Club EBIOS

Dispositifs médicaux connectés

08/10/2013

Adrien ROUSSEAUX

Expert à la Commission Nationale de l'Informatique et des Libertés

Définition

- **Qu’est-ce qu’un dispositif médical ?**

(*article L. 5211-1 du code de la santé publique*)

- « Tout instrument, appareil, équipement, matière, produit, à l'exception des produits d'origine humaine, ou autre article utilisé seul ou en association, **y compris les accessoires et logiciels nécessaires au bon fonctionnement de celui-ci**, destiné par le fabricant à être utilisé chez l'homme à des fins médicales et dont l'action principale voulue n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens ».

- Dispositifs médicaux **implantables actifs** : « dispositifs médicaux qui sont conçus pour être implantés en totalité ou en partie dans le corps humain ou placés dans un orifice naturel, et qui **dépendent** pour leur bon fonctionnement d'une source d'énergie électrique ou de toute source d'énergie autre que celle qui est générée directement par le corps humain ou la pesanteur ».

Définition

Les dispositifs médicaux sont séparés en 4 classes en fonction de la dangerosité du dispositif pour les individus. Les dispositifs médicaux implantables actifs n'en font pas partie

- Classe I : Risque potentiel faible (instruments chirurgicaux réutilisables, dispositifs médicaux non invasifs, dispositifs médicaux invasifs à usage temporaire) ;
- Classe IIa : Risque potentiel modéré (dispositifs médicaux invasifs à court terme, dispositifs médicaux invasifs de type chirurgical à usage unique) ;
- Classe IIb : Risque potentiel élevé (dispositifs médicaux implantables long terme) ;
- Classe III : Risque potentiel critique (dispositifs médicaux implantables long terme en contact avec le cœur, le système circulatoire central ou le système nerveux central, dispositifs médicaux implantables résorbables, implants mammaires, implants articulaires de hanche, de genou et d'épaule …).

Contexte : Exemples

- Au début des années 90, une patiente et un autre patient d'un grand hôpital parisien sont décédés. L'enquête à montrer que le marie de la patient s'était introduit dans le SI de l'hôpital pour modifier le paramètre des alarmes du dispositif (http://www.ina.fr/video/CAB98014776)

- Fin 2012, Jack Barnaby a monter la possibilité de prendre le contrôle de la pile cardiaque d'un pacemaker pour commander un choc électrique mortel (830 volts)

(www.scmagazine.com.au/News/319508,hacked-terminals-capable-of-causing-pacemaker-mass-murder.aspx)

Les dispositifs médicaux : le fonctionnement

- **L'appareil doit être paramétré pour fournir à la personne le fonctionnement optimal.**
  - Directement sur l'appareil
  - A distance, permettant de mieux le gérer en fonction des besoins du patient

- **L'administration de l'appareil**
  - Afin de vérifier son bon fonctionnement, le fournisseur ou le prestataire de soin à domicile vérifie que l'appareil est en fonctionnement et / ou que le patient l'utilise effectivement.
  - Les fournisseurs doivent également, dans certain cas, récupérer les données techniques de l'appareil pour les interpréter avant de les fournir aux professionnels de santé / patient.

Les dispositifs médicaux : les données

- **Les biens essentiels :**

  - **Données à caractère personnel :** données d'identification directe ou indirecte du patient (nom, prénom, identifiant de la machine, …) ;
  - **Paramètres du dispositif médical :** Les paramètres du dispositif médical sont liés à l'état de santé de l'utilisateur, ils seront distincts d'un patient à l'autre et seront considérés dans cette étude comme des données à caractère personnel.

Les dispositifs médicaux : les flux

- **Les dispositifs sont connectés au système d'information :**
  - Par câble ;
  - Par réseau sans fil (WiFi, Bluetooth, GSM, …).

- **Les transferts de données peuvent avoir lieu :**
  - Sur le réseau interne ;
  - Sur Internet ;
  - Par clé USB.

Les dispositifs médicaux : cas d'utilisation

Lieu d'utilisation	Maintenance du dispositif médical
Etablissement de santé	Etablissement de santé
Etablissement de santé	Fournisseur
Domicile du patient	Etablissement de santé
Domicile du patient	Fournisseur et / ou prestataire de soin à domicile

- **De plus en plus de dispositifs sont utilisés directement par les patients (« Quantified self »).**

Evénements redoutés

- **En fonction de la classification des appareils, l'impact sur la santé des personnes n'est pas le même.**

- **Quels sont les événements redoutés ?**
  - Interception de données (confidentialité) ;
  - Modification de données (intégrité) ;
  - Indisponibilité du dispositif (disponibilité).

Les événements redoutés

Evénement redouté	Caractère identifiant	Impacts potentiels les plus graves	Caractère préjudiciable	Gravité maximum
Accès illégitime aux données	4. Maximal	-Diffusion non maitrisée des données (accès par un employeur, atteinte à l'intimité de la personne) - Atteinte au secret médical	3. Important	4. Maximal
Modification non désirée des données	4. Maximal	-Traitement d'un mauvais patient - Mauvais traitement d'un patient	4. Maximal	4. Maximal
Indisponibilité de l'appareil ou des données	4. Maximal	-Impossibilité de soigner le patient - Non remboursement du patient	4. Maximal	4. Maximal

Menaces : vulnérabilités

- **Vulnérabilité des supports :**
  - Les dispositifs médicaux ne sont pas tous sécurisés de la même manière. Les fabricants commencent à penser à la sécurité.
  - La Food and Drug Administration (FDA) a émis des recommandations début juin (http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm)

- **On peut donc estimer que la vulnérabilité des supports (dispositifs médicaux dont les logiciels intégrés) est maximale**

Menaces : sources de risques

- Si les personnes sont aujourd'hui méconnues, les vulnérabilités peuvent intéresser des groupes terroristes ou mafieux pour opérer des attaques ciblées.

- Les vulnérabilités proviennent également des patients eux-mêmes, qui pourraient modifier les paramètres des dispositifs par méconnaissance.

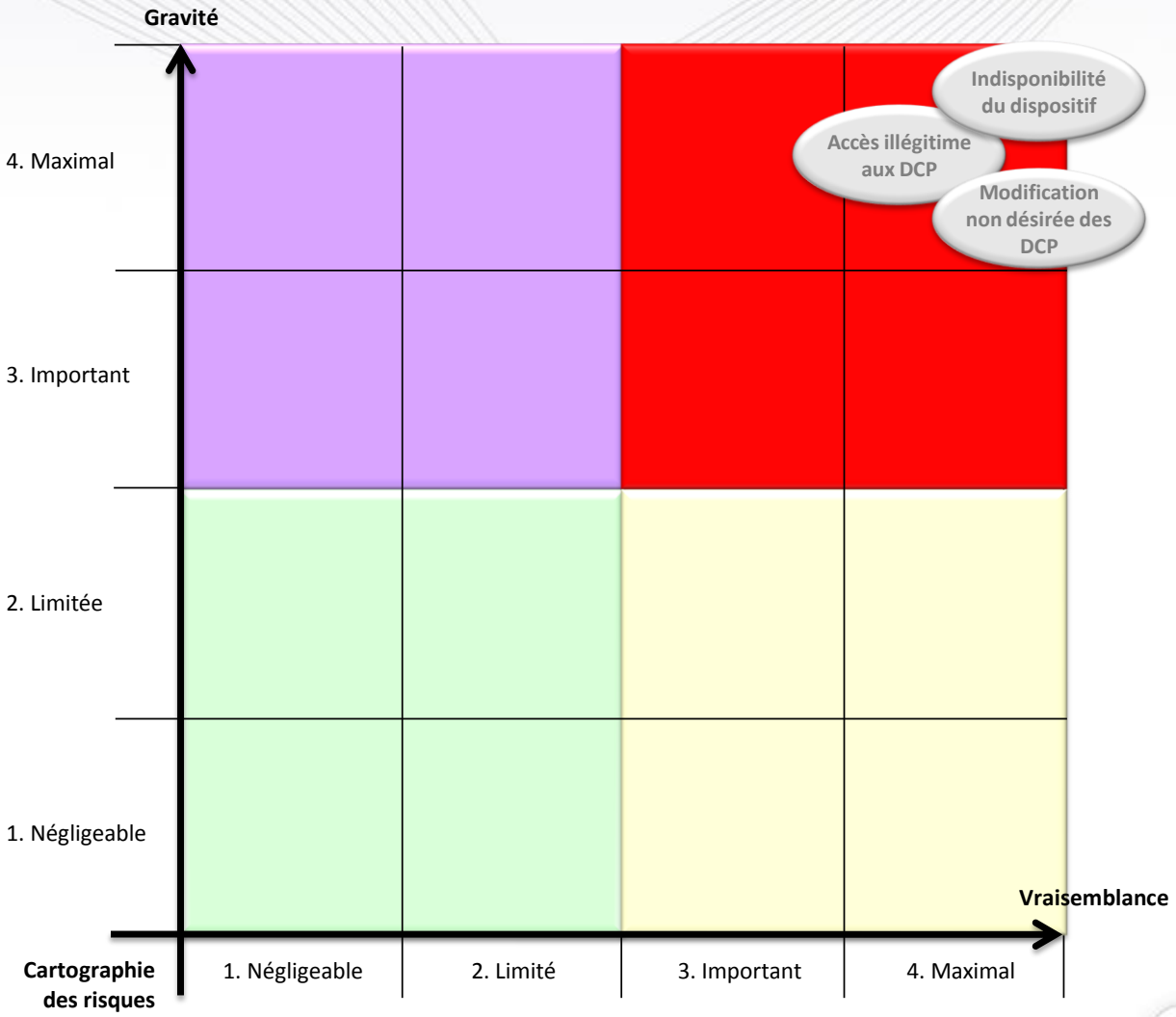
- Les professionnels de santé, par mégarde pourraient également administrer des doses mortelles de produits (ce cas n'est pas banales dans les établissements dans l'utilisation d'outils informatisés).

- **Ces personnes disposent de nombreux moyens et capacités financières, celles-ci disposent de capacité importantes à maximales.**

Menaces : vraisemblance

Evénement redouté	Menaces les plus vraisemblables	Vulnérabilité des supports	Capacité de la source	Vraisemblance maximum
Accès illégitime aux données	-Modification d'un logiciel - Vol de l'appareil - Interception de données	4. Maximale	4. Maximale	4. Maximal
Modification non désirée des données	-Modification d'un logiciel - Usage anormal du logiciel - Analyse d'un logiciel	4. Maximale	4. Maximal	4. Maximal
Indisponibilité de l'appareil ou des données	-Détournement d'usage du matériel - Coupure d'électricité	4. Maximale	4. Maximal	4. Maximal

Etude des risques : niveau des risques



Mesures : Eléments à protéger

- **Fixer et gérer des durées de conservation des données**
  - Est-il nécessaire de conserver les données sur le dispositif médical ?

- **Chiffrer les données**
  - Chiffrer les canaux de transmission ;
  - Chiffrer les données identifiantes, mais aussi les paramètres du dispositifs, notamment pour les dispositifs de classes IIa ou supérieure ;

- **Informer les personnes concernées**
  - Obligation légale d'informer, il s'agit de données de santé ;
  - Permettre à la personne de comprendre le fonctionnement du dispositif permet d'éviter les erreurs de manipulation ;

- **Obtenir le consentement des personnes concernées** lorsqu'imposer par la loi

Mesures : impacts

- **Sauvegarder les données**
  - Permet de reconfigurer l'appareil en cas de modification non désirée ;
  - Chiffrer les sauvegardes ;

- **Contrôler l'intégrité des données**
  - Générer des empreintes des données, et en cas d'erreur, afficher et ou remonter une alerte ; Permet également de lutter contre les codes malveillant (vérifier les fichiers de configuration)

- **Tracer l'activité sur le dispositif médical**
  - En cas de modification des données, conserver une trace de l'action ;
  - Dès que possible, centraliser les traces des dispositifs médicaux (attaque massive) ;
  - Informer les utilisateurs ;

- **Gérer les violations de données**
  - Prévoir un plan de réaction en cas d'indisponibilité : le personnel est-il assez formés pour soigner les patients en cas d'arrêt du dispositif ?

Mesures : sources de risques

- **Gérer les personnes qui ont un accès légitime**
  - Former le personnel médical à l'utilisation du dispositif ;
  - Prévoir une politique d'habilitation, par exemple tous les utilisateurs n'ont pas à paramétrer le dispositif ;

- **Gérer les tiers qui ont un accès légitime**
  - Activer les accès entrant en télémaintenance uniquement sur demande, les accès entrants étant inactifs par défaut ;
  - Prévoir un affichage sur le dispositif, permettant à la personne de verrouiller le dispositif ;
  - Clause de confidentialité ;

Mesures : sources de risques

- **Contrôler l'accès logique**
  - Pour les professionnels de santé, prévoir l'authentification par carte CPS ;
  - Prévoir une authentification serveur, le dispositif médical peut être à l'origine des communications ;
  - Fermer tous les ports non utilisés (Wifi, Bluetooth, …) ;

- **Se protéger contre les sources de risques non humaines**
  - Mettre en place des moyens de surveillance et de secours de l'alimentation électrique ;
  - Surélever le dispositif médical pour prévenir d'un dégât des eaux ;

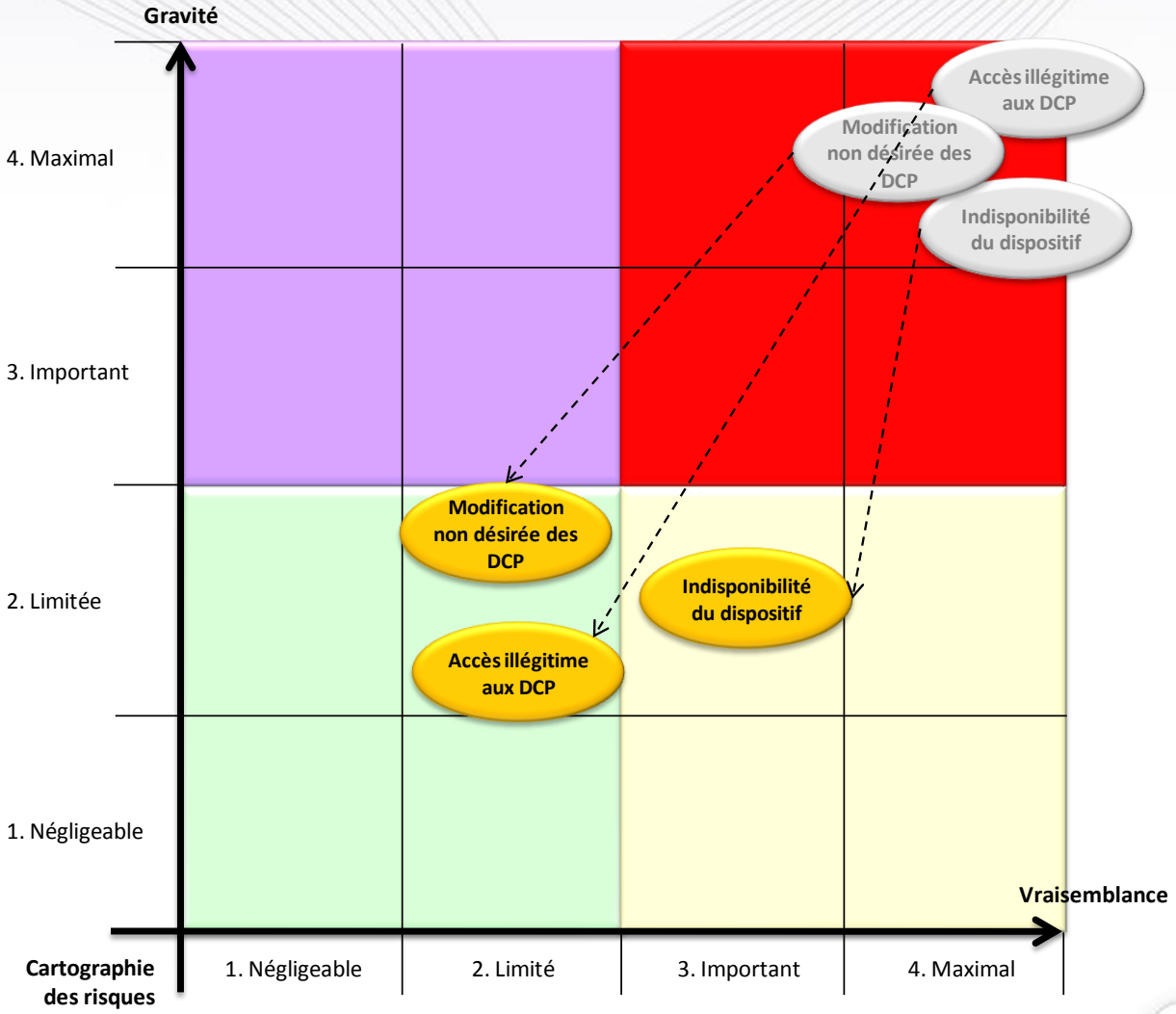
Application des mesures : gravité

Evénement redouté	Mesures prévues	Impacts potentiels les plus graves	Caractère préjudiciable	Gravité maximum
Accès illégitime aux données	- Chiffrer les données ; - Contrôler l'accès et gérer les habilitations ;	-Diffusion non maitrisée des données (accès par un employeur, atteinte à l'intimité de la personne) - Atteinte au secret médical	1. Négligeable	2. Limité
Modification non désirée des données	-Informer les personnes et les former ; - Contrôler l'accès et gérer les habilitations ; - Contrôler l'intégrité des données ; - Tracer les actions ; - Sauvegarder les données ;	-Traitement d'un mauvais patient - Mauvais traitement d'un patient	1. Négligeable	2. Limité
Indisponibilité de l'appareil ou des données	-Se protéger contre les sources non humaines ; - Former les utilisateurs ; - Prévoir un PCA	-Impossibilité de soigner le patient - Non remboursement du patient	1. Négligeable	2. Limité

Application des mesures : vraisemblance

Evénement redouté	Menaces les plus vraisemblables	Vulnérabilité des supports	Mesures prévues	Vraisemblance maximum
Accès illégitime aux données	-Modification d'un logiciel - Vol de l'appareil - Interception de données	1. Négligeable	-Chiffrer les données ; - Contrôler l'accès et gérer les habilitations ;	2. Limité
Modification non désirée des données	-Modification d'un logiciel - Usage anormal du logiciel - Analyse d'un logiciel	1. Négligeable	-Informer les personnes et les former ; - Contrôler l'accès et gérer les habilitations ; - Contrôler l'intégrité des données ; - Tracer les actions ; - Sauvegarder les données ;	2. Limité
Indisponibilité de l'appareil ou des données	-Détournement d'usage du matériel - Coupure d'électricité	2. Limité	-Se protéger contre les sources non humaines ; - Former les utilisateurs ; - Prévoir un PCA	3. Important

Etude des risques : niveau des risques



Merci de votre attention !