**GT Ethique 19/5/2025**

**Rencontre avec le Dr Pierre-Jean Verheyden, DPO-CISO au Centre Hospitalier Interrégional Edith Cavell (CHIREC)**

*Voir aussi le PPT du Dr Verheyden.*

Le docteur P.-J. Verheyden (PJV) est médecin et coordinateur d’implémentation du dossier médical informatisé. Il est devenu récemment DPO puis CISO (responsable de la cybersécurité). En tant que DPO, il est chargé du suivi de l’AI ACT et de ses nouvelles normes.

PJV : L’IA est un outil. Les hôpitaux et prestataires de soins en ont déjà déployé d’autres par le passé (robots). Une formation continue des prestataires de soins est mise en place pour assurer la meilleure qualité possible.

L’IA est un ensemble de données traduites en algorithmes pour simuler une intelligence humaine amplifiée. C’est un ensemble de règles qui disent aux machines comment effectuer leurs tâches. L’IA a besoin d’une grande quantité d’informations et a souvent recours au cloud. Beaucoup de changements ont lieu en permanence. Il est nécessaire se mettre à jour tout le temps.

Les principes à respecter en matière d’IA sont :

* la sécurité ;
* la transparence (= informer le mieux possible, or l’outil est présent partout, il est difficile d’imaginer l’avenir dans un contexte de révolution permanente des outils) ;
* la protection contre les biais discriminatoires (auditer Ies IA en place et contrôler les sources : les IA étroites (images) utilisent des informations étroites tandis que les IA génératives recherchent des informations dans des bases de données dont on ne contrôle pas les sources) ;
* la mise en place de contrôles pour assurer la responsabilité des décisions ;
* garantir l’inclusion et l’équité entre tous.

Le contexte européen est normé : protection des données, loi NIS2 (pour la sécurité des systèmes d’information). Cela crée une charge de mise en conformité. L’*IA officer*  s’occupe du registre des IA, de l’évaluation et de la gestion des risques, des mises en conformité, de former le personnel, d’assurer le suivi et l’audit des systèmes d’IA mis en œuvre. C’est un travail pour lequel les hôpitaux ne sont pas financés alors que les normes deviennent de plus en plus contraignantes.

IA en soins de santé ?

L’IA en soins de santé ne concerne pas seulement les soins. L’IA s’immisce dans toutes les structures des services hospitaliers (aussi administratifs). Elle répond aux besoins des prestataires de soins. Par exemple :

* Pour des dossiers lourds (800 pages) pour lesquels il est difficile de récupérer et de maîtriser toutes les données. L’IA permet de trouver des solutions pour économiser du temps et améliorer la prise en charge du patient.
* Premières IA = imageries médicales (IA étroites).
* Robots en chirurgie (gestion du mouvement) : permet l’amélioration des performances.
* Pharmacologie.
* Surveillance à distance des patients et détection des anomalies (chutes par exemple).

Formation du personnel soignant ?

La formation du personnel soignant ne concerne pas seulement l’IA. Il s’agit d’une formation continue pour toutes les évolutions technologiques. Car le principe est qu’il y a toujours une supervision humaine qui contrôle les outputs lorsqu’un système d’IA est implémenté. Il faut donc en avoir la capacité. Cela nécessite une adaptation de la part du personnel et, par conséquent, une obligation de formation dans le cadre des hôpitaux.

Transparence des diagnostics ?

Dans l’implémentation de systèmes d’IA, il faudra que les médecins s’adaptent en apprenant à réfléchir à ce que propose l’IA, à contrôler les sources (avec la difficulté des IA génératives). Des contrôles de qualité sont implémentés. On compare avec des solutions existantes ou humaines. Parfois ce n’est pas concluant, alors l’IA est abandonnée. Le CHIREC contrôle les IA en mode projet et se penche sur le RGPD, la cybersécurité, l’efficacité : on vérifie les sources des données contrôlées et la maîtrise des algorithmes ; on évalue les risques (si risques il y a, des contrôles spécifiques sont organisés ; s’il s’agit de hauts risques, les IA sont interdites). Les médecins doivent avoir accès aux informations de l’implémentation, à la façon dont fonctionnent les algorithmes et participer aux interactions avec les développeurs pendant l’implémentation.

Principes déontologiques dans l’utilisation de l’IA ?

* Bienveillance : l’IA améliore performance.
* Information au patient.
* Autonomie du patient.
* Consentement éclairé : le patient doit pouvoir comprendre le recours à l’IA et y adhérer librement.

La gouvernance se réalise au niveau du comité de direction.

Impact sur la pratique médicale ?

L’IA modifie la pratique et libère du temps pour la prise en charge des patients. La relation patient/médecin va être modifiée : d’une part, le médecin est aidé par l’IA dans la mise à jour du dossier ; d’autre part, le médecin communique au patient le type d’outil utilisé. La relation doit être de confiance. Le patient reste maître de sa décision.

PSH ?

Les PSH ne peuvent pas être exclues. L’accès doit être garanti pour tous les patients. Certaines études demandent l’inclusion de certains profils, cela dépend de l’objet de l’étude. Toutefois, l’égalité de traitement doit être garantie.

Discriminations ?

Oui il y en a, mais il faut pouvoir les analyser et les contrôler. Cela demande un contrôle humain de la qualité des IA. Voir ci-dessus la gestion de projet pratiquée au CHIREC, avec décision oui/non.

Consentement pour les programmes de recherche ?

Le patient a le droit de retirer son consentement. C’est supervisé par les comités d’éthique. Exception : la réutilisation des données de santé mais ce n’est pas encore clair. Le RGPD reste la base. C’est de là que vient l’obligation d’avoir un DPO dans les hôpitaux et un *AI officer* pour contrôler les risques. Il faudrait voir comment les hôpitaux peuvent être financés pour cette charge de travail. Les recherches sont supervisées par les comités d’éthique. Les données secondaires sont anonymisées. C’est une question en cours de discussion.

Qui collecte les données ? Le prestataire de soins. Elles sont traitées par le responsable du traitement (médecin directeur). L’institution a l’obligation de protéger les données. C’est une obligation légale générale, pas seulement liée à IA. Quand les données sont envoyées dans des IA génératives, elles doivent être anonymisées.

Les principes du secret professionnel et de la confidentialité ne changent pas. Cela relève du code pénal. Il est de la responsabilité du médecin de ne pas rompre ce secret. Il faut donc maîtriser la façon dont l’IA utilise les données. Cela peut aboutir à des condamnations.

Défis de l’utilisation de l’IA ?

* Contrôler.
* Utiliser l’opportunité d’améliorer soins.
* Responsabilité de la gouvernance : vérifier que les principes de responsabilité, de transparence, de conformité aux lois, de respect des personnes et des données soient respectés.
* Obligation des hôpitaux de tenir à jour les données, de les protéger (principe de robustesse). Lutter contre les cyberattaques (Loi NIS2).
* AI ACT.
* Supervision par le Centre pour la Cybersécurité Belgique (CCB).

La durée de conservation des données est de 30 à 50 ans. Cela limite le droit du patient à la suppression de ses données. Mais le droit de correction existe. Ici, la supervision reste humaine. Il n’y a pas (encore) d’IA qui s’en charge.

Gestion et mise à jour des données dans l’entrepôt des données de l’hôpital

1. Qui identifie les erreurs ?

Au moment où l’IA est mise en place, un contrôle de l’outil est effectué. Le niveau de performance est certifié. Au CHIREC, cela fonctionne en mode projet (voir ci-dessus), dans un processus d’amélioration continue parce que l’IA évolue sans cesse. Cela nécessité une transparence et des audits permanents.

1. Stockage des données

Dans la prise en charge, les médecins généralistes ont leur rôle à jouer. Les données sont transmises via des *hubs*. Les dossiers sont partagés avec l’accord du patient. Si le médecin traitant ne participe pas, l’accès est garanti au patient lui-même. Ont également accès les infirmiers, les kinésithérapeutes, les pharmaciens, etc. Face à un hôpital très automatisé, une coordination sans médecin généraliste est-elle possible ? L’avenir nous le dira. Pour le moment, en l’absence d’un médecin traitant, c’est au patient à transmettre ses données à qui de droit. Face aux biais et aux hallucinations de l’IA, il faut comparer avec ses propres connaissances et maintenir éveillé son esprit critique.

1. Protection des données

Le RGPD reste la base. Pour se protéger des cyberattaques, les accès aux données sont limités, contrôlés et soumis à l’authentification à double facteur. La mise en conformité est en cours.

Libre circulation des données ?

Il s’agit de faire bénéficier des agences de santé belges et européennes d’un accès aux données. Ces données sont secondaires et anonymisées pour pouvoir entrer dans des testings. Cela nécessite la mise en place d’un système pour l’optin/optout des patients. Il est crucial de participer si notre pays veut pouvoir bénéficier des avancées dans la fabrication de nouveaux médicaments.

Commercialisation des données ?

Pas encore en application. Cela nécessite un optin/out du patient. Le patient doit être sensibilisé au fait que ses données peuvent aider à l’amélioration de la santé publique. Il y a des réunions en cours à ce sujet. Cela implique une gouvernance des institutions et dépend de la décision des responsables de traitement.

Cloud ?

Tous les hôpitaux n’utilisent pas le cloud. Dans ce cas, les données sont stockées sur les serveurs. Le cloud permet de délocaliser et protège des pannes mais demande une gestion de la cybersécurité. Certains hôpitaux passés au cloud en reviennent. En tout état de cause, les hôpitaux possèdent des générateurs de secours pour assurer la continuité des services. Il existe des normes strictes avec des tests annuels.

Problématiques rencontrées ?

On reçoit surtout des demandes d’exercice de droits de la part du patient. Le droit de suppression est limité par des obligations légales. Les données sont conservées minimum 30 ans. Beaucoup de données se trouvent dans les dossiers partagés, si le patient a donné son accord pour cela. Dans ce cas, le patient a le droit de demander une copie de son dossier. Cela suppose une charge de travail supplémentaire pour l’hôpital.

Objets connectés ?

Ces objets doivent toujours faire l’objet d’un inventaire de cybersécurité pour protéger les données sensibles contre les cyberattaques. Des protocoles de sécurité sont mis en place. Le niveau de cybermaturité des hôpitaux augmente progressivement. La mise en place des conformités légales améliore la sécurité grâce à la loi NIS2 et aux obligations du CCB.

Financement et continuité des soins ?

Certains modules d’IA peuvent être supprimés. Actuellement, lorsque l’IA est mise en place, c’est pour remplacer des protocoles existants. En cas d’abandon, on revient au protocole précédent. D’où il n’y a pas de risques de rupture de la continuité des soins.

Regard du patient sur ses données ?

Les droits du patient concernant ses données sont : les droits d’accès, de rectification, d’effacement (limité dans le cas des données de santé), de portabilité (transfert d’un fournisseur de service à un autre). Des mécanismes de consentements sont nécessaires pour assurer que le consentement du patient est éclairé, libre et révocable. Enfin, des procédures doivent être établies pour que ce consentement (ou refus) soit respecté.

Concilier progrès de la recherche et respect de la confidentialité ?

Pour respecter la confidentialité des données, on recourt à la pseudonymisation et à l’anonymisation. La pseudonymisation consiste à remplacer les identifiants par des pseudonymes. L’anonymisation vise à supprimer les informations personnelles afin que la personne en question ne puisse pas être identifiée. L’anonymisation par couches multiples rend difficile la réidentification des personnes.

Pour concilier recherche et confidentialité, les défis sont nombreux : le respect de normes strictes en matière de protection des données, une bonne gouvernance des données, la mise en place de pratiques éthiques dans la réutilisation des données.

Défis ?

Un des principaux défis est de créer la confiance par rapport à la gouvernance et à la protection des données. Des régulateurs vont se mettre en place en Belgique mais comment ? La puissance de calcul de l’IA va permettre d’améliorer les soins, des évolutions de traitements vont être possibles, les traitements vont pouvoir être personnalisés. Avec le défi du RGPD et dans un contexte où l’influence de l’IA est sans cesse grandissante. Il va falloir pouvoir déterminer les risques que supposent les IA et mettre en place des mesures préventives. A cela s’ajoute le fait que les IA étroites sont basées sur des sources identifiées, contrairement aux IA génératives. Cela nécessite un suivi constant avec une supervision humaine.

Rôle des autorités de régulation ?

Pas encore de retours.

Robots ?

Oui, on a aujourd’hui recours à des robots chirurgicaux. Mais on ne les utilise pas encore dans l’accompagnement. Cela pose des questions éthiques qui vont limiter *peut-être* les applications de l’IA, afin d’éviter des dérives.

Chatbox ?

Les IA hybrides interposent des agents IA par rapport à des humains. Certains hôpitaux installent déjà cela pour augmenter la rapidité de prise en charge. Le principe reste que les sources doivent être contrôlées pour limiter les hallucinations de l’IA.

Plaintes ?

Elles aboutissent chez le DPO. Il existe un process de correction de données erronées de santé, sous la responsabilité du responsable de traitement. C’est le service Relations Patients qui reçoit les plaintes, entre autres celles concernant la protection des données et les biais.

Régulation des droits ?

Le CHIREC n’a pas encore de relations avec les organes de contrôle. Le CHIREC est demandeur car il n’a pas encore la maîtrise de ce sujet. Une collaboration avec UNIA va permettre d’augmenter les compétences dans ce domaine, notamment dans les systèmes de contrôle. Des agents contrôleurs devraient apparaître. *Le CSNPH peut jouer un rôle crucial en offrant des recommandations sur les normes de l’AI ACT et en assurant la conformité éthique des outils d’IA.*

Avenir ?

On est au début de la révolution de l’IA. Ce sera exponentiel. Il est essentiel de garder la main, de pouvoir garantir le contrôle de l’utilisation. L’IA est un outil parmi d’autres. Il est nécessaire de maîtriser l’évolution et de l’accompagner, d’éviter les dérapages éthiques, de laisser le patient au centre : c’est un défi. Car la grande régulation européenne crée une charge de travail en constante augmentation. Les hôpitaux sont démunis par rapport à cette lourdeur. Ils ont besoin d’accompagnement par rapport à ces conformités et par rapport aux implémentations de l’IA. Et qu’en est-il des budgets ?

GM : Grand merci pour l’exposé et pour avoir pris nos questions au sérieux ! Il y a plusieurs enjeux. L’IA est un outil parmi d’autres, dont il ne faut pas avoir peur. Mais il existe un besoin de limites. Il est important de voir les faiblesses comme des défis. Tous les hôpitaux ne sont pas au même niveau. Il y a également besoin d’un organe de contrôle. Quelle sera l’implication des DPO dans les organes de contrôle à venir ? Il y a aussi un besoin d’accompagnement et de financement. Enfin, reste l’enjeu des ventes éventuelles de données. C’est normalement interdit mais le Prof. G. Briganti estime que le risque existe.

PJV : Certaines études cliniques sont financées par des sociétés pharmaceutiques. Pour rémunérer les personnes qui y travaillent, les sociétés pharmaceutiques bénéficient de retours avec des données de santé. Le cadre est réglementé. Avec l’arrivée des agences de santé et les courants de données de santé européens, oui la question va se poser d’une éventuelle commercialisation des données. Le but est ici d’améliorer la santé publique, l’accès à des médicaments mis sur le marché. Il n’y a pas de but lucratif dans le chef des directions hospitalières. Mais comment financer la mise à disposition et l’anonymisation des données tout en laissant au patient le droit de consentir ou pas ? Il est difficile d’imaginer ce qui va venir. En tout état de cause, une collaboration entre hôpitaux et instances nationales est nécessaire.

PJV envoie au GT son PPT et est demandeur d’échanges successifs pour un partage de connaissances.