# Avant-propos

L'Agence Régionale de Santé Océan Indien est l'une des cinq ARS à avoir été retenue par le Commissariat général aux Investissements d'Avenir dans le cadre d'un appel à projets « Territoire de Soins Numérique » (TSN). Elles ont été sélectionnées pour développer, sur leur territoire, des organisations et des outils numériques innovants au service de la santé. L'ARS OI a reçu une enveloppe de 19 millions d'euros pour déployer un programme, dénommé PLEXUS, concernant quatre maladies chroniques prioritaires : le Diabète, l'Accident vasculaire cérébral (AVC), l'Insuffisance rénale chronique (IRC) et l'Insuffisance cardiaque chronique (ICC).

Bâti sur quatre ambitions[1] fortes afin de décloisonner le système de santé et de mieux coordonner le parcours de soin du patient, il vise, en particulier, à permettre à chacun d'être acteur de sa santé.

Entré dans sa phase opérationnelle, PLEXUS est devenu Océan Indien Innovation Santé (OIIS). Des équipes projets pluri professionnelles (dont les membres sont issus de l'ARS-OI, du GCS[2] TESIS et d'un groupement d'entreprises) construisent ce projet avec des acteurs de santé et des patients de la Réunion.

Inscrit dans une démarche de construction de « la santé de demain », il incite à s'interroger sur les transformations structurelles et culturelles qu'il implique. Ainsi, les questionnements éthiques intrinsèques ont rapidement interpellés les responsables de l'ARS-OI. Ils ont proposé la mise en place d'un Comité d'Ethique regroupant des personnalités indépendantes issues de la société civile. Le Comité Ethique Réunion « Technologies de l'Information et Santé » (CERTIS) a ainsi vu le jour.

CERTIS a lancé des réflexions sur les enjeux éthiques mais aussi déontologiques (égalité de l'accès aux soins, solidarité), juridiques (confidentialité et sécurisation des données) ou encore sociaux (changements des usages, relation professionnel-patient) inhérents au programme OIIS.

Afin de conforter les thématiques qu'il avait retenues, il les a soumises aux réflexions de professionnels de santé, d'usagers et des équipes projets de OIIS lors d'un séminaire.
Le CERTIS a ainsi pu constater que ses thèmes rejoignaient les préoccupations des participants au séminaire, voire les avaient anticipées.

Les réflexions concernant la sécurisation et la confidentialité des données de santé constituent ce premier avis.

---

1 Mieux informer et orienter sur les questions de santé,
Favoriser la coordination,
Construire des outils numériques aidant les professionnels dans leur pratique,
Mieux connaître l'état de santé de la population.

2 Groupement de Coopération Sanitaire

# Avis n°1 : Sécurisation et confidentialité des données de santé dans le cadre du programme OIIS

## Table des matières

# Introduction

L'objectif du CERTIS est de tenir compte dans ses réflexions tant de ce qui existe ici ou ailleurs (réglementation et recommandations) que de la situation du territoire réunionnais et de ses habitants. C'est dans cet esprit qu'il a souhaité travailler, en apportant une contribution face aux interrogations relatives à la e-Santé en général et à OIIS en particulier.

Sa conviction première et profonde est que le développement des technologies de l'information et des techniques au service de la médecine est inéluctable.

Conscient des appréhensions et craintes exprimées lors de l'annonce de la mise en place de OIIS, le Comité s'est proposé de se saisir en priorité du thème de « la sécurisation et la confidentialité des données de santé ». Cette auto-saisine concerne les risques induits par le stockage, l'ouverture et le partage numérique des données de santé des patients.

Le CERTIS s'est donc interrogé sur des mesures concrètes susceptibles de concilier la nécessité d'un accès des acteurs de santé aux informations des patients dans le cadre de leur parcours de santé avec le droit des uns et des autres à en garder le contrôle de la diffusion.

Il n'est pas parti de rien. De nombreuses dispositions relatives à la sécurisation et la confidentialité des données existent. De même que des avis sur ces thématiques ont été émis au plan national.

L'arsenal législatif protecteur des données de santé dont se prévaut aujourd'hui la France est conséquent pour assurer la confidentialité et l'intégrité des données médicales. On y trouve en particulier :

- **La loi Informatique et Libertés du 6 janvier 1978**
  Elle réserve aux données de santé des dispositions particulières relatives à leur protection. La Commission Nationale de l'Informatique et des Libertés (CNIL) assure un suivi pratique dans le traitement des données de santé. Elle se prononce sur les modalités optimales à adopter dans le cas où un professionnel de santé héberge ou traite des données médicales. Elle fait également des recommandations aux professionnels de santé, relatives à la sécurité informatique minimale à adopter (mot de passe, supports de sauvegarde externes).

Source : Loi 78-17 du 6 janvier 1978 modifiée : https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee

- **Le Code de la Santé Publique**
  Il s'intéresse aux conditions d'accès des patients à leurs données relatives à la santé (article L. 1111-7 du Code de la Santé Publique) et à leur traitement (hébergement, stockage des données) par les professionnels de santé (article L. 1111-8 du Code de la Santé Publique).

Source : Code de la Santé Publique :
https://www.legifrance.gouv.fr/affichCode.do;jsessionid=21CA75A62DA37B182D0CEBF8003445C5.tpdila15v_3?cidTexte=LEGITEXT000006072665&dateTexte=20160313

- **La loi dite «Kouchner»** sur les droits des malades et la qualité du système de soins du 4 mars 2002
  Elle encadre l'activité d'hébergement des données de santé à caractère personnel. Le décret du 4 janvier 2006 précise les conditions de son agrément particulier. Les professionnels et les

établissements de santé peuvent ainsi déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostics ou de soins, auprès de personnes physiques ou morales agréées par l'Agence des systèmes d'information partagés de Santé (ASIP Santé). L'hébergement ne peut avoir lieu qu'avec le consentement exprès de la personne concernée par les données.

Source : Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000227015

- **Le Code de déontologie**

  Le code de déontologie formule la règle du secret médical dès son article 4 pour en montrer l'importance. Il le fait de façon beaucoup plus explicite que le code pénal et sur le seul terrain de l'exercice de la médecine. L'article 4 en pose le principe et en définit la substance. Ses conséquences sont développées à l'article 72 en ce qui concerne les personnes qui assistent le médecin, aux articles 73 et 104 en ce qui concerne les documents médicaux. Le secret n'est pas opposable au patient. Au contraire, le médecin lui doit toute l'information nécessaire sur son état, les actes et soins proposés ou dispensés (article 35). Si le médecin est amené à retenir une information vis-à-vis du patient, usant ainsi de la faculté que lui ouvre l'article 35, c'est pour le protéger d'une révélation traumatisante et non au nom du secret médical.

Source : Code de déontologie médicale : https://www.conseil-national.medecin.fr/sites/default/files/codedeont.pdf

- **La loi de modernisation du système de santé français du 26 janvier 2016**

  Elle encourage et encadre l'accès ouvert aux données de santé traduit dans l'article L. 1111-8 du Code de la Santé Publique (en cas d'externalisation de l'hébergement, obligation de recourir à un hébergeur agréé, tant pour le secteur de la santé, que pour celui du secteur social).

Source : Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé : https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=21CA75A62DA37B182D0CEBF8003445C5.tpdila15v_3?cidTexte=JORFTEXT000031912641&categorieLien=id

Plusieurs organismes et instances nationales[3] ont déjà été saisis à propos de la sécurisation et de la confidentialité des données dans le cadre du développement d'un programme de e-Santé (exemple du dossier médical personnel). L'informatisation actuelle du système de santé dans les secteurs hospitalier et libéral ne semble pas avoir atteint le niveau quantitatif et qualitatif nécessaire en matière de sécurisation et de confidentialité des données des patients.

Source : Avis n°104 – Le « dossier médical personnel » et l'informatisation des données de santé : http://www.ccne-ethique.fr/sites/default/files/publications/avis_104.pdf

[3] CNIL, ASIP Santé, Comité Consultatif National d'Ethique pour les Sciences et la Vie et de la Santé.

# 1. La sécurisation et la confidentialité des données de santé à l'échelle nationale et de l'océan Indien

## 1.1 Les programmes de e-Santé en France

La e-Santé connaît une forte croissance en France[4], comme dans le reste du monde, avec pour objectif d'apporter des solutions de soins et de prévention, supplémentaires et novatrices, à notre système de santé. Les systèmes d'information de santé et de télésanté (dont la télémédecine et les objets connectés en santé) ont pour ambition de répondre aux défis auxquels est confronté le modèle de soins notamment :

- **La qualité des soins** prodigués dans un contexte de vieillissement de la population (personnel de santé compris), grâce notamment à une optimisation du temps médical ou à l'organisation de l'offre autour du patient (logique de parcours) ;
- **L'efficacité et l'efficience de notre système de santé publique** grâce au partage des informations de santé sur lequel pourraient s'appuyer des politiques de prévention efficaces ;
- **Une meilleure gestion des comptes de l'assurance maladie** grâce à des gains d'efficience multiples (ex : éviter la redondance des pratiques et des actes).

Les projets d'innovation en e-Santé portés par des hôpitaux, universités ou organismes publics se développent dans des espaces d'innovation : les incubateurs. Plusieurs exemples peuvent être cités, en voici deux :

- Le Clubster Santé (30 entrepreneurs du Nord-Pas de Calais) et le CHRU de Lille se sont unis et ont présenté dès 2012 un prototype de chambre d'hôpital du futur qui répond de manière efficace aux exigences hospitalières : le concept room.
- Paris Innovation Boucicaut, dédié au design et à la « ville de demain », accordera une place prépondérante à la e-Santé. Construit sur l'ancien site hospitalier, cet espace permettra la naissance de projets innovants autour de la télémédecine, du diagnostic ou du suivi des malades à distance.

Par ailleurs, des fonds spécifiques ont été mobilisés pour soutenir le secteur de la e-Santé, dont le programme « Territoires de Soins Numériques ».

Cette révolution numérique qui touche le système de santé français ne se met en pas en place sans crainte. La remise en cause de la sécurisation et de la confidentialité des données de santé anime le débat public sur l'ensemble du territoire.

Source : *E-Santé, faire émerger l'offre française* : http://www.entreprises.gouv.fr/etudes-et-statistiques/e-sante-faire-emerger-offre-francaise

[4] Elle devrait progresser en France de 4% à 7% par an d'ici 2020 - http://www.lefigaro.fr/flash-eco/2014/11/06/97002-20141106FILWWW00378-l-e-sante-en-france-un-secteur-en-croissance.php

## 1.2 Les programmes de e-Santé à La Réunion et dans la zone océan Indien

### 1.2.1 Le développement de la e-Santé sur les territoires réunionnais et mahorais

Dès sa création en 2010, l'Agence Régionale de Santé de l'Océan Indien a fait de la santé numérique une priorité majeure sur les territoires de La Réunion et de Mayotte. Chantal de Singly, directrice de l'ARS OI (2010-2015) témoigne de cette priorité : *« A mon arrivée, à La Réunion, il y avait des choses qui étaient réfléchies et mises en place pour les cirques et notamment celui de Mafate sur l'utilisation de la télémédecine portée par le Groupement d'Intérêt Economique Télémédecine Océan Indien (GIE TOI), l'ancêtre du Groupement de Coopération Sanitaire TESIS. Il y avait ici, une perception qu'en matière de santé, les systèmes d'information et la communication à distance étaient nécessaires et qu'il fallait les développer. J'ai rapidement compris que dans les priorités de l'Agence il fallait y inscrire le développement des systèmes d'information ».*

Afin de développer ces programmes de santé numérique, l'ARS OI s'appuie sur le Groupement de Coopération Sanitaire TESIS (GCS TESIS) en tant que maîtrise d'ouvrage régional délégué. Le GCS TESIS compte aujourd'hui trente-quatre adhérents (établissements publics de santé, établissements privés de santé, établissements médico-sociaux, professionnels libéraux). Il met entre autres en place des projets de télémédecine (*TéléAVC*). Il met à disposition de ses adhérents un réseau sécurisé (R2S) haut débit d'interconnexion des acteurs de santé et du médico-social de La Réunion et de Mayotte. Le GCS TESIS a construit un *datacenter* régional agréé hébergeur de données de santé de ses adhérents.

### 1.2.2 Les projets de télémédecine dans la zone océan Indien

L'émergence de la e-*Santé* s'étend dans l'ensemble de la zone de l'océan Indien. Plusieurs projets de télémédecine sont déployés.

**A Madagascar,** le sous-projet *Imailaka* du *Pan African e-Network* (qui consiste à relier les 53 pays de l'Union africaine par voie satellitaire et fibre optique avec l'Inde) est développé à l'Institut Médical de Madagascar à Anosy. Il vise à bâtir un réseau de télécommunication autour de trois volets : éducation, médecine, e-gouvernance. Dans ce cadre, la télémédecine permet d'améliorer la qualité des soins par des consultations à distance, dispensées par des spécialistes, en complément de conférences virtuelles par le système « *VVIP Connectivity* ».

**A Maurice**, un projet de télé-éducation est conçu au Mauritius College of the Air. Les membres du corps médical pourront bénéficier des cours issus de douze institutions médicales basées en Inde (All India Institute of Medical Sciences ou Apollo Hospital). Maurice pourra proposer des services de télémédecine aux pays du continent ouest africain via son centre de télémédecine.

**En Afrique du Sud**, The South African Medical Research tente de développer la télémédecine. Le gouvernement s'engage à proposer des soins de première nécessité à tous les citoyens sud-africains et ceci comme droit fondamental. La télémédecine a été l'outil stratégique retenu pour délivrer un accès égal aux soins et à l'éducation. Plusieurs projets sont en cours autour de cette plateforme de télémédecine comme la «*Teledermatology*» qui permet le transfert des photos des patients à un spécialiste pour une opinion à travers des emails et des réseaux de télémédecine.

**En Australie**, The Australian College Of Rural and Remote Medecine s'est engagé à fournir de meilleurs soins pour les zones rurales et éloignées en offrant des programmes éducatifs spécialisés. C'est la première plateforme d'e-learning faite spécialement pour les docteurs ruraux. Cet outil en ligne permet l'accès à des avis sur des diagnostics et des traitements de maladies de différents types : peau (*Télé-Derm*), radiologie (*Radiology Online*), transports sécurisés des patients (*Retrieval medicine*). De plus, le projet Télémédecine Australia propose des solutions de technologie médicale pour la télémédecine au niveau des soins primaires et des soins aux personnes âgées.

Source : document de travail des projets de télémédecine dans la zone Océan Indien.

## 1.3 La sécurisation et la confidentialité des données de santé

Dans cette ère du tout connecté où les flux sont incessants, une catégorie de données est sujette à une attention particulière : les données dites personnelles, regroupant en leur sein les données de santé nominatives.

### 1.1.1 La protection des données à caractère personnel en France

La France est pionnière en matière de protection des données à caractère personnel avec la loi Informatique et Libertés du 6 janvier 1978 qui a pour objectif d'en assurer la sécurité du traitement.

**Que faut-il entendre par données personnelles ?** Selon l'article 2 de cette loi : « *constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ».

### 1.1.2 La forte protection des données médicales ou de santé en France

Le terme de « données médicales » englobe tout ce qui a trait à une méthode de conservation de la connaissance de l'état de santé d'un patient. Plusieurs définitions légales recouvrent cette notion de données médicales ou de santé.

- **Les données de santé garantissent l'anonymat lorsque cela est souhaitable :** aucune identification de la personne n'est possible. Constituent des données anonymes, les données collectées à la source sans identification de la personne. Constituent des données anonymisées, les données à caractère personnel ayant fait l'objet d'un procédé d'anonymisation préalablement reconnu conforme à la loi Informatique et Libertés (article 8).
- **Les données à caractère personnel relatives à la santé :** article 8 de la loi Informatique et Libertés : « *Données à caractère personnel (…) qui sont relatives à la santé des personnes* ».
- **Les données de santé à caractère personnel :** article L. 1111-8 du Code de la Santé Publique : « *Données de santé à caractère personnel recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins* ».

- **Les informations médicales :** article L. 1110-4 du Code de la Santé Publique : *« Données concernant une personne prise en charge par un professionnel de santé, un établissement de santé, un réseau de santé ou tout autre organisme participant à la prévention et aux soins, (…) venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes* ».

### 1.1.3 Une protection française menacée avec l'ouverture des réseaux à l'international

Bien que, en France, les données de santé des patients soient strictement protégées par un cadre législatif le plus contraignant connu, cette protection s'avère menacée au vu de certaines législations internationales qui n'y accordent pas autant d'importance.

A l'échelle de l'Europe, la plupart des Etats ont adopté une CNIL ou un équivalent, permettant une certaine uniformisation de la protection des données personnelles et donc par ce biais des données de santé. Une législation européenne sur la protection des données de santé serait la bienvenue pour en renforcer l'harmonisation.

Néanmoins, la sécurité des données de santé d'un ressortissant français n'est pas la même aux Etats-Unis. Le principe de « Patriot Act » permet au gouvernement américain de disposer des données personnelles d'un individu sur le fondement d'une seule suspicion de terrorisme ou d'espionnage. Ce principe apparaît contradictoire avec la protection française des données de santé.

De même, la possibilité aujourd'hui de stocker des données à distance sur des serveurs en nuage (« cloud computing ») engendre des risques de volatilité des données de santé. La mise en place d'un « cloud souverain » (projet « Andromède » de 2009) issu d'un partenariat public-privé avorté pour le moment en France permettrait d'alléger ces risques de fuite de données constatés aujourd'hui.

## 2. La perception de OIIS sous l'angle de la sécurisation et de la confidentialité des données

Il n'y a pas de changements sans crainte.

Pour certains professionnels de santé, le programme OIIS viendrait modifier les pratiques traditionnelles dans lesquelles prédomine le dialogue singulier entre le soignant et le patient. OIIS Ce nouvel outil viendrait modifier ce paradigme en mettant en place une nouvelle organisation transverse du système de soins en s'appuyant sur des services et outils numériques. Leurs préoccupations portent tant sur la Plateforme Territoriale d'Appui, qui viendrait s'interposer entre le patient et eux, que sur l'usage des outils informatiques déployés. Ces derniers entraîneraient : complexité d'utilisation et perte de temps par les contraintes de sécurité et de maîtrise de la fiabilité des données transmises.

En revanche, les professionnels de santé engagés dans la co-construction de ces services et de ces outils y voient un programme les aidant dans leurs pratiques quotidiennes. Ainsi, les informations de santé devraient être partagées et accessibles par les différents professionnels de santé qui accompagnent le patient. Pour ce dernier, les services et outils offerts par OIIS lui permettrait permettront d'avoir accès à tout moment à ses propres données de santé. Cependant, ceci doit se faire dans le respect de son consentement éclairé.

Le programme OIIS suscite des questions légitimes sur :

- Son efficacité
- Son aboutissement
- Son retour sur investissement

Il suscite également des craintes quant à l'utilisation des données personnelles de santé à des fins mercantiles.

Autant de difficultés auxquelles est confronté le programme OIIS.

En favorisant le partage des données de santé, par l'intermédiaire de services adaptés aux conditions d'exercice des acteurs de santé, le programme OIIS présente des avantages à la fois pour les patients et pour les professionnels de santé.

Parmi ces services, OIIS devrait favoriser favorise l'accès aux données du patient en mobilité via smartphone, proposer propose des solutions permettant la communication des logiciels des professionnels de santé, ainsi que des portails WEB à destination des acteurs de santé, des patients et des usagers.

Par ailleurs, OIIS mettra également à disposition des professionnels de santé une messagerie sécurisée ainsi que des outils de communication simplifiés (types chat, SMS et visio mais sécurisés). Le partage de données de santé évitera les redondances dans la prescription et favorisera l'observance et l'adéquation entre le comportement du patient et le traitement proposé. Ce dispositif concourra à mieux informer et responsabiliser le patient dans sa prise en charge coordonnée. Cet exercice partagé avec les différents professionnels est un facteur d'évolution des pratiques bénéfique, tant pour les professionnels que pour leurs patients. Cet exercice coordonné et simplifié devra également être étudié au titre des économies générées.

Source : Direction stratégique du programme OIIS.

# 3. Les avis du CERTIS sur la sécurisation et la confidentialité des données dans le cadre du programme OIIS

Le CERTIS est favorable à la mise en place de services et d'outils numériques qui seraient en mesure de faciliter le parcours de santé du patient, au profit des personnes atteintes de pathologies chroniques lourdes.

Ces patients peuvent, en effet, être fortement pénalisés dans leur prise en charge par un manque de coordination et de suivi. Ainsi, tous dispositifs humains, organisationnels ou technologiques, susceptibles de faciliter suivi et coordination doivent permettre de renforcer les moyens et services à disposition du patient et de son médecin traitant. L'échange rapide et exhaustif d'informations peut se révéler décisif pour une prise en charge optimale.

Aujourd'hui, si aucun système informatique n'est susceptible d'offrir des garanties absolues contre l'usurpation, le piratage, etc, il se doit d'assurer une obligation de sécurisation des données à hauteur de la sensibilité des informations traitées et en fonction des possibilités techniques disponibles.

Enfin, les données partagées ne doivent pas porter atteinte aux libertés individuelles.

S'il importe à OIIS de répondre aux craintes et aux questionnements (présentés dans le chapitre 2) que suscite le programme, CERTIS fait part des remarques suivantes :

1) Concernant la relation médecin traitant/patient :

   - Le médecin traitant doit rester au centre du réseau de partage de l'information. Il revient aux médecins traitants de renseigner les informations qui lui semblent utiles dans l'accompagnement du parcours de santé du patient.
   - Il est dans l'intérêt du patient de favoriser le partage des données sécurisées afin d'optimiser sa prise en charge.
   - Seules les informations pertinentes dans le cadre de la prise en charge des patients doivent être partagées.

2) Le projet développé par OIIS se doit de déployer les moyens nécessaires pour garantir la sécurisation et la confidentialité maximales des données de santé échangées.

3) Ce projet OIIS doit rester un outil supplémentaire mis à la disposition du médecin traitant et des autres professionnels de santé.

4) Le patient se voit offrir la possibilité d'adhérer à une organisation de coordination de soins à laquelle des professionnels de santé et les acteurs de cette coordination participent. Cette adhésion doit lui être expliquée, et doit être encouragée lorsque cela est dans son intérêt.

5) Le patient reste, toutefois, le seul décisionnaire in fine. Le consentement fait partie intégrante de la sécurisation des données. Ce consentement éclairé du patient ou de la personne de confiance qu'il aura désignée doit être recueilli par le médecin traitant.

6) Le patient a le libre arbitre d'intégrer ou non le programme OIIS et la Plateforme territoriale d'appui[5]. Il est partie prenante de son plan personnalisé de santé. Il accepte de ce fait et dans son intérêt des modalités de prise en charge éventuellement différentes de ce qu'il pouvait connaître auparavant.

7) Une évaluation du programme OIIS en matière de sécurisation et de confidentialité des données doit être réalisée périodiquement selon des modalités de critères proposées à l'avance.

8) Un programme d'information doit accompagner le déploiement de ce nouvel outil sur le territoire, en utilisant l'ensemble des supports possibles, en particulier les moyens audiovisuels pour prendre en considération le fort taux d'illettrisme à la Réunion. De même, qu'un module de formation, relevant de la formation continue, devrait être proposé aux professionnels de santé qui le souhaiteraient. Tout nouvel utilisateur doit connaître les règles déontologiques et éthiques qu'impose son utilisation. Il incombe à OIIS d'en définir les modalités de diffusion (charte, règlement, avis de CERTIS, …).

[5] Article 14 de la loi de modernisation du système d'information : cet article vise à mettre en place pour les professionnels du territoire un service lisible d'appui à la coordination des parcours de santé complexes. Cette offre aux professionnels prendra la forme de plateformes polyvalentes pilotées par les agences régionales de santé en lien avec les collectivités territoriales, l'assurance maladie et les autres acteurs du territoire. Elle viendra soutenir en particulier l'offre de soins de proximité et le médecin traitant.