CENTRE HOSPITALIER D'ARLES

Hôpitaux de Provence
Groupement Hospitalier et Universitaire des Bouches-du-Rhône

Un laboratoire dans la tourmente
Cyber attaque au CH Arles

11/2023

Dr DAUMAS Martine

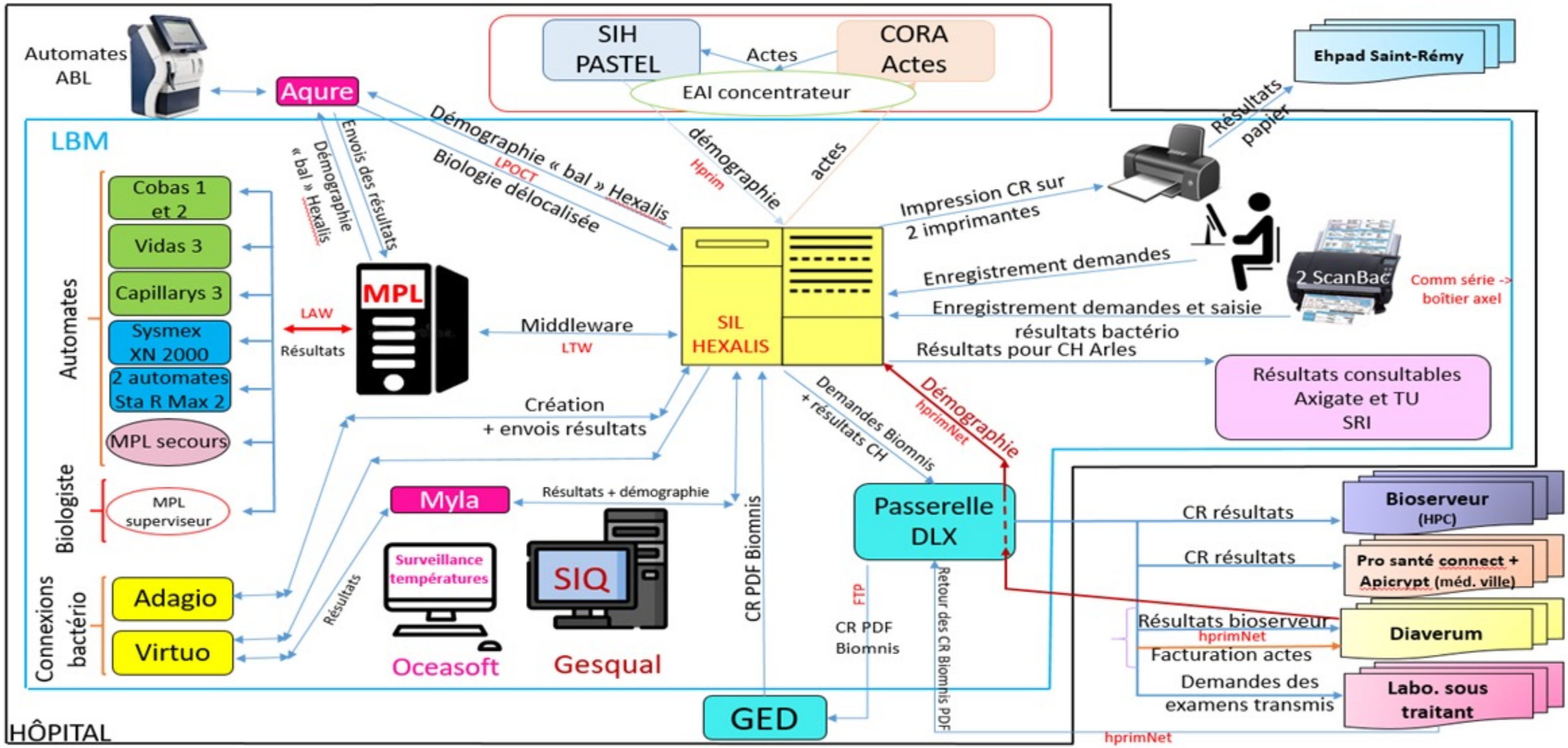
CENTRE HOSPITALIER D'ARLES

Etablissement partie du GHT « Hôpitaux de Provence » qui regroupe la totalité des 13 établissements publics de santé des Bouches-du-Rhône autour de l'Assistance Publique - Hôpitaux de Marseille (APHM)

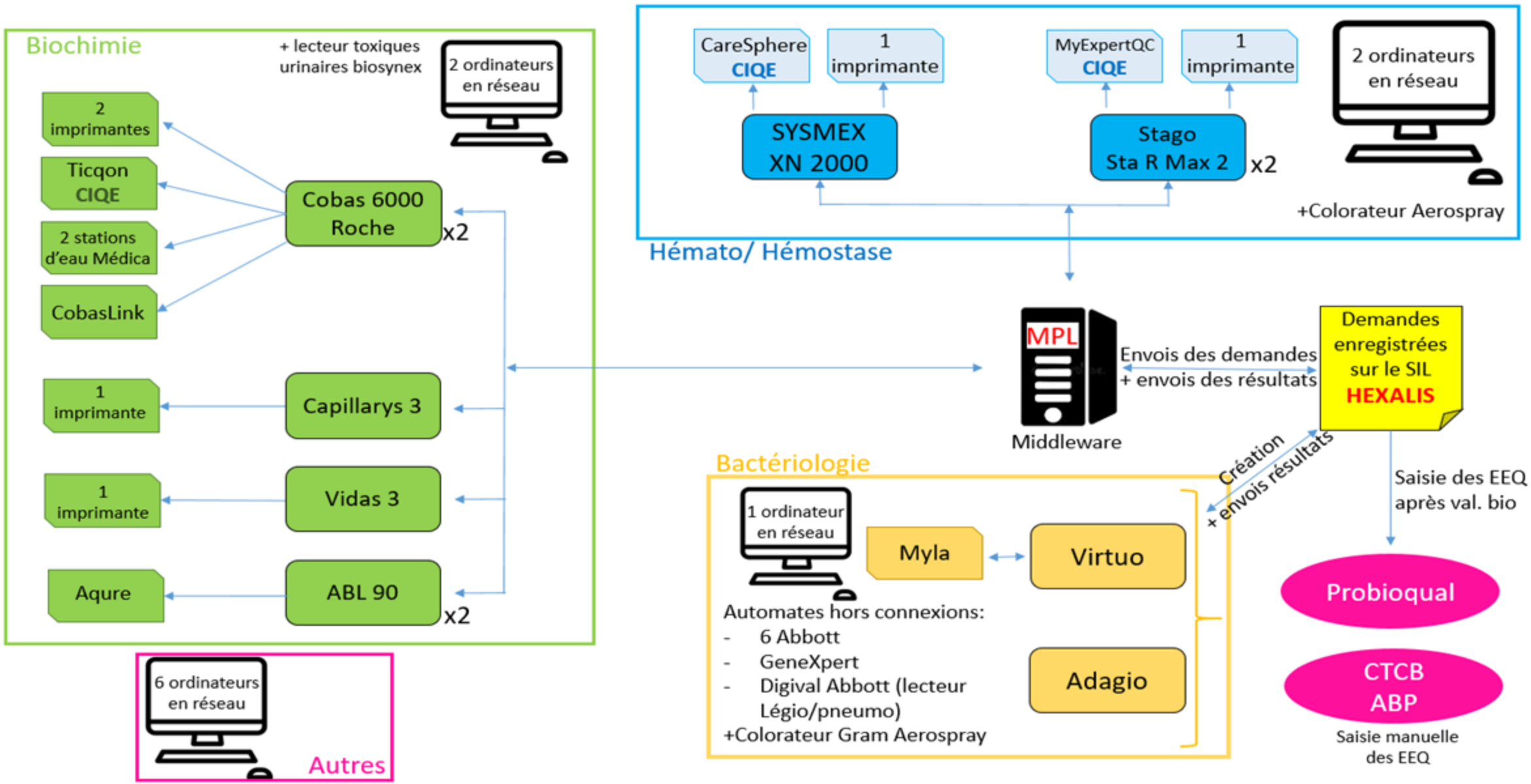
Centre hospitalier de référence pour le Pays d'Arles

- ✓ **Activité diversifiée:** Médecine, Chirurgie, Obstétrique, Réanimation, Psychiatrie (CS, Moyen séjour, CATTP, CMP...) , SSR Personnes âgées, EHPAD, CAMPS, IFSI-IFAS, SAU, SMUR...
- ✓ **Plateau technique complet:** Laboratoire, Imagerie (IRM, TDM, échographes, conventionnel), bloc opératoire (7 salles)
- ✓ **Quelques chiffres**
  - Activité: 17.000 séjours MCO, 126.000 venues externes, 6.700 interventions chirurgicales, 900 naissances, 38.000 passages au SAU
  - Budget: 102 millions d'euros de dépenses d'exploitation
  - Effectifs: 1 260 équivalents temps plein médicaux et non médicaux

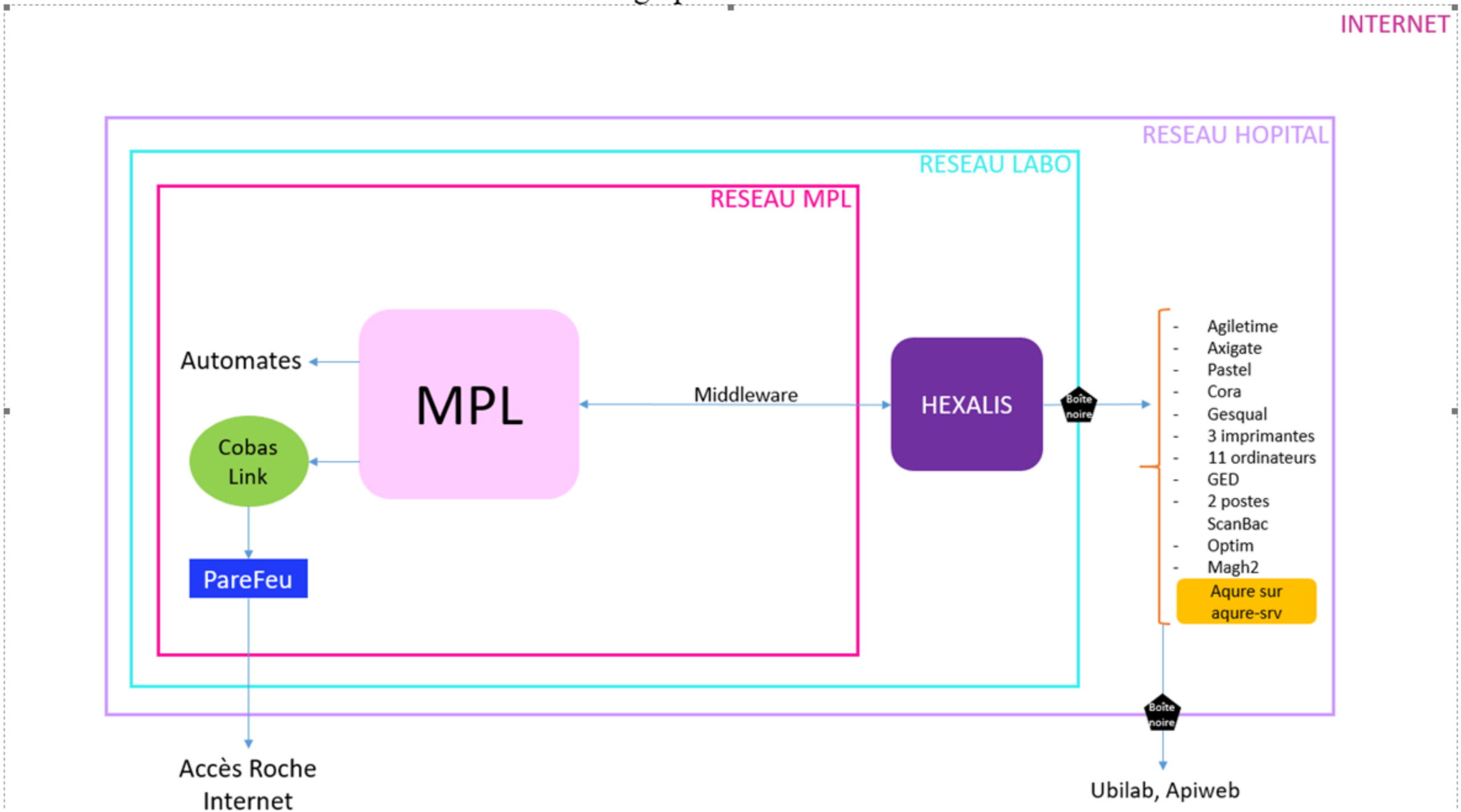
Cartographie générale des flux informatique du laboratoire du CH ARLES



Cartographie par secteur du laboratoire :



Cartographie des réseaux :



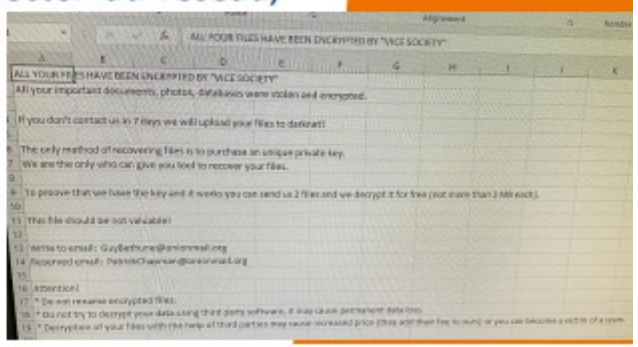
Cyberattaque subie par le CH d'Arles en plein été

Circonstances de la découverte

- ✓ Nuit de Dimanche au Lundi 2 août (3 h du matin) : appel de l'astreinte informatique suite à une panne du logiciel du laboratoire
- ✓ Connexion à distance avec difficultés permettant de constater des anomalies → déplacement sur site à 4h → constat que plusieurs fichiers sont renommés *« !!! ALL YOUR FILES ARE ENCRYPTED!!! Zeppelin »*

Actions immédiates

- ✓ Respect de la procédure en isolant immédiatement le SIH pour limiter la propagation (cœur de réseau, internet, sauvegarde, liens fibres vers les autres établissements et structures…) puis Alerte (administrateur de garde à 5 h et DSI à 7 h)
- ✓ Consigne donnée aux clients internes en raison d'un *« incident sur l'infrastructure informatique »* → ne pas utiliser les postes de travail, les déconnecter du réseau, passer en « mode dégradé » pour les logiciels métiers
- ✓ En l'absence de messagerie et d'outils de diffusion sur les postes, dès 8h, la communication s'appuie sur 2 canaux conjointement via les techniciens informatiques et les cadres supérieurs de santé (Appels téléphoniques + Passages physiques)



Cyber attaque

Arrêt de tous les ordinateurs de l’hôpital
de tous les accès à internet ,des sauvegardes , fax

On est au mois d’aout + épidémie COVID

Procédure dégradée : PAPIER +CRAYON

Préanalytique

Demande d'analyse sur feuille scanbac

- Nom + prénom +date de naissance : écriture manuscrite
- Nom du service : écriture manuscrite
- **Type de tube à prélever** est noté sur les feuilles de demande scanbac

Demande analyses expédiées (Biomnis etc) : Type de tube à prélever

- Accès via les téléphones personnels
- Feuille de demande papier uniquement

► **Renforcement des équipes** (pas évident au mois d'aout)

Analytique

Plus d’acces au middle ware (MPL)

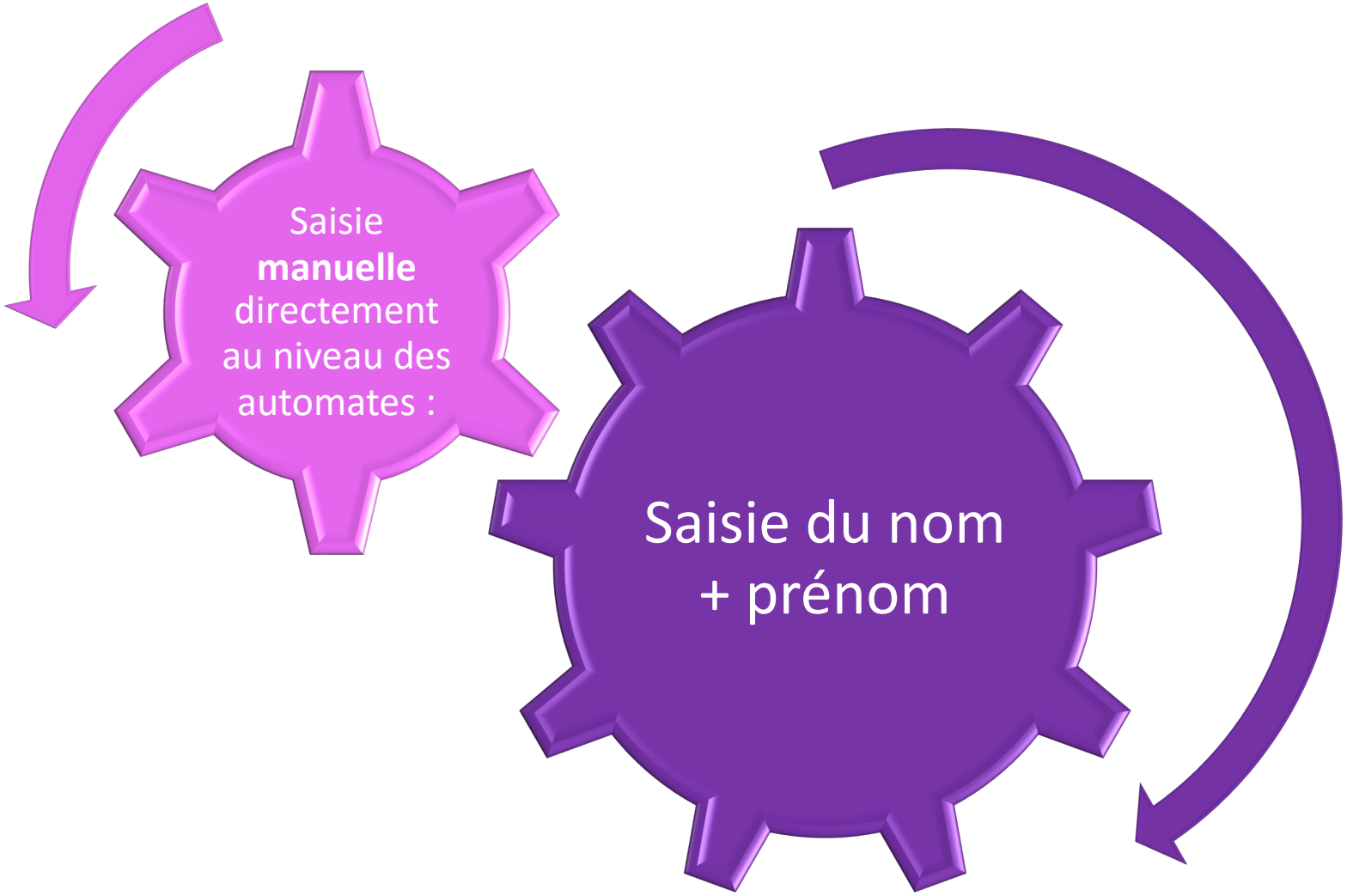
Reste uniquement les automates

Vérification par le service informatique des ordinateurs des automates

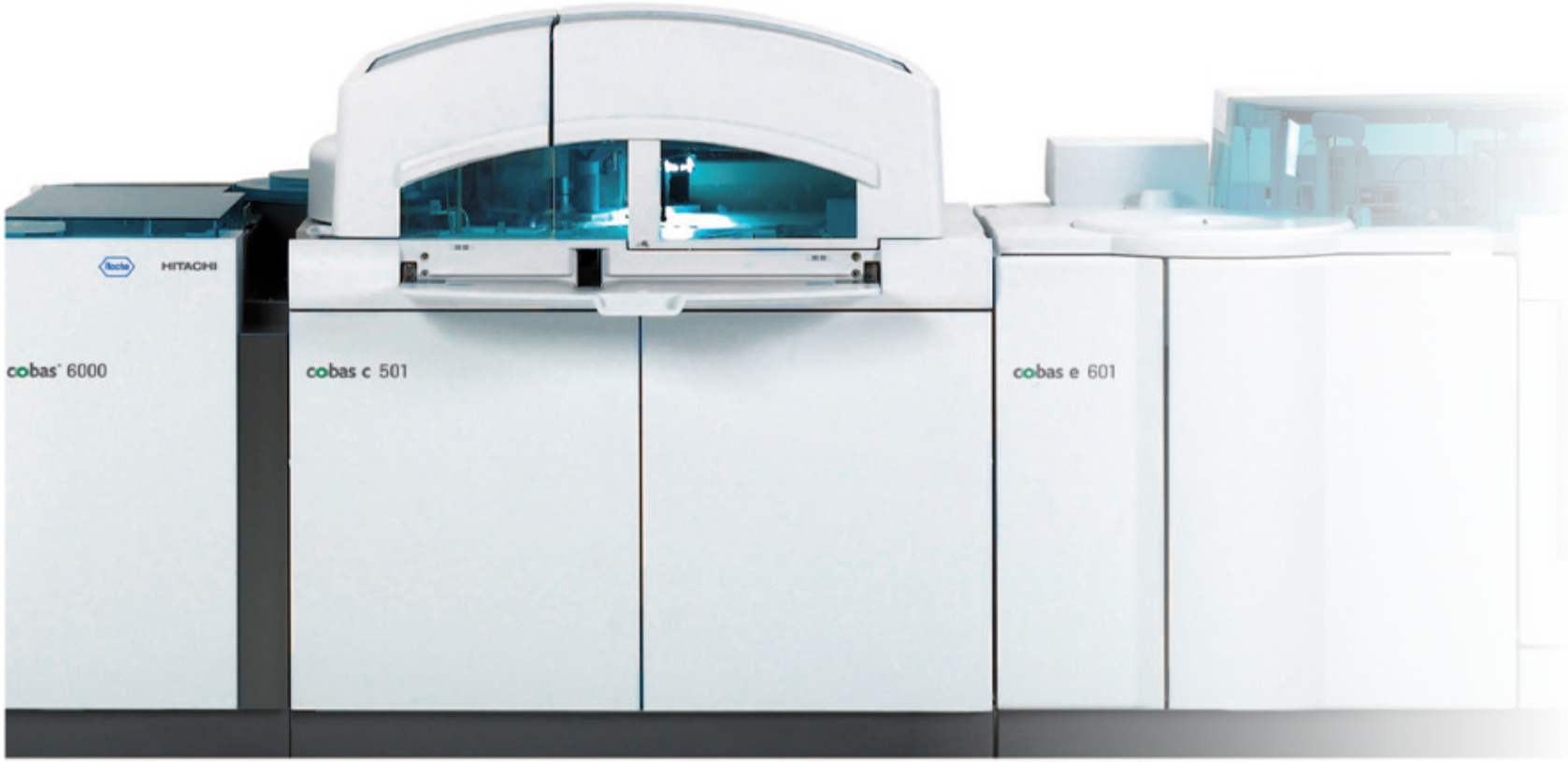
Seul le capillarys est touché :

- Désactivation du pare feu (conflit)
- Clef de sauvegarde laissé sur l’ordinateur (vigilance +++)

Enregistrement des patients et des analyses



Cobas 6000



→ Saisie du nom + prénom + **heure de prélèvement** +++ (quand plusieurs demandes dans la journée au niveau de l'automate)

→ Inscription sur feuille de demande du *n° portoir et position*

Les feuilles de demandes sont classées par ordre de passage des tubes.

Roche

Contrôle interne de qualité

On n’a plus de valeurs, de bornes car gérés par le MPL

Pas d’accès à nos valeurs des périodes probatoires car saisies dans notre GED

Pas d’accès au CIQ externalisé (ex tiqcon)

Demande aux différents fournisseurs des valeurs des contrôles

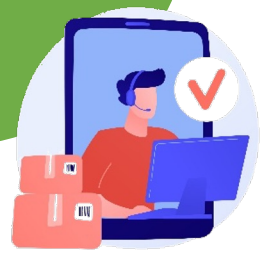
► **Sauvegarde sur un disque dur externe des données sensibles tels résultats périodes probatoires**

Calibration

Sur Cobas :

Téléchargement des valeurs des calibrateurs

appel ROCHE



Validation technique

Plus de règles d’expertise

Plus de valeurs de références

Les valeurs de références par analyses sont dans notre GED:

► **Récupération au niveau des feuilles de résultats pour des externes**

Impressions

En double des résultats à partir des automates

problèmes avec les imprimantes qui sont en réseau ++++

donc **Imprimante connectée en direct avec consommable**

1 feuille pour le service et 1 à garder au laboratoire

On note le nom du service ou UF sur la feuille de résultat

On vérifie la concordance entre les demandes d'analyses (feuille scan bac) et les résultats

Les feuilles sont rangées par service sur une table

Postanalytique

Feuilles de résultats des automates

Nom de certaines analyses :

différents ex

Unités :

conversion effectuée par le MPL !!!! connaitre facteur de conversion entre g/l et mmol/l (ex :alcool) / avertir les médecins ,donner les facteurs de conversions

Urines :

diurèse calcul pour résultat sur 24h00

Valeurs de références :

aucune

Antériorités :

aucune

Validation biologique

signature manuelle puis mis dans un trieur

- Pas de valeurs de références
- Pas d’antériorité
- Attention aux critères d’alerte

Distribution des résultats papiers

→ par le service intérieur

→ par la coursière du laboratoire

→ les services viennent chercher leur résultat (après midi + nuit)

→ Pour nos correspondants externes : seul le vieux fax du laboratoire peut être utilisé car pas en réseau (il a servi pour tout l'hôpital!!!)

- Avoir en version papier les procédures dégradées de bases
- Penser à tous les calculs automatiques effectués par le MPL
- Sauvegarder sur un disque dur externe les différentes données nécessaires ,sauvegarde mensuelle de nos documents qualité
- Feuille de rendu de résultats pour procédures manuelles(recherche de toxiques urinaires ,sang dans les selles ……)
- Avertir l'ensemble de la communauté médicale des différents problèmes : diffusion notes papier
- Photocopieuse pas en réseau

A penser :

- Gestion des stocks : manuelle
- Commandes : liste des fournisseurs

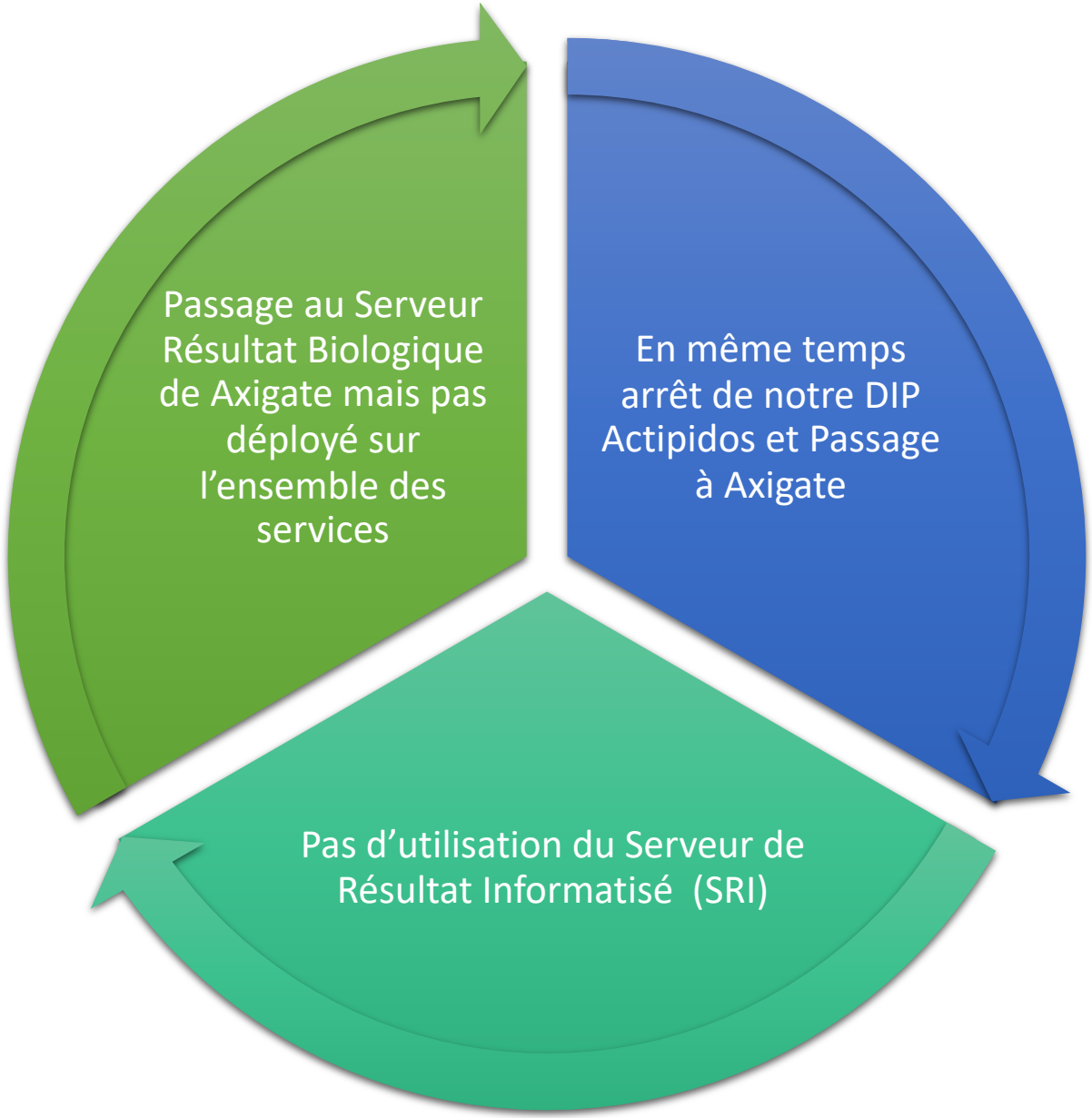
  papier + fax
- Blanchisserie : tenues
- Planning : maquette manuelle, paie manuelle
- Gestion des températures (Oceanosoft) pas en réseau au labo
- Biologie délocalisée

Pour les autres secteurs

Secteur Hématologie /Hémostase	• Hématologie (sysmex) : Planche imprimée avec n° de travail
Secteur Bactériologie	• Feuille de rendu de résultats papier avec carbone • Identification api web avec ordinateur portable • Antibiogramme : à la règle
Secteur Sérologie	• Cobas + Vidas idem

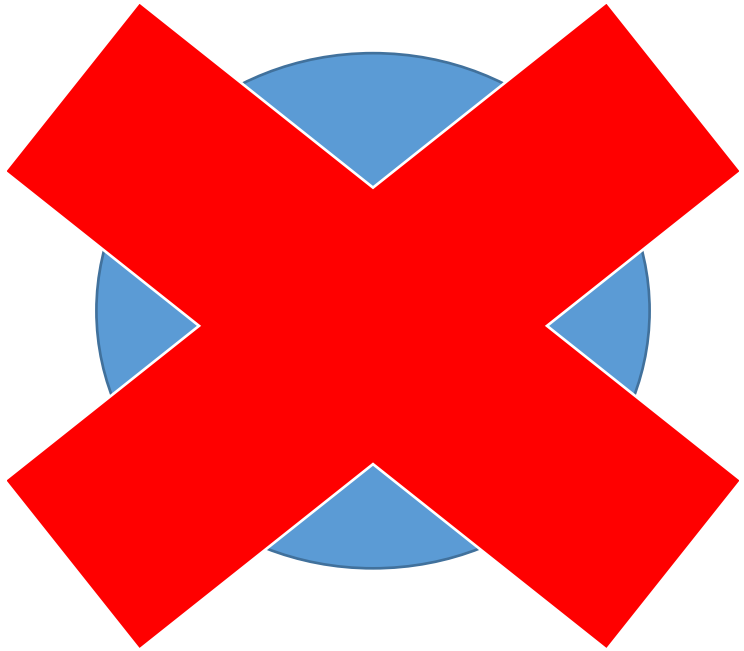
Et ensuite :

- Service des payes
- SIH (PASTEL) remis en service
- Les autres services : radiologie, pharmacie, stérilisation…
- SIL (Hexalis)+Middle ware (MPL) : novembre 2021
- Connection des appareils de Biochimie et Hématologie/Hemostase: novembre 2021 après contact avec les éditeurs de chaque automate
- pas pour les appareils des gaz du sang(Radiometer +Aqure)° et Capillarys (Sebia)
- Bactériologie : de Mars 2022 à juin 2022


Passage au Serveur Résultat Biologique de Axigate mais pas déployé sur l'ensemble des services
En même temps arrêt de notre DIP Actipidos et Passage à Axigate
Pas d'utilisation du Serveur de Résultat Informatisé (SRI)

Laboratoire

Bulles de sécurité



Conclusion

Vive l’informatique quand ça marche !!!!!!!