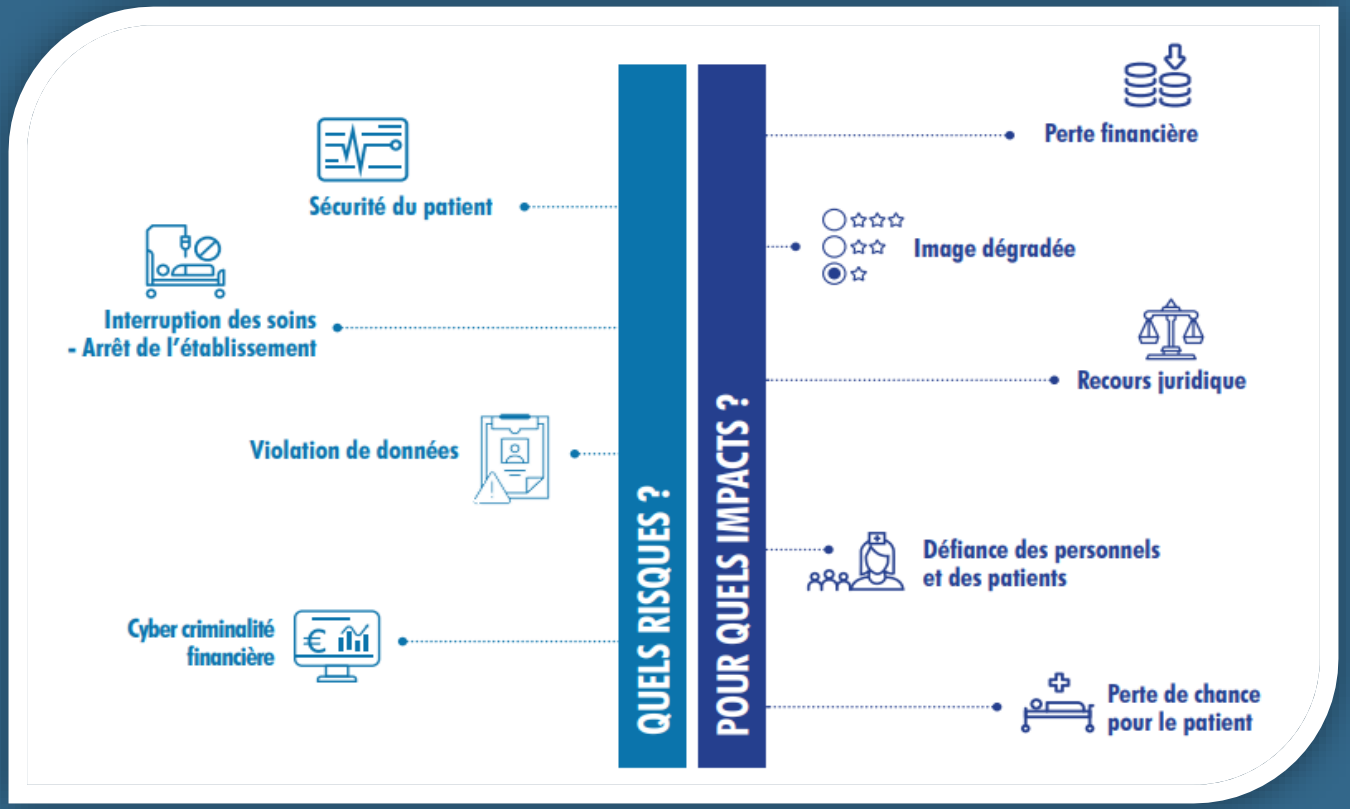
21ème Colloque ABCPH
Vendredi 30 septembre 2022

Cyberattaques dans les hôpitaux et impact sur les PUI

Patrick Nicolazo – DSI CH Auxerre - GHT UnYon

Cybersécurité

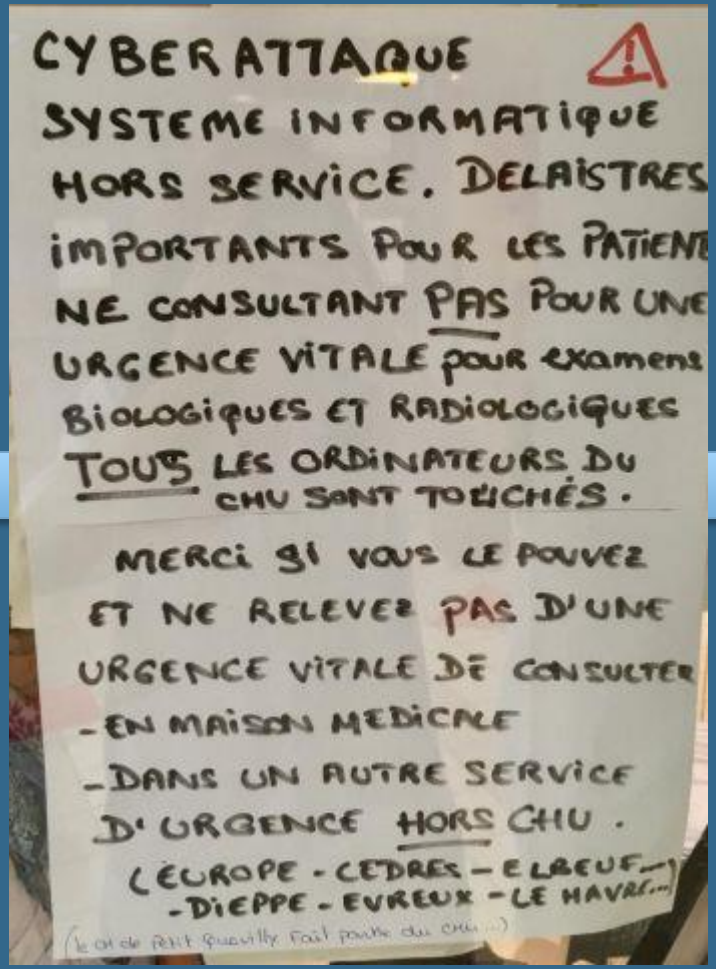
Les enjeux



Cybersécurité

Contexte
Rappel des faits

15/11/2019
CHU de Rouen



Cybersécurité

CHU Rouen

cyberattaque de grande ampleur, par le rançongiciel CLOP

Majorité des applications indisponibles paralysant l'ensemble des services du CHU

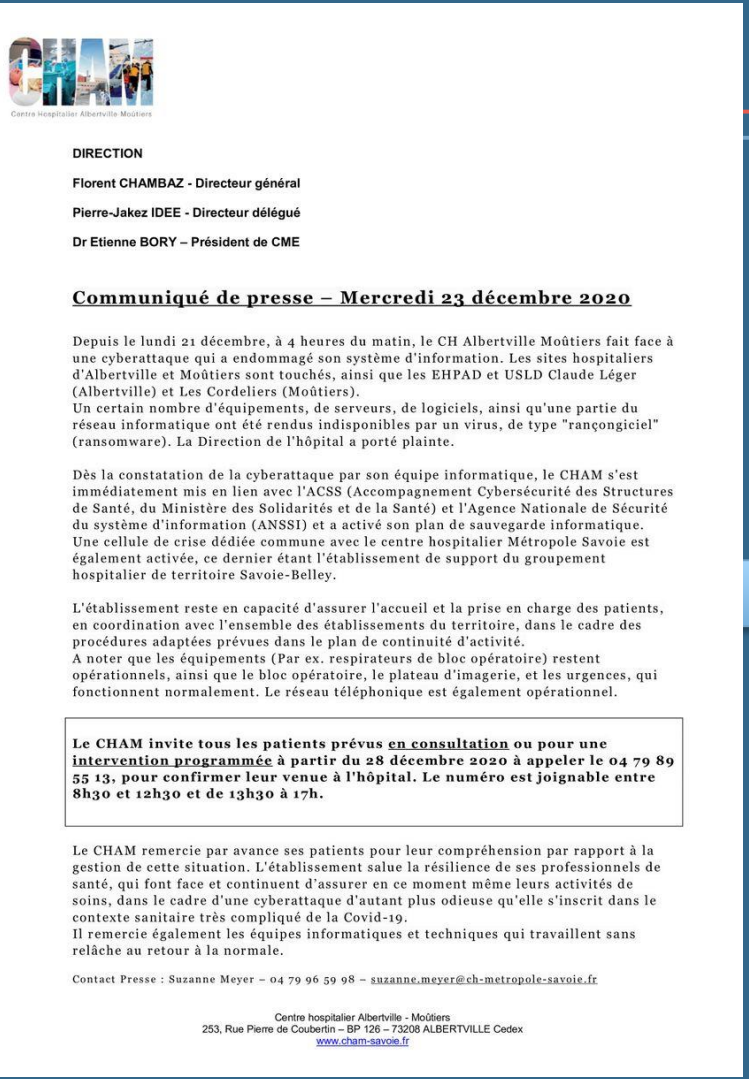
Transfert des patients dans d'autres ES et report des interventions programmées

Cybersécurité

CH d'Albertville-Moutiers

21/12/2020
CH d'Albertville-Moutiers

15/11/2019
CHU de Rouen



Centre Hospitalier Albertville Moûtiers

DIRECTION

Florent CHAMBAZ - Directeur général

Pierre-Jakez IDEE - Directeur délégué

Dr Etienne BORY – Président de CME

Communiqué de presse – Mercredi 23 décembre 2020

Depuis le lundi 21 décembre, à 4 heures du matin, le CH Albertville Moûtiers fait face à une cyberattaque qui a endommagé son système d'information. Les sites hospitaliers d'Albertville et Moûtiers sont touchés, ainsi que les EHPAD et USLD Claude Léger (Albertville) et Les Cordeliers (Moûtiers).
Un certain nombre d'équipements, de serveurs, de logiciels, ainsi qu'une partie du réseau informatique ont été rendus indisponibles par un virus, de type "rançongiciel" (ransomware). La Direction de l'hôpital a porté plainte.

Dès la constatation de la cyberattaque par son équipe informatique, le CHAM s'est immédiatement mis en lien avec l'ACSS (Accompagnement Cybersécurité des Structures de Santé, du Ministère des Solidarités et de la Santé) et l'Agence Nationale de Sécurité du système d'information (ANSSI) et a activé son plan de sauvegarde informatique.
Une cellule de crise dédiée commune avec le centre hospitalier Métropole Savoie est également activée, ce dernier étant l'établissement de support du groupement hospitalier de territoire Savoie-Belley.

L'établissement reste en capacité d'assurer l'accueil et la prise en charge des patients, en coordination avec l'ensemble des établissements du territoire, dans le cadre des procédures adaptées prévues dans le plan de continuité d'activité.
A noter que les équipements (Par ex. respirateurs de bloc opératoire) restent opérationnels, ainsi que le bloc opératoire, le plateau d'imagerie, et les urgences, qui fonctionnent normalement. Le réseau téléphonique est également opérationnel.

Le CHAM invite tous les patients prévus en consultation ou pour une intervention programmée à partir du 28 décembre 2020 à appeler le 04 79 89 55 13, pour confirmer leur venue à l'hôpital. Le numéro est joignable entre 8h30 et 12h30 et de 13h30 à 17h.

Le CHAM remercie par avance ses patients pour leur compréhension par rapport à la gestion de cette situation. L'établissement salue la résilience de ses professionnels de santé, qui font face et continuent d'assurer en ce moment même leurs activités de soins, dans le cadre d'une cyberattaque d'autant plus odieuse qu'elle s'inscrit dans le contexte sanitaire très compliqué de la Covid-19.
Il remercie également les équipes informatiques et techniques qui travaillent sans relâche au retour à la normale.

Contact Presse : Suzanne Meyer – 04 79 96 59 98 – suzanne.meyer@ch-metropole-savoie.fr

Centre hospitalier Albertville - Moûtiers
253, Rue Pierre de Coubertin – BP 126 – 73208 ALBERTVILLE Cedex
www.cham-savoie.fr

Cybersécurité

CH d 'Albertville-Moutiers

Attaque par rançongiciel

Mode dégradé pendant plusieurs semaines

Arrêt de la **quasi-totalité** du SI

Cybersécurité

CH de Dax

21/12/2020
CH d'Albertville-Moutiers

15/11/2019
CHU de Rouen

09/02/2021
CH de Dax

Cybersécurité

CH de Dax

Attaque particulièrement massive par rançongiciel

Chiffrement des données de l'établissement

Arrêt de tous les appareils électroniques (Téléphonies, ordinateurs, …)

Cybersécurité

Centre Hospitalier Sud Francilien

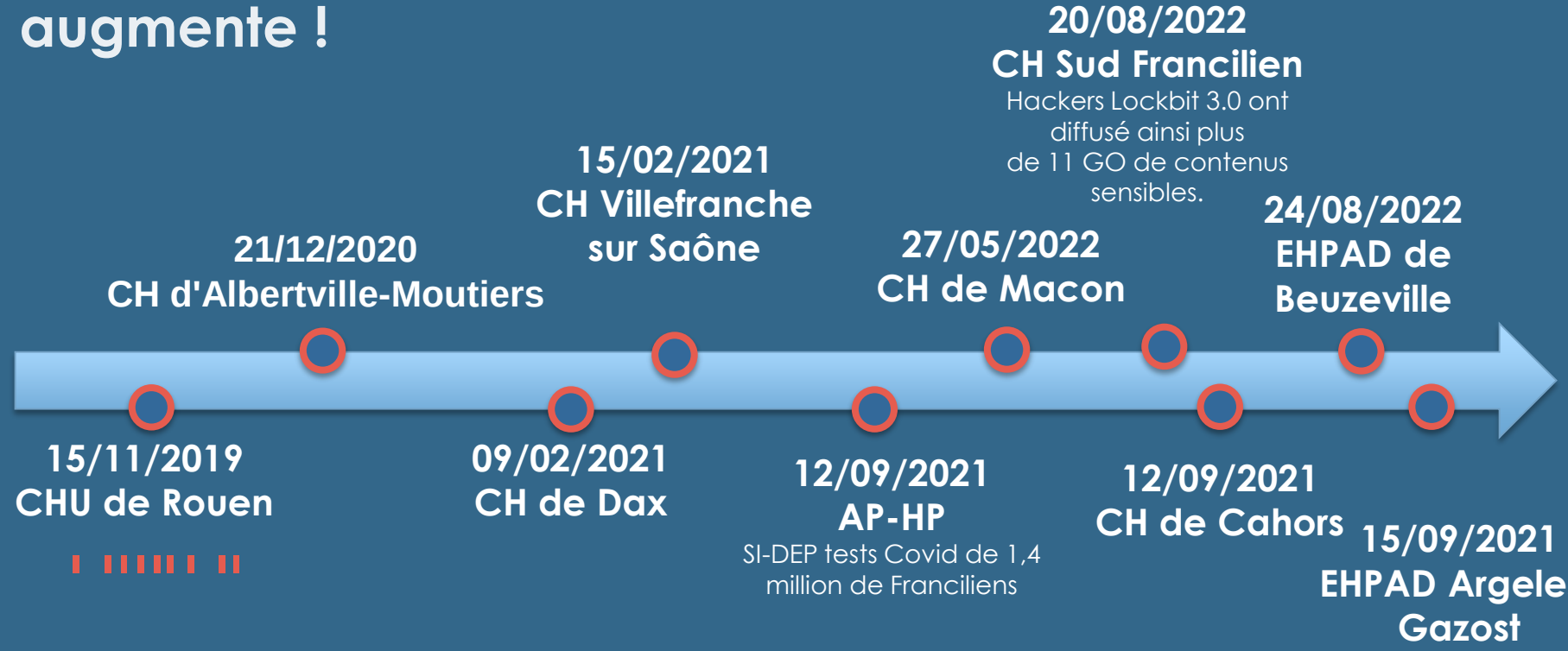
Tous les logiciels métiers de l'hôpital, les systèmes de stockage (notamment d'imagerie médicale) et le système d'information ayant trait aux admissions de la patientèle sont pour l'instant inaccessibles.

Malgré l'attaque qui le paralyse, le Centre hospitalier Sud francilien, à Corbeil-Essonnes, continue de fonctionner, mais comme s'il était revenu à un âge de pierre numérique.

« On est revenu au mode papier »

Cybersécurité

La liste s'allonge, la fréquence augmente !



Cybersécurité

Etat de la menace

Une forte dépendance aux risques systémiques :

- La dépendance aux fournisseurs d'hébergement (exemple : incident OVH), aux fournisseurs de logiciels en mode SaaS ;
- L'exposition à certaines vulnérabilités systémiques (LOG4J, VEEAM, …) qui touchent une part significative de l'écosystème numérique ;
- La dépendance aux accès distants (CHSF) ;
- La dépendance à la messagerie électronique !!! Un des plus important vecteur de phishing, mails avec pièces jointes contenant un crytovirus par exemple

Cybersécurité

Système d'Information d'une PUI, un agencement complexe

Les activités des PUI sont gérées au sein d'un système d'information complexe, outillé par de nombreux logiciels, qui adressent et nécessitent des compétences métiers hospitalières multiples :
Pharmaciens, médecins, biologistes, infirmiers, logisticiens, acheteurs, industriels (cf. les automates)) … informaticiens ☺

Ce SI traite de nombreuses données concernant à la fois les patients, mais aussi les références médicamenteuses, les interactions biologiques, les informations relatives à la qualité, les conditionnements et les péremptions, la gestion de stock, les données financières.

Système d'Information en PUI

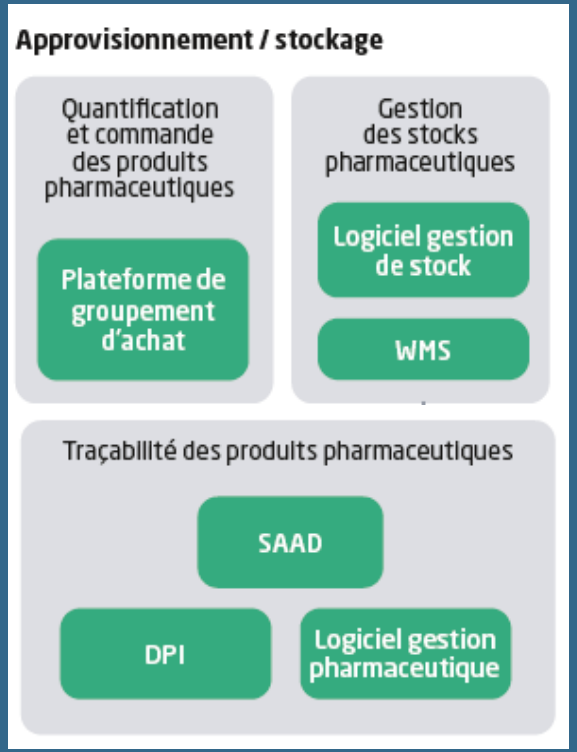
Exemple d'urbanisation du circuit du médicament

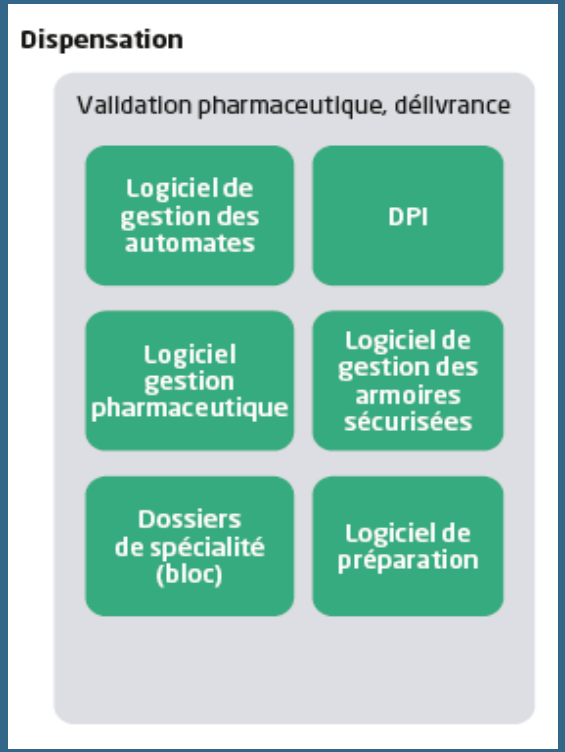
I – Système d'Information Hospitalier - Vision fonctionnelle et applicative

Sources ANAP

Système d'Information en PUI

II - Fonctions métier - Vision fonctionnelle et applicative





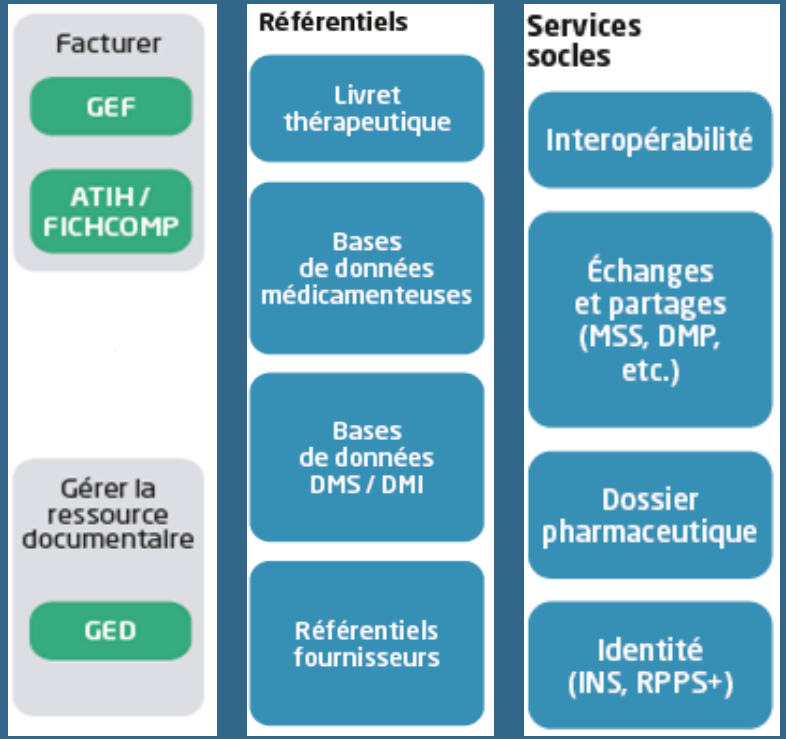
WMS : Warehouse Management System
SAAD : Système d'acquisition automatique des données
DPI : Dossier Patient Informatisé

Sources ANAP

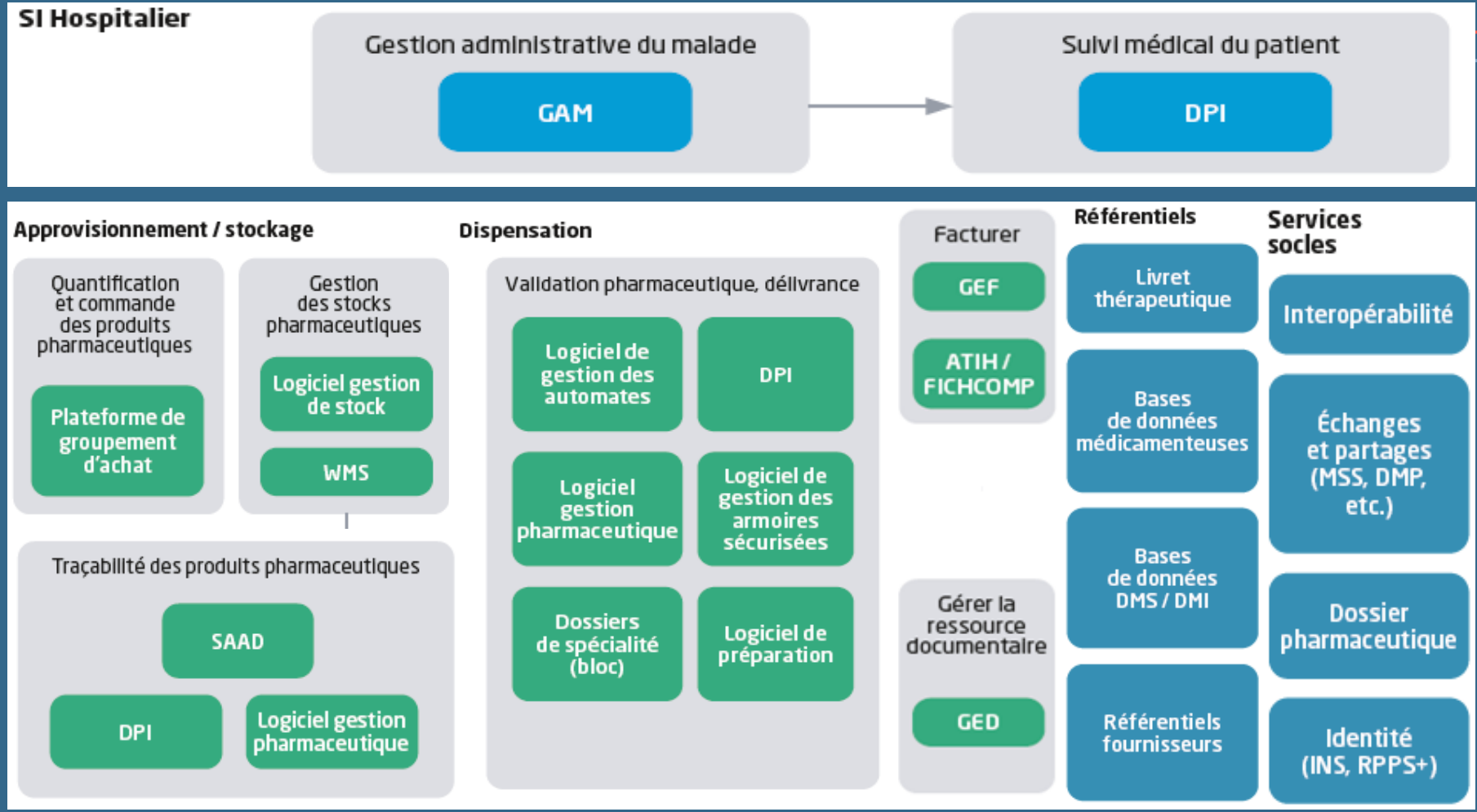
Système d'Information en PUI

III - Fonctions supports, référentiels et services socles

GEF : Gestion Economique et Financière
GAM : Gestion Administrative du Malade
GED : Gestion Electronique des Documents
MSS : Messagerie Sécurisé de Santé
DMP : Dossier Médical Partagé
INS : Identifiant National de Santé
RPPS+ : Portail RPPS+ outil indispensable à la sécurisation du parcours de soins

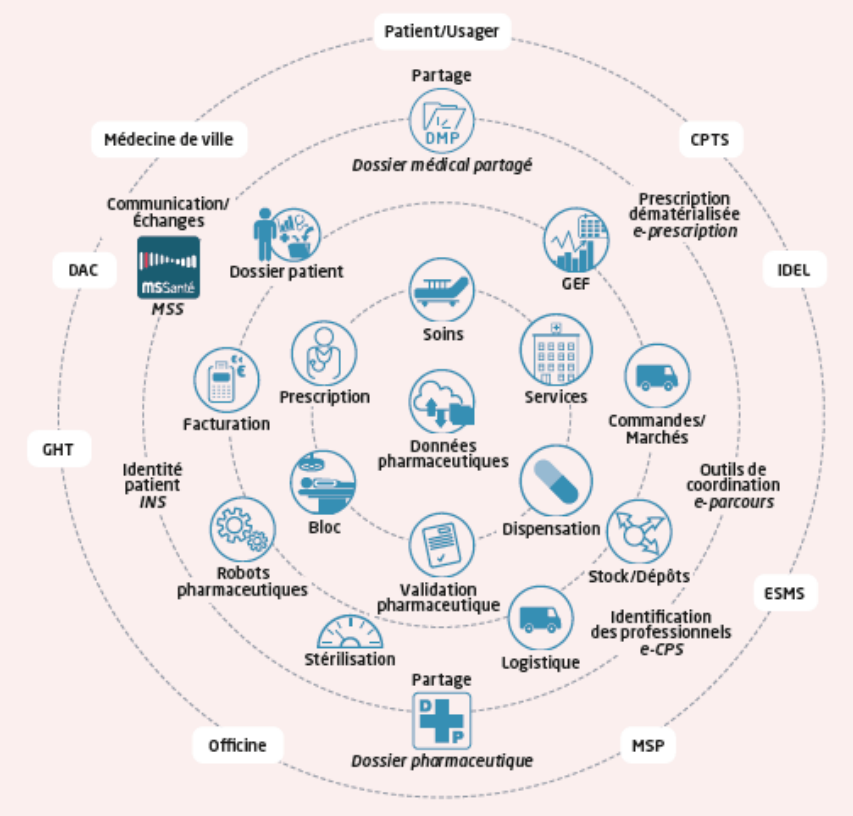


Sources ANAP



Sources ANAP

Système d'Information en PUI



Les circuits des produits de santé (médicaments, DMS, DMI, MDS) dans nos établissements sont fortement interconnectés entre eux, mais aussi aux autres processus, de l'admission à la sortie du patient en passant par toutes les étapes de la prise en charge (médecine, chirurgie, médico-technique).

Plus largement, les données pharmaceutiques sont au cœur de la prise en charge globale du patient et doivent être accessibles à toutes les étapes du parcours. En cela, le système d'information de la pharmacie s'étend bien au-delà de l'établissement au travers des données échangées par l'intermédiaire des outils numériques socles : Dossier pharmaceutique (DP), Dossier médical partagé (DMP)…

Sources ANAP

Merci pour votre attention