salles de coronarographie)
- **1 bloc ambulatoire** articulé autour de 4 salles d'une capacité totale de 14 fauteuils
- **1 bloc obstétrical** comprenant 8 salles d'accouchement et 2 salles de césarienne

Néphrologie-dialyse

- 10 postes d'hémodialyse
- 2 postes d'éducation à l'hémodialyse, autorisation pour la dialyse péritonéale

Rééducation/ Balnéothérapie

- 1 plateau

Pharmacie

- 2 isolateurs de préparation centralisée des médicaments anti-cancéreux (cytotoxiques)

INTRODUCTION

- https://www.google.com/search?q=gilles+calmes&client=safari&hl=fr&prmd=inv&sxsrf=AJOqlzXVlBaZSzB-QqnhYWHh_LAKRb5fdg:1675499503096&source=lnms&tbm=vid&sa=X&ved=0ahUKEwjN-8-Fuvv8AhUCTaQEHeStAMcQ_AUIHygD&biw=428&bih=743&dpr=3#fpstate=ive&vld=cid:26a1c574,vid:XzDlF5M5L38

- https://m.youtube.com/watch?v=d-v2hUH4NMs

SOMMAIRE

I) BONNES PRATIQUES PERMETTANT D'ANTICIPER UNE CYBERATTAQUE

H0 : Détection, alerte et déclenchement 21 août

Bonnes pratiques à retenir

- Cadres de nuit et garde du weekend avec connaissance des modes dégradés
- Intervention rapide de la DSI et confinement informatique
- Plan blanc et annuaires imprimés
- Déclinaison « Perte des SI » du Plan Blanc
- PCA couvrant le mode dégradé de tous les services et fonctions
- Réaliser des exercices Cyber

2H30
- Appel de l'ADG
- « Panne informatique »
- Appel de l'astreinte informatique

3H
- Déplacement de l'ADG
- Information SAMU91, SDIS, ARS : arrêt du flux entrant
- Confirmation de la cyberattaque et confinement informatique

3h – 9h
- Activation du Plan Blanc + cellule de crise
- Rappel de personnel
- Modes dégradés papier, notamment pour les prescriptions
- Plan de réadressage patients par le SAMU 91

J1
- Evaluation des impacts : conséquences directes de l'attaque et conséquences liées au confinement informatique
- Déploiement progressif des modes dégradés

Gestion et pilotage de crise

Bonnes pratiques à retenir

- Organisation qui permette les échanges entre métiers – direction – DSI de façon optimale
- Intégrer immédiatement toutes les fonctions support
- Moyens de communication agiles interne/externe et ascendante/descendante

Perte des moyens de communication : recours à Whatsapp ou à un outil sécurisé

Coordination générale : 3 CCH par semaine avec directeurs, chefs de pôles et cadres

Cellule de crise restreinte 1 à 2 fois par jour : CODIR

Cellule de crise informatique 1 à 2 fois par jour

Information quotidienne des cadres

Réunions d'information au personnel y compris de nuit (enregistrées)

Secteur médico-technique

Biologie

Forte réduction des capacités, arrêt des consultations externes

Pharmacie

Gestion des stocks et commandes manuelles, forte diminution des capacités

Imagerie

Appareils non impactés mais perte de la capacité de diffusion dans les services et réduction de la capacité de traitement

EFS

Gestion manuelle du stock de PSL. Maintien d'un stock à minima.

PMA

Cuves d'azote et étuves de cultures sur un réseau isolé. Limites de biologie. Maintien des inséminations et transferts.

Médecine nucléaire

Mode dégradé pour le suivi des prescriptions et des activités.

Bonnes pratiques à retenir

- Modes dégradés pour l'ensemble des fonctions supports médico-techniques
- Sur le plan informatique, isoler et sécuriser les matériels critiques
- Traiter ces points en très grande priorité en cas d'attaque

Impacts sur la prise en charge des patients

Soins critiques

Arrêt de l'admission de patients externes (impact de l'imagerie / biologie / pharmacie).

SAU : présentations spontanées.

Reprise progressive en cours.

Pôle mère-enfant

Transfert de la réa néonat par défaut de monitorage.

Accueil des urgences non régulées.

Réorientation des cas les plus critiques.

Médecine

Difficultés liées à la perte des listes de rendez-vous et dossiers médicaux.

Fonctionnement en mode dégradé.

Chirurgie

Evaluation bénéfice / risque au cas par cas, notamment au regard de la gestion du stock de PSL et des capacités réanimatoires limitées.

Bonnes pratiques à retenir

- Lien immédiat avec le SAMU et le tissu territorial
- Renforcement de la MMG
- Mode dégradés anticipés
- Stocks de supports papiers
- Cellule d'évaluation des patients candidats à la chirurgie

Fonctions supports et administratives

Secrétariats

Perte d'internet, outils bureautiques, imprimantes et moyens de communication.

Secrétariats médicaux

Perte des outils bureautiques et de la génération des compte-rendu : accumulation de retards importants.

Ressources humaines

Perte des outils de plannings et logiciels de paie. Modes dégradés de courte durée.

DAF

Perte des outils d'admission, de gestion financière, capacité de commande et de règlements très dégradée. Réduction d'activité de l'ordre de 5M€ / mois.

Téléphonie

Non impactée par l'attaque.

Infrastructure / bâtiment

Sur un réseau à part, qui n'a pas été impacté.

Bonnes pratiques à retenir

- PCA pour toutes les fonctions
- Clés 4G pour les fonctions critiques, PCs portables et imprimantes
- Annuaires papiers
- Sauvegardes des documents importants en externe (disque dur externe, …)
- Lien immédiat avec le comptable public
- Anticipation de la trésorerie

Focus : Communication et juridique

800 000 courriers envoyés suite à la fuite de données

Travail conjoint Juridique / Communication / DPO / ANSSI / CNIL pour traiter la fuite de données

Dépôt de plainte immédiat, lien avec le C3N

Points de situation réguliers à la presse, sur le site internet, sur Twitter

Difficulté à absorber le flux d'appels entrants d'usagers

Communication interne par tous les vecteurs disponibles

Bonnes pratiques à retenir

- Anticiper très tôt dans la crise les aspects communicationnels et juridiques, qui mobilisent des efforts et ressources conséquents
- Assurer les établissements de santé pour le risque Cyberattaque

Systèmes d’information

Les préconisations

- Idéalement :
  - Une salle informatique déportée
  - Définir PCA « externe » (fichiers et listings en OFF et accessible)
- Définir les Systèmes d’Information Essentiels (SIE) et les sécuriser
- Disposer d’une fiche reflexe en cas de cyber-attaque
- Intégrer tout de suite la recherche de cyber-attaque dans le diagnostic, quand la panne semble générale
- Disposer d’une cartographie technique, fonctionnelle et métier complete (outil + processus de mise à jour)
- Disposer d’un PRA avec une vision métier
- Anticiper les besoins en ressoures MCO (exploitation informatique) et restauration (expert)

Conclusion

Systèmes d'Information

- Cartographie du SIH
- Audits SSI réguliers
- Sécurisation des outils d'administration du SI
- Plan de Reprise Applicative (PRA)

Planification et préparation

- Plans de Continuité d'Activité (PCA) pour tous les secteurs et toutes les directions, en lien avec la cartographie des risques
- Traiter le scénario « Perte des SI » dans Plan Blanc et Plan de Sécurisation de l'Etablissement
- Exercices de préparation et maintien à jour des documents et des compétences

Juridique et communication

- Préparer et déployer un plan de communication interne / patients / externes très rapidement, mais avec peu ou pas de moyens de communications
- Traiter au plus tôt le volet juridique liés aux vols de données
- Prévoir une assurance cyberattaque des établissements de santé

Coordination

- Coordination avec SAMU, ARS IDF et ARS 91 primordiale dès le début pour donner de la lisibilité à tout le territoire
- Être capable d'identifier rapidement ce qui fonctionne ou pas, les impacts, modes dégradés et possibilités de prise en charge des patients
- Savoir que cela va durer au moins plusieurs semaines, et organiser l'offre de soins en fonction
- La cyberattaque est une crise **tout l'hôpital** qui va nécessiter l'engagement de **tous les acteurs**

Phase de stabilisation des modes dégradés jusqu'à 4 mois après l'attaque,
A partir de là s'ouvre une phase de plusieurs mois de reconstruction pérenne du système d'information. Durant cette phase, les équipes conserveront un mode « dégradé amélioré », et devront subir des perturbations, coupures, changements d'outils et de logiciels.
18 mois après l'attaque devrait s'ouvrir une nouvelle ère avec des outils plus performants, stables, et sécurisés.

II) LES 3 OBJECTIFS À ATTEINDRE DURANT LES PREMIÈRES SEMAINES QUI SUIVENT LA CYBERATTAQUE

► **3 OBJECTIFS RÉALISÉES OU EN COURS À CE JOUR** suite à la cyberattaque constatée le 21 août 2022.

01
ARRÊTER LA CYBERATTAQUE
Coupure des accès internes et internet

02
STABILISER ET SÉCURISER

03
RECONSTRUIRE

PLAN DE CONTINUITÉ

01 — **Semaine 1** (du 21 au 28 août 2022)

ÉTAT DES LIEUX

Inventaire de ce qui fonctionne et de ce qui ne fonctionne pas.

PRIORISATIONS

Choix des travaux de rétablissement prioritaires arbitrés par la cellule de crise :
- applications du plateau technique (biologie médicale, pharmacie, imagerie médicale) ;
- écosystème des Ressources Humaines (paie, plannings agile-time...) ;
- moyens de communication (dont la messagerie).

ACCÈS AUX SAUVEGARDES

Installation des équipements permettant d'accéder aux sauvegardes.

02 — **Semaine 2** (du 29 août au 4 septembre 2022)

EVALUATION DES SAUVEGARDES

Evaluation de l'état des sauvegardes (chiffrées/ non chiffrées) et des données (complètes /par-

SÉCURISATION DES MESSAGERIES

Migration des boites mails nominatives sur Office 365, un service fourni et sécurisé par Microsoft.

SÉCURISATION DES INSTALLATIONS

Actions de sécurisation des installations technico médicales (notamment Biomedicales) et transverses (téléphonie, postes de travail..).

SÉCURISATION DES DONNÉES CONSERVÉES

Construction d'une bulle sécurisée informatique permettant de redémarrer en urgence certains applicatifs métiers prioritaires en mode dégradé (sans interface).

INSTALLATION DE SOLUTIONS MÉTIERS

Remise en service des solutions métiers considérées comme prioritaires sur des postes informatiques.

03 — **Semaine 3** (du 5 au 11 septembre 2022)

INSTALLATION DE L'ANTIVIRUS EDR

Campagne d'installation du dispositif de protection EDR sur chacun des postes du CHSF.

REMISE EN SERVICE PROGRESSIVE DES MOYENS DE COMMUNICATION

✓ Messageries office (sur un nombre restreint de postes)

✓ AgileTime sur 4 postes non interfacés pour assurer les Eléments Variables de Paie et la saisie des Plannings par les cadres).

TRAVAUX PRIORITAIRES

► Trois service du plateau technique hospitalier ont été désignés comme prioritaires pour bénéficier des travaux de restauration de leurs solutions métiers (non interfacées pour l'heure avec les services de l'hôpital).
Ces trois services sont nécessaires à l'activité médicale.

Biologie

- ✓ Pilotage centralisé des automates
- ✓ Aide à l'interprétation des résultats

Pharmacie

- ✓ Accès aux protocoles,
- ✓ Préparation des Chimiothérapies
- ✓ Gestion du stock,
- ✓ Commandes

Imagerie

- ✓ Système d'archivage des images
- ✓ Transfert des images

✓ **AGILETIME**, logiciel de gestion du temps de travail du personnel hospitalier a été remis en fonctionnement et centralisé sur 4 postes lourds (2 postes pour les cadres de santé et 2 postes pour la DRH). Le versement des traitements et salaires reste garanti.

✓ **Les serveurs des installations de monitorage** pour la surveillance des patients ont été contrôlés. Un serveur a fait l'objet d'une action de dépollution dans la cadre de la démarche de sécurisation des installations informatiques.

✓ **Les solutions informatiques MAINCARE** ayant trait à la gestion administrative, financière et du dossier patient sont en cours de test pour être installées sur quelques postes lourds.

III) FEUILLE DE ROUTE DU SYSTÈME D'INFORMATION APRÈS LA PHASE DE STABILISATION ET DE SÉCURISATION

Préparation Feuille de route du SI – CHSF/CHA

- Aligner la feuille de route SI CHSF/CHA sur :
  - La feuille de route du numérique en santé 2023-2027 (en cours de validation au niveau du Ministère),
  - la Directive Européenne de Cybersécurité (NIS).

- Remettre en place une gouvernance du SI (avec le CSSI et les processus définis)

- En terme de méthode :
  - Un ensemble rapides de « petites victoires », plutôt qu'une grande victoire lointaine.

Feuille de route du SI CHSF/CHA

Vision organisationnelle

Mettre le numérique au service de la santé

FEUILLE DE ROUTE DU NUMÉRIQUE EN SANTÉ 2023-2027

Les quatre grands axes du numérique en santé

Prévention

Développer la prévention et rendre chacun acteur de sa santé

Prise en charge

Dégager du temps pour tous les professionnels de santé et améliorer la prise en charge des personnes grâce au numérique

Accès à la santé

Améliorer l'accès à la santé pour les personnes et les professionnels qui les orientent

Cadre propice

Déployer un cadre propice pour le développement des usages et de l'innovation numérique en santé

https://esante.gouv.fr/strategie-nationale

PRÉVENTION

AXE 1 - Développer la prévention et rendre chacun acteur de sa santé

- Sur la base du programme SEGUR, développer la dématérialisation des documents patients vers « Mon Espace Santé », avec la messagerie sécurisée citoyenne
- Projets associés :
  - CrossWay LIFEN : dématérialisation LS, CR, alimentation du DMP (2022)
  - Maincare IC : mise en place connexion directe alimentation DMP (2024)
  - Mise en place de la messagerie citoyenne en parallèle de la messagerie sécurisée MSSanté (2024).

PRISE EN CHARGE

AXE 2 - Dégager du temps pour tous les professionnels de santé et améliorer la prise en charge des personnes grâce au numérique

Feuille de route ministère

Feuille de route CHSF/CHA

- Simplifier et sécuriser l'accès des professionnels aux services numériques depuis leurs logiciels métiers (Maincare IC) et en mobilité (nouvelle infrastructure).
- Renforcer la digitalisation du parcours patient (notoriété internet, prise de RDV et pré-admission en ligne)
- Projets associés :
  - Déploiement de Maincare IC (socle + paramétrage dossier commun, 2023)
  - Déploiement Maincare IC (2024)
  - Déploiement outils mobilité (RainBow, 2023)
  - Refonte site internet avec renforcement notoriété du CHSF (2023)
  - Digitalisation du circuit patient : mise en place prise RDV en ligne (2023), puis la pré-admission (2024)

ACCÈS À LA SANTÉ

AXE 3 - Améliorer l'accès à la santé pour les personnes et les professionnels qui les orientent

Feuille de route ministère

Feuille de route CHSF/CHA

- Développer et simplifier l'usage de la télésanté
- Développer l'accès aux plateformes numériques (Terri@Santé), SAS
- Modernisation des outils numériques SAMU
- Projets associés :
  - Intégration accès télésanté au module Patients (digitalisation parcours patient 2024)
  - Connexion SRI à Terri@Santé (2023, puis sur solution pérenne)
  - Mise en place connexion logiciel SAMU à la plateforme SAS (2023)

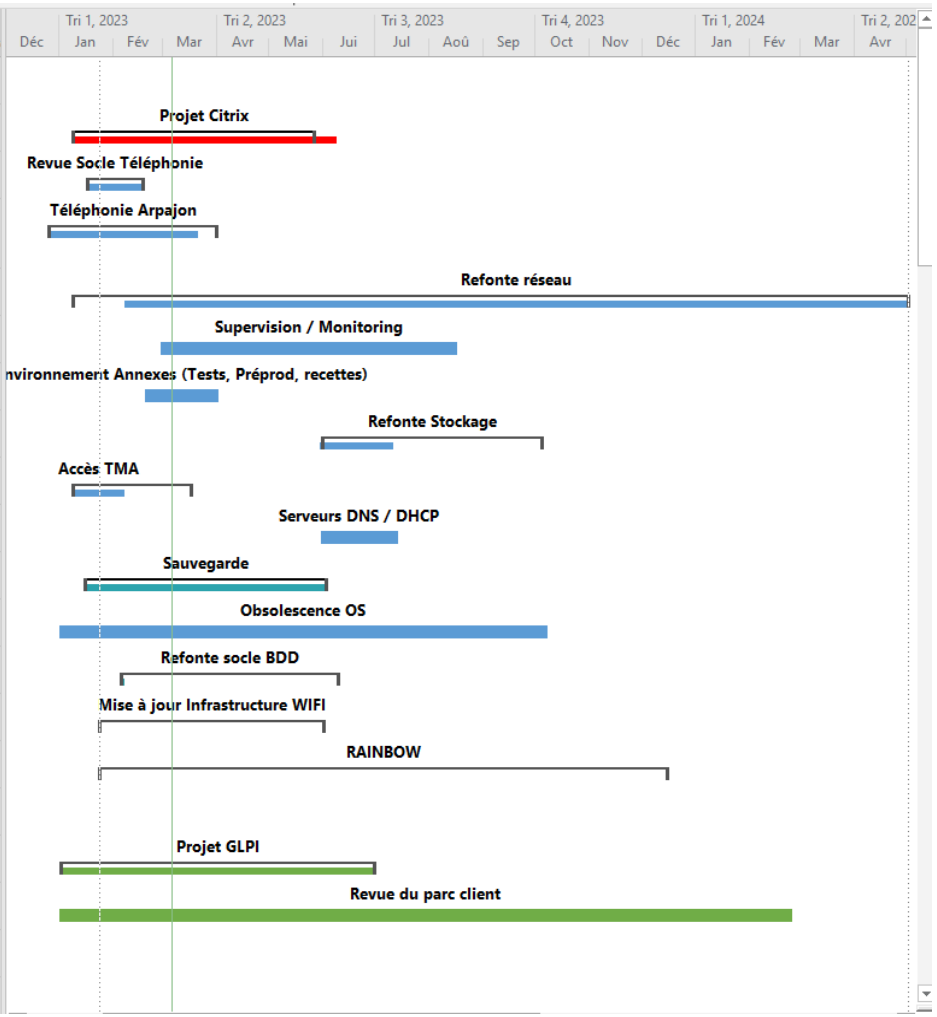
CADRE PROPICE

AXE 4 - Déployer un cadre propice pour le développement des usages et de l'innovation numérique en santé

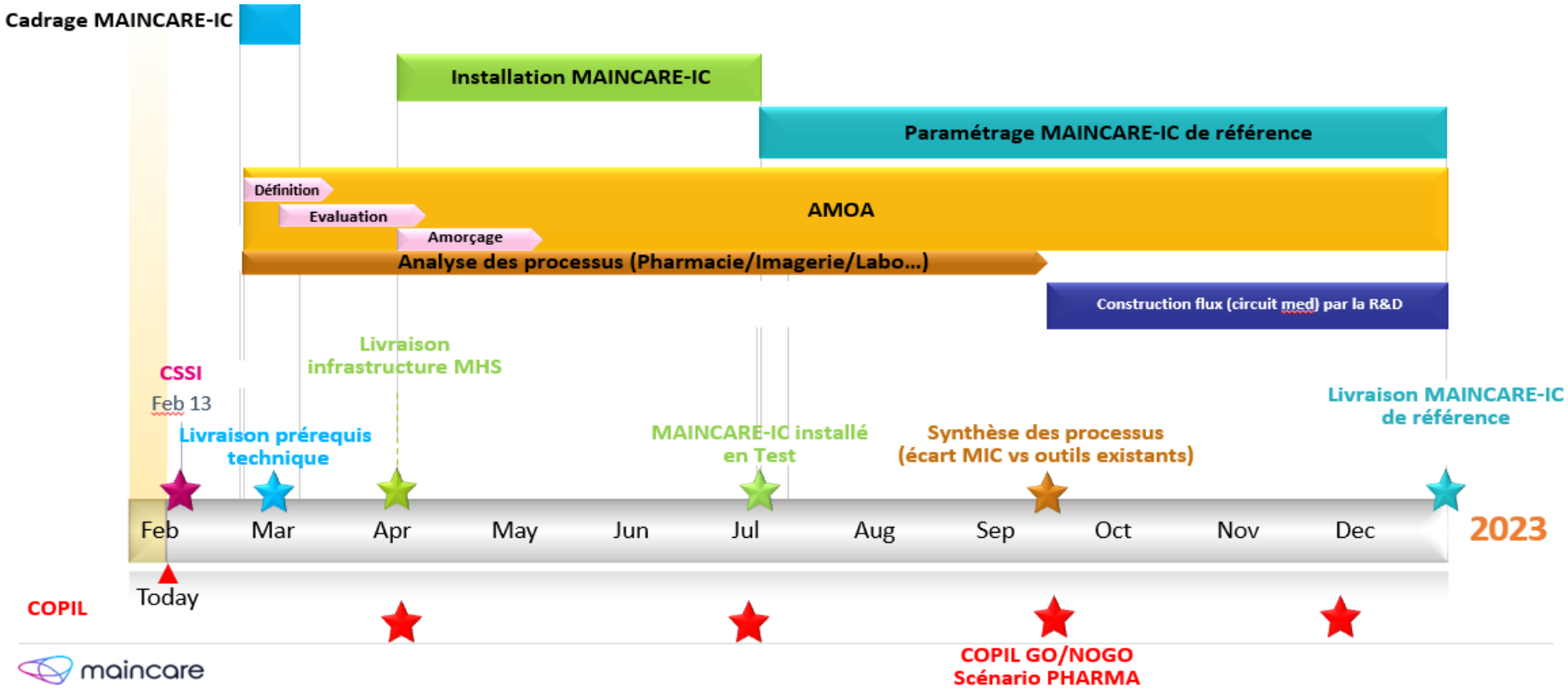
- Élaborer et mettre en œuvre un nouveau plan pluriannuel sur le renforcement massif de la cybersécurité
- Attirer des talents du numérique vers la santé (plan de recrutement, QVT, etc.)
- Projets associés :
  - Mise en place d'un système de management de la sécurité (2023)
  - Reconstruction du socle informatique vers une cible sécurisée (2023, 2024)
  - Mise en place d'un plan de recrutement de 6 personnes à la DSI, appuyé par un cabinet de recrutement

Planning projet Reconstruction SI

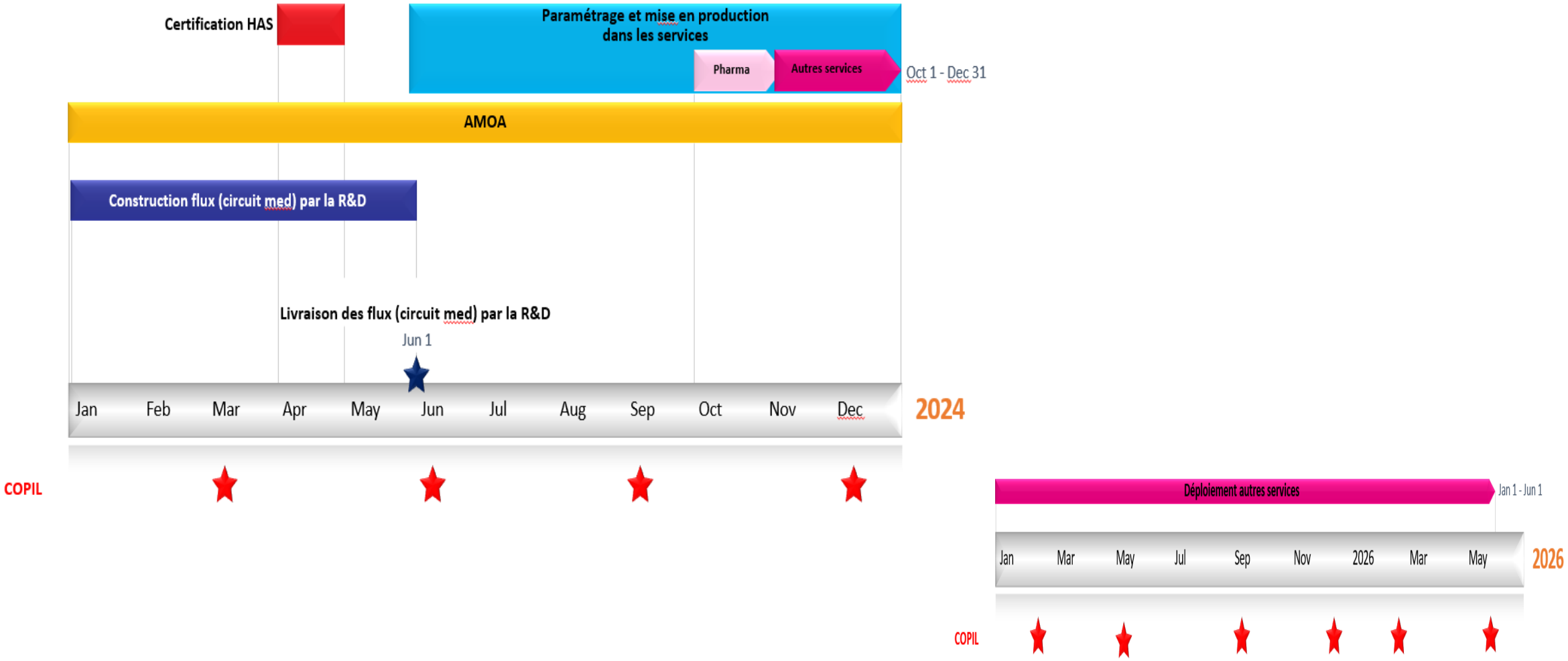
Nom de la tâche	Durée	Début	Fin	Prédécesseur	Noms ressources	% achevé
Technique						0%
Projet Citrix	100 jours	Lun 09/01/23	Ven 26/05/23		Eric CHATEL; Sébastien CAZO;Ty-mi	0%
Revue Socle Téléphonie	24 jours	Mar 17/01/23	Ven 17/02/23		Christophe FILLOUX; Eric CHATEL;Guy	0%
Téléphonie Arpajon	70 jours	Lun 26/12/22	Ven 31/03/23		Eric CHATEL; Eric GUIDE; Guy Mathieu ADJIVON	0%
Refonte réseau	343 jours	Lun 09/01/23	Mer 01/05/24		Eric CHATEL; Guy Mathieu ADJIVON	0%
Supervision / Monitoring	120 jours	Mer 01/03/23	Mar 15/08/23		Ayoub ALKAMA; Bertrand GAUTHIER	0%
Environnement Annexes (Tests, Préprod, recettes)	30 jours	Lun 20/02/23	Ven 31/03/23		Eric CHATEL	0%
Refonte Stockage	90 jours	Jeu 01/06/23	Mer 04/10/23		Eric CHATEL; Sébastien CAZO;Ty-mi	0%
Accès TMA	50 jours	Lun 09/01/23	Ven 17/03/23		Frank COMBEAU	89%
Serveurs DNS / DHCP	30 jours	Jeu 01/06/23	Mer 12/07/23		Eric CHATEL; Sébastien CAZO	0%
Sauvegarde	100 jours	Lun 16/01/23	Ven 02/06/23		Ayoub ALKAMA	0%
Obsolescence OS	200 jours	Lun 02/01/23	Ven 06/10/23		Eric CHATEL; Sébastien CAZO;Ty-mie	0%
Refonte socle BDD	90 jours	Lun 06/02/23	Ven 09/06/23			0%
Mise à jour Infrastructure WIFI	93 jours	Mar 24/01/23	Jeu 01/06/23		Eric CHATEL; Guy Mathieu ADJIVON	0%
RAINBOW	234 jours	Mar 24/01/23	Ven 15/12/23			0%
Support Informatique						0%
Projet GLPI	130 jours	Lun 02/01/23	Ven 30/06/23			0%
Revue du parc client	300 jours	Lun 02/01/23	Ven 23/02/24			0%
Revue du matériel des bornes QMATIC						0%
Projet TECHNIQUE CHA						0%



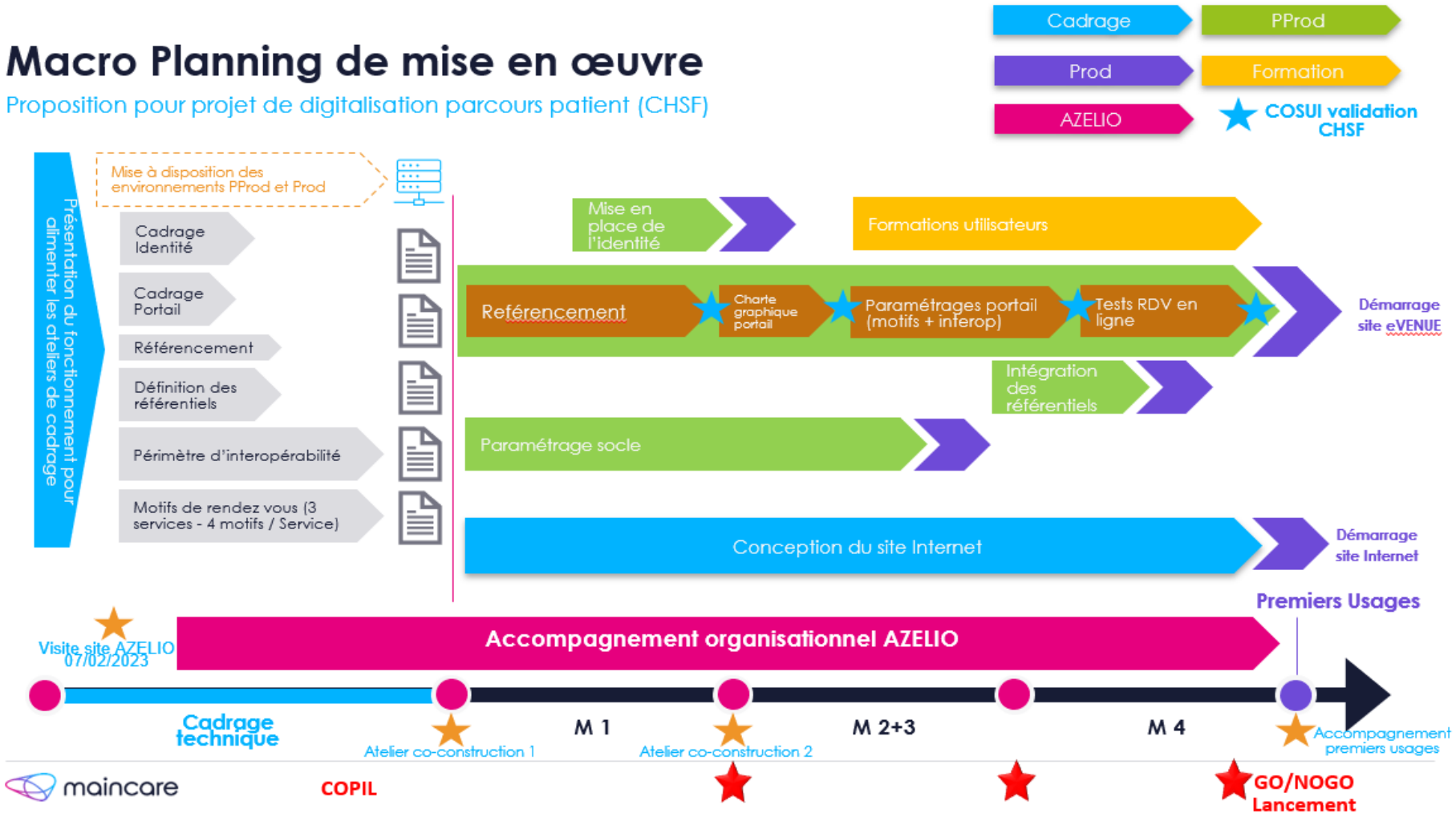
Planning déploiement MAINCARE IC

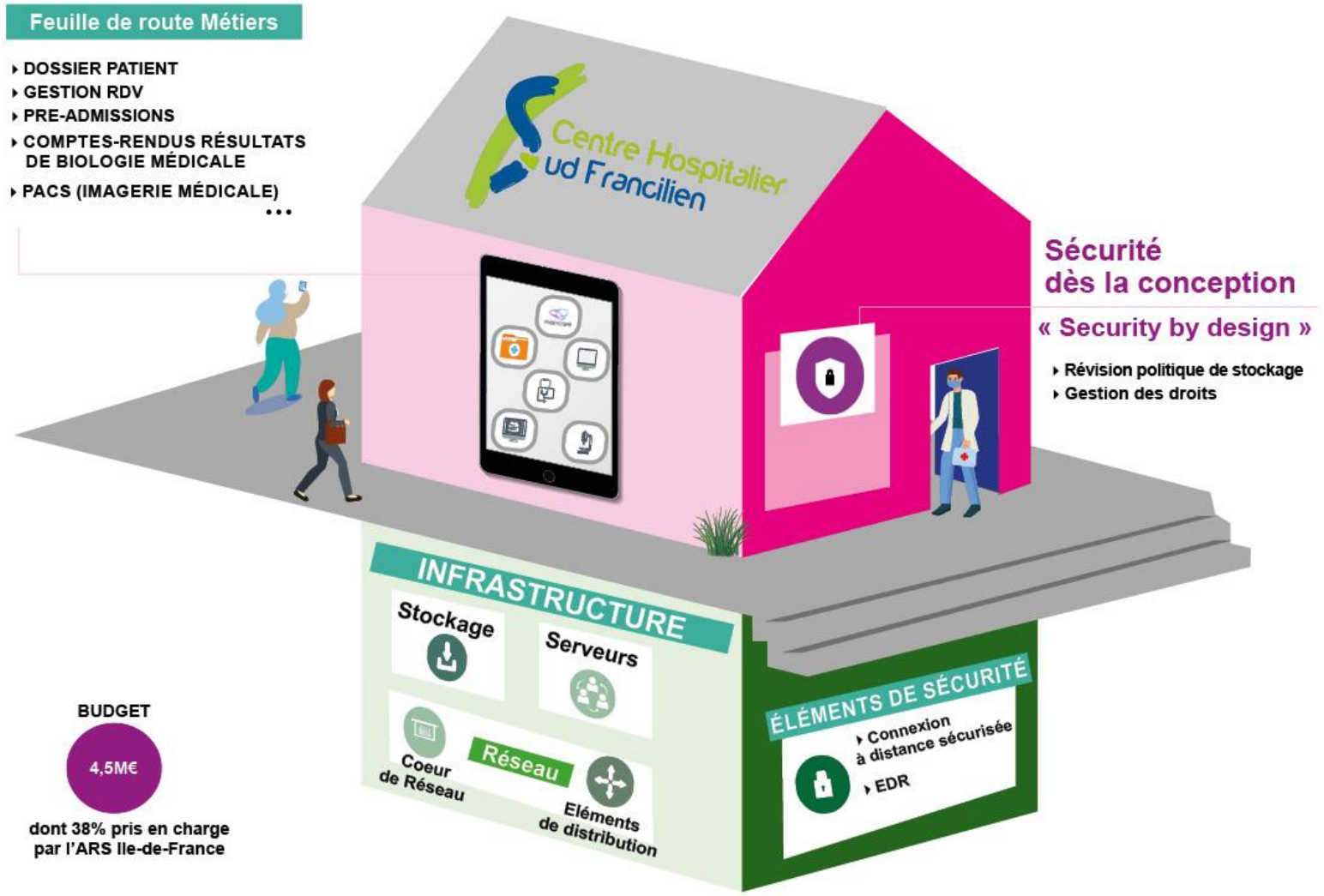


Planning déploiement MAINCARE IC



Planning déploiement Digitalisation du parcours patient





Centre Hospitalier Sud Francilien

Au total, nous retiendrons de cette crise majeure **les 3 « A »** suivants :

- Admiration des personnels hospitaliers dotés d'une capacité de résilience exceptionnelle

- Adaptation fulgurante et continue des organisations

- Avenir prometteur des services rendus à la population.