Confidentialité et Sécurité des données

CME- Séance plénière du 7 mars 2017

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Direction des Soins et des Activités Paramédicales

Sensibilisation à l'utilisation du Dossier Patient

Réunion de présentation de la campagne 2016

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

SÉCURITÉ DE L'INFORMATION

La confidentialité et la sécurité du dossier patient informatisé

- **Garantir au patient la confidentialité de son dossier, notamment par la conformité des accès**

- **Garantir au professionnel les droits d'accès nécessaires en lien avec ses besoins métiers**

  - Tout personnel soignant (PM et PNM) a accès à l'ensemble des données de santé d'un patient dont il a la charge ou pour lequel il est sollicité.
  - Tout personnel a accès aux seules données nécessaires à sa mission et limitées dans le temps

- **Répondre aux exigences légales et réglementaires (CSP, CNIL, Certifications, ...)**

- **Mettre en œuvre une démarche globale de maitrise des risques liés à la Sécurité SI**

Forces

- **Mobilisation forte** pour un SI performant et sécurisé

Faiblesses

- **Culture sécuritaire faible et poids des habitudes**
- **Processus** de gestion des habilitations perfectible

Opportunités

- Réglementation fournissant **un cadre exigeant de sécurité et confidentialité**
- **Synergie commune** pour disposer **d'habilitations adaptées** à une prise en charge des patients **partagée et sécurisée**

Menaces

- **SI « attrayant »,** riche en données sensibles et nombre de patients
- **Cyber-menace permanente et présente** dans le secteur de la santé
- **Nombre de personnes ayant des accès,**

- 65 000 personnes ont accès à Orbis
- Cible : 85461 utilisateurs

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Difficultés rencontrées dans le cadre de la mise en œuvre ORBIS – Risques

Des droits d'accès au SI Patient à sécuriser

- 80 métiers différents avec chacun ses besoins et ses règles

Circuit agent

- *Agents sans accès*
- *Comptes non fermés, non utilisés*

Conformité des droits métier

- *Règles appliquées de façon disparate*

Des points de confidentialité à améliorer

Confidentialité des dossiers de personnes sensibles

- *Règles trop partiellement mises en œuvre*

Traçabilité des accès

- *Traçabilité non exhaustive*
- *Absence de contrôle récurrent*

Risques

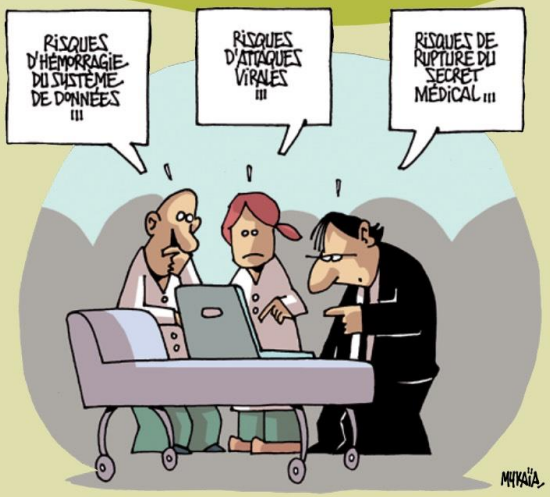
- Perte de confiance
- Dérives d'utilisation
- Usurpation de compte
- Divulgation d'information

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Actions à mettre en œuvre - Propositions

Sensibiliser à la confidentialité des données de santé	•Informer le personnel sur les risques, la réglementation et les sanction •**Responsabiliser le personnel** et rappeler les règles d'utilisation du SI
Sécuriser le circuit agent dans les GH	• Accélérer la maîtrise des arrivées, départs, mouvements des agents, • Disposer de métiers à jour pour s'appuyer sur les vraies fonctions
Mettre en œuvre le processus de gestion des habilitations	• Définition des règles d'habilitation métier • **Mise en place d'un Comité transverse d'habilitations, qui pilote et arbitre les règles** • Revue du processus d'évolution des habilitations
Renforcer les dispositifs de contrôles et d'alertes	• Vérification des comptes et des accès • Contrôles a posteriori : Organisation à définir
Accélérer l'amélioration de la sécurité dans Orbis	• Amélioration de la traçabilité • Renfort de la confidentialité : personnes ou dossiers à protéger

Sécurité de l'information : Les règles essentielles



Ensemble, prenons soin des informations de nos patients et de notre institution !

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Sécurité de l'information : et si nos données n'étaient pas suffisamment protégées ?

Ensemble, prenons soin des informations de nos patients et de notre institution !

http://ssi.aphp.fr/

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Sécurité de l'information : et si nos données n'étaient pas suffisamment protégées ?

Ensemble, prenons soin des informations de nos patients et de notre institution !

http://ssi.aphp.fr/

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Message

- « J'accède au dossier d'un patient dont je n'assure pas la prise en charge : **je commets une faute et viole le secret professionnel** »

Risques

- Risque d'atteinte à la vie privée des patients
- Risque de divulgation non intentionnelle d'informations
- Risque de recours du patient (accès par des personnes non habilitées)

Fondement juridique

La seule qualité de médecin ou de professionnel de santé n'ouvre pas de droit quelconque au partage d'informations y compris en mode « bris de glace » (Article L.1110-4 du Code de la santé publique). Jurisprudence : **condamnation** au paiement d'une amende pour un professionnel de santé ayant délivré au mari de la patiente, au motif qu'il était médecin, les résultats positifs de test de séropositivité de sa femme (**violation du secret professionnel** - Article 226-13 du Code pénal)

Art. L. 1110-12 : « **l'équipe de soins** est un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap ou de prévention de perte d'autonomie, ou aux actions nécessaires à leur coordination »

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Message

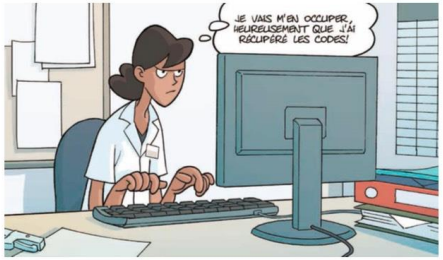
- « J'utilise les identifiants et mots de passe d'un tiers : **j'usurpe son identité et je commets une infraction pénale** »

Risques

- Risque d'erreur médicale ou d'accident de soin au nom d'un autre membre du personnel soignant

Fondement juridique

Le fait **d'usurper l'identité** d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni **d'un an d'emprisonnement** et de **15 000 € d'amende** (Article 226-4-1 du Code pénal)



ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Message

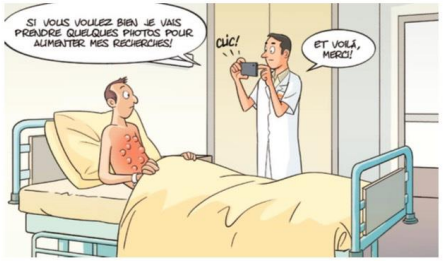
- « J'échange des informations concernant les patients avec des moyens non sécurisés (sms, photos, mails personnels, réseaux sociaux), et des personnes non habilitées (ne faisant pas partie de l'équipe de soins) : **je commets une faute et viole le secret professionnel** »

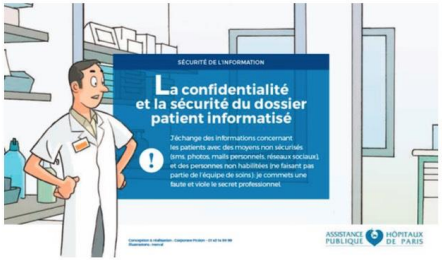
Risques

- Risque de fuite d'informations ou d'interception par un tiers malveillant ou non concerné
- Risque de dépôt de plainte d'un patient (informations confidentielles fuitant sur un réseau social…)

Fondement juridique

« La **confidentialité et l'intégrité des informations** envoyées par message électronique doivent être assurées […] notamment par le chiffrement des messages lors de leur transmission » (Préconisations de la CNIL) ; et les **destinataires habilités** (Article L.1110-4 du Code de la santé publique). Des sanctions pourront être engagées dans le cas contraire (**violation du secret professionnel** – Article 226-13 du Code pénal)





ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Message

- «Je laisse ma session « dossier patients » ouverte :
  je facilite la divulgation d'informations confidentielles
  la transcription des actes médicaux et des soins aux patients est tracée et effectuée en mon nom
  Ma responsabilité pourra être mise en cause »

Risques

- Risque de fuite d'informations (divulgation accidentelle d'un résultat positif de dépistage …)
- Risque d'altération (modification, suppression…) d'informations critiques pouvant conduire à une erreur médicale voire à un préjudice vital.

Fondement juridique

Les patients pris en charge peuvent à tout moment **prendre connaissance des traces d'accès** à leur dossier, et donc savoir qui l'a consulté. (Article L 1111-19 du projet de loi de santé –*à confirmer*). Jurisprudence : **condamnation** de CHU pour atteinte au respect du droit du patient de conserver le secret sur son état de santé.

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Message

- « Je communique mes identifiants et mots de passe à un tiers, les actes réalisés par ce tiers sont tracés en mon nom : ma **responsabilité pourra être mise en cause** »

Risques

- Risque d'erreur médicale ou d'accident de soin commis en mon nom, et qui pourront m'être imputés
- Risque de perte de traçabilité précise des actes de soin effectués (prescription, dosage…)

Fondement juridique

Les professionnels de santé sont **responsables des conséquences dommageables** d'actes de prévention, de diagnostic ou de soins en cas de faute (Article L.1142-1 du Code de la santé publique)

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

GAIA P

Gestion des Accès et des Identités pour l'AP-HP

Bureau de la CME

Gestion des accès et des identités pour l'AP-HP

23 mars 2016

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Actions à mettre en œuvre - Propositions

Sensibiliser à la confidentialité des données de santé	•Informer le personnel sur les risques, la réglementation et les sanction •**Responsabiliser le personnel** et rappeler les règles d'utilisation du SI
Sécuriser le circuit agent dans les GH	• Accélérer la maîtrise des arrivées, départs, mouvements des agents, • Disposer de métiers à jour pour s'appuyer sur les vraies fonctions
Mettre en œuvre le processus de gestion des habilitations	• Définition des règles d'habilitation métier • **Mise en place d'un Comité transverse d'habilitations, qui pilote et arbitre les règles** • Revue du processus d'évolution des habilitations
Renforcer les dispositifs de contrôles et d'alertes	• Vérification des comptes et des accès • Contrôles a posteriori : Organisation à définir
Accélérer l'amélioration de la sécurité dans Orbis	• Amélioration de la traçabilité • Renfort de la confidentialité : personnes ou dossiers à protéger