

Enjeux éthiques de la protection des données en e-Santé

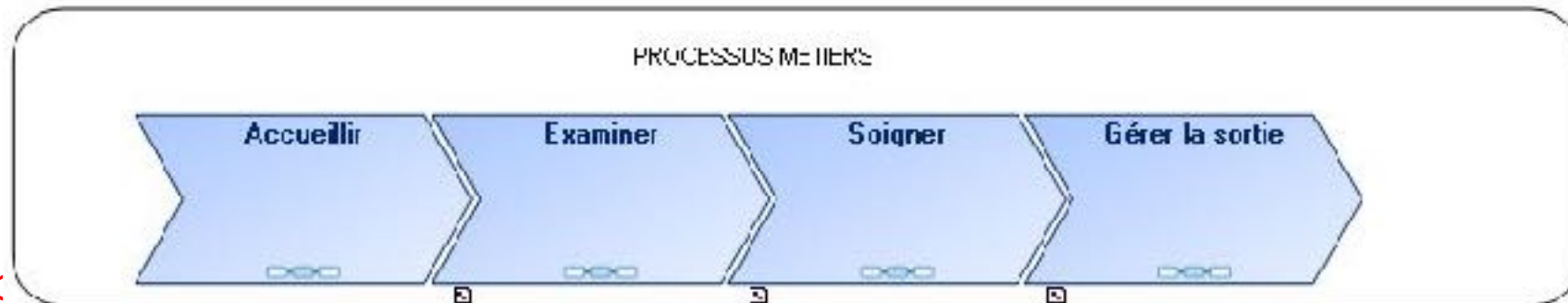


Saber ALOUI

Docteur de l'Ecole des Mines de Paris
Directeur du Système d'Information
Groupe Hospitalier Bretagne Sud

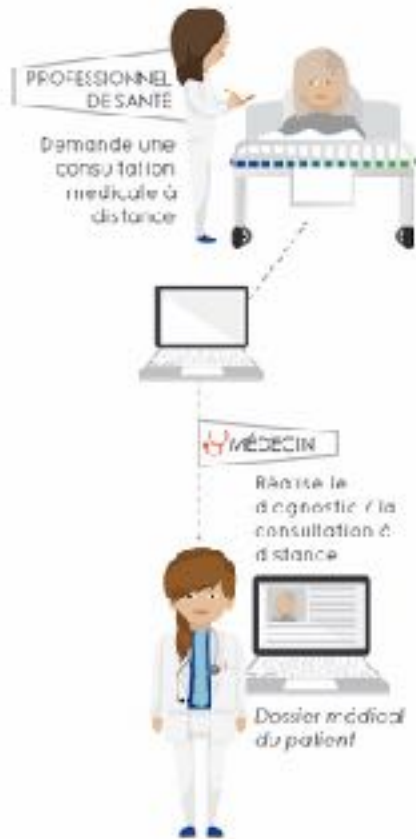
Les fondamentaux...définitions

- Un SI : **réseau complexe de relations structurées** où interviennent **hommes, machines et procédures** qui a pour but d'engendrer des flux ordonnés d'informations pertinentes provenant de différentes sources et destinées à servir de base aux décisions [Angot, 2006].
- *La SSI est l'ensemble des **moyens techniques, organisationnels, juridiques et humains** nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information. (Wikipédia, 2017)*



- Le SI a **a soulève des questions que les professionnels doivent appréhender pour une décision éclairée.**

Téléconsultation



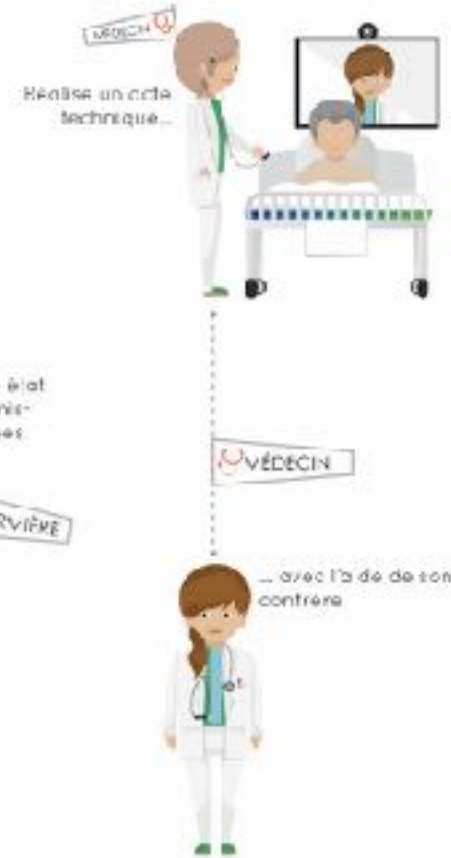
Téléexpertise



Télesurveillance



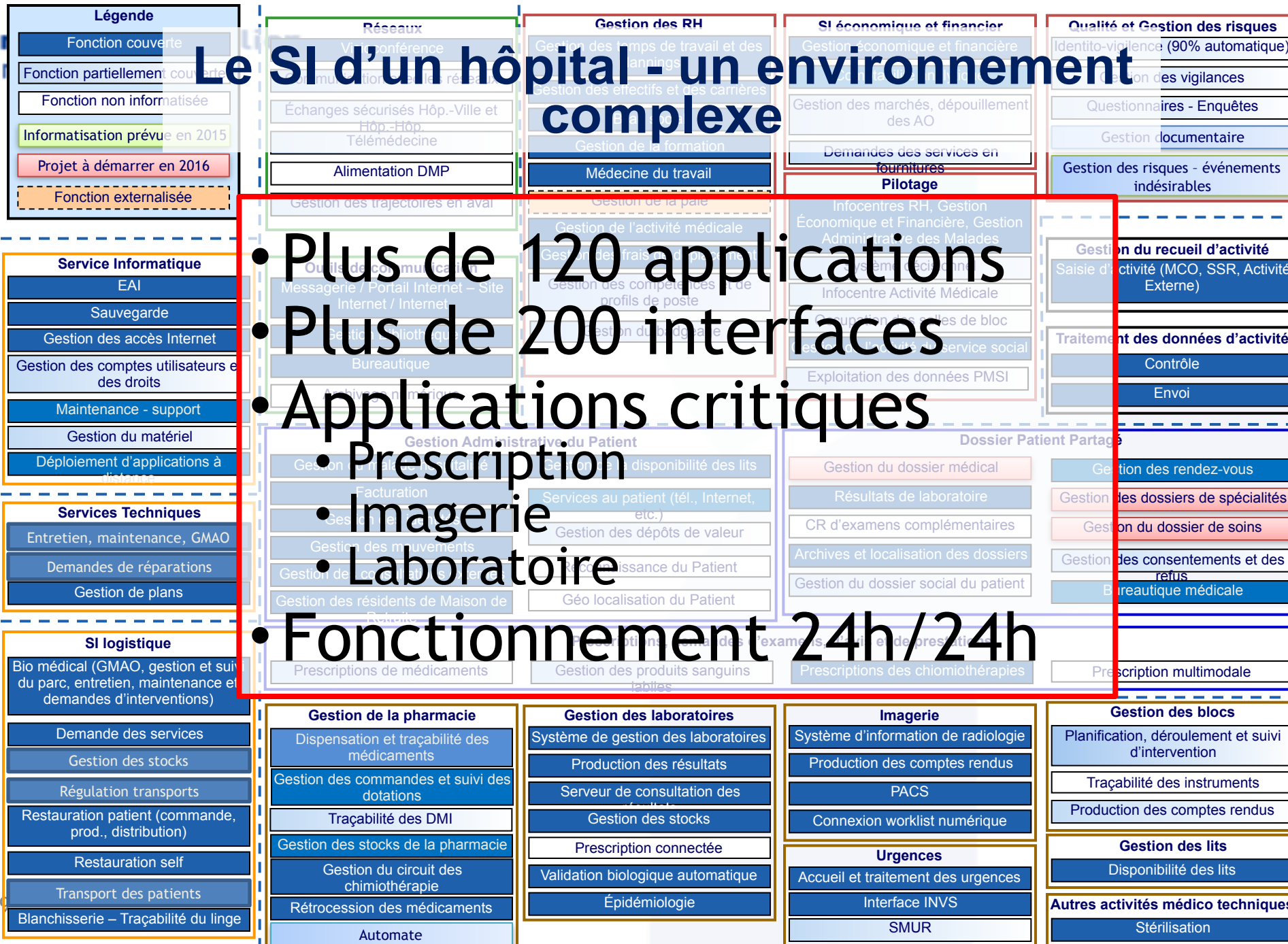
Téléassistance



Régulation médicale

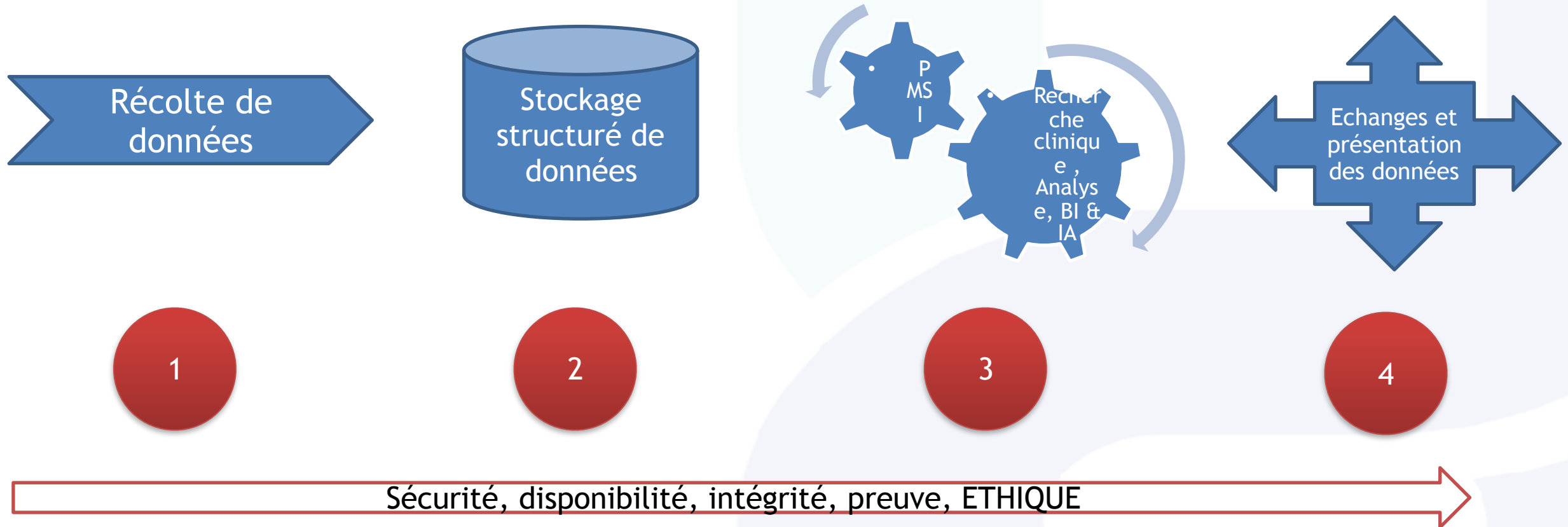


Le SI d'un hôpital - un environnement complexe



- Plus de 120 applications
- Plus de 200 interfaces
- Applications critiques
 - Prescription
 - Imagerie
 - Laboratoire
- Fonctionnement 24h/24h

Les différentes étapes



Processus itératif et non linéaire, chaque étape permettant d'améliorer la précédente et cela en continu

La récolte des données



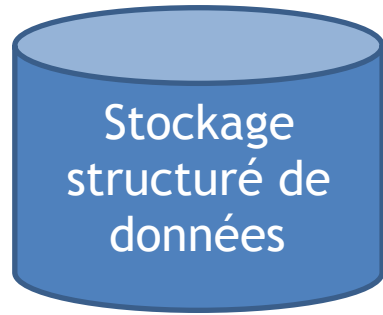
Récolte de
données



1

- Données disparates, multi-sources, multicanal :
 - Interne : saisie par les professionnels (IDE, médecins, assistantes sociales, etc.) , CR de biologie, images, CR imagerie, appareils biomédicaux, etc.
 - Partenaires externes (cellule de numérisation, mails sécurisées, parcours patient, GHT, Réseaux, libéraux, etc.)
 - Ne se limite pas aux données de santé (GEF, RH, etc.)
- Sécurité/protection du SI :
 - Questions autour de la typologie de saisie (données structurées ou pas) et également sur la qualité des données ?
 - Qui saisit quoi ? Quel matrice de droits ?

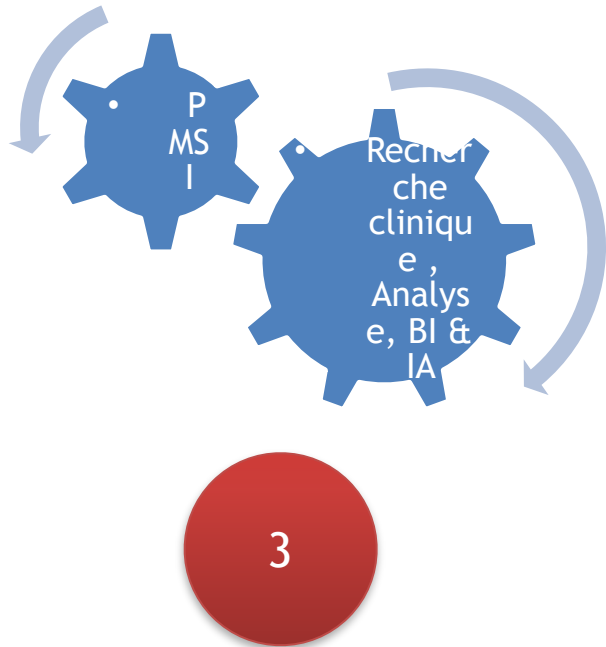
Les entrepôts de données



2

- Stockage structuré des données :
 - Physique : Dimensionnement de l'architecture de stockage avec explosion de la volumétrie. Quel type d'hébergement interne / externe / Hybride?
 - Logique : quels logiciels mettre en œuvre ? Données de production Vs Données pour analyse? Quel type d'archivage?
 - Organisation : quelle organisation mettre en œuvre pour gérer ce (s) stockage(s) (niveau local, GHT, Régional, national)? Quel gouvernance pour ces entrepôts de données?

L'analyse/Exploitation

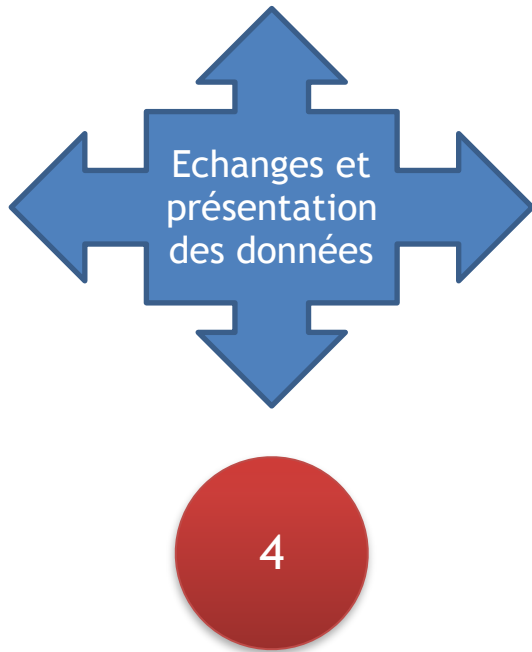


- Beaucoup d'acteurs sur le marché : de la Start Up à la multinationale, appétit des laboratoires pharmaceutiques pour notamment les données de cancérologie. **La donnée de santé a une valeur marchande.**
- Besoins de données bien structurées pour faire tourner les algorithmes → on revient au point 1 sur la récolte de données.
- La capacité accrue de traitement des données en masse permet d'espérer :
 - Des gains en efficacité pour le parcours de soins et les organisations
 - Une amélioration de la sécurité sanitaire
 - Le développement d'une médecine personnalisée, notamment grâce à la confrontation de bases de données « populationnelles » en recherche clinique

Enjeux

- Pour les établissements de santé, l'enjeu primordial est de conserver la maîtrise de « ses » données :
 - Maîtrise de la qualité des données : condition *sine qua non* pour une exploitation valide
 - Maîtrise architecturale : rassembler des données éparses, parfois cloisonnées et de nature différente au sein d'un « entrepôt » exploitable
 - Maîtrise des outils d'analyse : qu'il s'agisse d'améliorer son organisation, la qualité des soins dispensés ou de nourrir sa stratégie au sein du territoire
 - Maîtrise de l'intégrité et de la sécurité des données

Echange et restitution des données



- Comment présenter ces données une fois disponibles et vérifiées?
- Comment échanger ces informations avec l'extérieur de la structure?
- Quelle sécurité? Traçabilité? Fiabilité? Une fois la donnée sortie, comment être sûr de son « parcours »?
- L'aspect médico-légal dans le cadre de l'usage de l'IA...comment analyser la décision suggérée par une machine *a posteriori*?

En transverse - Sécurité

- La concentration et les échanges de données posent la question de la sécurité et de la protection des données :
 - Risque de fuite « involontaire » : perte ou piratage
 - Risque de fuite « volontaire » : en cas de d'exploitation indue (excessive et non prévue) de données transmises contractuellement
- La production de données et leur transmission pour exploitation en dehors des établissements posent la question du dessaisissement et de la perte de contrôle des données
- La mauvaise qualité des données pose la question des biais d'analyse et du risque de conclusions erronées (à l'image du sang contaminé)
- Fournir de la « preuve », des rapports formatés sur qui a accéder à quoi (dans le cadre de la certification des comptes, de la mise en œuvre des certifications HDS, Cofrac, etc.)

Sécurité, disponibilité, intégrité, preuve, éthique

Cadre réglementaire

Loi informatique et libertés

- Toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclarée auprès du correspondant informatique et libertés (CIL) de l'établissement

RGPD - Principales dispositions :

- Donner aux citoyens davantage de contrôle sur leurs données privées
- Droit à l'oubli
- Principes de « protection des données dès la conception » et de « sécurité par défaut »
- Notifications en cas de fuite de données (CNIL)
- Nomination obligatoire d'un délégué à la protection des données (Data Protection Officer)
- Concerne les organismes privés aussi bien que publics
- Applicable à partir du **25 mai 2018**
- En cas de non-respect : sanctions financières allant jusqu'à **4 % du chiffre d'affaires mondial annuel d'une entreprise ou 20 millions d'euros**

Cadre réglementaire

- **Code pénal et code de déontologie médicale**

L'utilisateur est soumis au secret médical qui consiste en l'obligation de discrétion et de respect de la personne d'autrui. Le secret médical est défini dans le code de déontologie médicale comme suit :

- article 4, alinéa 1 « le secret professionnel, institué dans l'intérêt des malades, s'impose à tout médecin dans les conditions établies par la loi » ;
- article 72, alinéa 1 « **le médecin doit veiller à ce que les personnes qui l'assistent dans son exercice soient instruites de leurs obligations en matière de secret professionnel et s'y conforment** » ;
- article 73, alinéa 1 « le médecin doit protéger contre toute indiscretion les documents médicaux concernant les personnes qu'il a soignées ou examinées, **quels que soient le contenu et le support de ces documents** ».

Le code pénal, de par son article 226-13 étend ces obligations à « toute personne qui, dans son état ou sa profession, ou en raison d'une fonction ou d'une mission temporaire, a reçu des informations auxquelles la loi accorde le caractère de secret ».

Exemples d'incidents et leurs conséquences

- **Une indisponibilité** des données de santé à un moment crucial (intervention chirurgicale, administration de médicaments, consultation,...) peut entraîner la répétition d'un acte, une imprécision, des retards ou des erreurs dans les diagnostics ou les soins, et se traduire par une perte de chance pour le patient par méconnaissance de son contexte et de ses historiques médicaux [DGOS, 2013]
- **Un défaut de confidentialité** d'un document de santé, comme la divulgation à la famille, aux services d'une société d'assurance ou d'un employeur d'un résultat positif de dépistage de tumeur maligne, pourrait porter préjudice au patient, puis par voie de conséquence, au professionnel de santé et/ou au responsable de la perte de confidentialité. [DGOS, 2013]
- **L'absence de preuve sur l'auteur** d'un document médical (ex. ordonnance) dont la lecture aboutit à une erreur médicale, ne permet pas d'imputer l'erreur à la personne réellement en cause et de trouver la source des erreurs. [DGOS, 2013]

