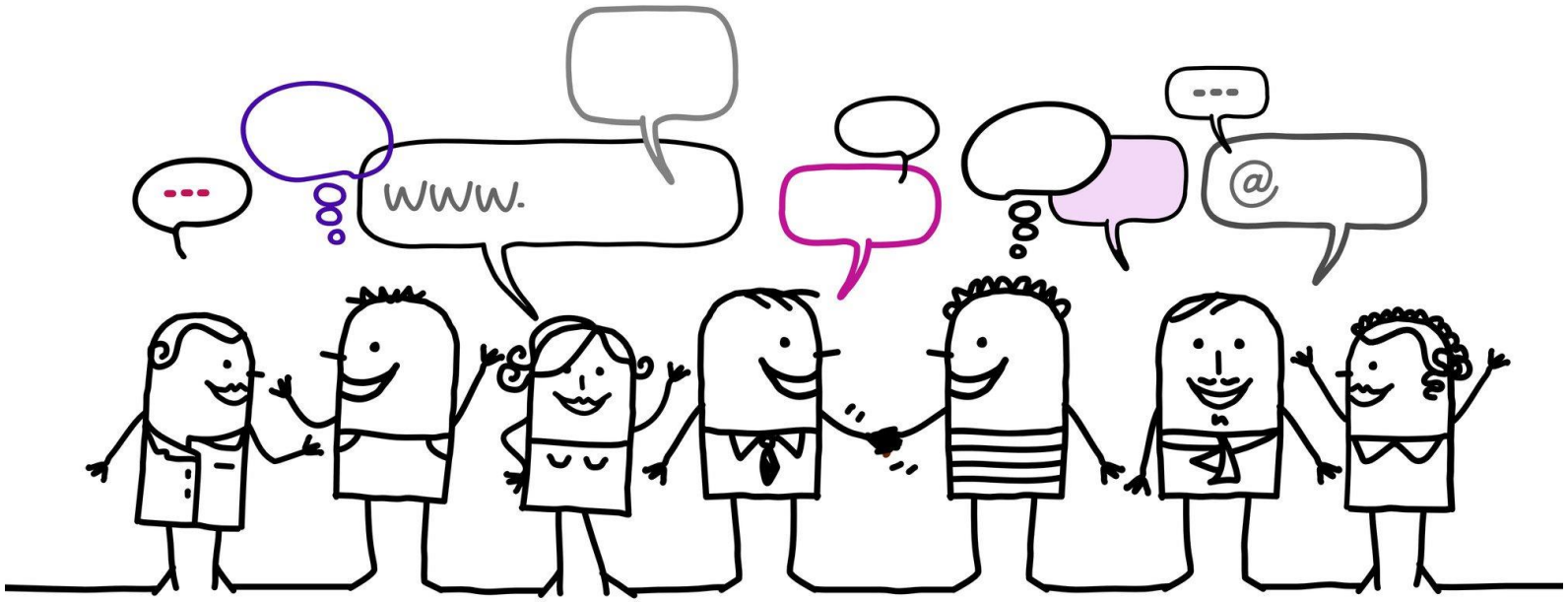
Sécurité des DM connectés

Animateurs :

Pr Xavier Armoiry (Lyon) Hervé Szymczak (Lille)

Faisons connaissance



Objectifs

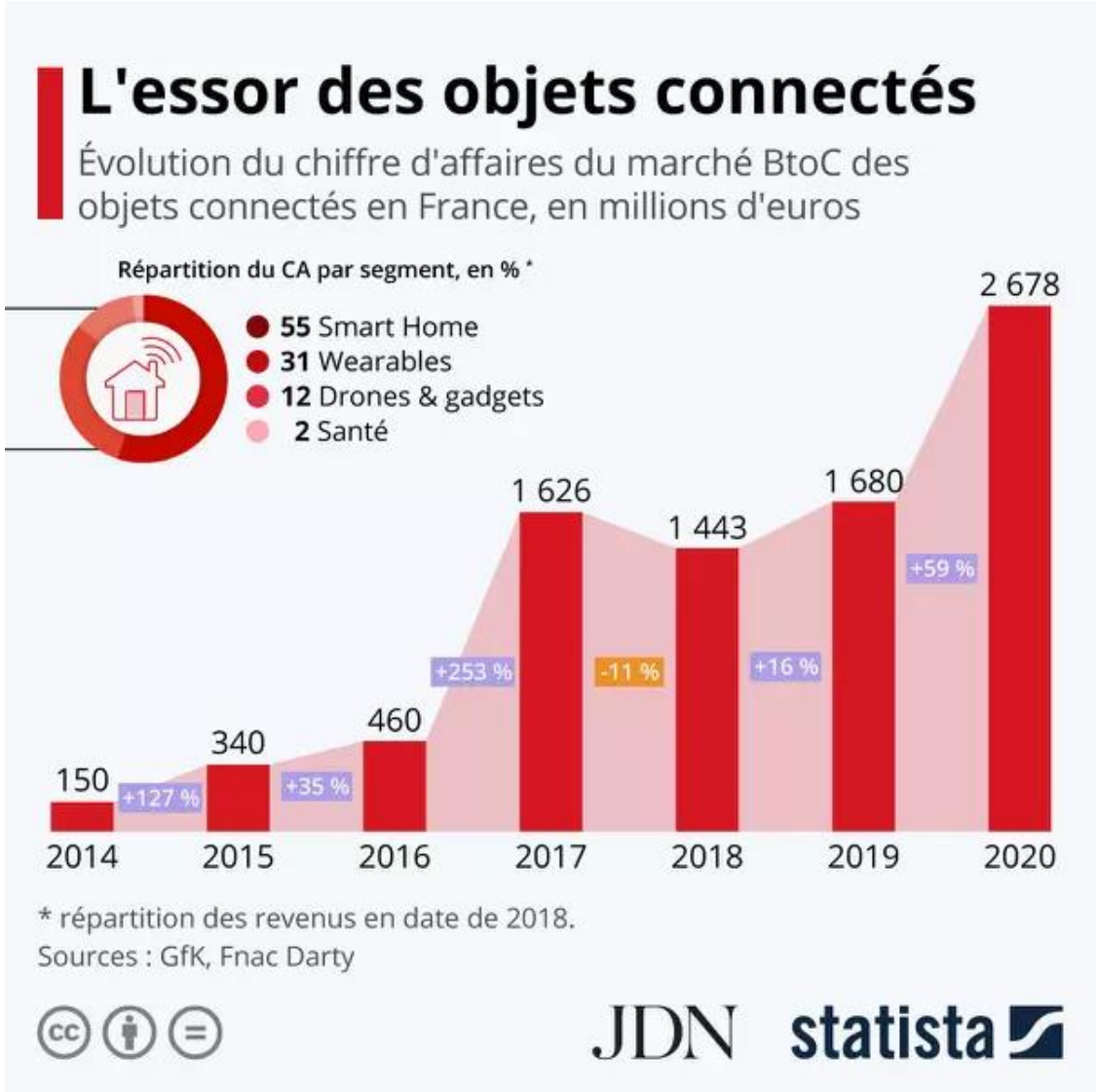
- Connaitre la place des DM parmi les objets connectés
- Comprendre les enjeux réglementaires autour des DM connectés
- Comprendre les enjeux de sécurité autour des DM connectés en milieu hospitalier

Donner un exemple de votre choix d'un objet connecté non médical (non DM)

Donner un exemple de votre choix d'un DM connecté

Quelques chiffres sur les objets connectés

- A l'échelle mondiale : 11,7 milliards d'objets connectés à fin 2020 (*cabinet d'études IoT Analytics*)
- 95% de la population Fr équipée d'un mobile, dont 77% d'un smartphone
- En 2020, plus de 350 000 Applications santé sont disponibles (App Store, Google Play Store, etc.)
- Vs 100 000 en 2013



Objet connecté :
ex de principe de fonctionnement

Association de l'objet connecté à l'application smartphone ou tablette

Installation de l'objet connecté sur soi (ou dans la pièce de maison la plus adaptée en fonction du type d'objet)

Les capteurs intégrés à l'objet connecté enregistrent l'activité observée sous forme de données brutes

Les données brutes sont traitées par l'application pour être restituées de manière compréhensible par l'utilisateur

L'utilisateur de l'objet connecté peut **analyser ses données personnelles** et chercher à **adapter son comportement**

http://www.guide-sante-connectee.fr/un-objet-connecte-pour-quel-usage

Dispositifs connectés à l'Internet pouvant collecter, stocker, traiter et diffuser des données ou pouvant accomplir des actions spécifiques en fonction des informations reçues (d'après HAS 2016)

Objets connectés en santé : définition

Définition → il n'existe aucune définition légale !

Deux catégories :

- Les objets non-médicaux → ont un effet potentiel sur la santé MAIS sans finalité médicale déclarée
  - Certains sont dits « *objets de bien-être* »

- Les dispositifs médicaux → ont une finalité médicale

Définition du Dispositif Médical

« Tout instrument, appareil, équipement, logiciel, implant, réactif, matière ou autre article, destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour l'une ou plusieurs des fins médicales …

…et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens»

D’après MDR 2017/745

Finalités médicales

- Diagnostic, prévention, contrôle, prédiction, pronostic, traitement ou atténuation d'une maladie
- Diagnostic, contrôle, traitement, atténuation d'une blessure ou d'un handicap ou compensation de ceux-ci
- Investigation, remplacement ou modification d'une structure ou fonction anatomique ou d'un processus ou état physiologique ou pathologique
- Communication d'informations au moyen d'un examen in vitro d'échantillons provenant du corps humain, y compris les dons d'organes, de sang et de tissus

Autres DMs :

- les dispositifs destinés à la maîtrise / assistance de la conception
- les produits spécifiquement destinés au nettoyage, à la désinfection ou à la stérilisation des dispositifs DM

slido

Indiquez la/les réponse(s) exacte(s)

ⓘ Start presenting to display the poll results on this slide.

Rôle des professionnels de santé comme acteurs de santé publique

- Connaitre les bases de la réglementation sur les produits de santé
- Savoir alerter les patients et autres professionnels de santé
- Savoir poser un regard critique sur les allégations de certains objets en santé

Rôle des autorités sanitaires par rapport à certaines revendications d'usage ou allégations 1/2

- Cas de figure 1 : Le fabricant met en avant de réelles allégations médicales fondées, sans pour autant présenter son produit comme un DM par méconnaissance de la règlementation.

⇒*Les autorités lui demandent de certifier son produit et de respecter les obligations propres aux dispositifs médicaux*

- Cas de figure 2 : Le fabricant met en avant de réelles allégations médicales fondées, sans pour autant présenter son produit comme un DM alors qu'il connait la règlementation.

⇒ *Les autorités lui demandent de certifier son produit et généralement sanctionnent l'opérateur pour mise sur le marché d'un DM sans certification*

Rôle des autorités sanitaires par rapport à certaines revendications d'usage ou allégations 2/2

- <u>Cas de figure 3 :</u> Le fabricant met en avant des allégations médicales ou de santé non justifiées aux fins de mieux positionner son produit d'un point de vue marketing.

⇒ *Les autorités interviennent pour faire enlever les allégations trompeuses*

Objet connecté en santé

Finalité médicale ?

NON → Objet non-médical

OUI → Dispositif médical

Réglementation

Respect des dispositions relatives au partage d'informations et aux traitements de données à caractère personnel

+

Les dispositifs médicaux connectés: fonctions, catégories

Fonctions potentielles d'un dispositif médical connecté

- Télécommunication → Communication à distance des données.

Ex. données importées dans le cadre d'une télésurveillance et d'une téléconsultation.

- Télésurveillance médicale → Permet à un professionnel de santé:
  - d'interpréter à distance les données de suivi d'un patient
  - de prendre des décisions relatives à la prise en charge de ce patient.

Enregistrement et transmission des données automatisés ou réalisés par le patient ou par un professionnel de santé.

- Téléconsultation → Permet à un professionnel de donner une consultation à distance à un patient.

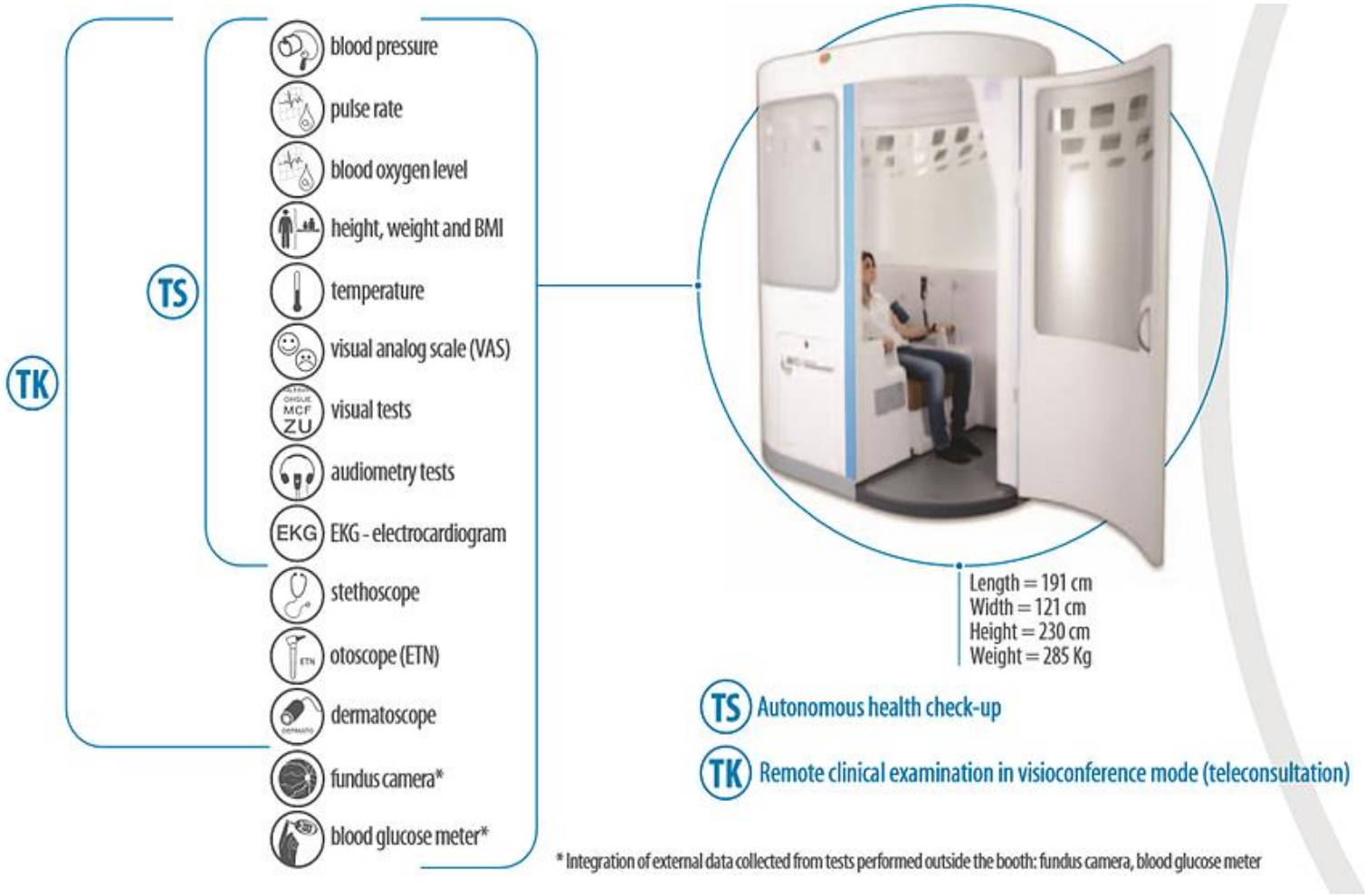
Fonction de télésurveillance: exemples

- Surveillance télé-respiratoire
  - Observance (temps d'utilisation de la machine), index d'apnées-hypopnées
  - SPO2 hors limite
  - Pression artérielle, fréquence cardiaque hors limite

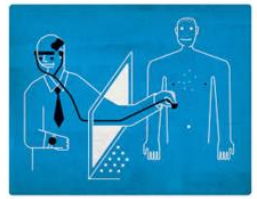
- Télé-diabétologie
  - Observance (non utilisation pendant plusieurs jours)
  - Hypoglycémie sévère
  - Objectifs glycémiques non atteints

- Télé-cardiologie
  - Elévation fréquence cardiaque
  - Episode d'arythmie

Fonction de téléconsultation: exemple de DM



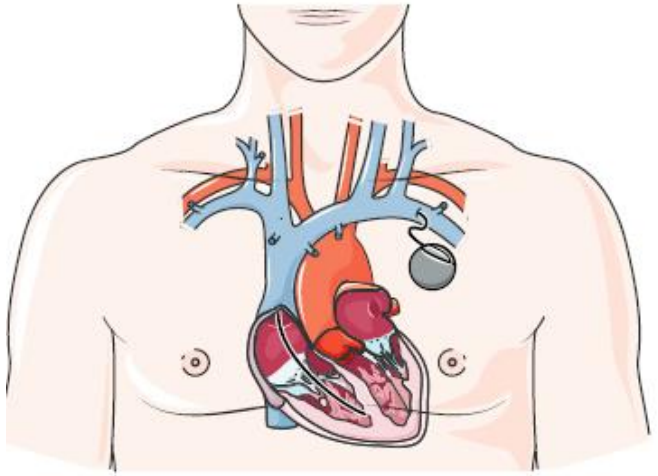
Tous les outils de téléconsultation ne sont pas des DM !

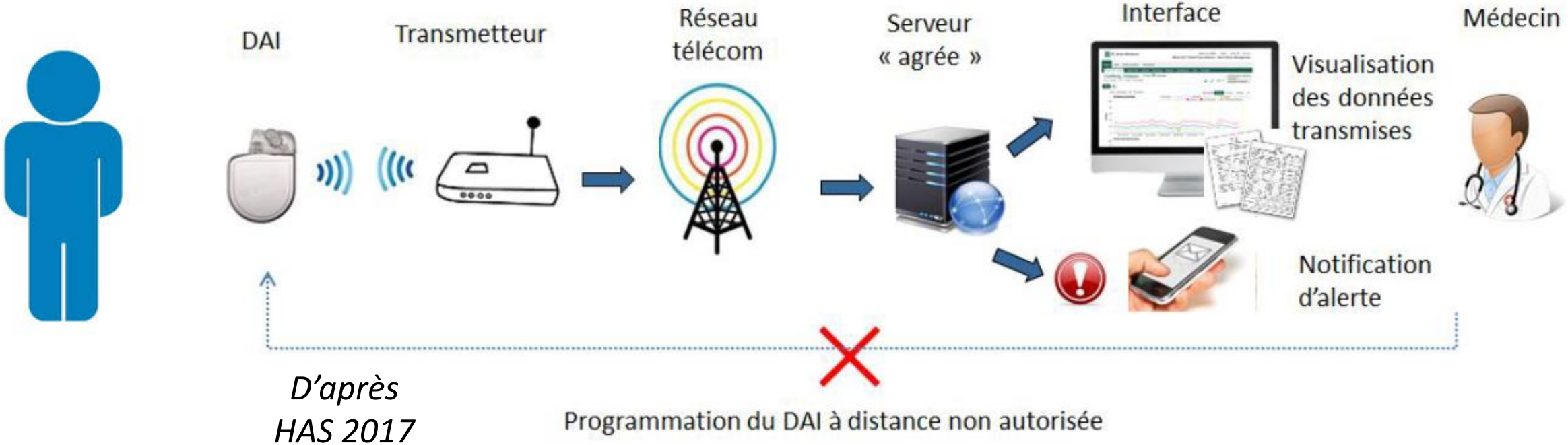


« Consult Station »: DM de classe IIa

1- DMC : fonction thérapeutique ou diagnostique indépendante de la fonction de télécommunication de données de santé

Exemple → Défibrillateur cardiaque implantable indiqué en prévention de la mort subite et possédant un système permettant le suivi à distance des fonctions du défibrillateur.





D'après HAS 2017

2-Les dispositifs médicaux connectés dont la finalité médicale est uniquement liée à la fonction de télé-communication de données de santé

- Fonction de télécommunication du dispositif médical connecté → surveillance de données de santé ↔ finalité thérapeutique ou diagnostique

- Ex. *Suivi à distance par télésurveillance réalisé via un DMC → prise en charge précoce d'un patient avec pathologie chronique*

Enjeux de sécurité des dispositifs médicaux connectés

Réalité ou science-fiction ?

Enjeux de cybersécurité

https://edition.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html

CNN Regions » Cheney's defibrillator was modified to prevent hacking International Edition +

Cheney's defibrillator was modified to prevent hacking

By Dana Ford, CNN
Updated 1351 GMT (2151 HKT) October 24, 2013

Doctors feared terrorists could hack into Cheney's heart defibrillator and kill him.

Story highlights

"I worried that someone could kill you," doctor tells Cheney

Cheney, 72, suffered his first of five heart attacks in 1978 -- at age 37

The former VP talks to CNN's Sanjay Gupta in

Cautious doctors replacing former Vice President Dick Cheney's heart defibrillator in 2007 modified it so it couldn't be hacked by terrorists who might try to kill him, Cheney told CNN's Sanjay Gupta in an interview that aired Sunday night on CBS' "60 Minutes."

Cheney's cardiologist, Dr. Jonathan Reiner, was

News & buzz

Roger Federer: Swiss star to skip French Open

Stephon Clark's grandmother says 'they didn't have to kill him...

Ad closed by Google

La sécurité des DM connectés en pratique à l'hôpital

Définition selon ANSM

- DMIL : Dispositifs médicaux intégrant du logiciel
  - **Dispositifs médicaux connectés**
  - **Logiciels DM**

Exemples de dispositifs médicaux intégrant du logiciel (DMIL)

- Logiciel de planification de traitement en radiothérapie (TPS) ;
- Application mobile d'évaluation des grains de beauté à risque de cancer ;
- Application mobile pour le calcul personnalisé des doses d'insuline. DM utilisant un logiciel pour leur fonctionnement et leur supervision :
- Pacemakers, pompes à perfusion ;
- Stations de monitoring ou d'anesthésie, …

Périmètre DM connectés

Insuffisamment sécurisé

→ Vol

Ports USB non sécurisés

→ Connexion clé USB contaminée

Télémaintenance sans contrôle

→ Transmission virus

Données non supprimées (retrait du service)

→ Transmission données Patients

Configurations non vérifiées

→ Création canal d'accès

Comptes non sécurisés

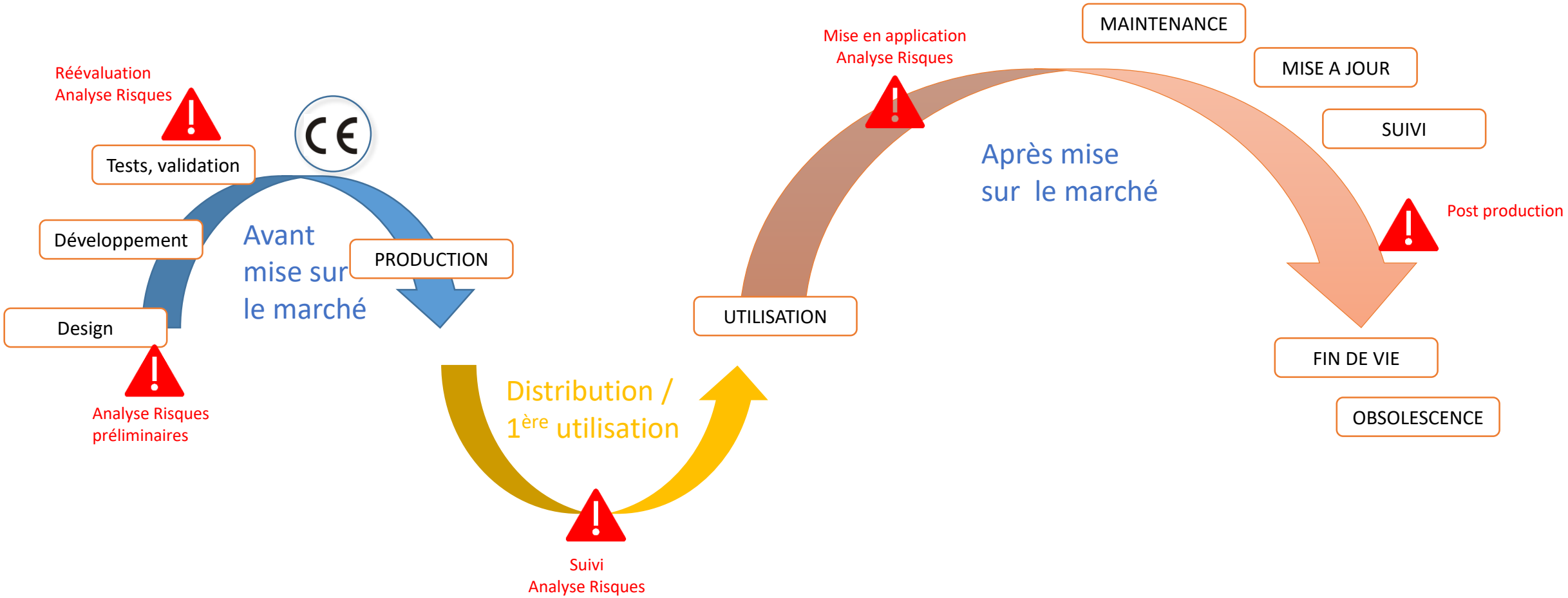
→ Accès données

Mise à jour non appliquée

→ Failles potentielles

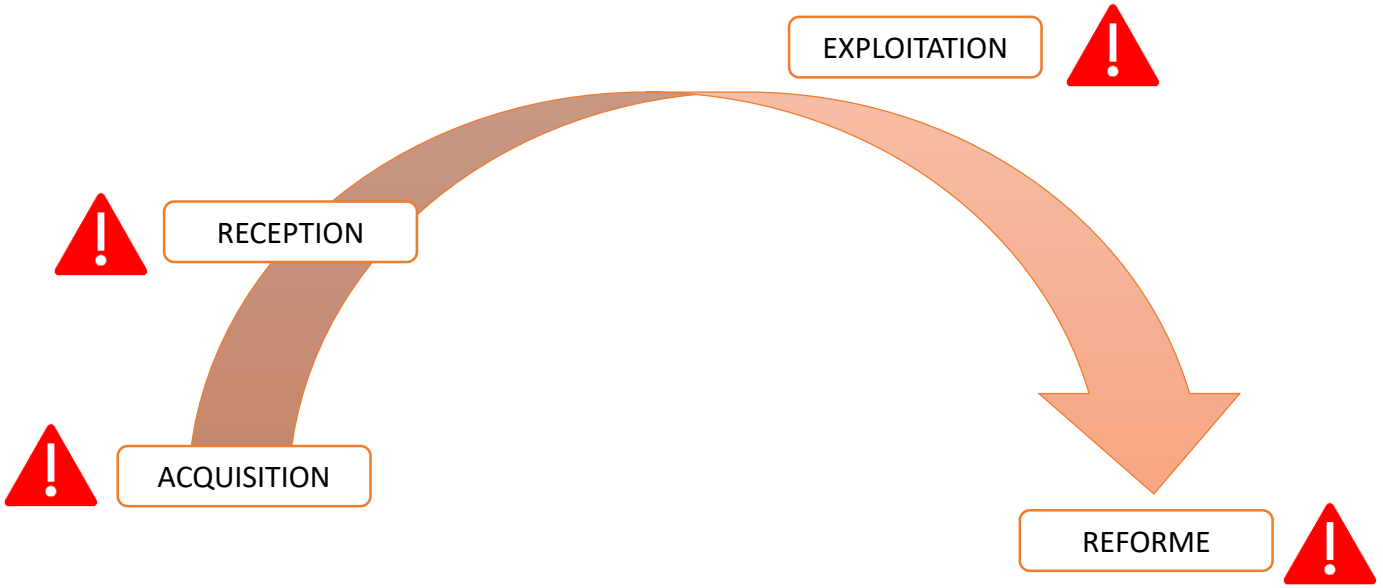
Source Proaxio

Quels risques pour les DMIL (fournisseurs) ?

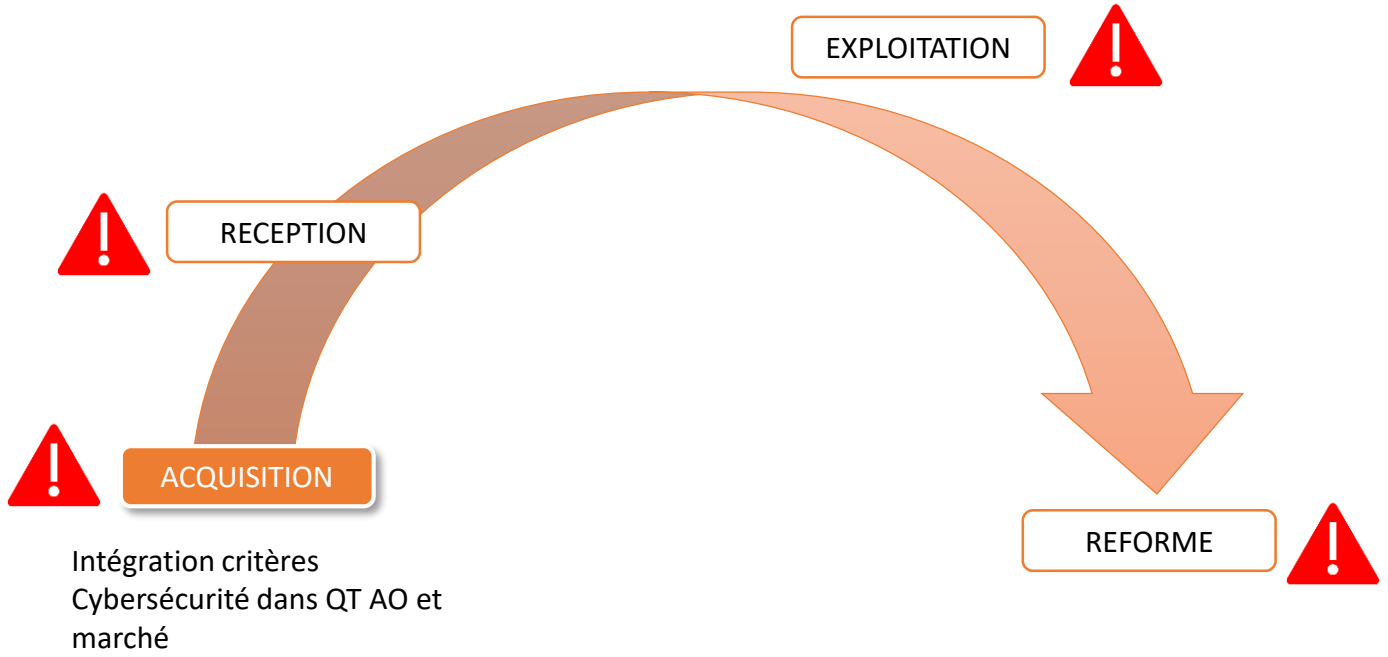


Reco ANSM Cybersécurité des DMIL : Analyse de risque durant cycle de vie

Quels risques pour les DMIL (utilisateurs)?

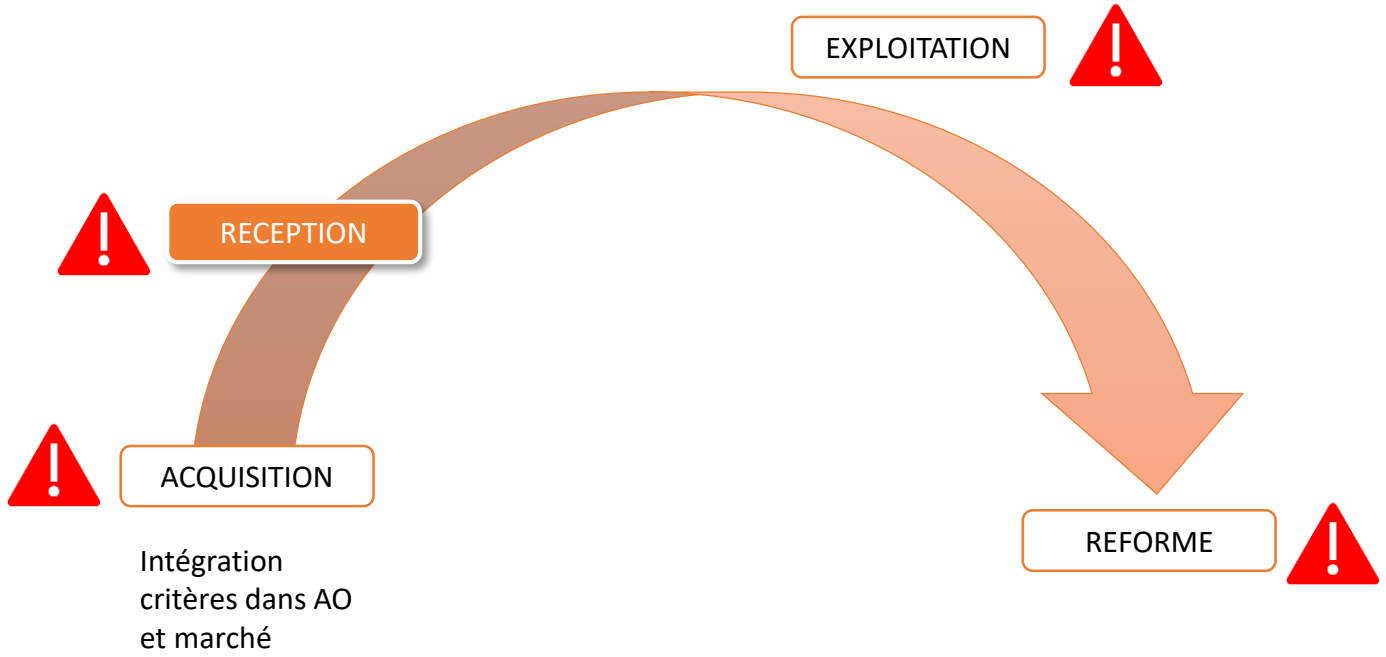


Quels risques pour les DM connectés (utilisateurs)?



Intégration critères Cybersécurité dans QT AO et marché

Quels risques pour les DM connectés (utilisateurs)?



PV de réception avec tous les critères DM classiques (Classe, garanties, …)

- Criticité PIEU
  - P : Incidence des pannes
  - I : Importance de l'équipement
  - E : Etat de l'équipement
  - U : Taux d'utilisation de l'équipement
- Matrice simplifiée risques cyber
  - Version système exploitation (W10, WS2016, …)
  - Antivirus (COL, Prestataire, Aucun)
  - Equipements dans le domaine
  - Accès à internet (O/N)
  - Equipement avec données patients (O/N)
  - Equipement protégé par firewall prestataire (O/N)

Quels risques pour les DM connectés (utilisateurs)?

EXPLOITATION

P : incidence des Pannes	I : Importance de l'équipement	E : Etat de l'équipement	U : taux d'Utilisation de l'équipement
Il s'agit de refléter les répercussions sur la santé du malade ou des utilisateurs et celles sur la qualité des soins apportés par l'utilisation du dispositif. 0,01 : répercussions graves sur la qualité des soins 1 : répercussions sur la qualité des soins 2 : corrections des soins possibles 3 : aucune répercussion	Ce critère permet d'évaluer l'importance du dispositif par rapport à l'activité de soins associée. 0,01 : équipement stratégique (pas de délestage possible) 1 : important (pas de délestage mais sous-traitance possible) 2 : équipement secondaire (délestage possible) 3 : équipement de secours	L'état de l'équipement varie selon son âge et l'état dans lequel il a été maintenu. 0,01 : équipement à rénover ou à réformer 1 : à réviser 2 : à surveiller 3 : à l'état spécifié	C'est le rapport du temps d'utilisation réel sur le temps maximum possible. 0,01 : saturé 1 : élevé 2 : moyen 3 : faible

- Matrice simplifiée risques cyber
  - Version système exploitation (W10, WS201
  - Antivirus (COL, Prestataire, Aucun)
  - Equipements dans le domaine
  - Accès à internet (O/N)
  - Equipement avec données patients (O/N)
  - Equipement protégé par firewall prestataire (O/N)

P x I x E x U = Criticité

Si PIEU < 1 → DM très critique

Si 1 < PIEU < 10 → DM moyennement critique

Si PIEU > 10 → DM peu critique

Ex :

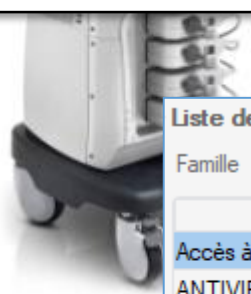
- Scanner d'imagerie : 0,01 x 0,01 x 3 x 1 = 0,0003
- Pousse seringue : 1 x 2 x 3 x 2 = 12

Quels risques pour les DM connectés (utilisateurs)?

Matrice simplifié Cybersécurité à réception enregistrée dans famille « équipements connectés » GMAO :

- Version système exploitation (W10, WS2016, …)
- Antivirus (COL, Prestataire, Aucun)
- Equipements dans le domaine
- Accès à internet (O/N)
- Equipement avec données patients (O/N)
- Equipement protégé par firewall prestataire (O/N)

→ Envoi systématique au SI à réception pour nouveaux équipements, travail en cours sur base de données DM
→ Requête BO partagée avec SI sur systèmes obsolètes (Ex : < W10), sans antivirus, …
→ Requête BO partagée avec résumé caractéristiques / équipement



intégration
critères dans AO
et marché

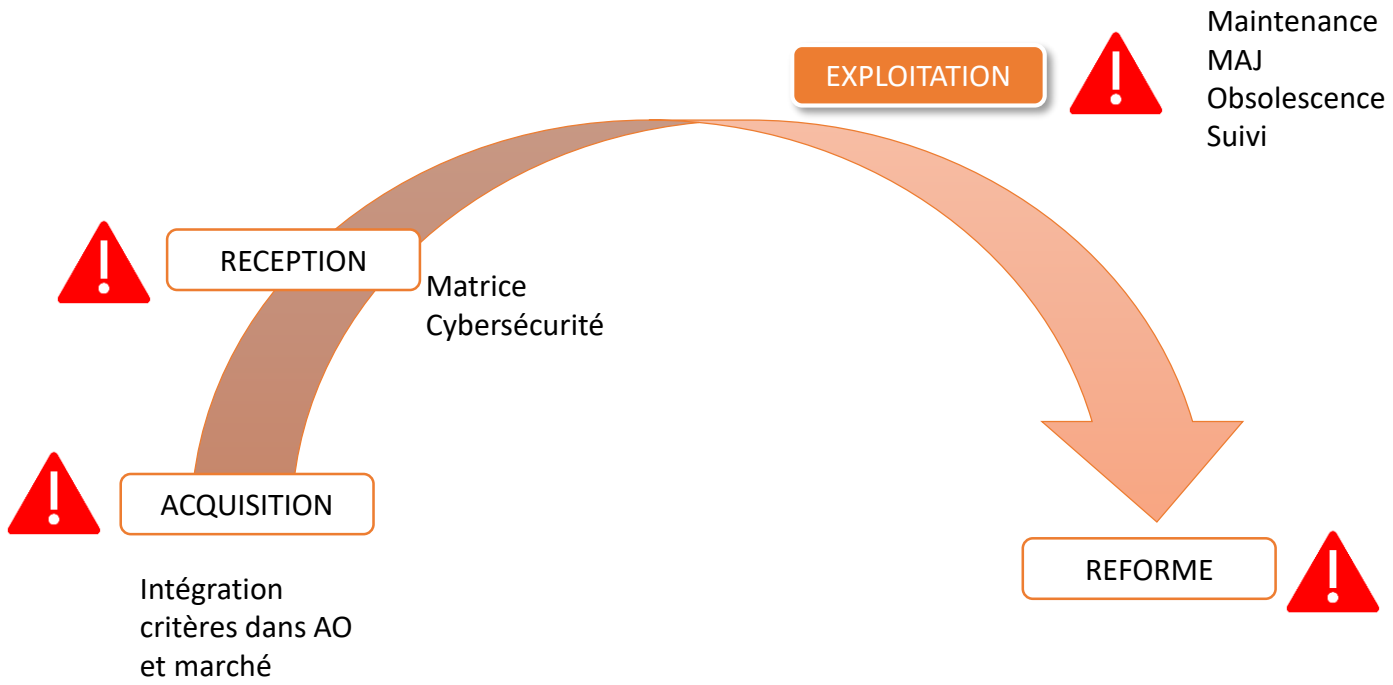
Liste des champs techniques liés à l'équipement

Famille 18 EQUIPEMENT CONNECTÉ

Name	Unité	Valeur
Accès à Internet	.	OUI
ANTIVIRUS	.	ANTIVIRUS COL
Equipement avec données patients	.	OUI
Equipement dans le domaine	.	OUI
Firewall Prestataire	.	NON
Mise à jour réalisée périodiquement	.	NON
SYSTEME EXPLOITATION	.	WINDOWS SEVEN
Version des applications supportée	.	NON

- Equipement avec données patients (O/N)
- Equipement protégé par firewall prestataire (O/N)

Quels risques pour les DM connectés (utilisateurs)?



Suivi des DM selon criticité PIEU via tableau de bord simplifié

- Equipements très critiques (Ex : Equipements lourds) → Indicateurs indisponibilité, temps arrêts, ..
- Equipement moyennement critiques → PM en retards, …
- Equipements peu critiques → Suivi programme maintenance, …

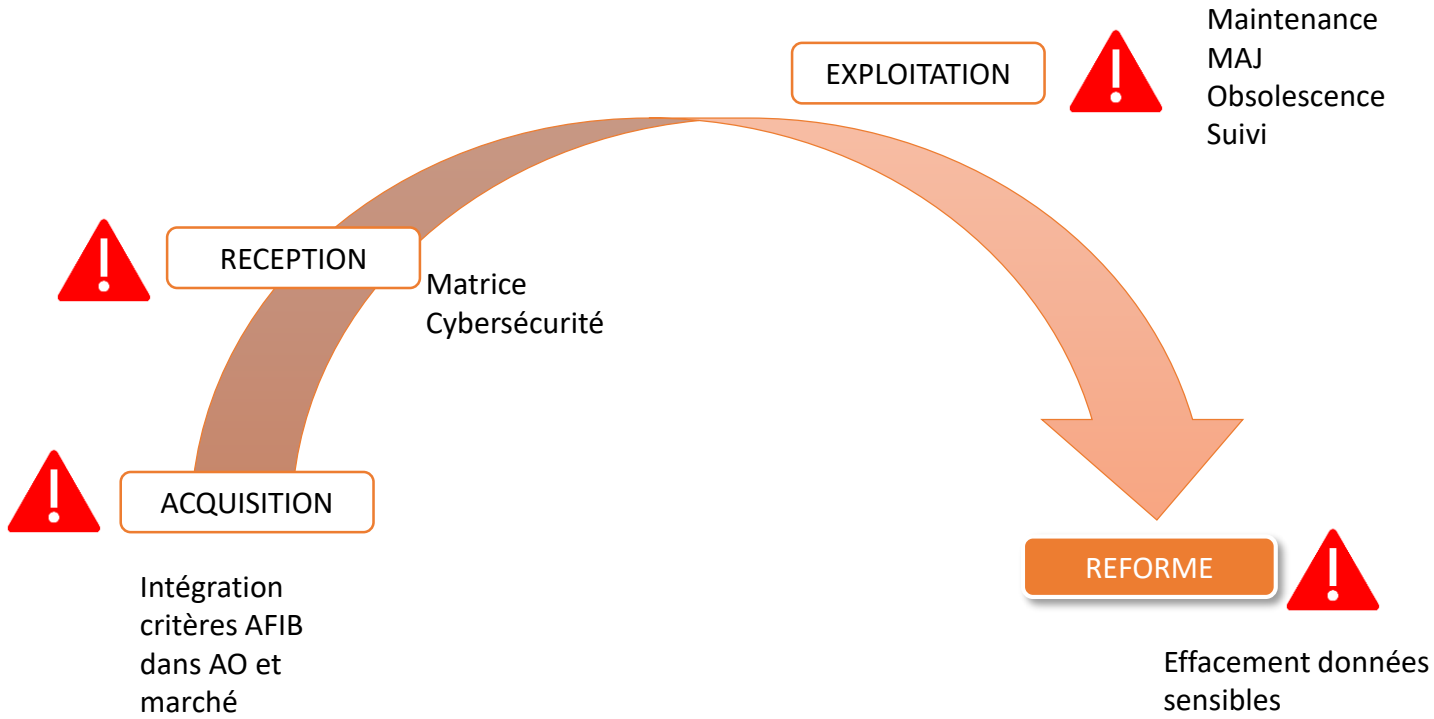
Matrice simplifiée risques cyber pour tout DMIL

- Mise à jour parc avec renseignements matrice
- Envoi systématique MAJ critères au SI
- Pas de plan d'actions établi pour l'instant mais vagues de MAJ
  - MAJ OS, antivirus, …
  - Suivi prestations fournisseurs, …

Cartographie partagée DM Logiciels (Biomed/SI) en projet 2025

→ Même process que DM (Réception, Traçabilité MAJ/Versions, …)

Quels risques pour les DM connectés (utilisateurs)?



Logiciels DM ?

Source Rumb

Logiciels DM

Si Logiciel = DM → Même process que tous les autres DM

- Classe de risque I, IIa, Ilb, III
- UDI
- Marquage CE MDR
- Suivi versions / MAJ
- Suivi interventions (sur site ou à distance)

Critères HAS

Crit.3.4-05-ee01-ASY : **L'établissement établit et met à jour, au moins une fois par an, une cartographie de l'ensemble des dispositifs médicaux numériques** à usage professionnel et, le cas échéant, analyse les risques et l'impact de chacun (transmission de données, réutilisation par l'industriel…).
Crit.3.4-05-ee02-ASY : Pour répondre aux besoins des équipes de soins, l'établissement dispose d'une organisation structurée pour l'acquisition des dispositifs médicaux numériques qui implique les services compétents, notamment les équipes informatiques et juridiques.
Crit.3.4-05-ee03-ASY : L'établissement organise la formation des professionnels utilisateurs d'un dispositif médical numérique afin que ces derniers en connaissent les performances, les conditions d'usage et les limites.
Crit.3.4-05-ee04-ASY : Dans le contexte de soins, pour les dispositifs médicaux numériques à usage professionnel, l'établissement se dote d'un processus de contrôle qualité impliquant, le cas échéant, un contrôle humain des résultats donnés par les dispositifs médicaux numériques en situation réelle d'utilisation.

Plan d'actions proposé au COL pour 2025

- Procédure de réception pour tout nouveau logiciel
- Travail sur listing des logiciels avec identification DM Logiciel
  → Si DM Logiciel
  - Relevé Marquage CE
  - Risque CE
  - Référent
    - Version
    - Historisation MAJ/Versions
  - Critère 4 HAS : CQ Utilisateurs ?

Avez-vous une vision exhaustive des DMIL ?

Avez-vous mis en place un plan d’action pour le parc des DM connectés ?

Avez-vous mis en place un plan d’action pour le parc installé des logiciels ?

Echanges

- Que faire pour un logiciel considéré DM développé in-situ ?

- Comment identifier les logiciels DM facilement ? Eudamed ? Fournisseurs ? Autres solutions ?

- Avez-vous développé des plans d'actions pour les DMIL ?
  - Acquisition des nouveaux DMIL
  - Exploitation …

- Comment mettre en œuvre critère 4 HAS : contrôle qualité des résultats donnés ?

Questions ?

Pr Xavier Armoiry
Xavier.armoiry@chu-lyon.fr

Hervé Szymczak
H-szymczak@o-lambret.fr