Interop'Santé
Pour des systèmes d'information communicants

Data Protection & Safety

La problématique liée à l'éthique et à la sécurité des données de santé

Journée Innovation & eSanté
Alger - 29 novembre 2016

Jean-Christophe Cauvin
Président Interop'Santé

- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Introduction

- Données de santé et éthique
- Sécurisation des données de santé
- Interopérabilité
- Questions & réponses

Interop Santé
Pour des systèmes d'information communicants

- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Données de Santé

- Définition

  Règlement européen (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des de ces données.

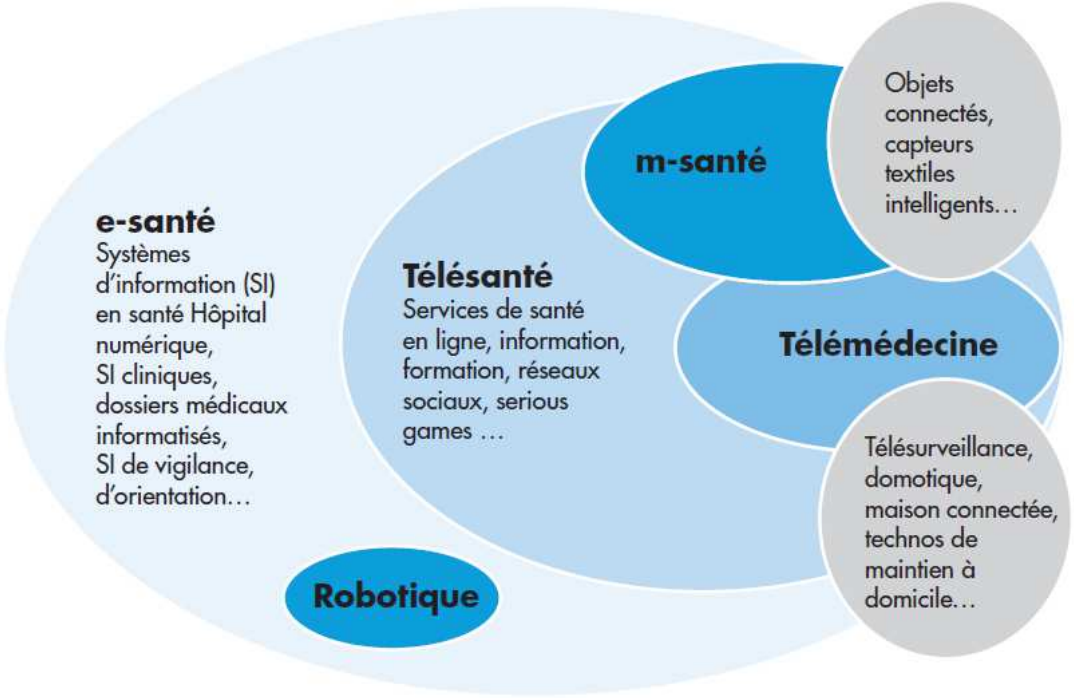
  « […] données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».

  « […] toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro »

- Introduction
- **Données de santé et éthique**
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Données de Santé

- Sources de données



Source : Conseil national de l'Ordre des médecins

Interop Santé
Pour des systèmes d'information communicants

- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Questions d'étique

- **Finalité**
  - Les informations qui concernent les patients ne peuvent être recueillies et traitées que pour un usage déterminé et légitime. Exemples :
    - suivi médical des personnes, prévention, gestion de services de santé;
    - traitements statistiques réalisés par un service ministériel;
    - recherche.
- **Pertinence**
  - Seules doivent être traitées les informations pertinentes et nécessaires au regard des objectifs poursuivis par le traitement des données. Exemple :
    - enregistrement de la nationalité d'un patient dans un Dossier Patient Electronique (DPI).

- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Questions d'étique

- **Droit à l'oubli**
  - Quelle doit être la durée légale de conservation des données médicales à caractère personnel ?
  - Sur quels critères est il possible de conserver ces donnés au-delà de la DLC ? Intérêt historique, médical, recherche …

- **Sécurité et Confidentialité**
  - Les professionnels de santé, comme le responsable des données de santé, est astreint à une obligation de sécurité. Des mesures doivent être prises pour :
    - garantir la confidentialité des informations;
    - éviter leur divulgation à des tiers non autorisée.

- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Questions d'étique

- **Respect des droits des personnes**
  - Information des personnes (affichette, livret …)
  - Droits d'accès et de rectification
  - Droit d'opposition

- **Responsabilité des données**
  - A qui appartiennent les données médicales à caractère personnel ? Patient, établissement, hébergeur des données …?
  - Quelle sont les responsabilités légales ?

- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Questions d'étique

- **Egalité**
  - Devoir de fournir à la population l'accès à un niveau adéquat de soins de santé.
  - Déploiement de système de eSanté :
    - Couverture du territoire
    - Fracture numérique
    - Egalité des chances devant la maladie
- **Fiabilité**
  - Système unique, plusieurs systèmes interopérables
    - Système unique : meilleure prise en charge des patients mais les défaillances (pannes, pertes de données, attaques malfaisantes) ont des impacts sévères.
    - Systèmes interopérables : plus de choix selon le contexte d'utilisation (salles de soins, polyclinique, hôpitaux, CHU) mais risques d'interopérabilité et d'erreurs de données.

- Introduction
- Données de santé et éthique
- **Sécurisation des données**
- Interopérabilité
- Questions & réponses

Sécurisation des données

- **Dispositifs organisationnels**
  - Politique nationale de sécurité pour la eSanté (identification, authentification, imputabilité, dispositifs connectés, interventions à distance …)
  - Correspondant sécurité != responsable sécurité
  - Formations, campagnes de sensibilisation de tous les PS
- **Dispositifs physiques**
  - Accès au locaux et aux postes de travail
  - Suppression des ports USB, lecteurs CD …
- **Dispositifs techniques**
  - Mise à jour des systèmes d'exploitation des derniers patchs
  - Antivirus, pare-feu
  - Cryptage des communications, des données

- Introduction
- Données de santé et éthique
- **Sécurisation des données**
- Interopérabilité
- Questions & réponses

Sécurisation des données

Identification des personnes

- Déterminer l'identité d'un acteur du système d'information via un identifiant qui lui a été attribué préalablement lors de la vérification et de l'enregistrement de ses traits d'identité.
- PS, personnel administratif, informatique, fournisseurs.
- Utilisée pour le contrôle des droits d'accès et la traçabilité.
- Différents niveaux de mise en œuvre :
  - Identifiant local
  - Identifiant national

- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Sécurisation des données

- **Authentification**
  - Vérification de l'identité d'un acteur pour l'autoriser à accéder au système d'information.
  - Différents niveaux de mise en œuvre :
    - Identifiant + mot de passe (règle de gestion des mots de passe)
    - One Time Password
    - Cartes à puce
    - Biométrie

- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Sécurisation des données

- **Imputabilité**
  - Attribution à chaque utilisateur (ou à chaque machine) l'intégralité des actions qu'il a effectué sur le SI.
  - Attribution de chaque action à l'utilisateur et/ou à la machine l'ayant effectuée.
  - Traces :
    - fonctionnelles (action métiers)
    - embarquées (métadonnées d'un document)
    - Techniques (journaux de systèmes d'exploitations, de pare-feu, de base de données…)
  - Traçabilité discrète et continue.
  - Durée de conservation des traces (cf droit à l'oubli).

- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Interopérabilité

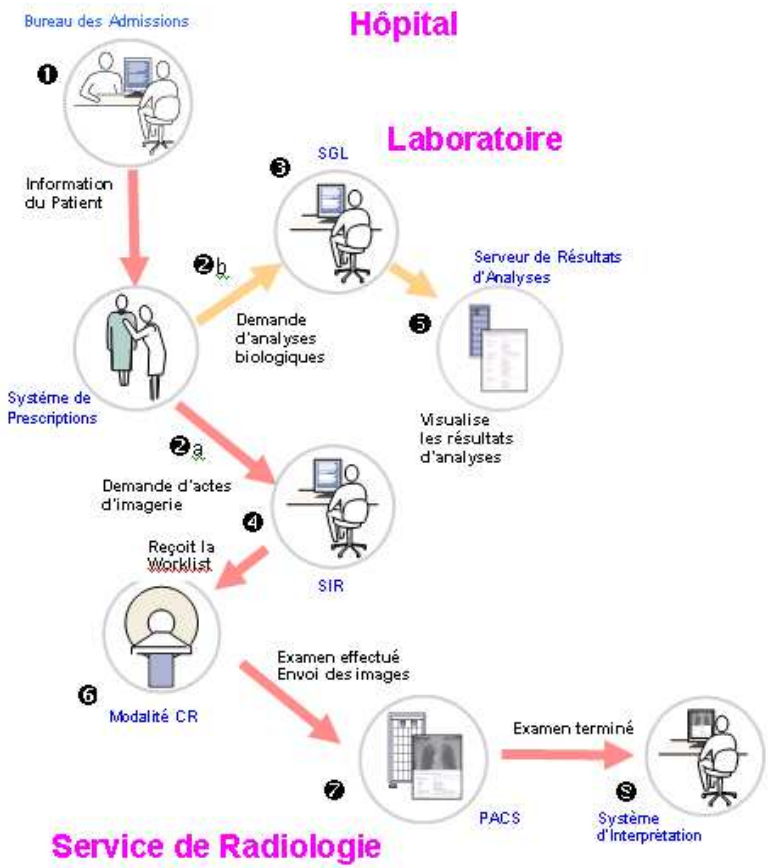
L'interopérabilité est la capacité des composants d'un système d'information de communiquer et d'échanger des données de façon fiable, efficace, cohérente et d'utiliser les informations qui ont été échangées.

- **Technique**
  - Transport des flux de données et services.
- **Syntaxique**
  - Compréhension et traitement des données échangée à travers un langage.
- **Contenus métier**
  - Modélisation commune des objets métiers transportés.
- **Sémantique**
  - Compréhension du vocabulaire utilisé pour coder des concepts médicaux.

Interop Santé
Pour des systèmes d'information communicants

- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Interopérabilité



Interop Santé
Pour des systèmes d'information communicants

- Introduction
- Données de santé et éthique
- Sécurisation des données
- **Interopérabilité**
- Questions & réponses

Interopérabilité

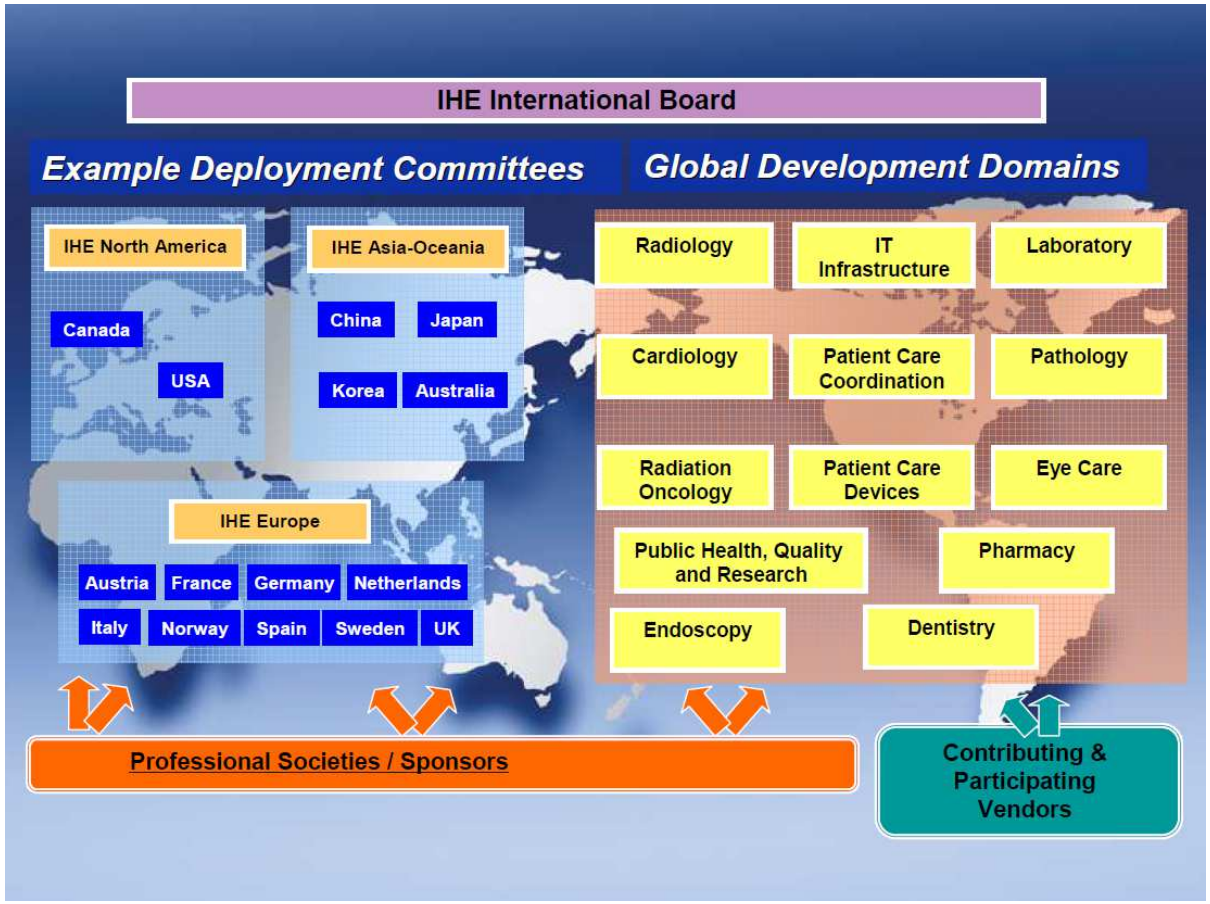
- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Interopérabilité

- IHE (Integrating the Healthcare Enterprise)
- Initiative lancée aux USA en 1997 à l'initiative du RSAN (Radiological Societty of North America) et HIMSS (Healthcare Information and Management Systems Society)
- Objectifs :
  - Faciliter l'intégration des différents composants (équipements, sous-systèmes) du Système d'Information d'un établissement de santé (SIH).
  - Automatiser la circulation des données entre les composants du SIH et les équipements au sein d'un domaine (radiologie, laboratoire) ou entre domaines.
  - Définir un cadre technique et un langage commun pour parler de l'intégration en suivant une démarche pragmatique (cas d'usages) et itérative (CP).
- Comment ?
  - Le principe est de réunir utilisateurs et industriels pour identifier et résoudre les problèmes de connectivité entre produits, matériels et systèmes d'origine diverse..
  - Utilisation de standards reconnus dans différents domaines du secteur de la santé (radiologie, laboratoire, médecine nucléaire, cardiologie, infrastructures,….).
  - Approche radicalement novatrice fondée sur une coopération étroite entre utilisateurs et industriels et basée sur un consensus global.

- Introduction
- Données de santé et éthique
- Sécurisation des données
- **Interopérabilité**
- Questions & réponses

Interopérabilité



Interop Santé
Pour des systèmes d'information communicants

- Introduction
- Données de santé et éthique
- Sécurisation des données
- Interopérabilité
- Questions & réponses

Interopérabilité

- CT (Consistent Time)
- PAM (Patient Administration Management)
- PDQ, PDQV3, PDQm (Patient Demographics Query)
- ATNA (Audit Trail and Node Authentication)
- EUA (Enterprise User Authentification)
- PWP (Personnal White Pages)
- HPD (Helathcare Provider Directory)
- IUA (Internet User Authorization)
- XUA (Cross Enterprise User Assertion)
- BPPC (Basic Patient Privacy Consents)
- APPC (Advanced Patient Privacy Consents)
- SVS (Sharing Value Set)
- DSG (Document Digital Signature)
- XDS, XDR, XDM (Cross-Enterprise Document Sharing/Exchange)
- DEN (Document Encryption)

QUESTIONS & REPONSES

Interop Santé
Pour des systèmes d'information communicants

Interop Santé
Pour des systèmes d'information communicants