Cycle de conférences sur Conformité et Sécurité

Apport des réglementations
dans le domaine de la santé

Agenda

Le contexte

Principaux textes

- **CSP**
- **A.C.**
- **HIPAA**
- **ISO 27799**
- **QREC**

Conclusions

Le contexte

- Loi «hôpital, patients, santé et territoires»
- Relance de grands projets
  - **plates-formes de services de santé**
  - **plate-forme nationale d'échanges sécurisés (CNOM)**
  - **Hébergement de données de santé**

- ⇨ Besoin d'interopérabilité entre les différents acteurs

- ⇨ Recherche de conformité

Le contexte (Centre Jean Monnet à EPINAL)

Les faits

- **Erreur d'affichage des dimensions d'un faisceau d'irradiation, dont l'équipe s'est aperçue en cours de traitement**
- **entre mai 2004 et août 2005 : 23 patients traités en radiothérapie pour un cancer de la prostate exposés à une dose de rayon d'environ 20% supérieure à celle initialement prévue pour leurs traitements**

Les conséquences

- **5500 patients sur-irradiés entre 1987 et 2006**
- **5 patient décédés de manière directement liée à ce surdosage**
- **Révocation du chef de service de radiologie**
- **mai 2008 : mise en examen de la directrice de J. Monnet (pour homicides et blessures involontaires)**
- **Indemnisation des victimes**

Le contexte (assureur)

Bancassurance

Dossier de Prêt

Dossier Patient

Le contexte (accès au dossier)

Indisponibilité du SIH

- **Perte d'efficacité des services**
- **Indisponibilité des informations médicales**
  - Impact sur la pose du diagnostic
  - Nécessité de refaire des examens
    - **Coût financier**
- **Incapacité de fournir le dossier au patient ou à ses ayant-droits (article L.1111-7 du CSP)**
- **Incapacité de fournir la preuve du consentement du patient en cas de litige sur faute médicale**
- **Coût des indemnisations**
- **Atteinte à l'image**

Le contexte réglementaire

Accréditation HAS

NIR

Traitements de données personnelles à des fins :
☞de recherche (ex. génétiques)
☞statistiques et épidémiologiques

Secret professionnel / Secret médical
Droits d'accès des PS aux données de santé
Code pénal (ex-Godfrain)
Secret des correspondances
Cybersurveillance des salariés

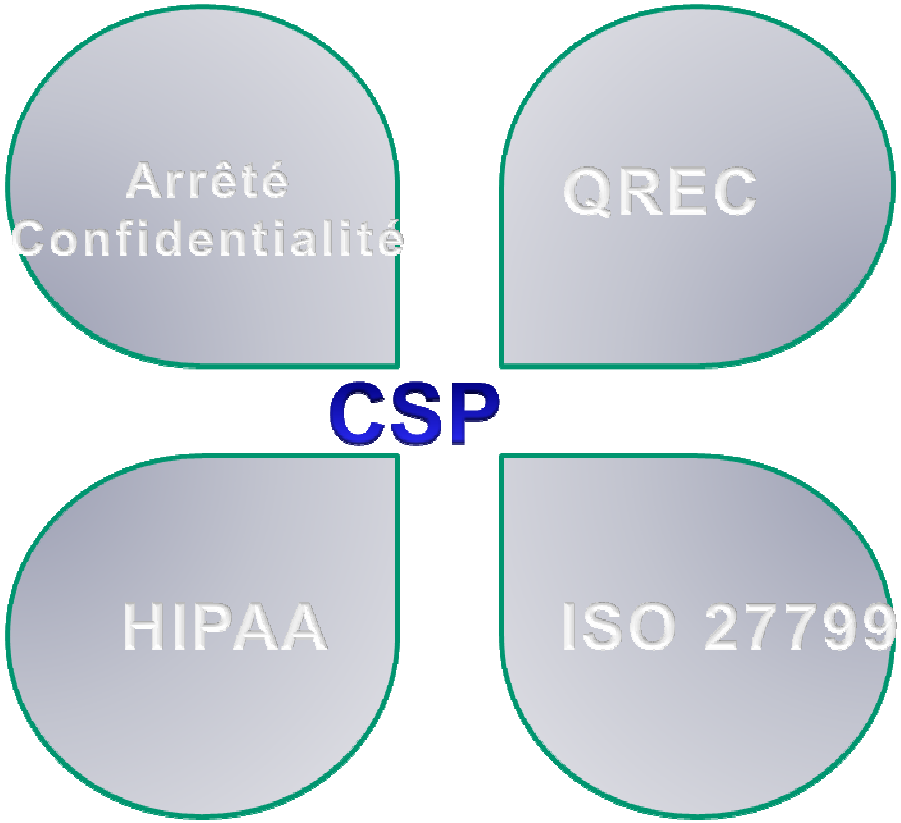
Traitements de données médicales
Droits d'accès des patients aux données de santé

Signature électronique et Cryptologie

Traitements de données personnelles et respect de la vie privée (CNIL)

Protection juridique des logiciels et bases de données (droit d'auteur) – Liberté de la presse

Principales réglementations en matière de sécurité (santé)



Décret 2007□960 et Arrêté Confidentialité

Prolongement de l'Article L1110-4 du CSP (mars 2002)

(Confidentialité des informations de santé et Secret médical partagé)

- **Devait préciser les cas où la carte CPS (…) est obligatoire**

Détermine

- **les fonctions de sécurité nécessaires à la conservation et à la transmission des informations médicales et fixe le niveau de sécurité requis pour ces fonctions**

Périmètre

- **S'applique aux PS et organismes délivrant des prestations médicales**
- **Porte sur les informations médicales à caractère personnel relatives aux personnes prises en charge**

Décret 2007□960 et Arrêté Confidentialité

Contenu

- **Exigences sur l'organisation, les politiques et procédures**
- **Exigences sur le système informatique**
  - Globalement neutre technologiquement
    - **(sauf 2 exigences sur l'emploi de CPS et S/MIME)**
  - Peu de règles obligatoires
  - Une majorité de recommandations

Avantages

- **Fixe des exigences minimales**

Limites

- **Des divergences entre les acteurs sur certaines exigences**

Arrêté Confidentialité

- **Contrôle d'accès aux données médicales et ressources critiques**
  - **Protection de l'accès**
  - **Gestion des droits d'accès**
- **Authentification des utilisateurs**
  - **Authentification des utilisateurs**
  - **Sécurité de l'authentification**
- **Transmission sur un réseau ouvert**
  - **Chiffrement des données**
  - **Authentification des parties**
- **Exploitation du système**
  - **Sécurité des services réseaux**
  - **Protection contre les codes malveillants**
  - **Dispositifs portables**

Recommandations

- **Contrôle des droits d'accès**
- **Identifiant unique**
- **Auditabilité**
- **Sauvegarde et archivage**
- **Documentation**

HIPAA

Health Insurance Portability and Accountability Act (1996)

- **Titre I : Encadrer les contrats d'assurance maladie, pour protéger les salariés en cas de perte ou de changement d'employeurs**
- **Titre II : Réduire les fraudes et simplifier les procédures administratives**

En matière de sécurité

- **Privacy Rule (2001 : 2003/2004)**
- **Security Rule (2003 : 2005/2006)**
  - 4 volumes de recommandations technologiquement neutres
    - **Administratif**
    - **Physique**
    - **Technique**
    - **Organisationnel**

HIPAA

Administratif (Processus de gestion de la sécurité) (9 exigences)

- **Risk Management**
- **Responsabilités et sanctions (circuit d'autorisation)**
- **Politiques d'accès aux informations**
- **Sensibilisation et formation**
- **Surveillance et revues de la sécurité**
- **Gestion des incidents et de la continuité**

Technique (5 exigences)

- **Contrôle d'accès, bris de glace**
- **Protection de l'intégrité des PHI (D+T), authentification, chiffrement,**
- **Audit**

Physique (4 exigences)

- **Contrôle d'accès et politique de préservation des moyens**
- **Sécurité des postes de travail et des supports**
- **Sauvegarde**

Organisationnel (4 exigences)

- **Politiques et procédures**
- **Contrat avec les associés, partenaires ...**
- **Gestion documentaire**

HIPAA (3)

Bénéfices

- **Information des personnels**
- **Mise en œuvre de moyens de chiffrement et de signature**
- **Amélioration globale de la disponibilité des données**

Coût de mise en œuvre

- **entre 10 et 50 Milliards de dollars**

Pour plus d'information

- ***www.hipaa.org***

ISO 27799

- Fournir un guide de bonnes pratiques pour la sécurité de l'information de santé
- Interprétation et l'implémentation de l'ISO 27002:2005 dans le domaine de l'informatique de santé
  - **(ISO 27002 : Information Technology - Code of practice for information security management)**
- Spécifier un ensemble de contrôles détaillés pour gérer la sécurité de l' information de santé
  - **Permettre aux organisations de santé et autres "gardiens" d'information de santé**
    - d'assurer un **niveau de sécurité requis minimum** approprié au contexte de leur organisation
    - de maintenir la confidentialité, l'intégrité, et la disponibilité de l'information personnelle de santé (personal health information)

ISO 27799

Intérêt

- **Package métier prêt à l'emploi**
  - Analyse de Risque
  - Liste de biens
  - Liste de menaces
  - Liste de bonnes pratiques

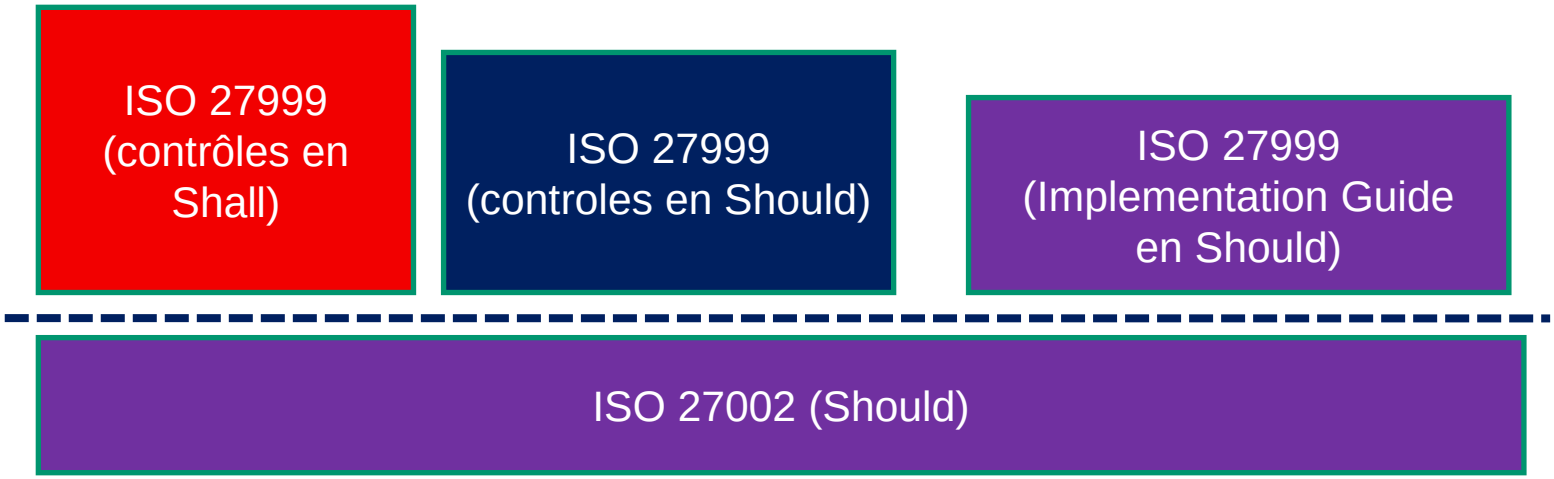
Inconvénients

- **Des ambiguïtés sur l'autonomie de la norme**
- **des points fondamentaux d'une démarche sécurité ne sont pas caractérisés comme obligatoires**
  - Gestion des actifs
  - Incidents
  - PCA
  - Réglementation

ISO 27799

2 manières d'aborder le contenu

- **11 domaines de contrôle**
  - rassemblant 39 catégories de mesures
- **Niveau d'exigence sur la mesure**
  - **Obligatoire (Shall)**
  - Optionnel (Should)
  - Recommandations d'implémentation



Le projet européen QREC

Quality Labelling and Certification of Electronic Health Record systems in Europe (EC, FP6, IST-27360, 2005-2008)

- **Harmonisation des dispositifs de certification des systèmes de dossiers de santé informatisés**
- **Conférences européennes sur les dossiers de santé informatisés (Conférences EUROREC) (Genève 2006)**

Relève du plan d'action proposé par la Communication pour la santé en ligne" COM (2004)356 avec pour objectifs

- **4.2.5 "Tests de conformité et accréditation pour un marché de la santé en ligne"**
- **4.2.2.2 "Interopérabilité des dossiers de santé informatisés**

http://www.eurorec.org/

Q-REC Exigences de sécurité

A7 Privacy and accountability services

- **A70 Authentication**
- **A71 Authorisation**
- **A72 Access control**
- **A73 Confidentiality and consents**
- **A74 Version management**
- **A75 De-identification services and processes**

A8 Technical security services

- **A80 Backup and integrity validation**
- **A81 Data retention, availability and destruction**
- **A82 Audit and event monitoring**
- **A83 Attestation and non-repudiation**

quality / safety / security

Conclusions

Le besoin de base en matière de sécurité dans le domaine de la santé porte sur

1/ La disponibilité des données

2/ L'intégrité des données (Id, IMCP)

3/ La confidentialité

La mise en œuvre de démarches sécurité dans d'autres pays démontre qu'elles apportent une amélioration de la sécurité