Livre Blanc

La Cybersécurité des Dispositifs Médicaux (IoMT)

Guide de bonnes pratiques pour ingénieurs et techniciens biomédicaux en milieu hospitalier

Convergence Santé
www.inkkreation.com

CONVERGENCE SANTÉ
MedTech • HealthTech • IA

Introduction – L’enjeu vital de la convergence Biomédical / IT

La transformation numérique de l’hôpital repose de plus en plus sur des dispositifs médicaux connectés, des logiciels cliniques et des infrastructures serveurs interopérables.

Cette convergence entre biomédical et informatique, bien qu’indispensable à la qualité et à la continuité des soins, introduit de nouveaux risques cyber pouvant impacter directement la sécurité des patients, la disponibilité des soins et la conformité réglementaire.

Ce livre blanc a pour objectif de fournir aux ingénieurs et techniciens biomédicaux une **vision opérationnelle et pragmatique** des bases de la cybersécurité appliquée aux dispositifs médicaux (IoMT – Internet of Medical Things), en tenant compte des contraintes spécifiques du milieu hospitalier : continuité de service, exigences réglementaires, dépendance aux constructeurs et coexistence avec les systèmes d’information hospitaliers.

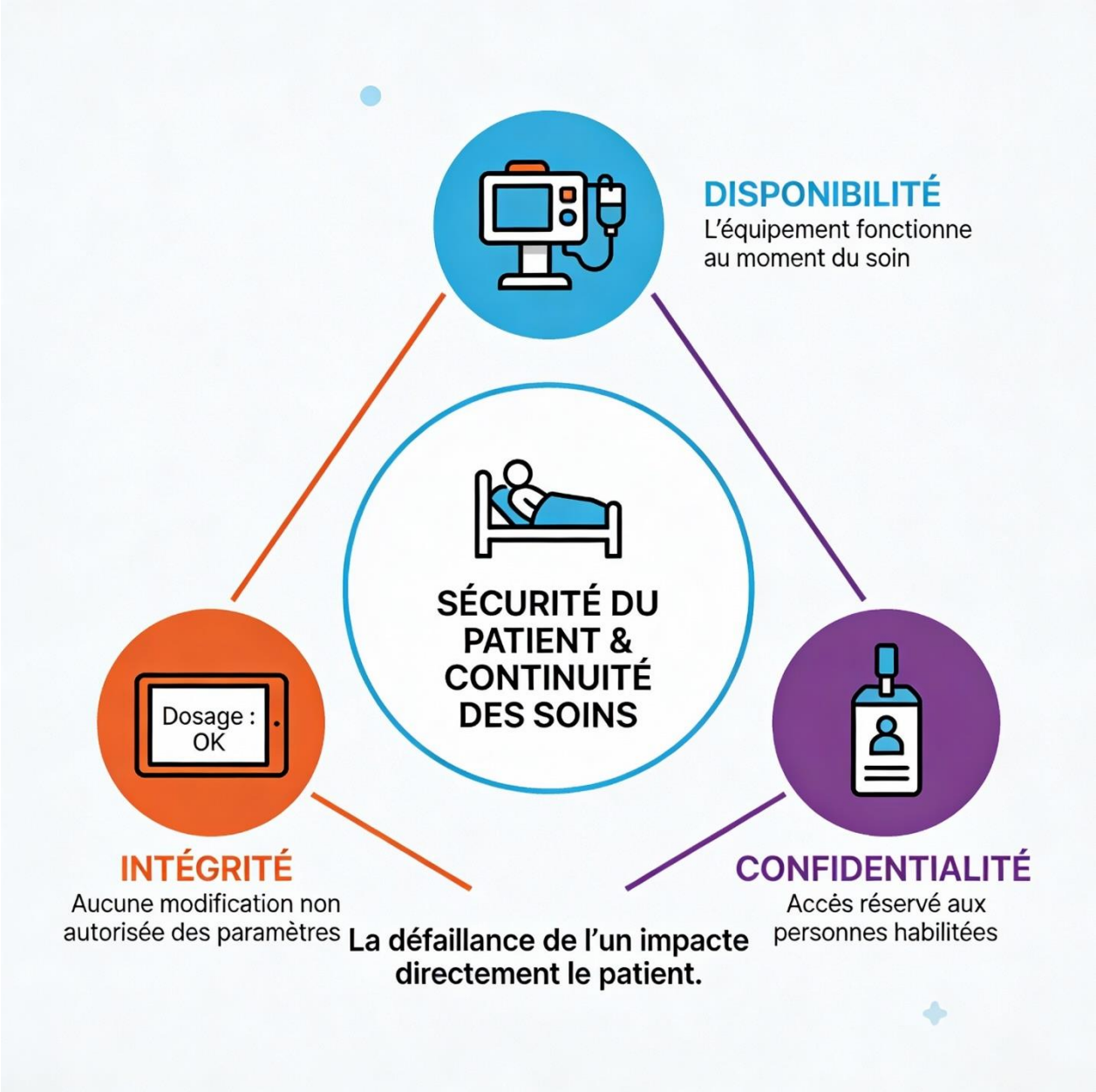
Historiquement, la maintenance biomédicale se concentrait sur la **sécurité électrique**, la **métrologie** et la **disponibilité fonctionnelle** des équipements. Aujourd’hui, un moniteur patient, une pompe à perfusion ou un automate de laboratoire est avant tout un **système informatique spécialisé**, connecté au réseau de l’hôpital et parfois à Internet.

Une faille de cybersécurité peut désormais entraîner : - un **arrêt de service critique** (ex. ransomware sur un automate), - une **altération de données cliniques**, - une **atteinte à la confidentialité des données de santé**, - voire un **risque direct pour le patient**.

La cybersécurité devient ainsi une **extension naturelle de la matériovigilance**.

1. Les trois piliers fondamentaux : la triade DIC

Toute démarche de cybersécurité repose sur la triade **Disponibilité – Intégrité – Confidentialité (DIC)**.



1.1 Disponibilité

Le dispositif doit être **opérationnel au moment du soin**.

Exemples de menaces : - ransomware bloquant un système d'imagerie, - saturation réseau rendant un moniteur patient injoignable, - défaillance serveur empêchant l'accès au DPI.

Point clé biomédical : un équipement indisponible est assimilable à une panne critique.

1.2 Intégrité

Les données et paramètres ne doivent pas être modifiés de manière non autorisée.

Exemples : - modification d'une posologie dans un logiciel de pompe, - corruption des résultats d'analyses biologiques, - altération de données DICOM.

1.3 Confidentialité

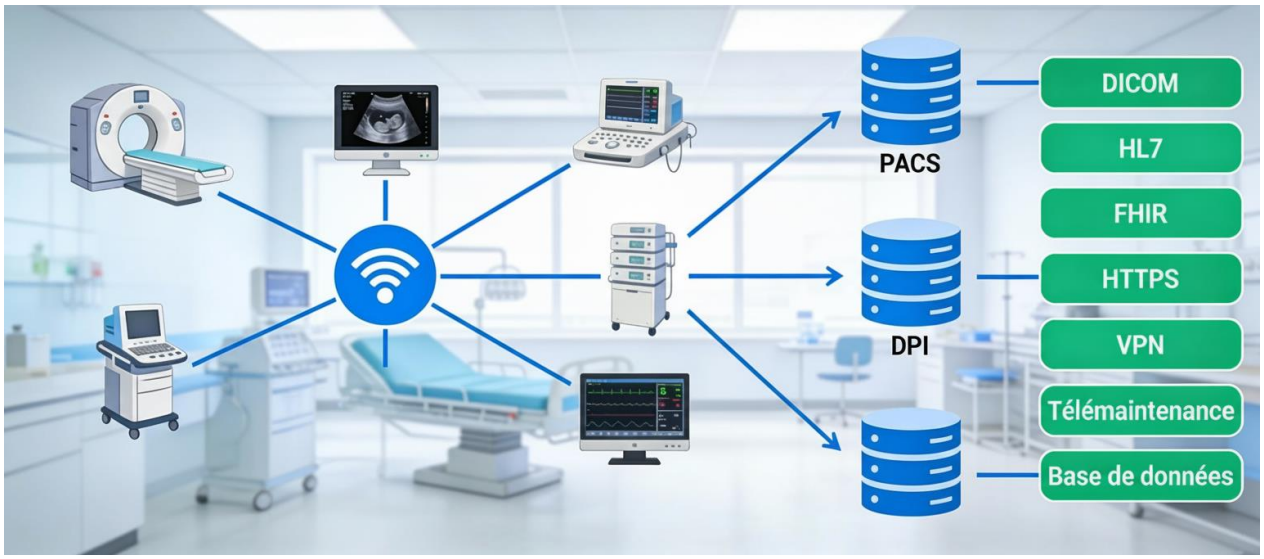
Seules les personnes habilitées peuvent accéder aux données de santé.

Enjeux réglementaires : - RGPD, - secret médical, - traçabilité des accès.

---

2. Cartographie et inventaire : « On ne protège pas ce que l'on ne voit pas »

La **cartographie des actifs biomédicaux connectés** est la pierre angulaire de toute stratégie de cybersécurité.



2.1 Inventaire technique minimal

Pour chaque dispositif ou logiciel associé : - **Identification** : fabricant, modèle, numéro de série, - **Localisation clinique** : service, salle, usage critique, - **Identité réseau** : adresse IP (fixe ou DHCP), adresse MAC, - **Système d'exploitation** : - Windows (souvent versions anciennes), - Linux, - OS propriétaire, - **Connectivité** : Ethernet, Wi-Fi, Bluetooth, USB.

2.2 Flux de données et dépendances

Identifier précisément : - les **protocoles utilisés** (DICOM, HL7, FHIR, SMB, HTTPS…), - les **serveurs cibles** (PACS, DPI, middleware), - les **accès distants** (télémaintenance constructeur, VPN), - les dépendances critiques (serveur de licence, base de données).

---

3. Stratégies de défense prioritaires

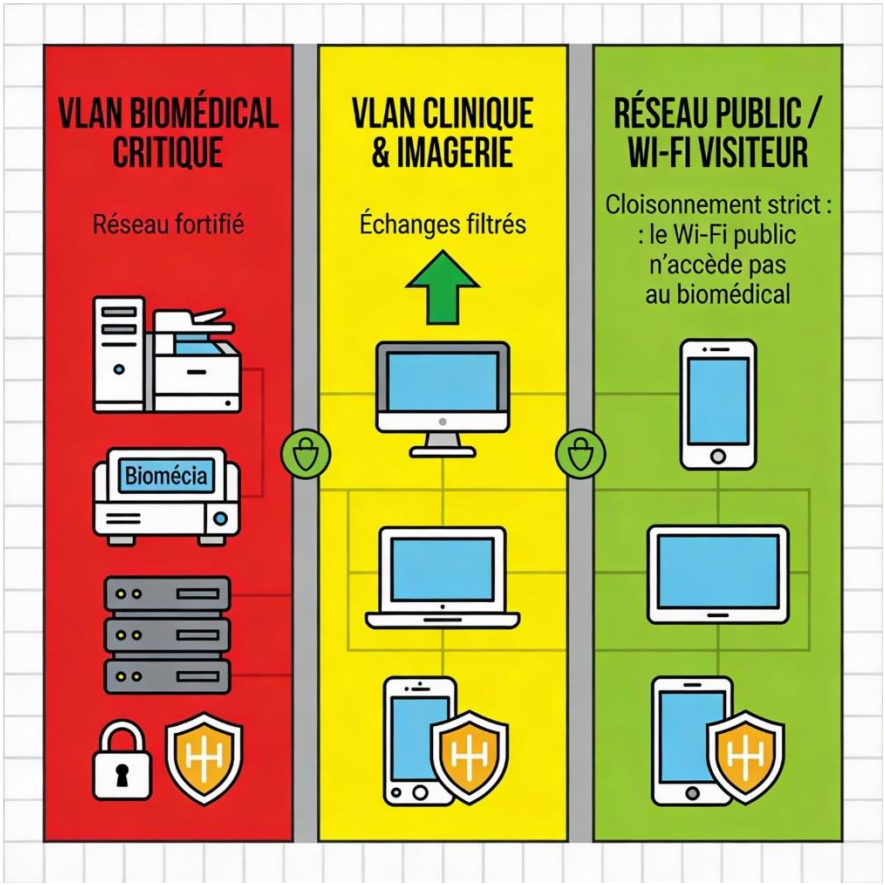
3.1 Cloisonnement réseau (VLAN et segmentation)

Le principe fondamental est la **séparation des usages**.

À proscrire : - dispositifs médicaux sur le Wi-Fi public, - mélange réseau biomédical / administratif.

Bonnes pratiques : - VLAN dédiés par famille d'équipements, - micro-segmentation pour les dispositifs critiques, - filtrage des flux par pare-feu.

Exemple : - VLAN imagerie (IRM, scanners), - VLAN pompes et monitoring, - VLAN automates de laboratoire.



3.2 Gestion des accès et des comptes

Mesures essentielles : - suppression des comptes par défaut (admin/admin), - mots de passe robustes et uniques, - limitation des privilèges (principe du moindre droit), - journalisation des accès.

Mesures complémentaires : - désactivation du Bluetooth et du Wi-Fi inutiles, - verrouillage ou condamnation des ports USB, - authentification forte lorsque possible.

3.3 Cycle de vie, mises à jour et correctifs

Le **patching** est un point particulièrement sensible en biomédical.

Contraintes spécifiques : - certification CE, - validation constructeur obligatoire, - risques fonctionnels.

Bonnes pratiques : - exiger le **MDS2** lors des appels d'offres, - documenter les versions logicielles installées, - planifier les mises à jour validées constructeur, - intégrer la cybersécurité dès la phase d'achat.

---

4. Focus sur les solutions serveurs et logiciels

Le dispositif médical n'est souvent qu'un **client** d'un système plus large.

4.1 Sécurisation des serveurs et passerelles

- durcissement des systèmes (hardening),
- limitation des services actifs,
- mises à jour régulières,
- sauvegardes testées et restaurables.

4.2 Antivirus, EDR et supervision

Si le dispositif repose sur Windows : - antivirus ou EDR validé par le constructeur, - exclusions adaptées aux processus critiques, - supervision conjointe avec la DSI.

4.3 Chiffrement des données

- chiffrement des flux réseau (TLS 1.2 minimum),
- chiffrement des disques durs ou bases locales,
- gestion sécurisée des certificats.

---

5. Procédure en cas d'incident – Le réflexe Bio-IT

5.1 Signes d'alerte

- lenteur inhabituelle,
- messages ou fenêtres anormales,

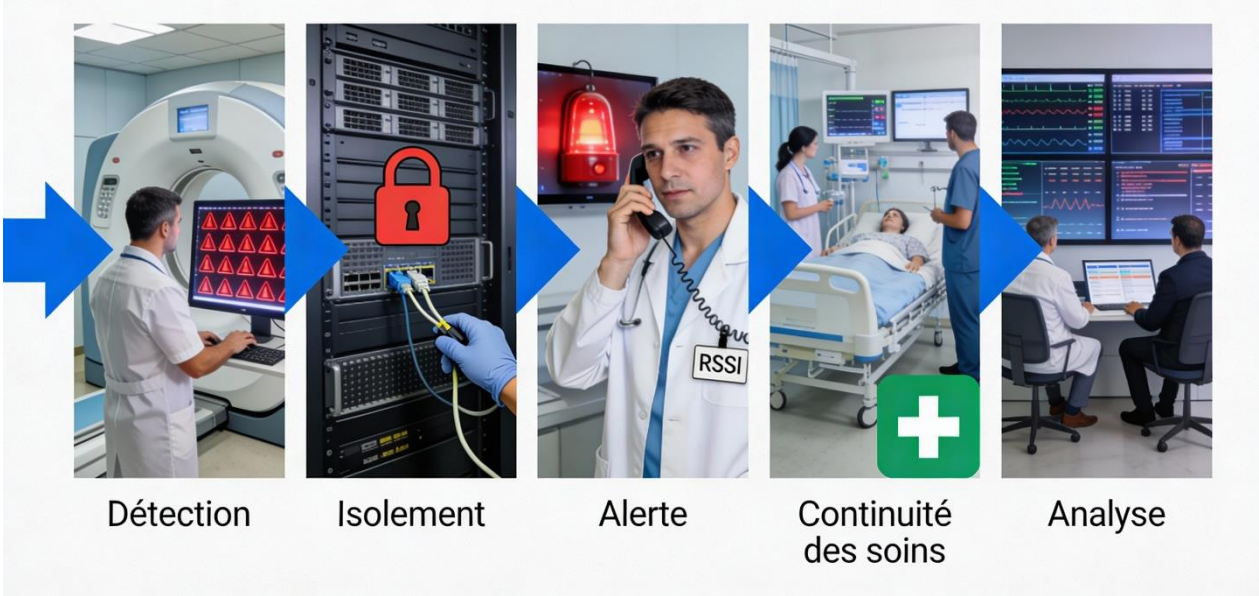
- redémarrages intempestifs,
- comportement incohérent de l'équipement.

5.2 Actions immédiates

1. **Isoler** : débrancher le câble réseau (sans éteindre l'appareil si possible),
2. **Alerter** : DSI et RSSI sans délai,
3. **Qualifier** : évaluer l'impact clinique et activer le mode dégradé si nécessaire.

5.3 Traçabilité et retour d'expérience

- documenter l'incident,
- analyser les causes,
- mettre à jour les procédures,
- sensibiliser les équipes.



---

6. Cadre réglementaire et normatif applicable en milieu hospitalier

La cybersécurité des dispositifs médicaux s'inscrit dans un **cadre réglementaire et normatif de plus en plus structurant**, qui concerne directement les établissements de santé et leurs services biomédicaux.

6.1 Directive européenne NIS2

La directive **NIS2** (Network and Information Security) renforce les exigences de cybersécurité pour les entités essentielles, dont les hôpitaux.

Impacts pour le biomédical : - obligation de **mesures techniques et organisationnelles adaptées**, - gestion des risques cyber sur les équipements

critiques, - **déclaration obligatoire des incidents majeurs**, - responsabilité accrue de l'établissement.

> Les dispositifs médicaux connectés critiques deviennent des actifs stratégiques au sens de NIS2.

6.2 Norme IEC 80001 – Gestion des risques IT-réseaux

La norme **IEC 80001** est spécifiquement dédiée à la gestion des risques liés aux réseaux IT intégrant des dispositifs médicaux.

Principes clés : - responsabilité partagée entre biomédical, IT et clinique, - analyse de risques avant toute mise en réseau, - prise en compte explicite de la **sécurité, efficacité et disponibilité**.

Pour le biomédical : - rôle central dans l'identification des usages cliniques, - participation aux analyses de risques réseau.

6.3 Référentiels et recommandations ANSSI

En France, l'**ANSSI** fournit des guides et recommandations applicables au secteur santé : - hygiène informatique, - segmentation réseau, - gestion des incidents cyber, - sécurisation des accès distants.

Ces référentiels servent souvent de base aux audits et contrôles internes.

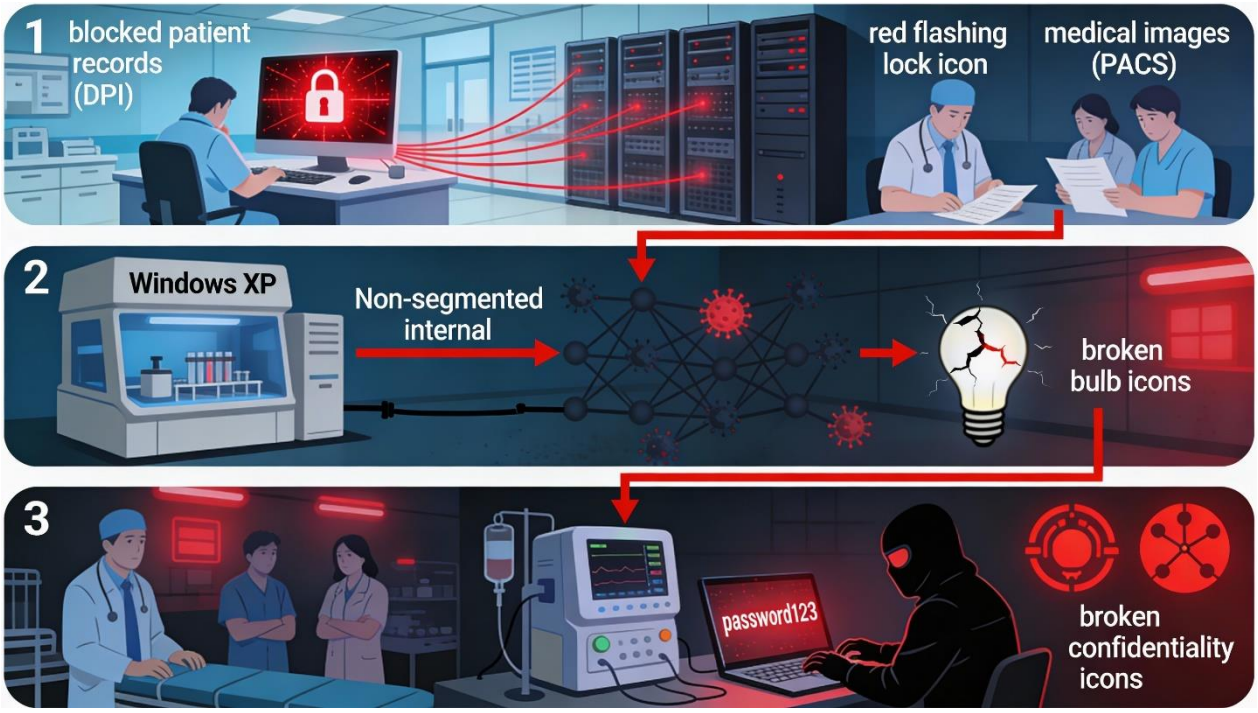
6.4 ISO 27001 et adaptation au contexte biomédical

La norme **ISO/IEC 27001** définit un système de management de la sécurité de l'information (SMSI).

Apports pour le biomédical : - approche structurée du risque, - formalisation des procédures, - intégration de la cybersécurité dans le cycle de vie des équipements, - amélioration continue.

---

7. Cas concrets d’attaques cyber en milieu hospitalier



7.1 Ransomware sur un hôpital

Scénario : un ransomware se propage via un poste bureautique et atteint des serveurs hébergeant des applications biomédicales.

Conséquences : - indisponibilité du DPI et du PACS, - reports d’examens, - retour au papier, - surcharge des équipes cliniques.

Leçons clés : - importance de la segmentation réseau, - sauvegardes isolées et testées, - procédures de continuité d’activité.

7.2 Automate de laboratoire compromis

Scénario : automate sous Windows obsolète, non segmenté, infecté via le réseau interne.

Conséquences : - résultats retardés ou indisponibles, - impact direct sur les décisions médicales, - arrêt temporaire de l’activité.

Leçons clés : - inventaire précis des OS, - cloisonnement strict, - coordination biomédical / DSI.

7.3 Accès distant constructeur mal sécurisé

Scénario : compte de télémaintenance avec mot de passe faible exploité.

Conséquences : - accès non autorisé au dispositif, - risque de modification de paramètres, - atteinte à la confidentialité.

Leçons clés : - contrôle des accès distants, - authentification forte, - traçabilité et journalisation.

Conclusion – La cybersécurité comme composante de la matériovigilance

La cybersécurité des dispositifs médicaux n'est plus une option ni un sujet purement informatique. Elle constitue un **enjeu clinique, organisationnel et réglementaire**.

La seule approche efficace repose sur : - une **collaboration étroite** entre services biomédicaux, DSI et RSSI, - une **connaissance fine de l'usage clinique**, - une **maîtrise des flux numériques**.

En intégrant la cybersécurité au quotidien du biomédical, l'hôpital renforce non seulement sa résilience numérique, mais surtout la **sécurité et la qualité des soins**.