

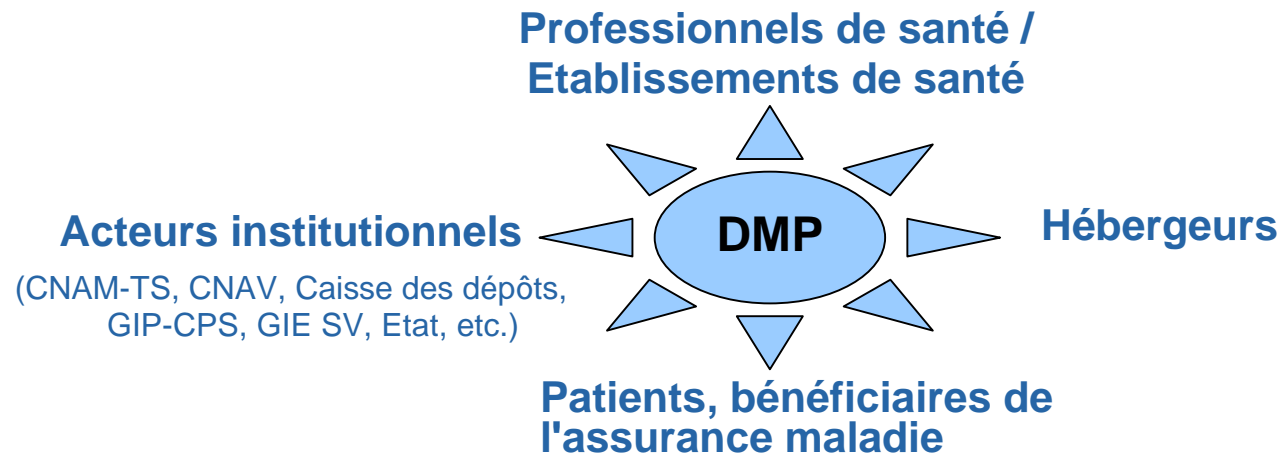
HIT 2007

Prise en compte de la sécurité dans la conception du DMP

Mai 2007

jean-francois.parguet@sante.gouv.fr

Le Dossier Médical Personnel est un système au coeur des échanges de données de santé.



Il participe, à travers la logique de “DMP compatibilité” à l’amélioration de l’interopérabilité des données de santé et à la multiplication des échanges

A ce titre la prise en compte de la sécurité doit être exemplaire

La « sécurité » d'un système complexe n'est pas un état objectif, observable par des effets mesurables, mais plutôt une perception :

- **La sécurité ne peut pas se décréter mais doit être reconnue par les acteurs du système** : patients et professionnels de santé (PS) avec des perceptions, des priorités différentes (par exemple confidentialité et intégrité)
- **Communication et sensibilisation sont partie intégrante de la sécurité** et permettent de maîtriser les éventuels écarts entre : ***Sécurité ressentie versus sécurité mesurée***
- **La confiance que l'on accorde à un système numérique dépend de l'idée que l'on se fait de « sa sécurité »**

La sécurité constitue donc, de fait, un facteur d'adhésion au Dossier Médical Personnel

Les principaux enjeux de sécurité du Dossier Médical Personnel sont :

- Le **respect du cadre légal et réglementaire**
- La **qualité et l'assurance des données**, sur la base des critères “classiques” de leur disponibilité, intégrité, confidentialité et traçabilité
- La **confiance des acteurs du système DMP**, avec une “orientation” :
 - confidentialité pour le patient
 - intégrité pour le PS
 - Mais également la traçabilité des accès et l'imputabilité des actions réalisées

Le cadre légal et réglementaire du DMP (non exhaustif)

- Cadre légal
 - Textes issus du code la sécurité sociale
 - Les articles L.161-36-1 à L.161-36-4 prévoyant la mise en oeuvre du DMP
 - Textes issus du Code de la santé publique
 - L'article L.1110-4 pose les conditions pour garantir la confidentialité des informations de santé
 - L'article L.1111-8 fixe les conditions du traitement informatique et de l'hébergement de données de santé à caractère personnel

- 4 décrets d'application nécessaires pour mettre en oeuvre le DMP
(détail du contenu de chacun présenté en annexes)
 - Le décret « Confidentialité », en application de l'article L.1110-4 du Code de la santé publique. Ce décret est paru le 15 mai 2007
(respect de référentiels – définis dans des arrêtés à venir - pour la conservation et l'échange de données médicales / utilisation obligatoire de la CPS pour tous les PS avec un délai de 3 ans pour les ES)
 - Le décret « hébergeurs », pris en application de l'article L.1111-8 du Code de la santé publique. Ce décret est paru le 6 janvier 2006
(conditions d'obtention de l'agrément, délivré par le ministre, pour l'hébergement des données de santé – suspension de deux ans sauf dans le cas du DMP)
 - Le décret Identifiant, pris en application de l'article L.1111-8-1 du Code de la santé publique
(création d'un identifiant de santé unique, distinct du NIR, pour chaque patient)
 - Le décret DMP pris en application de l'article L.161-36-4 du Code de la sécurité sociale
(modalités de gestion du DMP et liens avec le Dossier Pharmaceutique)

- Des arrêtés

Sous l'angle de la maîtrise de ses données par le patient :

- Le patient gère les autorisations d'accès des PS à son propre DMP
- Les données de santé sont stockées dans un « coffre-fort » numérique (rôle des hébergeurs) et les autorisations d'accès sont strictement appliquées (rôle du portail)
- Les données sont protégées en confidentialité pendant leur stockage et lors des échanges
- Tout accès à un DMP donne lieu à une génération incontournable de traces - Le patient a accès aux traces relatives à son DMP

Sous l'angle du contrôle d'accès patient :

- Le patient accède à ses données grâce à une authentification forte (mot de passe à usage unique transmis par SMS ou mail et ultérieurement carte Vitale 2 avec code porteur)

Sous l'angle du PS

- L'authentification des PS est réalisée via un dispositif CPS
- Toute modification de donnée est imputable à un PS à travers un dispositifs de signature électronique - toute modification illégitime d'une donnée serait soit impossible soit détectée a posteriori
- L'identification des patients est réalisée par un dispositif national unique : IS Identifiant de Santé

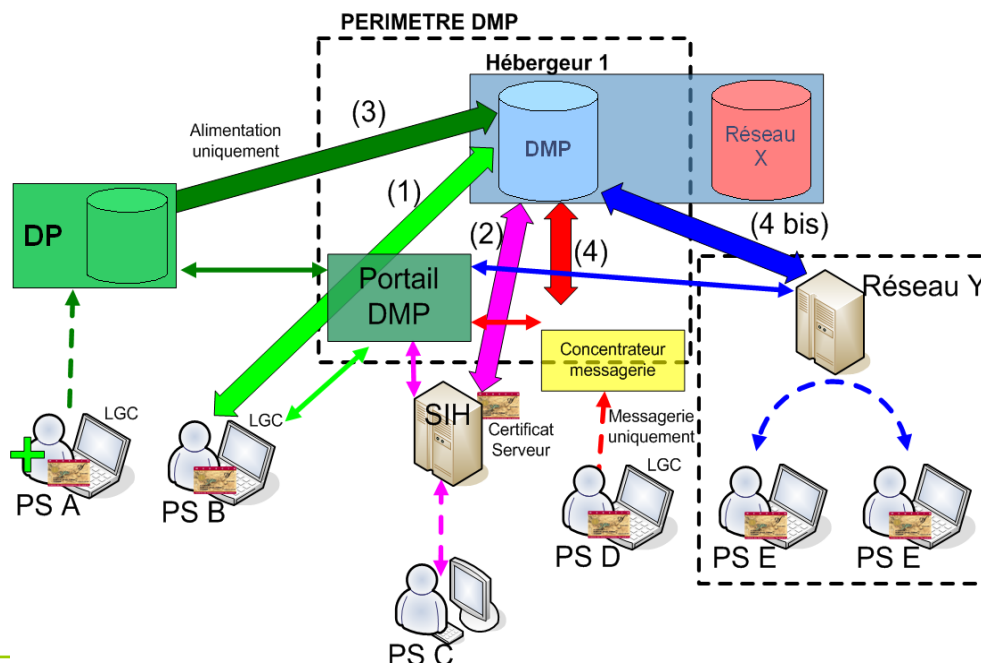
La prise en compte de la réalité opérationnelle

La prise en compte des spécificités de l'environnement santé :

- Une hétérogénéité des modalités d'exercice et des contextes techniques
- Des exigences de sécurité qui se confrontent à la réalité opérationnelle

=> **Des trajectoires de mise en oeuvre avec des exigences immédiates et des modalités transitoires** :

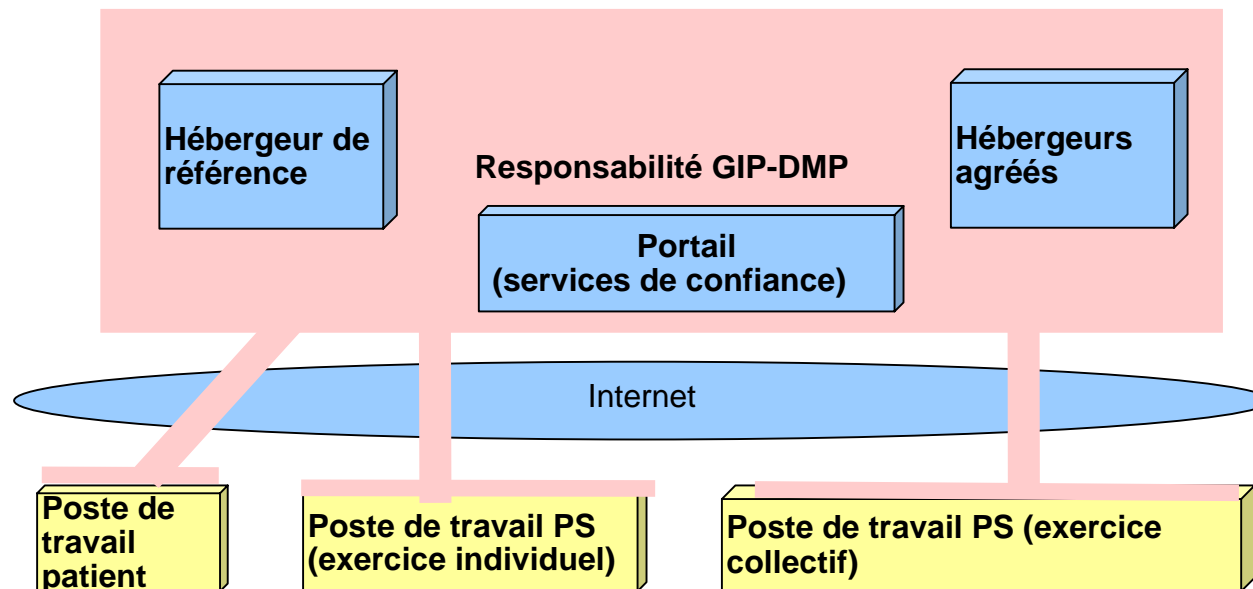
- Authentification des patients (OTP / Vitale 2)
- Authentification des PS (décret confidentialité)



Les domaines de responsabilité – problématique des PSSI

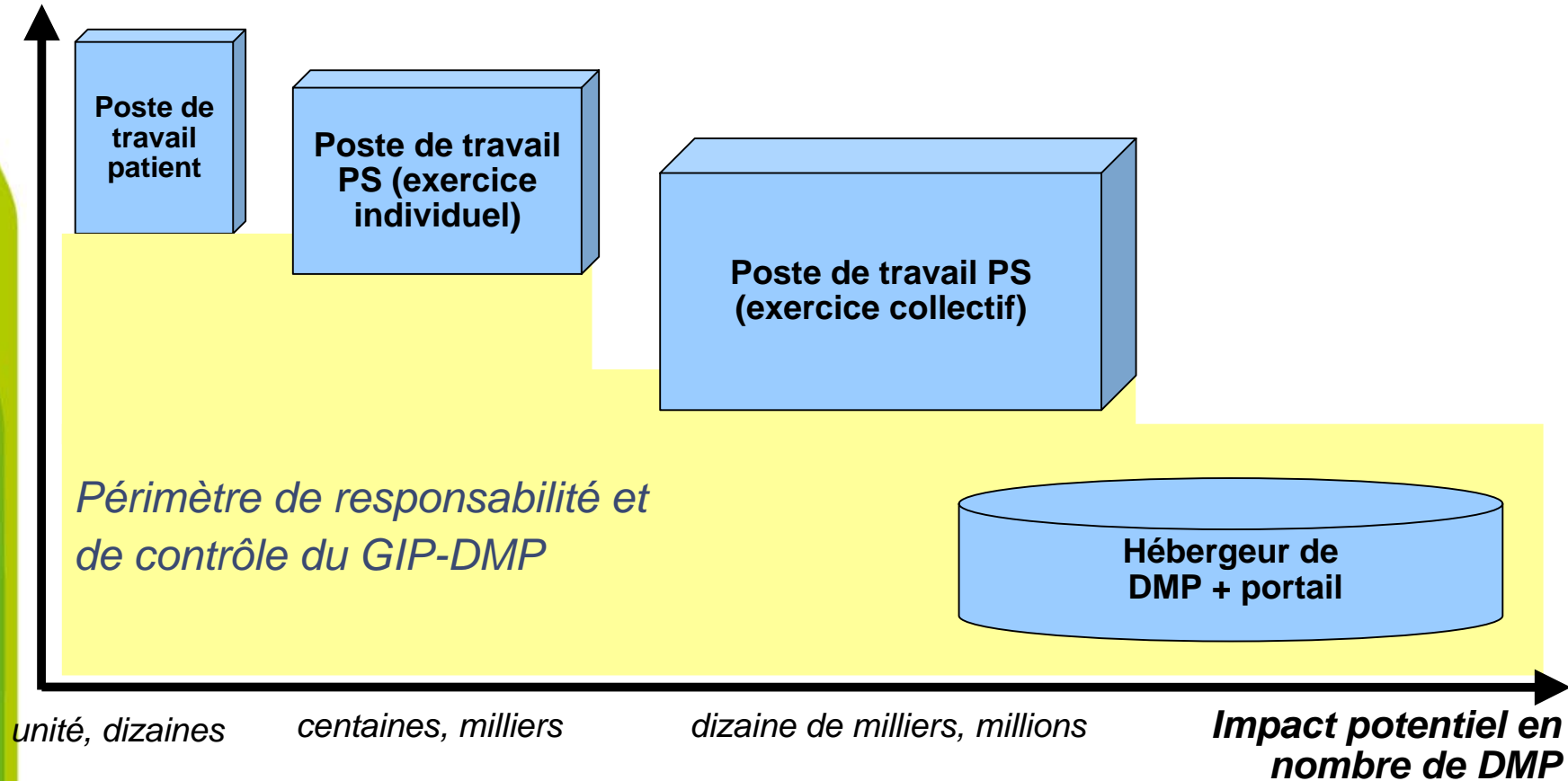
La sécurité des données doit être globale et pour cela différentes **politiques de sécurité doivent être articulées / urbanisées** suivant plusieurs axes :

- Périètre de validité : DMP, système remettant, SI extérieur au DMP
- Origine de validité : légale, réglementaire, conventionnelle
- Légitimité sur le périmètre



Les niveaux potentiels de vulnérabilité et d'impact pour le DMP

Niveau
potentiel de
vulnérabilité



Périmètres respectifs des domaines de responsabilité :

- Pour le système DMP
 - La PSSI du système DMP recouvre le domaine de responsabilité du DMP ainsi que les interfaces (*notions d'exigences au sens du cadre d'interopérabilité*) des systèmes souhaitant interagir avec lui
- Pour les systèmes interagissant avec le DMP
 - Postes patient
 - Absence de PSSI
 - Des “bonnes pratiques” sont disponibles (*CNIL, CERTA, DGME, ...*) / le moyen de les rappeler (mise à disposition en accès libre de bonnes pratiques en matière d'antivirus, d'anti spyware) est à l'étude
 - Systèmes PS
 - Multiplicité des situations en fonction des conditions et des situations d'exercice

Démarche retenue pour la sécurité du DMP (Phase BUILD)

Une démarche de sécurité “classique” (EBIOS) :

- Expression des besoins de sécurité sur la base :
 - des objectifs fonctionnels ;
 - de la stratégie et des principes de sécurité ;
 - des textes législatifs et réglementaires applicables ;
- Analyse des risques (étude des menaces et des vulnérabilités)
- Formalisation des objectifs de sécurité (sous forme de FEROS)

La sécurité étant consubstantielle des objectifs du DMP elle fait l'objet d'un volet majeur dans les cahiers des charges du Portail et de l'Hébergeur

Volet sécurité des cahiers des charges Portail et Hébergeur - principes

Principes ayant présidé à l'élaboration du volet sécurité des cahiers des charges des composants du système DMP (portail et hébergeurs) :

- Le fournisseur a le libre choix des solutions techniques, logicielles et organisationnelles dans la limite du strict respect des engagements attendus (exigences et contraintes)
- Le fournisseur s'engage formellement et explicitement sur des niveaux de disponibilité, d'intégrité, de confidentialité et d'auditabilité avec une liste exhaustive des risques non couverts
- Les risques non couverts doivent être clairement spécifiés afin d'être considérés comme des risques résiduels et pris en compte, à ce titre, par le GIP-DMP

Volet sécurité des cahiers des charges Portail et Hébergeur - les exigences de sécurité

Les exigences de sécurité du DMP s'expriment selon l'approche «DICA»:

- **La Disponibilité** (du service DMP et des données associées)
 - Une ouverture 7*7 24*24 et un taux de disponibilité de 99,9 % (8 heures d'arrêts cumulés par an) sont requis des différents composants
 - aucune indisponibilité totale ne doit durer plus de 4 heures consécutives
- **L'Intégrité** (données conservées et échangées de manière intègre)
 - Signature électronique des données déposées dans le DMP par leur auteur (contrôle, archivage, gestion de la preuve)
 - Chiffrement des échanges sur Internet
- **La Confidentialité des données et des traitements** (le respect des règles d'accès aux données et la traçabilité des accès)
 - Identification et authentification des acteurs (PS et patient) par le portail
 - Maîtrise des droits d'accès et des habilitations
 - Protection des données hébergées contre tout accès illégitime
- **L'Auditabilité** (capacité d'imputer les actes à leurs auteurs, constitution de preuves)
 - Elaboration et archivage de traces à valeur probante pour toutes les actions de dépôt et de consultation de données

Impact du DMP sur les données de santé :

- *Vos données de santé sont actuellement et seront toujours gérées (créées, stockées, échangées, ...) par des PS, indépendamment du DMP.*
- *Les impacts du DMP sur la confidentialité des données de santé sont :*
 - *la participation à la dématérialisation des données, et l'augmentation des échanges entre PS (le DMP est un facteur accélérateur de l'interopérabilité des données de santé),*
 - *la “concentration massive” de données chez un ou des hébergeurs (sous contrôle du GIP-DMP),*
 - *un nouvel acteur au niveau des échanges de données médicales : le patient.*

- Le DMP “est l'occasion” de généraliser une démarche de sécurité pour toutes les données de santé (à l'intérieur et à l'extérieur du périmètre DMP – en liaison avec le nouveau cadre réglementaire) :
 - pour les PS (en partenariat avec les autres acteurs institutionnels) :
 - sensibilisation, formation et « normalisation » des bonnes pratiques autour des données de santé (sur la base des nouveaux textes, décrets)
 - généralisation de la CPS à l'hôpital
 - amélioration de la sécurité des LPS (Logiciel de Professionnel de Santé) via homologation, agrément des LPS,
 - pour les patients :
 - sensibilisation au caractère important en terme de santé mais aussi de sécurité de l'accès à leurs données médicales ;
 - mise à disposition de guide de bonnes pratiques, anti-virus en ligne, anti-spyware en ligne.
- Le DMP permettra ainsi aux patients d'être acteurs de la sécurité de leurs données de santé, il participera à la démarche de sécurisation de l'ensemble des données médicales.