COURS 1: ENVIRONNEMENT NUMERIQUE DU MEDECIN

C2I 1.1:l'environnement du médecin

Informatisation de la santé

- décloisonnement entre les différents acteurs de la santé et les différentes activités
- favorise une médecine plus fluide, plus réactive, cooordonnée

Le médecin doit tirer bénéfice de cette informatisation dans sa pratique grâce à un ensemble d'outils qui vont lui faciliter le travail.

Outils informatisés d'aide à la décision dg/thérapeutique

Communication/Echange/partage d'infos sur le patient/coordination de soins: Messagerie électronique par partage de l'espace de travail: dossier médical partagé, dossier patient informatisé dont droit d'accès appartiennent au patient applications pour suivi patient

Télé-médecine

Médecin dans une relation de conventionnement avec l'AM: **rémunération** du médecin si

- atteinte d'un certain nombre d'**objectifs** de santé publique mesurés grâce à des **indicateurs**
- ex=**informatisation du cabinet médical**

Facilite la tâche du médecin : traitement informatisé des données des patients pour calculer automatiquement les indicateurs exigés ou vérifier les antériorités du patient.

Le médecin, en tant que producteur d'activité et maillon de la prise en charge des patients contribue à un système d'information de santé territorial. Médecin=producteur de données de santé

ARS exploitent les données d'activité, de localisation des professionnels de santé pour construire une cartographie de l'offre de soins afin d'avoir les moyens de réguler l'offre et la demande pour qu'il y ait une équité d'accès aux soins sur le territoire national.

HAS qualifie la qualité de l'offre de soins par la construction d'indicateurs à partir de données issues du soin. Ces indicateurs permettent de comparer des établissements de santé entre eux par exemple.

Veille sanitaire du médecin: Par les notifications qu'il fait aux organismes en charge des vigilances des populations, il contribue à la surveillance épidémiologique territoriale.

Nouvelle pédagogie dématérialisée: simulation pour la formation du médecin

C2I 1.2:le patient 2.0

Patient vivant avec des nouvelles technologies: outils utiles pour le médecin / détronement du médecin?

- prise de pouvoir «empowerement »/autonomie: **Patient acteur de sa santé**—>génère données de santé

Site internet:

- généraliste: doctissimo (vulgaire, pub)
- associatif:infos sur 1 type de pathologie par les patients experts=communauté de patients
- médicaux: orphanet (maladie rare)
- forums: modérés/non par 1 pro de santé, fiabilité - -

Analyse de l'offre de soin: coût, conventionnement, proximité, qualité, avis

- Sites scope santé: indicateurs publiques de qualité des établissements HAS
- sites hospitalidées: note sur les pro de santé
- sites pro des établissements de soin

Prise de RDV en ligne: doctolib, direct sur sites de médecin

Consultation en ligne: montant reste à la charge du patient

Technologie pour automatiser la PEC:

- suivi: objets connectés pour surveillance santé (lentilles, piluliers, tensiomètres connectées), applications de santé++ + (medissimo: ne pas oublier 1 TT)
- surveillance à distance (dispositif cardiaque implantable monitorés à distance par médecins)
- assistance: domotique (maison détecte chute du patient), robot

Patient peut notifier lui même les EI

Données de vie réelle au médecin: surveillance observance TT

Patient + exigeant mais responsabilisé, médecin + accessible

Relation verticale devient horizontale

C2I 1.3 le médecin 2.0

- Outils de travail numérique: ordinateur, smartphone (n° de tel au patient), tablette connectée
- réseau haut débit: imagerie (volumineux)
- système de sauvegarde
- Lecteur de carte à puce:authentifier médecin et patient, paiement+facturation à l'AM
- Objects connnectés: tensiomètre connectée au dossier du patient , objets réalisant mesures et interprétations mesures (ECG connectée)
- Hottline d'assistance: aide pour pb avec outils

Logiciel principal: **gestion du cabinet médical** édité par privés/associatifs:
Infos qu'il contient accessible uniquement par médecin mais il faut que toute l'information concernant un patient soient accessible par tous les professionnels de santé qui le prennent en charge et donc ces informations doivent se retrouver dans le dossier médical personnel du patient que le patient gère=DMP compatible(infos du logiciel—>dossier médical perso du patient)
- gestion du DMP : enregistrement élément consultation, aide à la prescription, intégration examens complémentaire, détection de situations à risque comme les IM, suivi des patients malades chroniques, planifier suivi conforme aux reco
- et gestion du cabinet médical (aide à la comptabilité, analyse rétrospective, indicateurs pr ROSP)

Messagerie sécurisée: authentification émetteur+récepteur et cryptage message= garantit l'identité de la personne qui envoie le message+celle qui lit le message et assure que le message lors de l'envoi n'a pas pu être lu par une tierce personne ou modifié.
Les données de santé sont des données sensibles et le médecin est responsable de leur sécurité. Les messageries non sécurisée sont balayées par des robots et leur contenu est en permanence analysé, il faut donc rejeter ce type de boites aux lettres pour envoyer des données concernant vos patients.

Prise de RDV en ligne: mise à jour du carnet de RDV
reseau de vigilance sanitaire
Service de notifications obligatoires (EI médocs, décès)
WebMédecin par l'AM=simplification démarches auprès de l'AM + consultation d'historique de remboursement de patient

Internet:Favoris=bibliothèque virtuel de sites de bonne qualité médicale:
- HAS:Reco de bonnes pratique
- VIDAL:médicaments
- sites spécialisées=CRAT: risques liés à la prise médocs F enceinte/ orphanet:maladie rare
- sites de société savantes: ex infectiologie.com
- Sites de formation continu, site de facultés de médecine
- journaux médicaux
- pubmed, Schoolar: moteur de recherche bibliographique
- Cismef: moteurs de recherche de sites médicaux/de documentation med
- google/Quant

Alerte/veille dès que nouvelle info sur ces sites
Smartphone=applications dont qualité à valider avant de les intégrer à la pratique:
- base médicaments
- outils pour calcul de scores, de formules biologiques
- outils utiles en dermato pour addresser image pour avis dermato ou pour reconnaitre une lésion à partir d'une banque de photographies
- outils pour résoudre cas clinique: maintien niveau de formation
- réseau social: réseau de professionnel, augmentation réputation

Identité numérique du médecin professionnel de santé: CPS (Carte Pro de Santé) après inscription à l'ordre et à l'AM, authentification, cryptage+décryptage des messages envoyés/recus
N° d'identification
Opportunité technologie: augmente visibilité+réputation en respectant règles de déontologie—> sites de médecins: coordonnées, infos médicales
Avant de s'équiper: comparatif (salons++)
Formation aux outils
Logiciel certifié, fonctionne avec données de médocs validés agréés, marquage CE
Attention à la sécurité+confidentialité des données de santé
Il doit être capable de rédiger un cahier des charges pour choisir ses outils de travail numérique. Il faut être attentif à l'ergonomie de ces logiciels de gestion de cabinets médicaux, car ils doivent se rapprocher au plus près de la façon dont le médecin travaille et ne doivent pas être entravant. Avant de s'équiper, il faut réaliser un comparatif et voir des démonstrations de ces logiciels. De nombreux salons « technologies en santé se déroulent au cours de l'année,
Le médecin doit être également attentif à l'évaluation des logiciels. Le médecin va devoir également adopter un comportement qui va garantir la sécurité et la confidentialité des données qu'il va emmagasiner dans ces outils, car les données une fois informatisées peuvent être perdues, volées, endommagées. Le médecin doit entrer dans l'ère du partage de données pour que le patient soit le mieux pris en charge, il doit construire son réseau, l'entretenir et échanger.
Enfin la technologie va faire tomber un certain nombre de barrières entre le médecin et le patient avec un patient plus informé, plus impliqué et un médecin beaucoup plus accessible.

C2I 1.4:l'esprit critique

Niveau de preuve scientifique plus difficile à obtenir, certains industriels donnent des qualités médicales à leur solutions technologiques qui relèvent plus de l'allégation commerciale que d'une véritable évaluation scientifique.

Points sur lesquels il faut être attentif lorsqu'on utilise des solutions technologiques et risques associés à la techologie
- respect de la **CONFIDENTIALITE** des données de santé: Attention aux disséminations de données de santé à l'insu de l'utilisateur
Solutions technologiques en santé collectent pour fonctionner des données personnelles de santé pour lesquelles normalement aucun traitement n'est autorisé sauf traitement déclaré à la CNIL.
L'usage des technologies mobiles rend plus facile l'accès aux données personnelles car les applications sont en interaction étroite avec le système d'exploitation.
Diffusion de données à des entreprises tierces:s'assurer que les solutions technologiques utilisées respectent bien la confidentialité et la protection des données, vulnérabilité,pas de failles de sécurité. Les données au moment de leur échange peuvent par exemple être interceptées si aucun procédé de cryptage n'est mis en œuvre. Les objets connectés sont de véritables passoires, 1/3 récupèrent des données à l'insu de l'utilisateur.
Données collectées: niveau d'intrusion accepté pour améliorer surveillance santé?

- **FIABILITE outils technologiques:** fiabilité des mesures et des calculs d'outils connectés?
la solution technologique a-t-elle des performances médicales acceptables?. Une solution technologique vantant un intérêt médical doit être validée, car ce n'est pas un dispositif médical pour lequel on a normalement des garanties en termes d'innocuité et d'efficacité.

Logiciel **à des fins dg/thérapeutique**=considéré comme un **dispositif médical**(relève de la législation sur les DM)=> **marquage CE: validation technique et scientifique**

Certification des logiciels de prescription=charte de la **HAS.** Les logiciels candidats à cette certification doivent passer avec succès un certain nombre de scenarii de prescription, certains comportant des situations à risque. L'objectif est de vérifier que le logiciel possède un certain nombre de fonctionnalités qui vont faciliter la prescription et qu'il est un véritable garde-fou en alertant en cas de prescription dangereuse.
Le médecin peut aller sur le site de la Haute Autorité de santé pour avoir la liste des logiciels certifiés, cela peut l'aider pour s'orienter dans l'offre de logiciels quand il décide de s'équiper.
L'agrément engage la responsabilité de l'industriel sur un certain nombre de points auquel son produit doit se conformer. Par exemple les **bases de données sur les médicaments sont agréées par la HAS** si l'éditeur certifie que sa base se conforme à la charte d'agrément (par exemple que l'**éditeur est indépendant de l'industrie pharmaceutique**, que la base de données est **mise à jour régulièrement,** qu'elle contient l'ensemble des médicaments commercialisés....).

Faire des recherches bibliographiques pour évaluation outils performance médicale des outils connectés/applications:
Etudes scientifiques, littérature médicale scientifique: étude médicale sur performance d'1 outil connecté
Test selon protocole pour vérifier sécurité, intérêt, commentaire des pros de santé
Les solutions technologiques peuvent faire l'objet d'**études scientifiques e**t les résultats de ces études peuvent être publiés dans la **littérature scientifique médicale** sous la forme d'articles. Il est donc possible de faire une recherche bibliographique pour trouver s'il y a des études mesurant les performances médicales d'un outil. On pourra trouver des réponses à des questions de type : **Est-ce que cet objet connecté est un bon outil diagnostique**? Est-ce que l'utilisation de tel outil améliore le contrôle d'une maladie chronique? Il faut cependant être vigilant à la construction méthodologique de l'étude et à sa validité, la généralisabilité de ses résultats.

Initiatives publiques ou privées de portail de référencement pour qualifier les application: **DMD ou MedAppCare en France, ImedicalApp aux Etats Unis.** Les applicatifs sont testés selon des protocoles pour vérifier leur sécurité, leur intérêt, ou font l'objet de commentaires de professionnels de santé. En Grande Bretagne, un tel portail appelé **NHS Choices=**référencer les applications de santé satisfaisant aux exigences en matière de sécurité et de protection de données. Une étude conduite sur ces applications promues par le NHS Choices a montré qu'un certain nombre d'entre elles présentaient des failles de sécurité, et cela a conduit à la fermeture de ce site de référencement public.
Il y a donc une gradation dans les processus garantissant la sécurité et l'efficacité d'une solution technologique, seul le marquage CE offre des garanties avec une vigilance des autorités identiques à celle exercée sur les médicaments, les autres processus peuvent laisser passer des failles et requiert donc votre vigilance.
Médecin responsable de ses décisions=>responsabilité engagé même si c a cause de la solution technologique (aide/erreur)/ S'il utilise un outil non fiable et prend de mauvaises décisions,
La solution technologique peut apporter de l'aide mais elle peut vous conduire à faire des erreurs si ses performances ne sont pas bonnes ou ne sont pas quantifiées.
Utilisation/ prescription de solutions technologiques:responsabilité du médecin reste engagée=> être vigilant.
Solution technologique=performance médicale acceptable? doivent être validées, pas 1 DM.
Ne pas avoir une confiance aveugle en ces outils technologiques, il faut pouvoir être critique vis-à-vis de la solution proposée tout comme vous pourriez être dubitatif devant le résultat d'un test biologique! Usage responsable de la technologie.
Vigilant car toujours la responsabilité du médecin engagé même si utilise 1 outil technologique
Mésusage outils technologiques/applications: **dommages liés aux soins**= « **e-iatrogénie** » (clique trop vite halopéridal/allopurinol, cliquer trop vite sur message d'alerte)
Les solutions technologiques peuvent vous apporter de l'aide, mais il faut les utiliser correctement. La technologie peut être facilitante pour certaines erreurs, par exemple se tromper lorsqu'on sélectionne un item dans une liste (par exemple prescrire de l'halopéridol à la place de l'allopurinol), ou parce qu'on clique trop vite sans regarder le message d'alerte s'affichant parce que c'est la dixième fenêtre qui s'affiche et que cela vient trop souvent interrompre votre travail.
Enfin les logiciels peuvent mal fonctionner parce qu'ils requièrent que vous rentriez des données sur le patient dans un format standardisé et que vous ne vous vous en êtes pas donné la peine.
Le médecin doit être capable de se forger un avis sur les outils technologiques quant à leur sécurité, leur fiabilité, leur validité scientifique. Il doit être vigilant car au final c'est toujours sa responsabilité qu'il engage lors de la décision, que l'outil qu'il utilise soit fiable ou non.

C2I 1.5:être formé en santé numérique

- Sécurité des données
- veille professionnel
- collaboration médiée par information
- maitrise des logiciels métiers

Spécialisation en informatique biomédicale: bioinformatique (niveau moléculaire/cellulaire médecine)
master d'informatique biomédicale tel que celui dispensé dans les universités Paris 5 et Paris 13 et faire un internat de santé publique
Méthodes très sophistiquées pour analyser les séquences de gènes.
Essor++ avecgénomique fonctionnelle, protéomique, transcriptomique et séquençage massif.
Du point de vue de la connaissance, la recherche progresse et va conduire à disposer d'un cadre rationnel pour expliquer les grands déséquilibres et leur traduction au niveau cellulaire ou moléculaire.
Les premières applications en Santé concernent la **médecine personnalisée,** qu'il s'agisse de diagnostic ou de traitement personnalisé. Les données de génomique fonctionnelle issues des puces à ADN sont utiles pour étudier les relations entre gènes et comprendre les déterminants et les mécanismes moléculaires de la gravité d'une maladie donnée chez un individu donné.
Elles peuvent aussi être utilisées en clinique pour choisir un traitement médicamenteux bien adapté au patrimoine génétique d'un individu donné.

L'informatique clinique ou bioclinique traite des données patients et des connaissances médicales associées à la prise en charge individuelle des patients. L'informatique clinique cherche à offrir des solutions méthodologiques et techniques pour la représentation des données et des connaissances, leur organisation, leur saisie, leur stockage, leur interrogation, leur interprétation, leur communication ou leur utilisation pratique. La prise en charge aidée par l'informatique peut se faire en présence du malade ou à distance grâce aux outils de la télémédecine.

Santé publique: outils techniques + applications informatiques pour raisonner au niveau des populations=registres maladie, système vigilance, pharmacovigilance, aide aux prises de décisions
Des méthodes spécifiques sont appliquées aux populations avec une approche de Santé Publique. La Santé Publique vise à développer des actions éducatives, préventives, curatives et sociales pour améliorer la santé globale des populations. Pour être efficaces ces actions doivent s'appuyer sur des systèmes d'information performants dont la conception relève de l'Informatique Médicale. L'OMS insiste maintenant pour que tous les états réfléchissent à la qualité de leur système d'information de Santé et cherchent à les améliorer.
L'informatique de Santé Publique regroupe les outils, techniques et applications informatiques permettant de raisonner non au niveau des individus mais des populations. Entrent dans ce cadre les outils de suivis de cohortes, les registres de maladies ou les systèmes de vigilance. C'est le cas par exemple de la pharmaco-vigilance, où l'on doit collecter des données sur plusieurs sites, rassembler et harmoniser les déclarations d'événements indésirables, les agréger en fonction de leur « ressemblance » et raisonner sur les cas observés en tenant compte des connaissances préexistantes. On sait également que le besoin d'agrégation de l'information, de fouille de données et d'alerte automatique est majeur pour aider à des prises de décisions pouvant avoir un fort impact sur la santé des populations.

COURS 1: L'INFORMATION DU DM

C2I 2.1:rôles et contenu du dossier patient

Dossier patient:

- Tracabilité=note + garder 1 trace de ce qui s'est passé/a été fait/dit pour le patient
- infos stockées au même endroit=outil pour regrouper tout ce qui est connu d'1 patient
- mémoire:Retrouver 1 info passé concernant le patient
- éléments de synthèse, d'analyse et de décisions
- communication entre les professionnels de santé et/ou avec le patient

Contenu réglementaire du DP (loi du 4 mars 2002)
=ensemble des informations concernant la santé du patient détenues par le professionnel, qui sont formalisées et ont contribué à l'élaboration et au suivi du diagnostic et du traitement ou d'une action de prévention, ou ont fait l'objet d'échanges écrits entre professionnels de santé.

HOPITAL:Le dossier patient doit contenir au moins:
infos recueillies A l'entrée :
- La lettre du médecin adressant le patient en consultation/admission à l'hopital
- motif(s) d'hospitalisation
- ATCDs et FDR
- Les conclusions de l'évaluation initiale
- La prise en charge+prescriptions à l'issue de l'examen initial

Durant le séjour :
- PEC :Les examens paracliniques, les soins et prescriptions effectués, l'état clinique , infos sur la démarche médicale adoptée
- Le dossier de soins infirmiers et les informations provenant d'autres professionnels de santé, correspondances entre pros de santé
- En cas d'examens invasifs ou de chirurgie : le dossier anesthésie, le compte rendu opératoire, le consentement écrit du patient, les actes transfusionnels+/- incidents, consentement écrit du patient si requis

A la fin du séjour :
- La lettre de liaison médicale et la fiche de liaison infirmière
- Les modalités de sortie, CRH, lettre sortie, prescription de sortie

Le dossier patient peut aussi contenir les informations recueillies auprès de tiers n'intervenant pas dans la prise en charge.

CABINET LIBERAL:
DP=fiche d'observation médicale=éléments actualisés nécessaires aux décisions dg et de tt

Evaluation de la qualité du DP:
résultats publiés sur SCOPE SANTE=site internet labélisé par HAS, informe sur qualité des hôpitaux et des cliniques

Indicateurs de Qualité et de Sécurité des Soins Tenue du Dossier Patient (TDP)
Qualité DP impact sur qualité de la PEC des patients
13 critères utilisés pour évaluer la qualité de la tenue du dossier des patients hospitalisés :
– Dossier retrouvé/présent
– Identification du patient présente
– Présence d'un document médical relatif à l'admission
– Examen médical d'entrée renseigné/décrit
– Rédaction des prescriptions médicamenteuses établies pendant l'hospitalisation (si applicable)
– Qualité de l'administration médicamenteuse pendant l'hospitalisation
– Présence du courrier de fin d'hospitalisation ou du compte rendu d'hospitalisation
– Rédaction d'un traitement de sortie (si applicable)
– Mention de l'identité de la personne de confiance
– Mention de l'identité de la personne à prévenir
– Présence d'un (ou des) CRO(s) et/ou d'un compte rendu d'accouchement (si applicable)
– Présence du dossier anesthésique (si applicable)
– Dossier transfusionnel renseigné (si applicable)

Score de qualité pour chaque dossier = Somme des critères satisfaits / Somme des critères applicables

Contenu hétérogène du dossier patient
Observations médicales rédigés par les médecins : données subjectives(plaintes), objectives(examen clinique, résultats examens complémentaires), interprétées (dg), décision et actions médicales(prescription, indication de chirurgie), notes perso+confidentielles appartenant au seul médecin qui les a prises,
Nature des données: Textuelle, numerique, signaux(ECG), images, numérisations
Infos provenant de différents acteurs de santé; interne, infirmiere, biologiste, externe, radiologue, médecin sénior
Prise de note chronologique à des moments différents: date

Droits des patients concernant accès au DM (réglementés)

Accès au dossier médical
Délai de conservation du dossier médical

❖ **Dans les établissements de santé publics et privés**

Patient	Dossier conservé pendant 20 ans, à compter de la date du dernier séjour ou de la dernière consultation externe du patient dans l'établissement
Patient mineur âgé de moins de 8 ans	Dossier conservé jusqu'à l'âge de 28 ans
Patient décédé moins de 10 ans après son dernier passage dans l'établissement	Dossier conservé 10 ans à compter de la date du décès

❖ **Cas particuliers**

Dossier médical partagé (DMP)	Dossier conservé pendant 10 ans, à compter de sa clôture
Acte transfusionnel et/ou fiche d'incident transfusionnel	Conservés pendant 30 ans à partir de la date de l'acte de transfusion
Recours grâcieux ou contentieux	Délais suspendus

Accès au dossier médical
Documents accessibles

Documents accessibles	Documents non accessibles
• Résultats d'examen • Comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation • Protocoles et prescriptions thérapeutiques mis en œuvre • Feuilles de surveillance • Correspondances entre professionnels de santé	• Informations recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique • Informations concernant un tel tiers (ex : membre de la famille) • Certaines notes des professionnels de santé pouvant être considérées comme personnelles (= ne contribuent pas à l'élaboration et au suivi du diagnostic et du traitement ou à une action de prévention)

Modalités d'accès réglementés

- Demande du patient adressée au professionnel concerné par courrier :
  - Directement au professionnel libéral
  - Au responsable de l'établissement de santé
- Quel est le délai de communication à compter de la réception de la demande ?
  - 8 jours pour un dossier récent
  - 2 mois pour un dossier dont la dernière pièce remonte à 5 ans
- Quel est le mode de consultation du dossier médical ? Au choix du demandeur
  - Consultation sur place : gratuite, par voie électronique
  - Par envoi de copies : remises sur place ou adressées par courrier, sur un support similaire à celui utilisé par le professionnel de santé, l'établissement de santé ou l'hébergeur (si dossier informatisé, la copie pourra être un CD-Rom), aux frais du demandeur.

Droit d'accès des patients

•Le patient mineur:Le droit d'accès est exercé par le titulaire de l'autorité parentale SAUF si refus du mineur

•Le patient majeur protégé a le droit d'accès au dossier médical. La personne chargée de la mesure de protection n'a pas l'accès SAUF si habilitation donnée par le juge des tutelles

• Le patient majeur et ses proches en cas de décès
  - Consultation gratuite
  - Délivrance de copies et envoie du dossier payants
  - Le patient peut demander que son dossier soit transmis à un autre médecin ou à une personne mandatée
  - Les ayants droits, le concubin ou le partenaire lié par un pacte civil de solidarité du patient décédé ont un accès avec restriction: l'objectif doit être de « connaitre les causes de la mort, défendre la mémoire du défunt, faire valoir leurs droits » SAUF si le défunt s'y est opposé de son vivant

En résumé, le dossier patient :

- Est un document médico juridique et administratif
- Il a un rôle clef dans la prise en charge coordonnée du patient
- Son contenu est hétérogène et réglementé

L'accès au dossier médical est réglementé

C2I 2.2:le dossier patient informatisé

Dossier patient papier:

- Observations médicales écrites à la main
- dossiers d'examens complémentaires:résultats d'examen bio, examens d'imagerie
- feuilles de liaison du suivi infirmier

Au cours de l'hospit: volume dossier patient augmente++
Classement dans différents sous dossiers rangés dans 1 pochette nominative + transportable(mais parfois volumineuse++) pour chaque patient rangée dans service où patient hospitalisé puis quand il sort, dans une Zone de stockage(archives) là où se trouve tous les dossiers des patients hospitalisés dans l'hopital.
Pb de classement des infos, d'archivage des dossiers, de TT, d'extraction et de communication
Communication: transmission dossier patient/courrier

Dossier patient informatisé:
Nouvelles perspectives:amélioration accessibilité des infos recueillis+réutilisation à des fins de soins/de recherche/de planification, regroupement de données pour faciliter évaluation+recherche et planification
Tend vers 1 médecine + organisée + ajustée et + sure
Organisé en sous-dossiers accessibles via différents dossiers: DM, dossier adminsitratif, dossier infirmier etc
Cf: ORBIS
Ordonnance générée automatiquement à partir du DP
Bénéfices informatisation:

- améliorer recueil et stockage de l'info + facilement de meilleure qualité, éléments + lisibles, + précis et + complets
- données multimédias intégrées dans le dossier
- volume de stockage augmenté—> dossiers patients informatisés stockés sur des serveurs

TT information amélioré++: construction de synthèse d'abstractions multiples et de regroupements de données (évaluation des soins, recherche clinique, épidémiologique, planification)
génération automatique d'alertes (réduction des erreurs): ex prescription d'1 médoc pr lequel patient allergique
outils d'aide à la décision dg ou thérapeutique pr aider médecin dans sa démarche clinique
Echanges simplifiés: pro de santé peut avoir accès au DP en se connectant sur le dossier médical
Echanges par messagerie sécurisée
Permet de tend vers 1 médecine + organisé + ajusté et + sure

C2I 2.3:structuration du dossier patient

Structuration du dossier patient informatisé
Saisies des données patients selon 2 approches:

1. Approche documentaire en texte libre: Structuration données +/- avancée
   + :saisie libre de l'info
   - : données difficilement exploitables et difficulté de connexion avec systèmes d'aides à la décision
2. Approche orientée données via formulaires:
   présence ou non d'1 douleur à l'arrivée etc
   +:données facilement exploitables, connexion avec systèmes d'aide à la décision
   -: contraignant, beaucoup d'items à remplir pas toujours adapté à al situation clinique, insuffisamment remplis

Infos indexées à partir de l'identifiant du patient
Stucturations du dossier patient (pas une mais des organisations de dossier patient) dépendent:

- de l'usage
- de l'origine des données
- des pb du patient
- de la chronologie

Possible de varier les vues sur les contenu pour s'adapter aux besoins du pro de santé qui PEC le patient
plusieurs types de structurations

- chronologique: par succession de venues, rend difficile recherche d'infos et exploitations des données
- selon la source : regroupement en f (origine) ex= CRH, résultats bio..
- selon la spécialité: ex:gyneco
- selon les acteurs de santé: en f(pro de santé)=médical, kiné, infirmier
- selon les pb: infos selon pb du patient:rapprochement d'éléments de sources différentes, suivi HTA, BPCO etc, difficultés quand différents pb intriqués entre eux

Dossier patient informatisé partagé entre pro de santé:
PB actuel: pas 1 seul dossier médical partagé pour faciliter coordination des soins (1 dossier médical/médecin voir hôpital voir par service par hopital)=cloissonnement du dossier patient
DMP : dossier médical partagé= 1 dossier patient unique

C2I 2.4:sécurité des données de santé=introduction

On informatise les données de santé des patients pour que, par ex, un Medecin TT puisse accéder rapidement et facilement aux infos de santé d'1 patient à n'importe quel moment, peut envoyer 1 courriel à 1 confrère pour lui adresser 1 patient/demander 1 avis +/- en lui envoyant 1 radio par courriel (**communication** facile+rapide avec les autres pro de santé + **partage** de données de santé des patients entre les pros de santé)= MEILLEURE PEC PATIENT

Risques à informatiser les données de santé: **multiples,** à tous les niveaux

- programmes malveillants: virus—>perte données
- vols sur lieu d'exercice
- données de santé transmises défectueuses
- failles de sécurité : révélation au grand jour de données de santé
- hacker peut prendre en otage données de santé et demander rancon: ransomware

Données de santé=marché très lucratif pour les hackers

Environnement sécurisé nécessaire à l'informatisation des données de santé:

garanti **confidentialité** des données patient pour respect secret professionnel et loi informatique et liberté, **intégrité** des données (exactitude des infos transmises), **tacabilité** des actes médicaux pour conserver mémoire des actes réalisés

C2I 2.5:sécurité des données de santé=cadre réglementaire

Pro de santé: obligation de **protection des données du patient car tenu au secret professionnel**

- fin des études, soutien thèse d'exercice—> prêter serment d'Hippocrate
- régi par la loi: article 4 du code de déontologie médicale—>devoir imposé à tout médecin
- CSP: Tous les pros de santé du champ sanitaire/social concerné par le secret pro

Secret pro a 1 définition + large, il inclu tout ce qui a été vu, entendu , dit compris ou confié + identité et état de santé du patient

Secret partagé entre pros de santé participant à la PEC+à la continuité des soins du patient pour garantir continuité des soins.Pros de santé consulté par le patient dans le cadre de sa PEC=considérés comme faisant partie de la même équipe de soins

Patient a 1 droit d'opposition sur le secret partagé: peut refuser que de infos soit communiqué à 1 autre pro de santé

> **Au sien d'1 meme equipe de soins:** partage d'infos ne nécessite pas de consentement préalable du patient, ne nécessite pas d'être expressément obtenu mais patient peut s'opposer à ce partage

> **Hors équipe de soins:** partage d'info **nécessite consentement préalable** du patient, nécessite d'être expressément obtenu

Violation secret pro: sanctions pénales 1 an d'emprisonnement 15 000 euros d'amende

Pro de santé: obligation de **protection des données du patient car données de santé à caractère personnels transmises:**

données de santé=données à caractère perso=sensibles=infos permettant d'identifier 1 personne directement/ indirectement (N° de tel, empreinte digitale): donc TT et collecte interdit sauf certains cas définis par la loi

Respect de la loi informatique et liberté (6 aout 2004): but=cadre légal pour protection de l'individu et de sa vie privée face au risque lié au développement de l'informatique

Loi=définition des principes à respecter lors de la collecte, du TT et de la conservation de données perso, assure protection renforcée aux données de santé sensibles

Loi s'applique dès lors que données à caractère perso TT dans 1 cadre non perso

5 principes clés de la protection des données à caractères perso à respecter:

1. Finalité= personnes concernée doivent être informés de la manière dont seront utilisées les données
2. Pertinence= seules données nécessaire doivent etre collectés
3. Conservation=données supprimés des que l'objectif est atteint
4. Droits= accès, opposition, rectification sur leurs données
5. Sécurité+confidentialité des données à garantir

TT et collecte de la données de santé possible: utilisation dans l'intérêt direct du patient+pour des besoins de santé publique

- Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf disposition contraire prévue par la loi.
- Les traitements nécessaires à la sauvegarde de la vie humaine.
- Les traitements nécessaires au suivi médical des personnes, à la prévention, au diagnostic, à l'administration de soins ou de traitements, à la gestion de services de santé.
- Les traitements statistiques réalisés par un service statistique ministériel.
- Les traitements intervenant dans le cadre de la recherche dans le domaine de la santé.
- Les traitements a des fin d'évaluation ou d'analyse des pratiques ou des activités de soins de prévention.
- Les traitements justifiés par l'Intérêt public et autorisés par la CNIL.
- Si les données sont appelées à faire l'objet, à bref délai, d'une procédure d'anonymisation

Exploitation des données de santé à des fins commerciales interdites

C2I 2.6:sécurité des données de santé: mesures de sécurité à mettre en oeuvre

En tant que profesionnel de santé:protéger **des données de santé de nos patients.**

Sécuriser le lieu de travail:

- **sécurité physique du lieu d'exercice**: ouvertures (portes et fenêtres) sécurisées par 1 système d'alarme. Equipement informatique: pièce non accessible au public+sécurisée
- **sécurité poste de travail:** utiliser 1 mot de passe robuste + mémorisable: > ou = 10 caractères et 1 combinaison de caractères alpha numérique et spéciaux. MDP doit être changé régulièrement et utilisation des 3 MDP précédents interdites. MDP mémorisé et non accessible à 1 tiers. Ne doit pas être mémorisé sur ordinateur/ navigateur internet. Antivirus+pare-feu sur poste de travail à mettre à jour régulièrement. Pare feu=empêche des utilisateurs/des logiciels malveillants (ex:vers) d'accéder à notre ordinateur via internet / 1 réseau. MAJ régulière du système d'exploitation et des logiciels à effectuer. Utilisation uniquement de logiciels originaux certifiés, éviter versions piratées/copiées.

Maitrise des accès au poste de travail:

- créer 1 compte administrateur distinct avec MDP distinct du compte utilisateur.
- créer des comptes utilisateurs nominatifs pour chacun des professionnels de santé pouvant être amenés à utiliser le poste de travail.
- Accès au poste de travail doit être protégé en notre absence: activer mise en veille automatique en cas d'inactivité, déverouillage de l'écran veille s'effectue via 1 MDP.
- Protéger accès WIFI et vérifier que seuls nos ordis sont connectés au réseau
- Accès aux donnés patient via logiciel métier doit se fair via carte CPS
  carte CPS (Carte Professionnelle de Santé) =carte d'identité professionnelle électronique, possède 1 certificat d'authentification protégé par 1 MDP, ne peuvent être lu que par lecteur homologué. Permet au professionnel de santé de: s'authentifier, de se faire reconnaître quand il se connecte à 1 logiciel pour accéder aux données de santé, d'apposer 1 signature électronique pour garantir validité et intégrité des documents, de chiffrer des données pour garantir confidentialité des données échangées.

Carte CPS utilisé pour:

- transmission des feuilles de soins
- envoi de mails sécurisés
- consultation de DMP
- accès aux locaux d'1 établissement de santé
- connexion aux logiciels métiers

Tracabilité pour assurer sécurité du poste de travail: accès et actions réalisés dans le logiciel métier tracés

Evenements informatiques tracès: activer la fonction de journalisation du système d'exploitation

Sauvegarde des données patient: fréquente, sauvegarde à effectuer sur des supports différents, conserver supports de sauvegarde dans des lieux différents

C2I 2.7:chiffrement, sécurité et hébergement des données de santé

1°) les menaces informatiques

Comprendre la typologie des menaces —> mieux appréhender les enjeux de cybersécurité+mieux comprendre l'utilité des procédures mises en œuvre par les Directions des Systèmes d'Information (DSI).

1.1 La chaîne de contamination

La chaîne de contamination en informatique peut schématiquement être décomposée en 4 étapes :

1. **l'inception**=le premier contact, le moment où l'attaquant rencontre sa cible
2. **l'intrusion**= processus durant lequel l'attaquant pénètre le système.
3. **l'infection** =moment où le code malveillant est déclenché
4. **l'invasion**=l'étape finale où l'attaque se réalise.

Cette chaîne permet de comprendre les étapes clés de déploiement d'une stratégie de défense. Par exemple, la restriction de l'accès à certains sites internet à partir des navitageurs d'un hôpital est clairement une stratégie de défense s'intéressant à limiter le risque d'inception. D'autre part, les DSI définissent une liste restrictive d'applications autorisées afin de limiter le risque d'intrusion et d'infection.

1.2 Typologies des codes et des effets

Codes/**logiciels malveillants** ou **malware**= code développé dans le but de nuire à un système=regroupe un ensemble d'entités hétérogènes et souvent intriquées. Il n'existe pas de classification exhaustive et consensuelle. De plus, les catégories de codes malveillant ne sont pas exclusives, il arrive souvent qu'un code malveillant combine plusieurs mécanismes.

Les malware regroupent :

- les **exploit** =exploitent les failles de sécurité
- les **dialer** =composent des listes de numéro pour rechercher des cibles
- des **injections** de codes **SQL/URL**=injection de code malveillant au sein d'1 code sain
- les vers ou **worms,** des programmes/automates autoréplicatifs ne nécessitant pas de programme hôte
- les **virus,** des programmes autoréplicatifs nécessitant un programme hôte
- les **trojan** (cheval de Troie)= programme légitime modifié pour permettre d'introduire un code malveillant (charge utile).

Un cheval de Troie est un moyen d'insérer un autre code malveillant (la charge utile). Sans la charge utile, il ne fera rien.

Un trojan peut être décliné en plusieurs types selon la charge utile qui les composent :

- **spyware** =programmes ayant pour objectif la collecte et le transfert d'informations à l'insu de l'utilisateur.Les spyware peuvent également être de plusieurs types :
  - scumware= programmes se téléchargeant sans le consentement de l'utilisateur.
  - adware = programmes affichant de la publicité, pouvant être ciblée. Nous discutons ici des adware de type malware. En effet, des adware peuvent ne pas être des malware, c'est-à-dire qu'il peut s'agir de programme exécuté en toute connaissance de cause et dont la fonction commerciale est acceptée par l'utilisateur.
  - hijacker bho= programmes qui vont modifier les paramètres du navigateur web. Ici aussi, ce type de programme peut ne pas être des malware (par exemple la barre d'outils de Google).
  - keylogger= enregistreurs de frappes. Ils permettent de récupérer l'ensemble des saisies du clavier de l'utilisateur.Exemple : Les keylogger pour l'enregistrement des frappes =Ils peuvent prendre une forme logicielle (un malware) ou une forme matérielle. Certains keylogger sont de petits dispositifs que l'on peut poser discrètement sur les ordinateurs ou bien les dissimuler complètement dans les claviers. Ce mode d'attaque permet notamment de récupérer l'ensemble des mots de passe saisis par les utilisateurs d'un ordinateur. Ce type d'attaque justifie le fait de limiter l'accès physique aux ordinateurs et/ou de renforcer le mode d'authentification (avec une carte CPS par exemple).
  - stealware= programmes qui visent à transférer de l'argent ou des données à une personne tierce à l'insu de l'utilisateur. Par exemple, un malware cherchant à envoyer des données hospitalières à une organisation non autorisée est un stealware.
- **rootkit**= programmes permettant d'accéder furtivement à un ordinateur
- **backdoor**= programmes exploitant une fonctionnalité inconnue (mais légitime) d'un système
- **fork bombs**= attaques par déni de service reposant sur l'exécution d'un grand nombre de processus de manière à saturer les ressources disponibles d'un ordinateur ayant pour conséquence l'impossibilité d'exécuter de nouveaux processus. Par exemple, l'ouverture simultanée de plusieurs milliers de pages internet sur un simple ordinateur peut nécessiter une telle quantité de ressources que les programmes antivirus par exemple ne pourront plus s'exécuter normalement.

1.3 Hacking et lutte contre le code malveillant

Hacking = recherche et/ou exploitation de failles de sécurité informatique.

Dans la lutte contre le code malveillant, on peut vouloir rechercher des failles de sécurité sans pour autant les exploiter. La pratique du hacking est, dans une certaine mesure, une pratique saine dans une organisation si elle permet à une organisation de renforcer sa sécurité.

D'ailleurs, certaines entreprises recrutent des hackers pour renforcer leur sécurité. Chacun dans une organisation peut être amené à trouver des failles de sécurité. Il s'agira alors de les communiquer au responsable de la DSI afin qu'il puisse prendre des contre-mesures.

1.4 Métiers de la cybersécurité

L' agence nationale de la sécurité des systèmes d'information (ANSSI) en France a fait un panorama des métiers de la cybersécurité.(2)Parmi les différents métiers, citons ceux d'auditeur, de post-auditeur, d'opérateur, d'architecte de sécurité et d'expert des tests d'intrusion.

L'auditeur ou contrôleur recherche la conformité d'un système aux référentiels et étudie les vulnérabilités.

Le post-auditeur intervient sur sollicitation à la suite d'un audit, d'un incident ou d'une intrusion, prend la mesure de la situation et propose un plan de remédiation. L'auditeur fait de la prévention, le post-auditeur traite après un constat.

L'opérateur met en œuvre la politique de sécurité de l'information.

L'architecte de sécurité structure les choix techniques, technologiques et méthodologiques d'un ensemble répondant à des exigences de sécurité, en cohérence avec les activités équivalentes réalisées au niveau de la solution qui l'intègre.

Et enfin, **les expert des tests d'intrusion** (ou « hacker éthique ») pénètrent le système d'information (SI) et identifient les divers chemins d'intrusions, les techniques classiques ou atypiques utilisées, traçant ainsi le profil (profiling) des attaquants, leurs habitudes et méthodes de travail.

La cybersécurité regroupe donc un ensemble de métiers qui ne constituent pas les fonctions premières d'une structure de santé. C'est la raison pour laquelle les DSI font appellent bien souvent à des sous-traitant et se réfèrent à des référentiels de sécurité prévus pour ça.

Wannacry », l'attaque mondiale du 12 mai 2017

Le 12 mai 2017 un malware de type ransomware pénètre près de 420 000 systèmes dans le monde. Il exploite une faille de sécurité d'un protocole d'échange de fichiers de Microsoft. De ce fait, il a pu se propager à grande vitesse en passant par les réseaux.Wannacry cryptait les données d'un ordinateur et demandait une rançon pouvant aller de 300 à 600 dollars en échange d'une libération du système. Le paiement s'effectuant par cryptomonnaie (bitcoin), il n'était donc pas possible de retrouver l'attaquant.

Parmi les victimes de wannacry, on trouve les hôpitaux britanniques du NHS. Ce type d'attaque, nous alerte sur la vulnérabilité des structures hébergeant des données de santé.

2°) chiffrement et hachage

Concepts de base de cryptographie et les différents modes d'authentification utilisés couramment dans le monde de la santé.

2.1 Concepts de base de cryptographie

La cryptologie est « la science du secret » et est constituée:

- de la cryptographie qui s'attache à la protection du message
- et de la cryptanalyse qui s'attache à rompre cette protection.

Chiffrement	Hachage
Le chiffrement consiste à transformer, à l'aide d'une clé, un message en clair (dit texte clair) en un message incompréhensible. Si on dispose de la clé, on peut revenir au message initial. **Le cryptage ou chiffrement est réversible**. C'est **la base d'un échange protégé**/de manière secrète **d'informations entre deux personnes.**	**Le hachage, irréversible en théorie permet de transformer une information claire** de grande taille en pseudonyme, information de taille réduite (**en concédant une perte d'information** mais en garantissant l'unité du pseudonyme)(exemple transformer un identifiant en pseudonyme). . En pratique, certains algorithmes peuvent être « cracké » et on peut alors retrouver l'information a été transmise dans le hachage. Les fonctions de hachage cryptographique s'intéressent à compliquer le travail des crackers.

Le chiffrement peut être de plusieurs types: chiffrement symétrique, chiffrement asymétrique et chiffrement hybride.

- Le chiffrement symétrique repose sur une clé unique qui permet de chiffrer et de déchiffrer l'information. Le récepteur dispose de la même clé que l'envoyeur.
- Le chiffrement asymétrique repose sur deux clés : 1 clé pour chiffrer (clé publique) + 1 clé pour déchiffrer (clé privée). Le destinateur génère une clé publique associée à une clé privée. La clé privé ne circule pas et permet de déchiffrer le message tandis que la clé publique est envoyée à l'envoyeur. L'envoyeur chiffre son message avec la clé publique et l'envoi au récepteur qui le déchiffre avec la clé privée. Si la clé publique est interceptée par une tierce personne alors la sécurité du message ne sera pas compromise car il ne pourra pas le déchiffrer.
-Le chiffrement par clé de session consiste à utiliser une clé de session unique pour chiffrer et déchiffrer le message (chiffrement symétrique) mais en se transmettant cette clé de session par le biais d'un chiffrement asymétrique. En effet, le chiffrement asymétrique peut être compliqué lorsque le volume de données à chiffré est important. C'est donc uniquement la clé de session qui est chiffré par un chiffrement asymétrique. Cette clé est unique donc les risque d'attaque sont faibles.

2.2 Typologie et modes d'authentifications

Authentification =processus permettant au système de s'assurer de la légitimité de la demande d'accès faite par un utilisateur. La plupart des authentifications se font à l'aide d'un nom d'utilisateur et d'un mot de passe. Ce sont des authentifications faibles.

La sécurité d'une authentification repose sur le mode de preuve de l'identité de l'utilisateur. Ce mode de preuve peut être constitué de 4 types de données :

- ce que l'on connaît (ex : mot de passe)
- ce que l'on possède (ex : carte à puce)
- ce que l'on est (ex : empreinte biométrique) - ce que l'on sait faire (ex : signature).

Une authentification est dite:

- simple si la vérification se fait par un seul type de preuve (demande d'un mot de passe).
- forte si la vérification se fait par deux types de preuve ou plus. Ex: nom d'utilisateur, mot de passe et code généré de manière aléatoire par une carte à cryptogramme dynamique. Ainsi pour se connecter il faut apporter deux niveaux de preuve de son identité. Dans certaines structures de grande sécurité, il peut être demandé des niveaux de preuve plus importants comme des empreintes biométriques.

2.3 Application : les pseudonymes dans les bases de données médico- administratives

Les bases de données médico-administratives en France regroupent toutes les données de facturation relatives à la consommation de soins : données hospitalières du PMSI (Programme de médicalisation des systèmes d'information), données de dépenses de ville de l'assurance maladie obligatoire, données de mortalité du CépiDc. Outre leur objectif de facturation, ces bases permettent de réaliser un pilotage médical du système de santé et d'aider les chercheurs. Les données individuelles sont permises grâce à un identifiant (presque) unique : le NIR. Le NIR (en langage courant, le « numéro de sécurité sociale ») est un identifiant unique permettant de lier des données de santé avec le registre national des personnes physiques (RNIPP).

Pour des raisons de sécurité, le NIR ne peut pas apparaître tel quel dans les bases de données nationales. En effet, il serait possible reconnaître directement et sans difficulté un individu dans ces bases. L'idée est donc de le masquer sans perdre sa propriété d'unicité permettant de réaliser des chaînages d'informations dans le temps.

Il a donc été décidé de le hacher. On transforme donc un numéro identifiant en pseudonyme. C'est la pseudonymisation. Afin de transformer un identifiant en pseudonyme, 3 fonctions de hachage sont appliquées. Ces fonctions de hachage permettent de perdre l'information sensible du NIR tout en gardant ses propriétés d'unicité.

Le terme « anonymisation » est employé abusivement. Il s'agit d'une pseudonymisation. Il ne s'agit pas d'un numéro anonyme mais d'un pseudonyme.

2.4 Application : accès au PMSI national

L'accès à la base au PMSI national se fait via un navigateur web où on accède à un poste à distance. L'authentification est forte car elle se fait à l'aide d'un nom d'utilisateur, d'un mot de passe ainsi que d'un numéro généré toutes les 30s environ via une clé RSA (de la taille d'un porte clé).

3°) référentiels et hébergement des données de santé

Présentation du cadre général qui s'applique aux hébergeurs de données de santé=> comprendre la démarche globale qui découle.

3.1 Référentiels sécurité

Les référentiels de sécurité permettent de poser un cadre général permettant de limiter les risques d'attaques ou de mésusages du S.I. Les référentiels opposables dépendent du risque accepté par les structures.(3)

En santé, 3 grands référentiels sont à connaître :

1. Politique générale de Sécurité des Systèmes d'information de santé (PGSSI-S). ASIP.

2. Politique de Sécurité des systèmes d'information pour les ministères chargées des affaires sociales (PSSI-MCAS) (NOR:AFSZ1523362A)

3. Référentiel de sécurité applicable au Système national des données de santé (NOR:AFSE1705146A)

Ces référentiels décrivent les principes généraux que doivent respecter les SI. A titre d'exemple, le PSSI-MCAS exige que les structures hébergeant des données de santé proposent un plan d'analyse et de gestion des risques, une politique de sécurité des infrastructures et une politique d'accès au système. Le PGSSI-S exige un référentiel d'identification, un référentiel d'authentification et un référentiel d'imputabilité. L'imputabilité est une notion fondamentale dans la gestion des SI. Toute action sur un SI doit pouvoir être relié à une entité qui s'est authentifiée, doit pouvoir être horodatée et doit pouvoir être décrite. Ces actions sont archivées de manière pérenne.

Récemment, le référentiel du Système national des données de santé (SNDS) a été publié de façon à clarifier le cadre permettant l'hébergement et l'accès aux données. Il aborde des points essentiels comme :

-L'intégration d'une démarche qualité : tous les systèmes du SNDS doivent être périodiquement contrôlés dans le cadre d'audits internes et d'audits externes

-tout projet ayant un impact sur la sécurité d'un système du SNDS doit donner lieu à une revue de l'analyse de risques du système concerné.

-un dispositif de journalisation des requêtes des règles de surveillance et de détection.

3.2 L'hebergement des données de santé

Le cadre réglementaire des hébergeurs de données de santé a changé avec la loi de modernisation du système de santé. L'ancienne approche reposait sur la constitution d'un dossier pour une demande d'agrément. Cette démarche fixait un cadre solide pour les hébergeurs de données de santé mais reposait sur une démarche purement française. L'union européenne a incité la France à s'aligner sur une approche internationale de certification.

3.2.1 Avant la loi de modernisation du système de santé

3.2.1.1 Notion d'hébergeur de données de Santé

L'hébergement des données de santé est encadré par le décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique (NOR:SANX0500308D). Il dispose que « toute personne physique ou morale souhaitant assurer l'hébergement de données de santé à caractère personnel (...) :

- Offrir toutes les garanties pour l'exercice de cette activité (...)
- Définir et mettre en œuvre une politique de confidentialité et de sécurité ».

Ce cadre s'applique donc à toute structure hébergeant des données de santé : hôpitaux, administrations, agences, entreprises etc.

3.2.1.2 Procédure d'agrément et Composition d'un dossier de demande d'agrément

CAH : Comité d'Agrément des Hébergeurs de données de santé

La procédure d'agrément (4) dure officiellement 6 mois. Elle consiste à déposer un dossier auprès de l'ASIP (Agence des Systèmes d'Information Partagés de Santé).

Le dossier d'agrément est composé de 3 parties : un dossier administratif et financier, un dossier technique et les modèles de contrats. Le volet administratif comprend : l'identification du demandeur, le lieu de l'hébergement, l'identification des sous- traitants et la description du service et des comptes prévisionnels. Le volet technique comprend : la garantie du respect des droits des personnes, la garantie de la sécurité de l'accès aux informations, la garantie de la pérennité des données hébergées, l'organisation et procédures de contrôle interne. Le volet regroupant les modèles de contrats permet de s'assurer du bon fonctionnement juridique entre les acteurs, notamment des prestations proposées par l'hébergeur.

3.2.1.3 Médecin de l'hébergeur

La présence d'un médecin dans l'organisation d'une structure d'hébergement de données de Santé est obligatoire. Ce médecin doit être inscrit à l'Ordre des médecins.

Le « médecin de l'hébergeur » doit être lié contractuellement avec celui-ci, mais il n'est pas obligatoirement un salarié de l'entreprise. Le contrat peut être un contrat de prestation de service, dès lors qu'il existe des clauses d'interdiction d'exercice d'activités incompatibles (médecin des assurances, médecin du travail). Il n'y a pas de cadre réglementaire sur les missions qui lui sont attribuées mais le conseil de l'Ordre propose un contrat cadre. Les deux missions qui lui sont attribuées : garantir la confidentialité des données personnelles et vérifier sur demande la cohérence des données personnelles de santé en cas de suspicion de collision ou de doublon

3.2.1.4 Quelques hébergeurs agréés

La liste des hébergeurs agréés ainsi que le cadre de leur agrément est disponible sur le site de l'ASIP: APHP, OVH, Carestream.

3.2.2 Après la loi de modernisation du système de santé

3.2.2.1 Contexte de la mise en place de la certification

Le cadre réglementaire des hébergeurs de données de santé a été modifié par l'article 204 de la loi du 26 janvier 2016 et l'ordonnance n°2017-27 du 12 janvier 2017

Il a été décidé de « remplacer l'agrément prévu au même article L. 1111-8 par une évaluation de conformité technique réalisée par un organisme certificateur accrédité par l'instance nationale d'accréditation »

3.2.2.2 Certification

La certification repose sur une démarche d'évaluation de conformité technique par des organismes de certification accrédités par le Comité français d'accréditation (COFRAC). Deux certificats ont été créés :

- Hébergeur d'infrastructure physique
- Hébergeur infogéreur

Le certificat d'hébergeur d'infrastructure physique concerne les locaux et l'infrastructure matérielle du SI de Santé. Le certificat d'hébergeur infogéreur concerne : la plateforme logicielle, l'infrastructure virtuelle, l'infogérance et les sauvegardes externalisées. On observe une distinction hardware/software qui nous rappelle la dualité de la sécurité des SI.

La procédure de certification se fait en deux étapes : un audit documentaire puis audit sur site. Elle s'apparente aux démarches de certification que l'on observe par ailleurs pour les établissements de santé. Les certificats sont attribués pour une durée de trois ans et les infrastructures sont auditées tous les ans.

Le référentiel de la certification est par ailleurs clairement affiché, il comprend notamment les normes :

- ISO 27001 « système de gestion de la sécurité des systèmes d'information »
- ISO 20000 « système de gestion de la qualité des services »
- ISO 27018 « protection des données à caractère personnel »
- ISO 27017 « code de pratique pour les contrôles de sécurité de l'information

fondés sur l'ISO/IEC27003 pour les services du nuage ».

Les principes sous-jacents à la certification sont de disposer de normes internationales, homogènes et d'inciter les structures à s'inscrire dans une démarche qualité et d'amélioration permanente.

L'importance des données de santé et les menaces informatiques pesant sur les SI obligent à disposer de structures agréées respectant les référentiels de sécurité et disposant de technologies d'authentification et de chiffrement non obsolètes.

Le passage d'une procédure nationale d'agrément à une démarche internationale de certification a pour effet de clarifier les exigences technologiques vis-à-vis des demandeurs et en même temps d'augmenter la sécurité des SI

COURS 3: SUPPORTS NUMERIQUES DE LA PRATIQUE CLINIQUE

C2I 3.5: représenter numériquement l'information médicale

Représentation des infos médicales **sous forme de données numériques:** description numérique d'1 situation clinique dans 1 procédure de SAD

1. Transmission numérique de l'info médicale
   >langage naturel: ambiguité, imprécision, variantes pour exprimer la même chose, connaissances implicites
   >utilisation par 1 ordinateur:
   ****sous forme textuelle=communication interhumaine mais peu adapté au TT automatique par ordinateur** du langage naturel (traduire, corriger orthographe, recherche et extraction d'info), pas les propriétés formelles requises pour le SAD, pas sous forme de paramètres décisionnels
   **sous forme de variables décisionnelles (HTA confirmée=oui, tabagisme=non) utiles à la décision, différents selon les logiciels d'aide à la décision et selon le type de décision à prendre—>pas de représentation unique
   Saisir manuellement: par 1 opérateur humain
   Obtenir info directement sous forme numérique: balance connectée
   Calculer, déduire des données de données déjà numérisées: IMC
   Réutiliser des données existantes déjà disponibles, parfois dans d'autres dossiers patients
2. Importance de la structure et du codage
   Information numérique sous forme de données adaptée au TT automatique informatique mais doit être:
   > Structurée: rangement des données dans des rubriques différentes, chaque info doit être datée
   > Codée: interface utilisateur—>champ contraint dans les paramètres de saisie (attention de ne pas se tromper dans la saisie)
3. Interopérabilité dans 1 environnement interconnecté
   Différents systèmes de TT de l'info doivent « parler la même langue »= INTEROPERABILITE= capacité que possède un produit ou un système dont interfaces intégralement connues, à fonctionner avec d'autres produits/systèmes existants ou futurs et ce, sans restriction d'accès/ de mise en oeuvre
   Capacité des logiciels à fonctionner ensemble et à **échanger/partage des données** sans perte

Reposent sur des conventions fixées par des normes/des standards=référentiels auxquels on doit se référer

3 niveaux d'interopérabilité qui requièrent que le niveau du dessous soit ok:

- **technique**= capacité des systèmes à communiquer sans se soucier du type d'infos à communiquer (différents types de prise électrique)- protocoles SMTP pour mails—>standard d'internet
- **syntaxique**=capacité des systèmes a reconnaitre type d'info échangés. Convention de codage de bas niveau. 101= pas le même sens selon système utilisé. Codage différent des accents, sens de lecture. Structure des infos échangées pour convenir du rôle des différentes infos:date(03/12/2016=3 décembre 2016 ou 12 mars 2016), adresse, formats spécifiques d'image—->**HL7** (Health Level 7):CD1 R2, FHIR; **ASIP santé CI-SIS**, DICOM(image médical) dans le domaine de la santé
- **sémantique**= capacité des systèmes a comprendre l'info: reconnaitre, la traiter de manière identique, en partager la signification avec l'utilisateur.Mot employé parfois non suffisant pour comprendre 1 notion. S'accorder sur notion à utiliser—>normalisation terminologique (hypertension artérielle, HTA, hypertension). Ensemble de termes synonymes de la même notion. Info codée dans 1 système ne doit pas être ambigué==>codage avec 1 identifiant unique, libellé et définition en langage naturel. Besoins de référentiels (différents selon le type d'infos):
  terminologie=ensemble de termes définis utilisés dans 1 domaine
  thesaurus=ensemble de termes normalisés+contrôlés, organisation conceptuelle d'1 domaine
  Nomenclature, taxonomie, classification=organisation, structurée, des notions d'1 domaine
  ontologie: modélisation conceptuelle/formelle d'1 domaine
  —->HL7 et ASIP
  —>**CIM-10** (OMS), CISP2, SNOMED CT, LOINC, DCI (OMS), CCAM, **HeTOP.**

  CIM-10 (équivalent anglais= ICD10)
  21 chapitres couvrant éventail complet des états morbides classés par organe/appareil fonctionnel
  organisation hierarchique: du + général au + spécifique
  Codage PMSI: dg principal+dg associés
  Selon le contexte: K du sein codé différemment en CIM-10 (Dg, ATCD perso ou ATCD personnel)—>se fait naturellement dans les applications.

C2I 3.6:les modèles pour l'aide à la décision

situation clinique décrites sous forme de données=Pb a résoudre TT au moyen de modèles
exploitation par le module de TT (modèles probabilistes, statistiques, basé sur les recos…)

1. calculs simples
   simple=facilement mis en oeuvre par programmes informatiques, codés par des algorithmes mathématiques bien définis:calculs
   >issus de formules totalement définis (ex: formule de l'IMC, formule pour la Cl de la creatinine)
   >calculs de scores médicaux
   >calculs basés sur des tableaux à entrées multiples
   ==>nouvelles données importantes pour la pratique clinique: utilisent données codés
2. modèles numériques
   Modèles manipulant des données numériques au moyen de calculs: statistiques, probabilistes
   Modèles prédictifs
   >méthode probabiliste basé sur Theoreme de Bayes (blablabla)=estimation de risque d'événements particuliers, dg « Dx plain «
3. modèles à bases de connaissance basé sur des approches logico-symbolique
   intelligence artificielle+informatique
   reproduction du raisonnement humain ; modélisation sous forme symbolique
   >**Base de faits**=ensemble de données connues décrivant la situation=données patient=varie selon cas clinique des patients. Enrichie au fur et à mesure par des données déduites à partir des règles.
   >**Base de connaissance=compétence d'1 système expert**=représentation symbolique des connaissances modélisée, dans différents formalismes distincts du langage naturel, compris par des programmes: règles de production, arbres de décision, réseaux sémantiques…
   Règles de production= utilisé pour expliquer+donner aux utilisateurs traces
   1.Prémice=condition suffisante à la conclusion
   2.Conclusion
   >**Modèles d'inférences=**programmes qui articulent les connaissances de la base des connaissances en f(données de la base de fait)=réalisent TT logico-symbolique: explosent base de connaissance en utilisant infos de la base de faits. Ajoute de nouveaux éléments dans la base de fait à partir des raisonnements effectués. 1 même moteur d'inférence selon la base de connaissance utilisée=>résultats différents. 3 sortes d'inférences logiques: déduction, induction(à partir de faits—>règle), abduction(à partir de règle et fait)
   Ex de la Déduction:
   Ex de règle: Si céphalée+raideur de nuque+nausée dans la base de faits=Sd méningé
   Si PL anormale+sd méningé=Méningite

Après engouement dans les années 80, systèmes experts critiqués: faible performance pour les situations réelles, médecin ont l'impression d'être exclu du raisonnement médical, que choisir comme source de connaissance?==>non utilisé en routine clinique.
EBM=> guides de bonnes pratiques, de recommandations dans des situations cliniques répertoriés=référentiels de bonne pratique professionnel
Construction de système d'aide à la décision fondé sur des recommandations professionnelle= objectivité source de connaissance mais difficulté traduire reco sous forme textuelles/tabulaires/algorithmiques traduites dans des formalismes compatibles avec SAD (sous forme de règles), cela sera limité aux connaissances des reco (pas de conseils au delà des reco elles mêmes)
Modalités de mise en oeuvre des SAD:
Système passif: doit être sollicité par l'utilisateur ou système actif: toujours en fonctionnement
Approche automatique: actif ou passif, nécessite données codés, SAD automatiquement ,asynchrone (alerte/reminders).
Approche documentaire: passif, à la demande, codage d'infos sous forme de donnés non nécessaires, réalisés lors de l'utilisation documentaire du système, utilisateur navigue dans les bases de connaissance.
Approche mixte: les 2

3.7
3.8
3.9
3.10

COURS 4:MAITRISER L'INFORMATION NUMERIQUE

C2I 4.1:savoir faire une recherche bibliographique pubmed

Médecine fondée sur les preuves= intégrer expertise praticien+besoins et demandes patients+données **les + actuelles** de la science issues de la recherche

1. formuler clairement question clinique
2. recherche de publications pertinentes dans la littérature médicale
3. analyse critique des résultats retenus
4. application au patient des résultats retenus

Meilleures types d'études répondant à la question:
niveau de preuve des études en f(qualité méthodologique)
Pyramide de preuve=classe littérature de synthèse > études individuelles :
Les + hauts niveaux de preuve:

- **essais contrôles randomisés** (fait partie des études individuelles):efficacité et tolérance d'1 TT, repartition aléatoire en 2 groupes: TT evalué et TT de référence/placebo
- et revues systématiques (littérature de synthèse)=regroupent toutes les etudes individuelles répondant à 1 question précise puis synthèse (si synthèse statistique=méta analyse)

==>Synthèse pour palier à ces contraintes: revues systématiques, Guides de bonne pratique, documents pédagogiques, ouvrages médicaux mais ne peut pas prendre en compte les données les + récentes
Medline: littérature biologique+biomédicale, anglais, principal base de données= accès via pubmed (résumé des articles en accès libre sous forme résumé) et via ovidmedline (payant)
Sur Pubmed:Filtrer en utilisant menu à gauche de l'écran=type d'article, mode d'accès (total, abstract), date de publication
Nb exponentielle de publications dispo qq soit recherche effectuée
Moteur de recherche avancée
Terminologie Mesh=anglais=thesaurus de mots clés, s 'appuie sur système medline pubmed.Recherche sur pubmed: Mesh a introduit or/and/not.
Accès a la terminologie Mesh: sur pubmed en sélectionnant Mesh au lieu de pubmed.
Traduction Mesh en français: sur portail INSERM.
HeTOP=portail en libre accès—>synonyme K du sein en francais+en anglais
Dans Pub med: Medline ne répertorie pas tout les journaux, seulement les + importants
doi: identification unique de chaque article, pas spécifique aux journaux biomédicaux=> se référer aisément à l'article lors de bibliographies
dans l'ordre chronologique
PMID: identification unique PUBMED
Auteur donnés dans un ordre précis en f (contribution): 1er et dernière place=ceux qui ont contribué le +
KEYWORDS: termes MESH pour indexer la publication

C2I 4.2:savoir faire une recherche bibliographique sur des autres moteurs de recherche que pubmed

- Cochrane Library: collaboration cochrane=Organisation indépendante ONG, 6 bases de données dont la principale=collection des revues systématiques de la collaboration Cochrane=> EBM. Revues systématiques sur efficacité des interventions en santé. Amélioration+diffusion de protocoles sur méthodologies des revues systématiques. Accès gratuit (grand public) / payant pour les revus complète (université). Anglais++

CDR:base de revues systématiques cochrane.
DARE:base de revues systématiques hors Cochrane.
CENTRAL: registre cochrane des essais contrôlés
CMR: registre méthodologique cochrane
HTA: registre évaluation technologies liées à la santé
NHS EED:régistre évaluations économiques à travers le monde destiné particulièrement aux décideurs en santé
Recherche simple: taper sur la base de recherche
ADVANCE SEARCH: + spécificités à 1 recherche simple
par thème (browse), par groupe de revue, trials (essais contrôlés)
Recherche MESH

- Google Scholar:moteur de recherche **académique** de Google, recherche dans les journaux académiques et la littérature, permet de créer sa propre bibliothèque en ligne accessible à partir de n'importe quelle ordi connectée, citations personnelles, alertes personnalisées.Accès à la littérature grise= instance publique, commerciale, industrielles, hors cercles privés, ex=les thèses appartiennent à la littérature grise. Classement par les + vues. Donnés le nb de citations par article. Suivi des profils google scholar.

C2I 4.3:publier à l'ère du numérique

Toute recherche doit être publiée car sinon ca sert à rien:

- faire valider intérêt travaux et leur qualité scientifique
- diffuser résultats des recherche
- archiver connaissance scientifique
- evaluation par ses tuteurs
- etre reconnu par ses paires
- obtenir contrats+crédits

Processus de publication d'1 recherche:

- choisir auteurs articles: doit avoir joué 1 role substantielle, doit avoir écrit/participer, doit approuver version finale, doit assumer responsabilité du contenu. Choisir ordre des auteurs selon importance de chacun= 1 er (le + important,junior) et dernier auteur(senior).
- ecrire article
- soumission à 1 revue: éditeur capital=lui qui sélectionne article pour publication. Chaque revue a 1 ligne éditoriale. Choix d'experts pour évaluer travail: article intéressant? nouveau? valide scientifiquement? apport? . Editeur gere échange entre pairs et auteurs pour répondre aux questions des pairs. Editeur met ensuite en forme l'article selon les standards du journal.

Productivité augmenté: diminution des délais (d'échange et de publication)
Plus de périodique==>continuum.
PLOS ONE=pas de ligne éditoriale: que si valide scientifiquement.
Evaluation chercheur passe de + en + par évaluation quantitative de leur publication, prestiges revues, position auteur=visibilité auteur dans la communauté scientifique:pas possible avant l'ère du numérique
Facteur d'impact=permet de quantifier prestige d'1 revue: ratio faisant émerger revues centrales d'1 domaine scientifique: les + prestigieuses=IF le + fort==>domaines émergents et ceux qui déclinent=outils pour allouer budjets + evaluation individuelle du chercheur.
IF=visibilité d'1 revue=nb moyen de citations recues pour les articles publiées d'1 revue sur une année/nb articles citables publiés sur la même année.
NB de citations établies sur la base du moteur de recherche Web of science: tous les articles de 11 000 revues mais pas toutes les revues sur Web Science==>on peut calculer IF que si revue appartient à Web Science.
JAMA: IF=37.7
IF sous estime l'importance des articles les + cités et sur estime l'importance des articles les - cités.
Sur la page d'accueil des revues et dans journal citation reports: IF
Points SIGAPS d'1 chercheur=que pour chercheur travaillant dans hôpital (public/privé) francais: synthèse production scientifique d'1 chercheur. Chaque revue=catégorie=percentile de l'IF dans sa discipline (A=le meilleur percentile —> E).
Ne pas pénaliser les disciplines avec IF les + faibles car disciplines non égales en terme d'IF. Interrogation SIGAPS de pubmed puis chercheur valide manuellement si c'est bien ses articles. Coefficient de 1 à 4.
SIGAPS font gagner de l'argent aux hopitaux.
dotation globale—>paiement à l'activité: sejour facturé selon acte et pathologie + recherche/enseignement qui a un financement spécifique.

C2I 4.4:outils de gestion des références bibliographiques

Intérêt d'utiliser logiciel de gestion de bibliographie

Bibliographie: articles font souvent référence à d'autres articles ou d'autres ouvrages—>données détaillés à la fin de l'article pour les retrouver.
Plusieurs formats de citations (n° par odre d'apparition entre crochet/par ordre alphabétique du nb du 1er auteur+date de publication)/de bibliographies—> risque d'erreur, travail à refaire si format doit être changé (ex: format donné d'1 revue donné)
Logiciels dispo: 3 principaux concurrents et beaucoup d'outsiders
Endnote=payant non libre
Mendeley=gratuit non libre
Zotero:gratuit + libre (modification et duplications autorisées)

Zotero

2 possibilités pour l'installer: extension du navigateur firefox+pluggin de l'éditeur de texte **OU version autonome**+extension pour navigateur web préféré
Logiciel multiplateformes= versions MAC, LINUX, WINDOWS…, applications pour tablette smartphone
ENtrer manuellement nom d'auteur, nb de l'article, année de publication=longue, fastidieuse, pas de contrôle du risque d'erreur
Entrer: PUBMED ID (n°) via interface zotero, depuis l'extension d'1 navigateur disposant de zotero en consultant un site supporté (la + rapide)
Insertion de références dans 1 document texte (word/libre office): zotero add edit, style de citation (spé à chaque revue). On peut citer 2 ouvrages dans la même citation.
Insert bibliography
Refresh: renuméroter si on a changé l'ordre des références (3 avant 2)
Bibliothéque: dossiers, sous dossiers=hiérarchisation
TAGG
Sauvegarder texte intégral et métadonnées
Synchronisation des références sur plusieurs terminaux en créant 1 compte gratuit sur zotero

C2I 4.5:mettre en oeuvre une veille scientifique

Indispensable pour tout médecin: Pour la formation continue car médecine en constante évolution=rester informer sur dernières actualités sur thème précis.

Stratégies Pull/push d'accès à l'information

- **PULL: aller régulièrement à la recherche de nouvelles infos sur des sites web.** Prend du temps, parfois sites non MAJ. Page web standard (format HTML):contenu graphique, non aggrégation.
- **PUSH: info vient à nous.** Si 1 site publie 1 article/1 actualité==>on en est automatiquement informé. Pas de perte de temps à chercher l'info.

Rester vigilant sur qualité info: sources institutionnelles, certification HON.

Ne pas passer trop de temps sur veille scientifique=chronophage.

Canal mail/newsletter, listes de diffusion, alertes

- Alertes mails= proposés par certains sites (PUBMED, GOOGLE SCHOLAR, WEB OF SCIENCE, nb blocs/sites de presses/sites institutionnelles)—>Maintenir à jour 1 bibliographie.
- Newsletter: envoi régulier d'1 mail avec fréquence définie à la base: reprend l'ensemble des dernières actualités publiés depuis le dernier envoi. Ensemble des dernières actualités depuis le dernier envoi.

Génération automatique par 1 serveur, lien de désabonnement.

- LIMITES DE ces 2 modes de veille: submergés par mail pollution boite de réception—>message automatiquement redirigé vers dossiers. Attention à l'espace de stockage du serveur mail: parfois très nombreux. Surveillance du dossier courrier indésirable, parfois catalogués comme SPAM.

- Listes de diffusion=mode de communication qui s'apparente aux alertes mails: inscription préalable, génération automatique mais source d'infos non unique—>ensemble des membres (dans 1 service hospitalier, dans 1 institution par ex). On peut modérer une liste de diffusion: relecture avant envoi

Flux RSS/aggrégateurs de flux

Flux RSS= Real Simple Syndication=**aggrégation** simplifiée de l'information

Liste de sites/de blogs publiant régulièrement des articles qui nous intéressent par stratégie PUSH:

- abonnement aux flux
- aggrégation: ensemble des abonnements arrivent au même endroit, consultation d'ensemble des nouveautés sur des domaines différents au mêmes endroits.

FLUX RSS: langage XML, adresse différente, rendu austère, consultable de manière automatique par 1 agrémenter de flux—>Sites de presse, revues médicales, INVS, Pubmed (à partir d'1 recherche pubmed: création d'1 flux PERSONNALISE basé sur les résultats de MA recherche)

Pour lire ces flux:

1. logiciel dédié: tiny tiny RSS
2. navigateur web (rendu austère, pas optimable)
3. client de messagerie mail+abonnement à des flux RSS (outlook, thinderbird sur « nouveau compte:blog et nouvelles »)
4. portail web personnalisable utilisable en page d'accueil(Netvibes): agrégation de plusieurs flux en onglets/marque-pages=créer 1 compte, ajouter 1 adresse de flux RSS au dashboard.

EN bas/en haut: logo orange=flux RSS

Autre canaux

Sites de Microblogage: Twitter, viadeo, linkedin, FB

Inscription, réutilisations de données

Suivi d'1/plusieurs utilisateurs (des veilleurs) qui publient régulièrement des infos==>profiter du travail des veilleurs mais identifier les bons veilleurs

Forums de discussions mais aucun contrôle sur qualité infos: poser 1 question, en appeller à la communauté pour répondre aux questions—>Alertes mails pour savoir si réponse

Application médicales: Medpics=échanges autour de cas cliniques partant d'1 iconographie mais participations non modérées et qualité info pas sure.

Formation continue

=obligation pour les médecins:

- veille informationnelle
- portail unf3s.org= rassemble contenu pédagogique+médicaux provenant de plusieurs universités=>maintien à jour des connaissances médicales (université virtuelle)
- plateformes de MOOC (FUN=France université numérique, Coursera)

C2I 4.6:propriété intellectuelle et plagiat

Législation sur les oeuvres numériques

1. Protection des oeuvres

   En France: droit d'auteur=droit moral (reconnait paternité auteur et intégrité oeuvre)+droit patrimonial(auteur/héritier rémunéré pour chaque utilisation d'1 oeuvre)

   Code de la propriété intellectuelle

   Oeuvre protégé du seul fait de leur création mais preuve peut être déposé auprès d'1 huissier de justice: oeuvre doit être formelle, on ne peut pas protéger 1 simple idée

   Oeuvre tombe dans le domaine public 70 ans après la mort de l'auteur (droit patrimonial tombe): utilisation libre à condition de respecter droit moral

   Pays anglosaxons: copyright, ' tout droit réservé'=rôle informatif mais en France aucune valeur juridique.

2. Plagiat

   Laisser croire qu'on est l'auteur d'1 oeuvre en empruntant son oeuvre à 1 autre personne.

   Contrefacon=délit: ressort du droit et des tribunaux

   fautes déontologiques et éthiques liés au plagiat:INSTANCES UNIVERSITAIRES=sanctions disciplinaires

   Bibliothèques électroniques avec accès internet facile=>risque accru de plagiat

   Omission de citer source d'ou sont tirés infos

   Auto plagiat=répandu dans recherche biomédicale=double publication (1 même travail pour la validation de 2 diplomes différents par ex), saucissonage de résultats dans différentes publications, réutilisation d'1 texte, copyright

   Paraphrase=modifié qq mots du texte original/les substituer par 1 synonyme, citer source sans mettre entre guillemets

   1 des conséquences du plagiat=diminution de la capacité de réflexion nécessaire au dev des connaissances, contresens, déformation…

   Prévention plagiat:

   >Universités mise à dispo des enseignants: logiciel de détection du plagiat= détection des copier coller « compilatio magister »

   >Charte anti-plagiat

   Causes plagiat: manque de temps, ignorance risques encourus, faire comme tout le monde

   Plagiat= souci principal des grandes revues médicales, utilisation systématique de logiciels de détection du plagiat lors de la soumission d'article avant même de décider si article scientifiquement intéressant ou non

   Conférence européenne tous les 2 ans sur le plagiat dans l'enseignement sup.

Cours 5 : collaboration numérique en santé

Séquence 1 : Les outils numériques collaboratifs

Travail coopératif = travail divisé en plusieurs tâche, réalisation des tâches indépendamment par chacun (le médecin prescrit, me pharmacien délivre, l'infirmier administre)

Travail collaboratif = effectué par plusieurs sans découpage en tâches individuelles (chaque acteur échange et partage sur ce qu'il fait et ce que font les autres, en toute transparence) ; modèle centré patient, suppose communication

-> en santé il faut maintenant passer d'un travail collaboratif à un travail coopératif

Outils génériques permettant la collaboration : 2 dimensions
- utilisation synchrone (= les utiliser au même moment ; ex de synchrone à distance : chat, téléconférence, vidéoconférence, téléconsulation; ex de synchrone avec unité de lieu : parole) / utilisation asynchrone (ex : email, liste de diffusion, forums, flux RSS, organisation de réunion, wikis, plateforme de formation à distance)
- utiliser au même endroit / à distance

Outils de la bureautique collaborative : interagir à plusieurs sur un même document
- mode asynchrone = suivi des modifications
- synchrone = travail à plusieurs sur le même document (Google document de la suite Google drive par exemple)
- outils de type Google, Facebook etc non conseillés dans le domaine de la santé (protection des données)

Outils spécifiques à la santé

Doodle : permet d'organiser des réunions, gratuit
- planification de l'évènement
- proposition des dates
- choix d'une invitation simple (oui/non) ou avec des critères plus fins (oui/ non/si nécessaire)
- envoie d'une invitation : liste des destinataires -> invitation via Doodle / URL de l'invitation à la liste des participants sans utiliser Doodle
- à la réception de l'invitation : cocher oui/non/si nécessaire +/- commentaires
- quand toute les réponses sont reçues : tableau où figurent les dates possibles et les dates impossibles -> voix de la date et l'heure qui maximise le nombre de participants

Séquence 2 : Du colloque singulier à la médecine de parcours

Nécessité de changement d'organisation des soins car épidémiologie : vieillissement de la population :
- maladies chroniques, polypathologies, polymédication
- prise en charge plurielle (différents intervenant), pluri professionnelles, pluri sectorielle (secteurs sanitaire, médico-social, social)

Mutation des pratiques médicales -> *loi dite de modernisation du système de santé du 26 janvier 2016* : 3 axes
- prévenir et agir sur ce qui influence la santé
- organiser les soins autour du patient et révolution du premier recours
- démocratie sanitaire et déconcentration

Objectif : mettre en place une médecine de parcours en échangeant/partageant, se coordonnant/ collaborant pour assurer continuité et qualité des soins

ASIP = Agence Nationale des Systèmes d'Information Partagés de Santé : créée en 2009, sous la tutelle du Ministère de la santé (DSSIS = Délégation à la Stratégie des Systèmes d'Information de Santé)

- favoriser le développement des systèmes d'information partagés dans les secteurs de la santé et du médico-social
- promotion des TIC au service de la coordination des soins
- pertinence et qualité des soins dans le respect des droits de malades
- veille à l'inter-opérabilité, la cohérence avec la stratégie globale et les conditions de sécurité de tous les projets assurant le partage et l'échange des données de santé
- espace de confiance autour duquel s'articulent le DMP, le cadre d'inter-opérabilité, les référentiels de sécurité, la messagerie sécurisée de santé

Séquence 3 : La messagerie sécurisée

Objectif : garantir la sécurité et la protection des données personnelles échangées afin de protéger la responsabilité des professionnels de santé

loi dite de modernisation du système de santé du 26 janvier 2016 : reconnait la même valeur à l'écrit sur support papier et sur support électronique sous deux conditions

- identification du patient et authentification des producteurs de l'information
- intégrité garantie (c-a-d pas modifié depuis sa création) du procédé retenu pour établir/ conserver le document

Messagerie électronique

- expéditeur -> opérateur 1 -> client de messagerie -> contact du premier **serveur de messagerie** = serveur expéditeur -> message au serveur destinataire
- le destinataire veut accéder au message : client de messagerie d'un opérateur 2 -> requête au serveur destinataire -> lui transmet ses messages
- il existe une « liste blanche » des opérateurs référencés qui ne peut être altérée

—> la plupart des clients de messagerie interrogent régulièrement le serveur de messagerie : le destinataire n'a pas a suivre toutes ces étapes

Si non sécurisée :

- opérateur 1 -> email au service expéditeur -> email au destinataire
- pas de contrôle pour vérifier que le nom de domaine existe et est associé à un serveur de messagerie -> si le domaine n'existe pas : message d'erreur
- pas de contrôle pour vérifier l'origine du mail quand le destinataire le reçoit : il peut avoir été intercepté et modifié

MMSanté = système de messagerie sécurisée élaboré par l'ASIP en collaboration avec la CNIL

- identification des utilisateurs par un certificat électronique d'identification adossé à un annuaire (=RPPS) et une authentification forte (=carte CPS ou autre).
  - RPPS = Répertoire partagé des Professionnels de Santé (arrêté du 6 avril 2009) : répertoire unique identifiant les professionnels de santé, inaliénable et opposable
  - numéro RPPS attribué à chaque professionnel de santé
  - pour obtenir un numéro : site du RPPS hébergé par le CNOM (Conseil National de l'Ordre des Médecins) et documenter ses infos
- doit répondre à la Loi Informatique et Liberté : respect des règles de conservation des messages et de leurs traces
- avantages : échanges plus rapides, annuaire quotidiennement actualisé, responsabilité professionnelle protégée, droits des patients garantis

Séquence 4 : Le dossier médical partagé (DMP)

Mise en place :
- 2004 (avec ouverture en 2007): *dossier médical personnel* : numérique, support de coordination, respecte les droits des patients (accès à leurs information, sélection des professionnels de santé pouvant y avoir accès) —> échec car non opérabilité du dispositif au niveau national
- 2009 : relance du DMP et création de l'ASIP —> non convaincante
- 2013 : relance par Marisol Touraine d'un DMP de 2è génération : *dossier médical Partagé*, acté par la *loi dite de modernisation du système de santé du 26 janvier 2016*

- limites :
  - le DMP ne peut être créé que par les assurés sociaux en leur nom (et pas les ayant droits) -> 1,5% des français disposent d'un DMP en 2016
  - le DMP peut être créé par le médecin mais prend beaucoup de temps : explications à donner au patient, recueil du consentement
  - nombreux DMT vides

—> la CNAMTS a réalisé les développements techniques qui permettront au bénéficiaire de créer lui-même son DMP (via son compte Ameli); versement dès la création des DMP de l'historique des remboursements (liste sur 12 mois de tous les soins permettant la vérification des interactions médicamenteuses, des médecins consultés) pour qu'il n'y ait plus de DMP vide; versement des CRH

La création et l'accès au DMP:
- le DMP peut être créé par le patient, le médecin, le préposé à l'accueil dans l'établissement de santé, l'agent des organismes d'assurance maladie obligatoire, après recueil du consentement du patient
- seuls les professionnels de santé autorisés ont accès au DMP, autorisation acquise au sein d'une équipe de soin (un médecin de l'équipe peut avoir accès au dossier sans y être expressément autorisé, sauf si le patient s'y oppose), nécessité de l'autorisation du patient pour qu'un médecin hors de l'équipe de soin ait accès au dossier

- le patient
  - peut accéder à son DMP sur internet
  - ne peut pas s'opposer au versement des informations utiles à sa prise en charge dans son DMP
  - peut masquer certaines informations qui ne seront alors accessible qu'à lui et aux professionnels de santé auteurs de l'information en question
  - une notification lui est envoyé à chaque modification
  - il peut clôturer le DMP à tout moment

- le professionnel de santé
  - peut rendre « sensible » certaines informations (=invisibles au patient) mais de durée bornée à 15 jours : après quoi le patient est informé d'un modification de son DMP et invité à consulter un professionnel de santé ; au bout d'1 mois l'information sensible devient visible
  - information sensible = information qui nécessite une consultation d'annonce

Décret DMP : « information utiles à la coordination »
- volet de synthèse médicale = résumé structuré de l'état du patient , élaboré par le médecin traitant si nécessaire et au moins 1 fois par an -> médecins rémunérés pour l'élaborer (ROSP = Rémunération sur Objectifs de Santé Publique)
- CRH = lettre de liaison sortie
- comptes rendus de biologie
- fiches de RCP, programme personnalisé de soin

Séquence 5 : Les dossiers professionnels partagés (DPP)

- le patient n'y a pas accès
- permet aux différents acteurs de la prise en charge de coordonner leurs soins

Dossier Communicant Cancer/ DCC

- le médecin traitant est le coordonateur du parcours patient : doit être informé des différentes étapes
- les documents du DCC doivent être versés dans le DMP ou envoyés par messagerie sécurisée si le patient n'a pas de DMP
- construction d'une base de donnée nationale : épidémiologie, évaluations es politiques de santé, recherche —> tableaux de bord d'activité et d'évaluation de la qualité des prises en charge à l'intention de l'INCa, des ARS, des réseaux régionaux de cancérologie (RCC), des 3C, des établissements de santé
- mise à disposition du grand public d'un annuaire de RCP avec contact de coordonateurs des RCP

Dossier pharmaceutique/ DP

- utilisé par les pharmaciens
- créé par la loi de janvier 2007 et mis en oeuvre par le Conseil National des Pharmaciens
- ouvert après recueil du consentement du patient pour chaque bénéficiaire de l'Assurance Maladie
- contient la liste des médicaments délivrés les 4 derniers mois
- le pharmacie peut identifier les interactions médicamenteuses et corriger les prescriptions après appel du médecin prescripteur
- accessible à tous les médecins
- connexion sécurisée : nécessite la lecture de la carte vitale patient et de la CPS médecin

Séquence 6 : Télémédecine et objets connectés

= prestation de soins à distance, échange de l'information médicale s'y rapportant

Décrit dans le code de la Santé publique
- acte médical : présence d'un médecin : diagnostic, suivi, avis spécialisé, surveillance
- pratique à distance : relation patient- médecin ; médecin-médecin pouvant éventuellement passer par l'intermédiaire d'un auxiliaire médical

Avantages :
- patient : accès à des soins de qualité et à la totalité de l'offre de soins spécialisée
- médecin : enrichissement personnel par le travail collectif et la confiance dans la sécurisation des pratiques
- pouvoirs publiques : diminution du recours à l'hospitalisation, réduction des transports

5 actes reconnus par la télémédecine :
- **téléconsultation** : consultation à distance à un patient qui peut être éventuellement assisté localement par un professionnel de santé. Action synchrone. consentement du patient nécessaire et accord du médecin traitant nécessaires
- **télé-expertise** : professionnel de santé sollicite un avis. Action asynchrone. (téléradiologie ++ notamment télé-AVC)
- **télésurveillance médicale** : interprétation des données nécessaires au suivi (par exemple via balance connectée et boitier recueillant des données cliniques comme la dyspnée -> si anormales, un infirmière téléphone au patient pour vérifier la bonne utilisation du matériel -> si valeur anormales confirmées, le patient devra aller consulter)

- **téléassistance médicale** : permet à un professionnel médical d'assister à distance un autre professionnel lors de la réalisation d'un acte (ex : robot chirurgicaux et opérations à distance, déjà réalisé au début des années 2000 par un médecin aux Etats Unis sur une patiente à Strasbourg!!)
- **régulation** (centre 15)

Objets connectés
- fiabilité ?
- protection des données ? (hackés, manipulés à distance
- acteurs privés d'évaluation des solutions de santé mobiles : DMD santé, Medappcare

Séquence 7 : Les autres outils numériques

- prise de RDV en ligne :
  - Doctolib (chirurgiens et anesthésistes ++), utilisé en ville mais aussi à l'APHP
  - MonDocteur (généralistes et dentistes ++, s'appuie sur Doctissimo)

- Conseil médical personnalisé : MesDocteurs (réponse en moins de 15 minutes, 7/24, questions payantes, la première est gratuite; ou demande de 2e avis après envoi du dossier médical, réponse obtenue en 7j)

Séquence 8 : L'assurance maladie à l'ère du numérique

1- Organisation de la protection sociale

Sécurité sociale (créée en 1945)
- protection obligatoire contre les risques de vieillesse, maladie, maternité, accident de travail, charges de famille pour les salariés du commerce et de l'industrie
- financement assuré par des prélèvements sur les revenus du travail
- concerne les salariés mais aussi d'autres catégories de population
- principe de démocratie sociale = gestion paritaire des caisses par les partenaires sociaux au sein d'un conseil d'administration

Ordonnance de 1967 : création de trois caisses nationales de SS (maladie, vieillesse, allocations familiales) et d'une agence centrale

Ordonnance de 1995 : régime universel d'Assurance maladie -> ouverture automatique du droit de sécurité sociale à toute personne > 18 ans résidant régulièrement sur le territoire français + politique de maîtrise des dépenses de soins + création de la contribution au remboursement de la dette sociale (CRDS)

Organismes :
- branche famille : allocations familiales
- assurance maladie : caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) au niveau national + caisse primaire d'assurance maladie (CPAM), caisse d'assurance retraite et de la santé au travail (CARSAT), caisse générale de sécurité sociale (CGSS) au niveau régional
- retraite : caisse nationale d'assurance vieillesse des travailleurs salariés (CNAVTS) en national + CARSAT et CGSS en régional

Objectif : remboursement des frais selon le type de soins et pathologie
- 70% si secteur 1
- ALD30 si pathologie sur liste établie par le ministre de la santé ou nécessitant un traitement > 6 mois ou très onéreux

CMU (1999) : accès à l'assurance maladie à toute personne de nationalité française ou étrangère, résidant en France > 3 mois de manière stable et régulière, avec ou sans domicile fixe
- gratuite si revenu < plafond (9 601/ an en 2014)
- cotisation de 8% de la part des revenu fiscaux supérieurs à ce plafond

PUMA : remplace à CMU depuis 2016 -> pour toute personne résidant ou travaillant en France, simplifie les conditions d'ouverture des droits (plus à justifier d'un activité professionnelle minimale)

AMC (assurance maladie complémentaire) : remboursement des « reste à charge »
- obligatoire (assurance groupe dans certaines entreprises)
- ou facultative (assurance ou mutuelle)

CMU-c (1999): gratuite, prend en charge ce qui n'est pas couvert par les régimes d'assurance maladie
- accordée pour 1 an
- sous condition de ressources (< 8653€ /an)

AME (2000) : résidants en France en situation irrégulière : prise en charge à 100% et tiers-payant (dispense d'avance des frais)
- doit résider en France depuis > 3 mois et < 12 mois
- ressources < au plafond fixé par la CMU-c
- doit être redemandée chaque année

2- Dématérialisation des échanges entre professionnels de santé et assurance maladie

- facilite les échanges
- concerne plus de 90% des échanges
- feuille de soin électronique : échanges entre professionnels de santé- assurance maladie - complémentaires santé / exemple de logiciel : crossway (facturation, transmission des informations médicales
- économie d'€ dans la gestion des feuilles de soins électronique VS papier
- pilotage de soins : informations agrégées facilement
- indicateurs de performance (organisation et qualité de la pratique médicale) -> rémunération sur objectifs de santé publique
- sécurisation fondée sur deux cartes : 1) identifier le patient (carte Vitale, conçue par SESAM-Vital), 2) identifier le professionnel (CPS, délivrée par le GIP ASIP Santé)

Carte vitale
- identité du patient et celle de ses ayant-droits (<16 ans)
- numéro d'immatriculation (sexe - année de naissance - mois de naissance - département d naissance - code de commune - numéro d'ordre - clé
- régime d'assurance maladie d'affiliation, caisse de rattachement, droit à une exonération (ALD, maternité), à la CMU-C ou au tiers-payant intégral (au titre de l'aide au patient à une complémentaire santé ACS)
- aucune information d'ordre médical, n'est pas une carte de paiement

CPS
- signature électronique
- télétransmission, accès au DMP, aux messageries sécurisées MSSanté, procédures de télédéclaration des maladies à déclaration obligatoire, E-FIT (déclaration accident transfusionnel), CERT-DC (déclaration de décès)

Séquence 9 : Les déclarations obligatoires à l'ère du numérique

Télétransmissions sécurisées via carte CPS.

Vigilance de l'ANSM (x8) : pharmacovigilance, pharmacodépendance/ addictovigilance (substance psychoactives), hémovigilence, matériovigilance, réactovigilance (dispositifs de diagnostic in vitro), biovigilance (chaine de la greffe d'organes, tissus, cellules), cosmétovigilance, vigilance des produits de tatouage.

Accidents transfusionnels

- vigilance organisée par ANSM (1993) : EI chez les donneurs et les receveurs
- signalement aux réseaux de vigilance qui les déclarent à l'ANSM
- déclarants : correspondants d'hémovigilance des établissements de transfusion, des établissements de santé, les syndicats interhospitaliers et groupement de coopération sanitaire
- avantages de la télédéclaration : grande réactivité, amélioration de la sécurité de la transmission des données (pas de données perdues), qualité et complétude des données grâce à des alertes (non-conformité de la déclaration), exploitation facilitée, meilleur pilotage
- application e-fit (2004) : EI receveurs, EI graves donneurs, informations post-don, incidents graves

Maladies à déclaration obligatoire

- piloté par Santé Publique France
- 32 maladies dont 30 sont des maladies infectieuses
- par médecin ou biologiste : fiche de notification à l'ARS qui transmettra ensuite à InVS
- nom/ prénom/ adresse du déclarant, anonymat du patient
- voie postale ou télétransmission (actuellement possible que pour VIH)
- connexion à l'application via carte CPS : les co-déclarants (médecin, biologiste) déclarent indépendamment

Causes de décès

. papier : depuis 1968 :

- caractériser les disparités de santé (sexe, âge, régions) ou décrire les évolutions -> hiérarchiser les problèmes de santé, évaluer les actions de santé publique
- partie supérieure : déclaration à l'Etat civil, nominative
- partie inférieure : anonyme, renseignements médicaux, nom de la commune de décès, nom de la commune de domicile, date de naissance et date de décès, cachetée par le médecin
- remis à la commune de décès -> permis d'inhumer
- bulletin de décès par l'officier d'état civil à la mairie, dupliqué : bulletin 7 (anonyme) et 7 bis (nominatif, transmis à l'INSEE, sans causes médicales)
- transmis au médecin de santé publique de l'ARS, transmission au CépiDc de l'Inserm -> analyse du diagnostic -> codage selon CIM (classification internationale des maladies) -> statistique nationale de mortalité
- désavantages : délai trop long pour utiliser les données dans un objectif d'alerte

. certification électronique :

- diminution des délais (alertes et statistiques), amélioration de la qualité et de la fiabilité des données, renforcement de la confidentialité (grâce à un chiffrement, conservées sur le site que quelques heures pour permettre éventuellement de modifier)
- dès validation par le médecin, envoi à l'INSEE (nominatives) et l'INSERM (médicales)
- connexion possible sans carte CPS mais identification sur répertoire partagé de professionnels de santé (RPPS)
- volet médical complémentaire possible si les causes du décès sont connues après la déclaration (établi par le médecin qui procède à l'autopsie)

Séquence 10 : Le programme de médicalisation des systèmes d'information (PMSI)

avant 1984 : budget des hôpitaux = nombre de journées d'hospitalisation x prix d'une journée (donc budget calculé sur la base d'un nombre de jour d'hospitalisation -> durées de séjour augmentent pour augmentation des bénéfices)

1983 : réforme hospitalière (établissement de santé public et privés non lucratifs) -> création de la Dotation Globale de Fonctionnement -> induit une réduction des investissements et n'incite pas à l'innovation (retard d'équipement en IRM par rapport aux autres pays dans les années 90 par exemple)

1991 : **tarification à l'activité**, objectif : affecter chaque patient à un GHM (= Groupe Homogène de Malades = patients ayant mobilisé les mêmes ressources) -> objectifs : maximiser l'écart de coût entre les groupes, réduire l'écart de coût au sein d'un groupe

- pour créer ces groupes : nécessité d'uniformiser les modes de recueil des informations (codification précise des diagnostics et des actes)
- production de groupes homogènes de patients (3000 groupes existants): résumé d'unité médicale (description de la prise en charge) + résumé de séjour standardisé
- résumé d'unité médicale (produit par les médecins) = données administratives + informations sur le séjour + information médicales (avec code diagnostic et code d'acte : diagnostic principal, diagnostics associés, actes médicaux réalisés, médicaments et DMI)
- résumés d'unité médicale -> regroupés en résumé de sortie standardisé -> groupe homogène de malades selon un algorithme en 3 étapes
    - 1) 1 séjour = 1 catégorie majeure de diagnostic
    - 2) orienter le séjour dans une des racines (environ 700) de Groupes Homogènes de Malades (GHM) réparties dans les catégories majeures de diagnostic
    - 3) comorbidités : permet de passer des racines de groupes aux GHM (soit 3000 groupes en 2016)
- la durée de séjour n'est pas prise en compte dans la tarification : le prix d'hospitalisation par journée diminue lorsque la durée d'hospitalisation augmente pour un même groupe de patients -> incitation à diminuer les durées d'hospitalisation

4 types de diagnostics

- diagnostic principal : problème de santé ayant motivé l'hospitalisation
- diagnostic relié : maladie chronique ou état permanent
- diagnostic associé significatif (DAS) : comorbidités actives
- diagnostic associé documentaire (DAD) : antécédents du patient

Codage de l'activité

- selon CIM-10 édité par l'OMS : données de mortalités et de morbidité : chapitres pour chaque maladie pour chaque organe
- actes : réalisés par des médecins, diagnostics ou thérapeutiques, validés par la HAS
- unité de codage -> 4 lettres , 3 chiffres (2 premières lettres correspondent à l'organe, 3eme lettre à l'action, 4eme lettre à l'accès)

Utilisation des données du PMSI :

- description de l'activité des établissement de soins : disponible sur le site scansanté
- indicateurs de qualité de soins
- palmarès et classements des établissements en fonction des différentes pathologies -> publication dans des hebdomadaires
- études médico-économiques : inégalités territoriales
- indicateurs de santé
- pharmacovigilance (exemple du mediator/benfluorex)
- surveillance de la population et des établissements de santé : écart de moralité entre les établissements pour un même GHM