



**HAL**  
open science

# Évolution de la e-santé : impact réglementaire sur le développement de nouveaux projets

Magali Coustellier

► **To cite this version:**

Magali Coustellier. Évolution de la e-santé : impact réglementaire sur le développement de nouveaux projets. Sciences pharmaceutiques. 2023. dumas-04137387

**HAL Id: dumas-04137387**

**<https://dumas.ccsd.cnrs.fr/dumas-04137387v1>**

Submitted on 22 Jun 2023

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

## THESE

PRESENTEE ET PUBLIQUEMENT SOUTENUE DEVANT LA FACULTE DE  
PHARMACIE DE MARSEILLE

LE 19 JUIN 2023

PAR

Mme Magali COUSTELLIER

Née le 21 novembre 1995 à Martigues

EN VUE D'OBTENIR

LE DIPLOME D'ETAT DE DOCTEUR EN PHARMACIE

**TITRE :**

EVOLUTION DE LA E-SANTE : IMPACT REGLEMENTAIRE SUR  
LE DEVELOPPEMENT DE NOUVEAUX PROJETS

**JURY :**

Président : M. François DEVRED

Membres : Mme Véronique ANDRIEU, Directeur de thèse  
Mme Carine APERTET  
M. Matthieu KALITA

27 Boulevard Jean Moulin – 13385 MARSEILLE Cedex 05  
Tel. : 04 91 83 55 00 – Fax : 04 91 80 26 12

**ADMINISTRATION :**

<i>Doyen :</i>	M. Jean-Paul BORG
<i>Vice-Doyens :</i>	Mme Florence SABATIER-MALATERRE, M. François DEVRED, M. Pascal RATHELOT, Mme Alexandrine BERTAUD
<i>Chargés de Mission :</i>	Mme Pascale BARBIER, Mme Alexandrine BERTAUD, M. David BERGELFRANC, Mme Manon CARRE, Mme Caroline DUCROS, M. Philippe GARRIGUE, M. Guillaume HACHE, M. Thierry TERME
<i>Conseiller du Doyen :</i>	M. Patrice VANELLE, Mme Françoise DIGNAT-GEORGE
<i>Doyens honoraires :</i>	M. Patrice VANELLE, M. Pierre TIMON-DAVID,
<i>Professeurs émérites :</i>	M. José SAMPOL, M. Athanassios ILIADIS, M. Philippe CHARPIOT, M. Riad ELIAS
<i>Professeurs honoraires :</i>	M. Guy BALANSARD, M. Yves BARRA, Mme Claudette BRIAND, M. Jacques CATALIN, Mme Andrée CREMIEUX, M. Gérard DUMENIL, M. Alain DURAND, Mme Danielle GARÇON, M. Maurice JALFRE, M. Joseph JOACHIM, M. Maurice LANZA, M. Patrick REGLI, M. Jean-Claude SARI
<i>Chef des Services Administratifs :</i>	Mme Sylvie BUREAU
<i>Chef de Cabinet :</i>	Mme Manon BONIFAY
<i>Responsable de la Scolarité :</i>	Mme Nathalie BESNARD

**DEPARTEMENT BIO-INGENIERIE PHARMACEUTIQUE**

Responsable : Professeur Philippe PICCERELLE

**PROFESSEURS**

BIOPHYSIQUE	M. Vincent PEYROT M. Hervé KOVACIC M. François DEVRED
GENIE GENETIQUE ET BIOINGENIERIE	M. Christophe DUBOIS
PHARMACIE GALENIQUE, PHARMACOTECHNIE INDUSTRIELLE, BIOPHARMACIE ET COSMETOLOGIE	M. Philippe PICCERELLE

## MAITRES DE CONFERENCES

BIOPHYSIQUE	Mme Odile RIMET-GASPARINI Mme Pascale BARBIER Mme Manon CARRE M. Gilles BREUZARD Mme Alessandra PAGANO
GENIE GENETIQUE ET BIOTECHNOLOGIE	M. Eric SEREE-PACHA Mme Véronique REY-BOURGAREL
PHARMACIE GALENIQUE, PHARMACOTECHNIE INDUSTRIELLE, BIOPHARMACIE ET COSMETOLOGIE	M. Pierre REBOUILLON M. Emmanuel CAUTURE Mme Véronique ANDRIEU Mme Marie-Pierre SAVELLI
BIO-INGENIERIE PHARMACEUTIQUE ET BIOTHERAPIES PHARMACO ECONOMIE, E-SANTE	M. Jérémy MAGALON Mme Carole SIANI Mme Muriel MASI

## ENSEIGNANT CDI

ANGLAIS	Mme Angélique GOODWIN
---------	-----------------------

## A.H.U.

PHARMACOTECHNIE	Mme Mélanie VELIER
-----------------	--------------------

## DEPARTEMENT BIOLOGIE PHARMACEUTIQUE

Responsable : Professeur Françoise DIGNAT-GEORGE

## PROFESSEURS

BIOLOGIE CELLULAIRE	M. Jean-Paul BORG
HEMATOLOGIE ET IMMUNOLOGIE	Mme Françoise DIGNAT-GEORGE Mme Laurence CAMOIN-JAU Mme Florence SABATIER-MALATERRE Mme Nathalie BARDIN M. Romaric LACROIX
MICROBIOLOGIE	M. Jean-Marc ROLAIN M. Philippe COLSON
PARASITOLOGIE ET MYCOLOGIE MEDICALE, HYGIENE ET ZOOLOGIE	Mme Nadine AZAS-KREDER

### MAITRES DE CONFERENCES

BIOCHIMIE FONDAMENTALE, MOLECULAIRE ET CLINIQUE	M. Edouard LAMY Mme Alexandrine BERTAUD Mme Claire CERINI Mme Edwige TELLIER M. Stéphane POITEVIN Mme Sandra GHAYAD
HEMATOLOGIE ET IMMUNOLOGIE	Mme Aurélie LEROYER Mme Sylvie COINTE
MICROBIOLOGIE	Mme Anne DAVIN-REGLI Mme Véronique ROUX M. Fadi BITTAR Mme Isabelle PAGNIER Mme Sophie EDOUARD M. Seydina Mouhamadou DIENE
PARASITOLOGIE ET MYCOLOGIE MEDICALE, HYGIENE ET ZOOLOGIE	Mme Carole DI GIORGIO M. Aurélien DUMETRE Mme Magali CASANOVA Mme Anita COHEN
BIOLOGIE CELLULAIRE BIOLOGIE CELLULAIRE ET MOLECULAIRE	Mme Anne-Catherine LOUHMEAU Mme Alexandra WALTON

### A.H.U.

HEMATOLOGIE ET IMMUNOLOGIE	Mme Amandine BONIFAY
----------------------------	----------------------

### MAITRES DE CONFERENCE ASSOCIES A TEMPS PARTIEL (M.A.S.T.)

PRATIQUE OFFICINALE	M. Jérôme JOUVE Mme Emmanuelle TONNEAU-PFUG
---------------------	--

### DEPARTEMENT CHIMIE PHARMACEUTIQUE

Responsable : Professeur Patrice VANELLE

### PROFESSEURS

CHIMIE ANALYTIQUE, QUALITOLOGIE ET NUTRITION	Mme Catherine BADENS
CHIMIE PHYSIQUE - PREVENTION DES RISQUES ET NUISANCES TECHNOLOGIQUES	M. David BERGE-LEFRANC
CHIMIE THERAPEUTIQUE - CHIMIE MINERALE ET STRUCTURALE	M. Pascal RATHELOT M. Maxime CROZET
CHIMIE ORGANIQUE PHARMACEUTIQUE	M. Patrice VANELLE M. Thierry TERME
PHARMACOGNOSIE, ETHNOPHARMACOLOGIE	Mme Sok Siya BUN

## MAITRES DE CONFERENCES

BOTANIQUE ET CRYPTOLOGIE, BIOLOGIE CELLULAIRE	Mme Anne FAVEL M. Quentin ALBERT
CHIMIE ANALYTIQUE, QUALITOLOGIE ET NUTRITION	Mme Catherine DEFOORT M. Alain NICOLAY Mme Estelle WOLFF Mme Elise LOMBARD Mme Camille DESGROUAS M. Charles DESMARCHELIER M. Mathieu CERINO
CHIMIE PHYSIQUE – PREVENTION DES RISQUES ET NUISANCES TECHNOLOGIQUES	M. Dujé BURIC M. Pascal PRINDERRE
CHIMIE THERAPEUTIQUE - CHIMIE MINERALE ET STRUCTURALE	Mme Sandrine ALIBERT Mme Caroline DUCROS M. Marc MONTANA Mme Manon ROCHE Mme Fanny MATHIAS
CHIMIE ORGANIQUE PHARMACEUTIQUE HYDROLOGIE	M. Armand GELLIS M. Christophe CURTI Mme Julie BROGGI M. Nicolas PRIMAS M. Cédric SPITZ M. Sébastien REDON
PHARMACOGNOSIE, ETHNOPHARMACOLOGIE	Mme Valérie MAHIOU-LEDDÉ Mme Béatrice BAGHDIKIAN M. Elnur GARAYEV

## MAITRES DE CONFERENCE ASSOCIES A TEMPS PARTIEL (M.A.S.T.)

CHIMIE ANALYTIQUE, QUALITOLOGIE ET NUTRITION CHIMIE PHYSIQUE – PREVENTION DES RISQUES ET NUISANCES TECHNOLOGIQUES	Mme Haïfa LAYACHI RAHABI M. Cyril PUJOL
DROIT ET ETHIQUE	Mme Laurie PAHUS
GESTION PHARMACEUTIQUE, PHARMACOECONOMIE ET ETHIQUE PHARMACEUTIQUE OFFICINALE, DROIT ET COMMUNICATION PHARMACEUTIQUES A L'OFFICINE ET GESTION DE LA PHARMAFAC	Mme Félicia FERRERA
DISPOSITIFS MEDICAUX	Mme Valerie MINETTI-GUIDONI

**DEPARTEMENT MEDICAMENT ET SECURITE SANITAIRE**

Responsable : Professeur Benjamin GUILLET

**PROFESSEURS**

PHARMACIE CLINIQUE	M. Stéphane HONORÉ
PHARMACODYNAMIE	M. Benjamin GUILLET
TOXICOLOGIE ET PHARMACOCINETIQUE	M. Bruno LACARELLE M. Joseph CICCOLINI
TOXICOLOGIE GENERALE	Mme Caroline SOLAS-CHESNEAU

**MAITRES DE CONFERENCES**

PHARMACIE CLINIQUE	M. Florian CORREARD Mme Marie-Anne ESTEVE
PHARMACODYNAMIE	M. Guillaume HACHE Mme Ahlem BOUHLEL M. Philippe GARRIGUE
PHYSIOLOGIE	Mme Sylviane LORTET
PHYSIOLOGIE / PHARMACOLOGIE	Mme Anaïs MOYON
TOXICOLOGIE ET PHARMACOCINETIQUE	Mme Raphaëlle FANCIULLINO Mme Florence GATTACECCA Mme Anne RODALLEC M. Nicolas FABRESSE
TOXICOLOGIE GENERALE	M. Pierre-Henri VILLARD

**A.H.U.**

PHYSIOLOGIE / PHARMACOLOGIE	M. Vincent NAIL
PHARMACIE CLINIQUE	Mme Maeva MONTALEYTANG Mme Charlotte BERARD

## CHARGES D'ENSEIGNEMENT A LA FACULTE

Mme Valérie AMIRAT-COMBRALIER, Pharmacien-Praticien hospitalier  
M. Pierre BERTAULT-PERES, Pharmacien-Praticien hospitalier  
Mme Martine BUES-CHARBIT, Pharmacien-Praticien hospitalier  
Mme Annie CILIA, Pharmacien-Praticien hospitalier  
M. Yann COTTE, Pharmacien Assistant  
M. Nicolas COSTE, Pharmacien-Praticien hospitalier  
Mme Nicole FRANCOIS, Pharmacien-Praticien hospitalier  
Mme Sophie GENSOLLEN, Pharmacien-Praticien hospitalier  
M. Sylvain GONNET, Pharmacien titulaire  
Mme Céline HIRSCH, Pharmacien Conseil de l'Assurance Maladie  
Mme Christelle LABRANDE, Pharmacien-Praticien hospitalier  
Mme Florence LEANDRO-DIJON, Pharmacien adjoint  
Mme Nathalie MARTIN, Pharmacien-Praticien hospitalier  
Mme Sophie MERLIN, Pharmacien Assistant  
Mme Vanessa METZ, Pharmacien hospitalier  
Mme Alice PERINEAU, Pharmacien Assistant  
Mme Florence PEYRON, Pharmacien-Praticien hospitalier  
M. Stéphane PICHON, Pharmacien titulaire  
M. Bertrand POURROY, Pharmacien-Praticien hospitalier  
Mme Clémence TABELLE, Pharmacien-Praticien attaché  
M. Badr Eddine TEHHANI, Pharmacien – Praticien hospitalier  
M. Joël VELLOZZI, Expert-Comptable

Mise à jour le 23 février 2023

## Remerciements

Je tiens à remercier chaleureusement tous les membres du jury.

A Monsieur François Devred, pour l'honneur que vous me faites de présider ce jury de thèse et de juger mon travail.

A Madame Véronique Andrieu, pour avoir accepté d'être ma directrice de thèse. Merci pour votre disponibilité, pour le temps que vous m'avez accordé dans le cadre de la préparation de cette thèse ainsi que pour votre soutien.

A Madame Carine Apertet, merci d'avoir accepté d'être membre de mon jury et de m'avoir accompagné tout au long de ce travail de thèse. Merci de m'avoir tant appris dans le domaine des affaires réglementaires, je suis très reconnaissante d'avoir pu travailler, échanger et partager avec toi durant mon année d'alternance. Merci pour ta confiance, tes encouragements et la qualité de ton encadrement.

A Monsieur Matthieu Kalita, pour m'avoir fait découvrir ce domaine passionnant qu'est la e-santé. Travailler ensemble a été pour moi une expérience très enrichissante et particulièrement motivante. Merci d'avoir accepté de faire partie de mon jury de thèse, pour la relecture de mon travail et pour tes suggestions toujours avisées.

Merci à mes camarades de promotion et amis, Valentine, Amélie, Andréa, Alexandre et Grégoire. Notre entraide et notre soutien mutuel pendant ces années d'études m'ont été précieux. Nous pouvons être fiers de nos parcours. Merci pour ces souvenirs et pour ces moments passés ensemble.

Merci à Clémentine, pour notre amitié si chère à mes yeux. Merci d'avoir été là depuis le début : ça y est, j'y suis enfin.

Merci à Valérian, d'être toujours à mes côtés et de croire en moi. Merci pour ta patience et ton amour.

Merci à ma famille pour votre précieux soutien durant toutes ces années d'études. Vos conseils et votre amour m'ont permis d'aller jusqu'au bout de mon parcours.

Enfin, merci à mes parents et à ma sœur, Cécile, pour tout ce que vous avez fait pour moi. Votre présence et vos encouragements sont les piliers fondateurs de ce que je suis et de ce que je fais.

*« L'Université n'entend donner aucune approbation, ni improbation aux opinions émises dans les thèses. Ces opinions doivent être considérées comme propres à leurs auteurs. »*

# Sommaire

<b>REMERCIEMENTS.....</b>	<b>8</b>
<b>SOMMAIRE .....</b>	<b>10</b>
<b>LISTE DES FIGURES .....</b>	<b>12</b>
<b>LISTE DES TABLEAUX.....</b>	<b>13</b>
<b>GLOSSAIRE .....</b>	<b>14</b>
<b>INTRODUCTION.....</b>	<b>15</b>
<b>I. CADRE REGLEMENTAIRE EUROPEEN : QUALIFICATION ET CLASSIFICATION D’UN LOGICIEL VIS-A-VIS DES REGLEMENTS EUROPEENS 2017/754 ET 2017/746.....</b>	<b>17</b>
1. QUALIFICATION : MON LOGICIEL RELEVE-T-IL DU STATUT DE DM OU DE DMDIV ? .....	17
1.1. <i>Mon logiciel est-il un SaMD ?</i> .....	19
1.2. <i>Mon logiciel est-il un DM ou un DMDIV ?</i> .....	24
1.3. <i>Résumé de la démarche de qualification</i> .....	26
2. CLASSIFICATION : A QUELLE CLASSE APPARTIENT MON LOGICIEL SELON LE REGLEMENT APPLICABLE ?.....	29
2.1. <i>Classification d’un logiciel selon le MDR 2017/745</i> .....	29
2.2. <i>Classification d’un logiciel selon l’IVDR 2017/746</i> .....	34
3. ÉVALUATION DE LA CONFORMITE D’UN LOGICIEL DM OU DMDIV .....	36
3.1. <i>La mise en conformité</i> .....	37
3.1.1. Les procédures d’évaluation de la conformité .....	37
3.1.2. Démonstration de la conformité .....	39
3.2. <i>Évaluation clinique des logiciels</i> .....	45
3.3. <i>La surveillance après commercialisation et vigilance</i> .....	48
<b>II. PANORAMA DE LA REGLEMENTATION FRANÇAISE DU NUMERIQUE EN SANTE .....</b>	<b>49</b>
1. CONTEXTE GENERAL .....	49
1.1. <i>La e-santé en France</i> .....	49
1.2. <i>Une accélération du virage du numérique en santé</i> .....	50
1.3. <i>La doctrine du numérique en santé</i> .....	53
2. LES REFERENTIELS ET SERVICES SOCLES .....	55
2.1. <i>La sécurité et la protection des données de santé</i> .....	55
2.1.1. Le Règlement Général sur la Protection des Données (RGPD).....	56
2.1.2. L’hébergement des données de santé.....	56
2.1.3. La politique générale de sécurité des systèmes d’information de santé (PGSSI-S).....	60

2.1.3.a) Référentiel d'identification électronique .....	62
2.1.3.b) Référentiel d'imputabilité.....	64
2.1.3.c) Référentiel force probante des documents de santé.....	65
2.1.4 L'identité Nationale de Sante (INS).....	67
2.2 <i>Le cadre d'interopérabilité des systèmes d'information de santé (CI-SIS)</i> .....	69
2.2.1 Pourquoi l'interopérabilité en santé est-elle importante ?.....	69
2.2.2 Le cadre d'interopérabilité mis en place par l'ANS.....	71
<b>III. ILLUSTRATION DU POSITIONNEMENT REGLEMENTAIRE : EXEMPLES DE LOGICIELS ET APPLICATIONS.....</b>	<b>73</b>
1. EXEMPLES DE QUALIFICATION DE LOGICIELS SELON LA METHODOLOGIE DU MDCG 2019-11 .....	73
1.1. <i>Algorithme de prédisposition au syndrome de Down</i> .....	73
1.2. <i>Logiciel d'analyse d'images uPath HER2</i> .....	75
1.3. <i>Le cas des Middlewares</i> .....	76
2. EXIGENCES A PRENDRE EN COMPTE POUR LA MISE SUR LE MARCHE FRANÇAIS D'UNE SOLUTION LOGICIELLE.....	77
2.1. <i>Diagnostic réglementaire</i> .....	77
2.2. <i>Exemple illustratif : solution de prescription connectée à domicile</i> .....	78
<b>CONCLUSION.....</b>	<b>80</b>
<b>REFERENCES.....</b>	<b>82</b>

## Liste des figures

Figure 1 : Logigramme aidant à la qualification des logiciels dispositifs médicaux .....	20
Figure 2 : Logigramme aidant à la qualification d'un logiciel en tant que DM ou DMDIV .....	24
Figure 3 : Arbre décisionnel de la Règle numéro 11 de classification selon le MDR 2017/745 .....	33
Figure 4 : Les normes harmonisées aident à prouver la conformité avec les réglementations de l'UE .	40
Figure 5 : Harmonisation des normes ISO pour la réglementation Européenne relative aux DM et DMDIV .....	42
Figure 6 : Schéma du cycle en V de l'IEC 62304 et de l'IEC 82304.....	43
Figure 7 : Résumé de la norme IEC 62366-1 .....	44
Figure 8 : Normes applicables à un logiciel DM ou DMDIV autonome tout au long de son cycle de vie .....	45
Figure 9 : La maison de la e-santé.....	54
Figure 10 : Étapes de la procédure de certification Hébergeur de Données de Santé.....	58
Figure 11 : Répartition du marché des services d'hébergement cloud .....	59
Figure 12 : Processus d'identification électronique d'une personne physique .....	63
Figure 13 : Flux de documents dans les SI de santé.....	65
Figure 14 : Identité Nationale de Santé.....	68
Figure 15 : Cadre d'Interopérabilité des systèmes d'information de santé.....	70
Figure 16 : Exemple d'articulation des volets du CI-SIS .....	71

## Liste des tableaux

Tableau 1 : Impact de différents éléments sur la qualification d'un logiciel.....	26
Tableau 2 : Exemples de solutions logicielles DM versus non-DM .....	27
Tableau 3 : Procédures d'évaluation de la conformité applicables selon la classe du DM ou du DMDIV .....	39
Tableau 4 : Synthèse du corpus documentaire de la PGSSI-S.....	61

## Glossaire

ANS : Agence du Numérique en Santé

ANSM : Agence Nationale de Sécurité du Médicament et des produits de santé

CE : Conformité Européenne

CI-SIS : Cadre d'Interopérabilité des Systèmes d'Information de Santé

CNIL : Commission Nationale de l'Informatique et des Libertés

CPS : Carte Professionnel de Santé

CSP : Code de la Santé Publique

DM : Dispositif Médical

DMDIV : Dispositif Médical de Diagnostic *In Vitro*

DMP : Dossier Médical Partagé

DNS : Délégation ministérielle du Numérique en Santé

DPI : Dossier Patient Informatisé

DT : Documentation Technique

HDS : Hébergeur de Données de Santé

IA : Intelligence Artificielle

IEC : International Electrotechnical Commission

IHM : Interface Homme Machine

IMDRF : International Medical Device Regulators Forum

INS : Identité Nationale de Santé

ISO : International Organization for Standardisation

IVDR : In Vitro Medical devices Regulation 2017/746

MDCG : Medical Device Coordination Group

MDR : Medical Devices Regulation 2017/745

ON : Organisme Notifié

PGSSI-S : Politique Générale de Sécurité des Systèmes d'Information de Santé

PSUR : Periodic Safety Update Report

RGPD : Règlement Général sur la Protection des Données

RNIV : Référentiel National d'Identitovigilance

SaMD : Software as Medical Device

SMQ : Système de Management de la Qualité

TIC : Technologies de l'Information et de la Communication

UE : Union Européenne

VIH : Virus de l'Immunodéficience Humaine

## Introduction

Les innovations et les solutions numériques se propagent peu à peu à toutes les aires thérapeutiques, à différents moments du parcours patient et dans le quotidien de tous les acteurs du système de santé. Au niveau mondial, la valeur du marché de la e-santé est estimée à 234,5 milliards de dollars en 2023, soit une hausse de près 160 % comparée à 2019 selon l'étude prospective *Global Digital Health Outlook 2020* publiée fin 2019 par le cabinet Frost & Sullivan [1]. En France, les entreprises de la e-santé ont levé 1,79 milliard d'euros en 2022, soit trois fois plus que les 577 millions collectés en 2021, selon un recensement du fonds de capital-risque Karista [2].

Défini par la Commission européenne comme *“l'ensemble des outils et services qui utilisent les Technologies de l'Information et de la Communication (TIC) pour améliorer la prévention, le diagnostic, le traitement, le suivi et la gestion des questions liées à la santé, ainsi que le suivi et la gestion des habitudes de vie qui ont un impact sur la santé”*, la santé numérique ou e-santé couvre un large éventail de solutions, de services et de soins en santé. On y retrouve notamment les dossiers médicaux électroniques, les systèmes d'information de santé, les services de surveillance et de consultation à distance (par exemple, télésanté, télémedecine, télésoins), les outils destinés à l'autogestion ainsi qu'à l'analyse des données de santé (Big Data) [3]. Cette définition de la e-santé regroupe les “simples” logiciels de santé mais également les logiciels qui sont des dispositifs médicaux en soi. On les appelle les SaMD pour *"Software as Medical Device"*. Certaines solutions numériques, en fonction de leur finalité, sont donc susceptibles de tomber dans le champ d'application du règlement 2017/745 relatif aux dispositifs médicaux (MDR) ou du règlement 2017/746 relatif aux dispositifs médicaux de diagnostics *in vitro* (IVDR).

Le point commun entre tous ces logiciels est qu'ils traitent de la donnée de santé. Ces données de santé sont des données personnelles considérées comme sensibles selon l'article 9 [4] du Règlement Général sur la Protection des Données (RGPD). Elles bénéficient donc d'un encadrement spécifique afin de garantir leur confidentialité, leur intégrité et leur sécurité. Cette évolution vers le numérique soulève un certain nombre de questions sur l'environnement réglementaire qui régit ces technologies. Il est nécessaire de connaître le cadre normatif et réglementaire qui s'applique au développement de ces solutions numériques afin qu'elles puissent être déployées et intégrées dans l'environnement des systèmes de santé en prenant en compte la sécurité et la protection des données de santé qui y sont traitées.

Ce travail fait un état des lieux des réglementations qui s'appliquent aux logiciels en santé et comment celles-ci influencent le développement des projets par les industriels du monde de la santé. Nous aborderons dans une première partie, le cadre réglementaire européen en détaillant notamment la démarche de qualification et de classification des logiciels en tant que dispositif médical ou dispositif médical de diagnostic *in-vitro* au regard de la réglementation et les différentes normes applicables. La deuxième partie détaillera le cadre réglementaire spécifique aux solutions numériques mis en place par l'Etat en France. Des référentiels d'exigences et des guides de bonne pratique ont été établis et proposent un cadre commun pour sécuriser les systèmes d'information, l'accès aux données de santé et rendre interopérables les services entre eux. Enfin, nous verrons plusieurs exemples de logiciels et applications en santé afin d'illustrer différents cas de positionnement réglementaire.

# **I. Cadre Réglementaire Européen : qualification et classification d'un logiciel vis-à-vis des règlements Européens 2017/754 et 2017/746**

Pour être commercialisé dans l'Union Européenne (UE), un Dispositif Médical (DM) ou un Dispositif Médical de Diagnostic In Vitro (DMDIV), numérique ou non, doit répondre à des exigences générales en matière de sécurité et de performance. Celles-ci sont définies dans les règlements européens relatifs aux dispositifs médicaux : le Règlement 2017/745 relatif aux Dispositifs Médicaux et le Règlement 2017/746 relatif aux Dispositifs Médicaux de Diagnostic *in vitro*. La conformité à ces exigences permet d'obtenir une certification appelée marquage CE (Conformité Européenne).

Tout éditeur doit s'interroger quant à la possibilité que son logiciel constitue un DM ou un DMDIV au sens des règlements européens. Tous les logiciels ou applications en santé ne répondent pas à la définition d'un DM ou d'un DMDIV mais dès lors qu'ils ont une finalité médicale, au sens du MDR ou de l'IVDR, ils devront être qualifiés comme tels. Dans ce cas, ils seront marqués CE au même titre que les autres dispositifs afin d'attester de leur conformité réglementaire et tomberont dans le périmètre de surveillance de l'ANSM. L'obtention d'un marquage CE et la question du statut du logiciel doivent être anticipés dès la phase de développement d'un produit. La réponse aura un impact sur l'ensemble du processus de développement et du cycle de vie du produit. En fonction du statut on saura quelles réglementations seront à appliquer et il sera nécessaire de démontrer la conformité du produit à ces réglementations afin qu'il puisse être mis sur le marché. Une compréhension des exigences cliniques et réglementaires complexes dès le début du cycle de vie du produit permettra de mettre un produit plus rapidement sur le marché.

Nous verrons dans cette partie la démarche de qualification et de classification d'un logiciel en fonction des règlements européens 2017/745 et 2017/746. Puis, nous verrons les obligations qui incombent aux fabricants lorsqu'un logiciel est qualifié de DM ou DMDIV.

## **1. Qualification : mon logiciel relève-t-il du statut de DM ou de DMDIV ?**

Entrés en application depuis le 26 mai 2021 pour le MDR et depuis le 26 mai 2022 pour l'IVDR, les règlements européens viennent abroger respectivement la directive 93/42/CEE du 14 juin 1993 relative aux DM et la directive 98/79/CE du 27 octobre 1998 relative aux DMDIV. Ces règlements prévoient un cadre plus strict et un renforcement de toutes les étapes clé de la mise sur le marché des dispositifs. Ce durcissement a également un impact sur les logiciels ayant une finalité médicale et donc qualifiés de DM ou DMDIV : les SaMD.

Que ce soit dans le MDR ou l'IVDR, le terme "logiciel" est inclus dans la définition d'un DM :

- "On entend par «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 précises suivantes:
  - 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,

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. [...]" (Article 2(1) du MDR [5])

Ou d'un DMDIV :

- "On entend par «dispositif médical de diagnostic *in vitro*», tout dispositif médical qui consiste en un réactif, un produit réactif, un matériau d'étalonnage, un matériau de contrôle, une trousse, un instrument, un appareil, un équipement, **un logiciel** ou un système, utilisé seul ou en association, destiné par le fabricant à être utilisé *in vitro* dans l'examen d'échantillons provenant du corps humain, y compris les dons de sang et de tissus, uniquement ou principalement dans le but de fournir des informations sur un ou plusieurs des éléments suivants :

- a) concernant un processus ou état physiologique ou pathologique;
- b) concernant des déficiences congénitales physiques ou mentales;
- c) concernant la *prédisposition à une affection ou à une maladie*;
- d) permettant de déterminer si un traitement donné est sûr pour des receveurs potentiels et compatible avec eux;
- e) permettant de *prévoir la réponse ou les réactions à un traitement*;
- f) permettant de définir ou de contrôler des mesures thérapeutiques. [...]" (Article 2(2) de l'IVDR [6])

Il est également intéressant de relever que le MDR élargit la portée des fins médicales par rapport à celles listées dans la directive, en ajoutant notamment la notion de "*prévision*" et de "*pronostic*" dans

la définition d'un DM. En ce qui concerne la définition des DMDIV, on voit apparaître les notions de “*prédisposition à une affection ou à une maladie*” et de “*prévision de la réponse ou réaction à un traitement*”. Ces nouvelles définitions élargissent le champ des définitions des dispositifs et de ce fait, certains logiciels permettant de prédire une maladie pourraient y correspondre. Ce serait le cas, par exemple, des logiciels qui fournissent aux professionnels de santé des informations sur les perspectives d'évolution de l'état de santé d'un patient ou encore des prévisions de résultats d'une thérapie ciblée. Un autre exemple pourrait être celui d'application permettant d'établir un pronostic quant au risque que son utilisateur développe le COVID-19 sur la base de ses contacts récents à l'aide de l'intelligence artificielle [7], alors que l'application ne serait pas en mesure de diagnostiquer réellement l'infection.

La démarche de qualification d'un logiciel ne se fait pas uniquement sur la base des définitions énoncées dans les règlements. Déterminer le statut réglementaire d'un logiciel est un exercice d'analyse complexe qui doit être menée au cas par cas. Pour être qualifié de DM ou DMDIV, le logiciel doit présenter plusieurs critères cumulatifs. Ces critères sont décrits dans un guide, le *MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR* mis à disposition des industriels par la Commission européenne. Établi par le Groupe de coordination des dispositifs médicaux (Medical Device Coordination Group : MDCG) composé de représentants de tous les états membres et présidé par un représentant de la Commission européenne, ce guide a été publié en 2019 et décrit une méthodologie d'analyse pouvant être représentée sous la forme d'arbres de décision permettant :

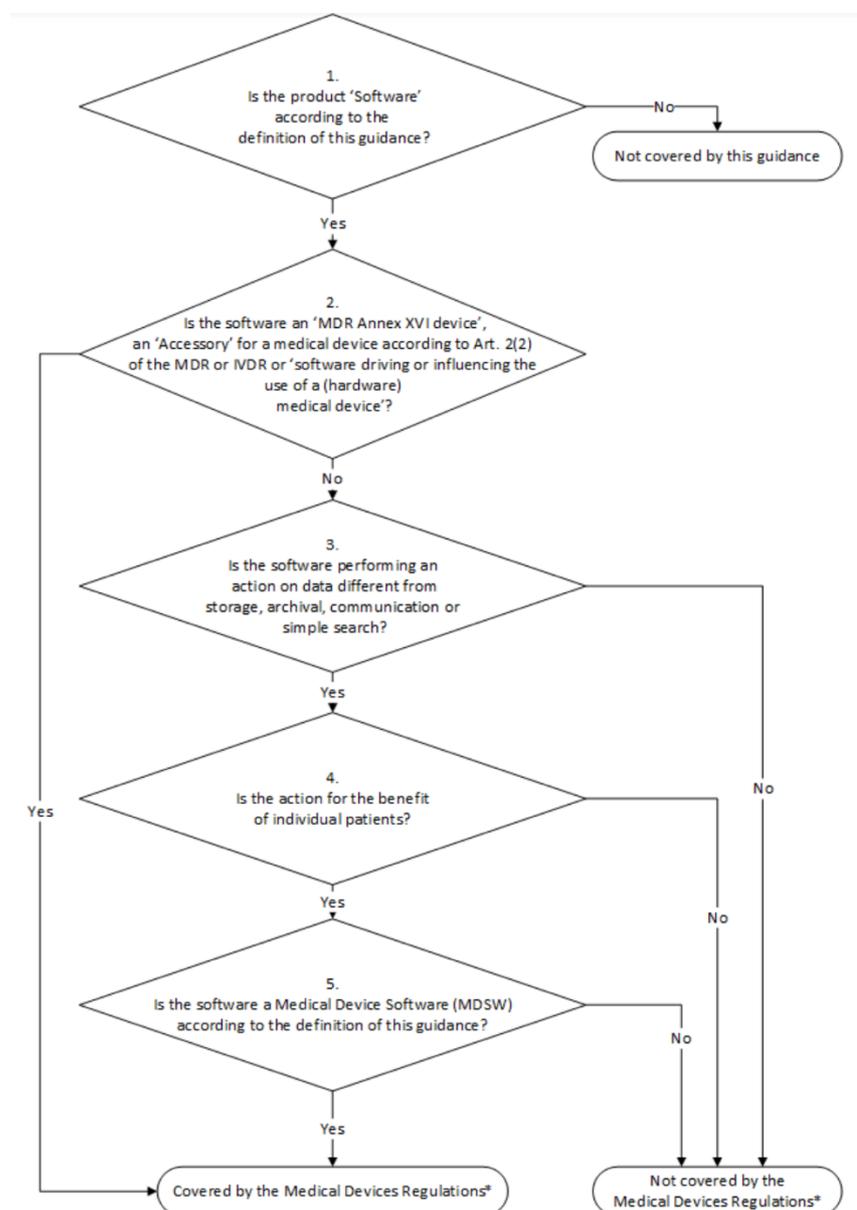
- de qualifier un logiciel : SaMD ou “simple” logiciel en santé ;
- si le logiciel est qualifié de SaMD, de définir à quel règlement (MDR ou IVDR) il répond ;
- de déterminer sa classe en suivant les règles de classification spécifiques aux logiciels énoncées dans le règlement applicable.

Le MDCG a été établi par l'article 103 du MDR et doit conseiller et aider la Commission et les États membres à assurer une mise en œuvre harmonisée des règlements sur les dispositifs médicaux.

### **1.1. Mon logiciel est-il un SaMD ?**

Le terme “logiciel” apparaît dans la définition d'un DM et celle d'un DMDIV mais n'est pas défini en tant que tel dans les règlements. La définition d'un logiciel est donnée dans le guide MDCG 2019-11, il est défini comme “*un ensemble d'instructions qui traite les données d'entrée et crée des données de sortie*” [8].

Identifier si un logiciel correspond à cette définition donnée par le MDCG 2019-11 constitue la première étape de l'arbre de décision aidant à la qualification d'un logiciel. Celui-ci permet en cinq étapes de déterminer le statut d'un logiciel ou d'une application en se basant sur son utilisation prévue, également appelé "destination", et sur l'exploitation qui est faite des données. L'utilisation prévue est fixée par le fabricant ou l'éditeur du logiciel. Elle est définie dans l'Article 2(12) du MDR et de l'IVDR comme "l'utilisation à laquelle un dispositif est destiné d'après les indications fournies par le fabricant sur l'étiquette, dans la notice d'utilisation ou dans les documents ou indications publicitaires ou de vente, et comme celles présentées par le fabricant dans l'évaluation clinique/l'évaluation des performances" [5][6]. L'usage prévu est l'élément critique sur lequel se base l'analyse et qui permet de qualifier réglementairement le statut d'un logiciel. Voyons maintenant en détail les étapes de qualification. L'arbre de décision qui décrit ces étapes se trouve dans le guide MDCG-2019-11.



**Figure 1 : Logigramme aidant à la qualification des logiciels dispositifs médicaux**

Source : MDCG 2019-11

### **Première étape :**

La première question posée par l'arbre décisionnel est : est-ce que le produit répond à la définition d'un logiciel donnée dans le MDCG 2019-11 ? Il s'agit de la définition citée précédemment c'est à dire *“un ensemble d'instructions qui traite les données d'entrée et crée des données de sortie”*. Le guide précise ce qui est considéré comme une donnée d'entrée et une donnée de sortie :

- *“Toute donnée fournie au logiciel dans le but d'obtenir des données de sortie après traitement de ces données, peut être considérée comme donnée d'entrée.”*
- *“Toute donnée produite par un logiciel peut être considérée comme une donnée de sortie.”* [8]

Ainsi, des données saisies dans un logiciel par son utilisateur, des images ou fichiers contenant des données médicales (compte rendu biologique, dossier médical électronique etc.) ou encore des données transmises par d'autres dispositifs sont des exemples de données d'entrées. En données de sortie, on pourra avoir par exemple l'affichage d'informations dans un écran récapitulatif ou encore la création de documents numériques (image, PDF etc.). Si le logiciel correspond à cette définition, on passe à l'étape suivante de l'arbre de décision. Sinon, le logiciel ne sera pas couvert par le MDCG 2019-11.

### **Deuxième étape :**

Cette étape nécessite d'identifier si le logiciel appartient à différentes catégories notamment :

- S'il fait partie des produits mentionnés dans l'annexe XVI du MDR ;
- S'il est un accessoire pour dispositif selon l'article 2(2) du MDR ou l'article 2(4) de l'IVDR ;
- S'il est considéré comme un logiciel qui pilote ou influence l'utilisation d'un DM ou d'un DMDIV.

L'annexe XVI du Règlement 2017/745 liste des groupes de produits n'ayant pas de destination médicale prévue telles que décrites dans l'Article 1(2) mais pour lesquels le Règlement s'applique.

Il s'agit des produits suivants :

1. Lentilles de contact ou autres articles destinés à être introduits dans l'œil ou posés sur l'œil.
2. Produits destinés à être totalement ou partiellement introduits dans le corps humain par un moyen invasif chirurgical en vue de modifier l'anatomie ou de fixer des parties anatomiques, à l'exception des produits de tatouage et des piercings.
3. Substances, combinaisons de substances ou articles destinés à effectuer un comblement du visage, de la peau ou des muqueuses par injection sous-cutanée, sous-muqueuse ou intradermique ou toute autre mode d'introduction, sauf ceux destinés au tatouage.

4. Équipements destinés à être utilisés pour réduire, enlever ou détruire des tissus adipeux, tels que ceux destinés à la liposuction, la lipolyse et la lipoplastie.
5. Équipements émettant des rayonnements électromagnétiques à haute intensité (infrarouge, lumière visible, ultraviolet par exemple) et destinés à être utilisés sur le corps humain, y compris les sources cohérentes et non cohérentes, monochromes et à large spectre, tels que les lasers et les équipements à lumière intense pulsée utilisés pour le resurfaçage cutané, la suppression de tatouages, l'épilation ou d'autres traitements cutanés.
6. Équipements destinés à la stimulation cérébrale transcrânienne au moyen de courants électriques ou de champs magnétiques ou électromagnétiques afin de modifier l'activité neuronale du cerveau.

Dans la mesure où le logiciel entre dans une de ces catégories, il sera couvert par la réglementation applicable aux DM.

Un accessoire pour DM est défini comme : *“tout article qui, sans être lui-même un dispositif médical, est destiné par son fabricant à être utilisé avec un ou plusieurs dispositifs médicaux donnés pour permettre une utilisation de ce ou ces derniers conforme à sa ou leur destination ou pour contribuer spécifiquement et directement à la fonction médicale du ou des dispositifs médicaux selon sa ou leur destination”* (Article 2(2) du MDR)

Un accessoire pour DMDIV est défini comme : *“tout article qui, sans être lui-même un dispositif médical de diagnostic in vitro, est destiné par son fabricant à être utilisé avec un ou plusieurs dispositifs médicaux de diagnostic in vitro donnés pour permettre spécifiquement une utilisation de ce ou ces derniers conforme à sa ou leur destination ou pour aider spécifiquement et directement au fonctionnement médical du ou des dispositifs médicaux de diagnostic in vitro selon sa ou leur destination;”* (Article 2(4) de l'IVDR)

Les accessoires entrent dans le champ d'application des règlements. Si un logiciel répond à l'une de ces définitions, alors il sera de ce fait directement couvert par le MDR ou l'IVDR.

Enfin, un logiciel qui pilote ou influence l'utilisation d'un DM ou DMDIV est considéré comme dispositif médical au même titre que le dispositif avec lequel il est utilisé en combinaison. Selon le 3.3 du MDCG 2019-11, la définition de ce type de logiciel se décline en deux points :

- Le logiciel n'a pas ou n'exécute pas une finalité médicale par lui-même.
- Le logiciel ne crée pas lui-même d'informations ayant une ou plusieurs finalités médicales décrites dans la définition d'un DM ou d'un DMDIV.

Ceux-ci ont uniquement pour finalité de faire fonctionner, modifier l'état d'un dispositif ou encore le contrôler, soit par une interface, soit par l'intermédiaire d'un opérateur. Par exemple, un logiciel qui n'est utilisé que pour afficher des images d'IRM ou d'échographie ou encore un logiciel servant à faire fonctionner un analyseur de chimie clinique appartiennent à cette catégorie.

Dans le cas où le logiciel analysé n'entre dans aucune de ces catégories, alors on passera à l'étape suivante du logigramme.

### **Troisième étape :**

Ici on s'intéresse à l'opération que le logiciel sera amené à faire sur les données. Si le logiciel effectue un traitement ou une action sur les données autre qu'un simple stockage, un archivage, une communication, ou une recherche, il sera considéré comme un DM ou un DMDIV.

En effet, un logiciel utilisé pour rechercher ou extraire une information, c'est-à-dire récupérant simplement des données pour les faire correspondre à des critères de recherche, alors celui-ci ne sera pas considéré comme un SaMD. Il peut s'agir, par exemple, d'un logiciel ayant une fonction de recherche d'information dans un tableau sans les exploiter, et cela même si le tableau contient des données de nature médicale.

Un logiciel qui est, quant à lui, destiné à traiter, analyser, créer ou modifier des données peut être qualifié de SaMD si la création ou la modification de ces informations à une finalité médicale. Par exemple, une application d'analyses de données de signaux physiologiques propres à un patient et dotées de fonctions d'alertes à finalité médicale sera qualifiée de DM.

Si un logiciel n'effectue pas une réelle action sur les données, alors on arrête à cette étape. Sinon, on poursuit le logigramme.

### **Quatrième étape :**

Dans cette étape, on s'intéresse à la portée de l'action du logiciel : est-elle au bénéfice de patients individuels ? Lorsqu'un logiciel est destiné par exemple, à l'agrégation de données de population, à la construction de modèles ou destiné à être utilisé uniquement dans le cadre d'études ou de registres épidémiologiques, celui-ci ne sera pas considéré comme étant au bénéfice individuel d'un patient et ne rentre pas dans le scope du MDR ou de l'IVDR. En revanche, un logiciel qui a une action au bénéfice d'un seul patient sera concerné par ces règlements. On passera à l'étape suivante uniquement si le bénéfice apporté par le logiciel concerne un patient.

## Cinquième étape :

Le MDCG-2019 définit un logiciel DM comme : “*tout logiciel destiné à être utilisé, seul ou en combinaison, à une fin spécifiée dans la définition d'un dispositif médical selon le MDR ou l'IVDR.*”

La dernière étape du logigramme décisionnel consiste à déterminer si le logiciel correspond à cette définition. Si c'est le cas, celui-ci sera couvert par la réglementation applicable aux DM ou aux DMDIV.

### 1.2. Mon logiciel est-il un DM ou un DMDIV ?

Nous savons maintenant que notre logiciel entre dans le champ d'application des Règlements Européens relatifs aux dispositifs médicaux. Il faut ensuite déterminer si celui-ci sera un DM ou un DMDIV. Cette étape peut, elle aussi, être réalisée à l'aide d'un arbre de décision présenté dans le MDCG-2019-11.

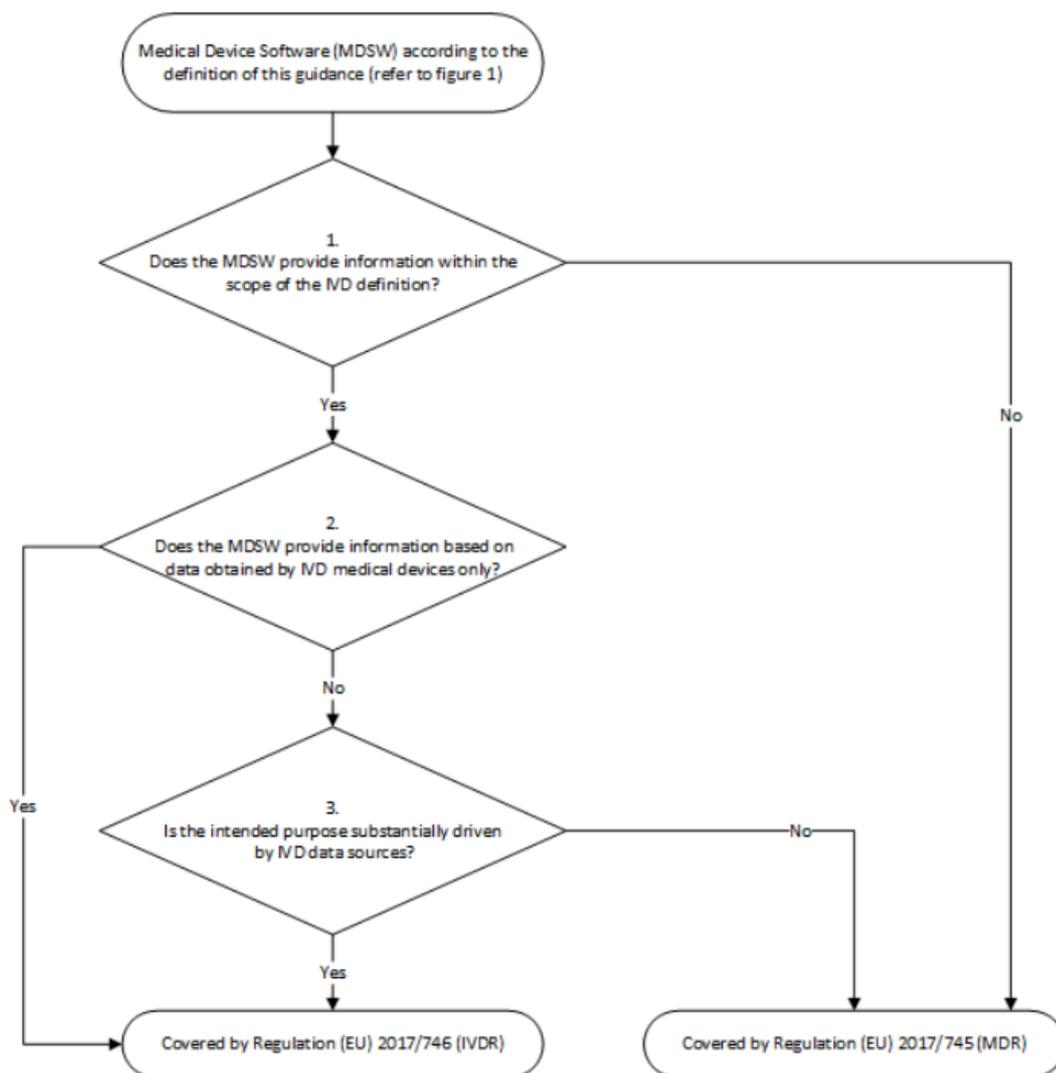


Figure 2 : Logigramme aidant à la qualification d'un logiciel en tant que DM ou DMDIV

Source : MDCG 2019-11

### **Première étape :**

Cette étape classe le logiciel selon s'il répond ou non à la définition d'un DM ou d'un DMDIV. Si le logiciel fournit des informations sur l'un ou plusieurs des éléments compris dans la définition d'un DMDIV selon l'article 2, paragraphe 2 du Règlement (UE) 2017/746 c'est à dire :

- concernant un processus ou état physiologique ou pathologique;
- concernant des déficiences congénitales physiques ou mentales;
- concernant la prédisposition à une affection ou à une maladie;
- permettant de déterminer si un traitement donné est sûr pour des receveurs potentiels et compatible avec eux;
- permettant de prévoir la réponse ou les réactions à un traitement;
- permettant de définir ou de contrôler des mesures thérapeutiques;

Dans ce cas, il sera qualifié de DMDIV.

Un logiciel qui répond à la définition énoncée dans l'article 2, paragraphe 1, du Règlement (UE) 2017/745, c'est à dire que sa finalité a un but de :

- 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;

Ici, le logiciel sera considéré comme un DM.

### **Deuxième étape :**

Pour confirmer la qualification du logiciel, on s'intéresse à la provenance des données sur lesquelles il se base pour fournir des résultats :

- Si les résultats fournis sont basés sur des données obtenues uniquement par des dispositifs médicaux de diagnostic *in vitro*, alors le logiciel est un DMDIV.
- Si les résultats sont obtenus à partir de données obtenues depuis des dispositifs médicaux de diagnostic *in vitro* et de dispositifs médicaux, il faudra passer à l'étape 3.

### Troisième étape :

Dans le cas où les données d'entrée qui permettent au logiciel de réaliser sa finalité prévue proviennent à la fois de DM et de DMDIV, une pondération des données sources visant à évaluer la contribution de chaque donnée à l'obtention du résultat permet au fabricant de déterminer le règlement à appliquer. Si la finalité du logiciel est essentiellement obtenue par des sources de données provenant de DMDIV, alors la législation applicable est le règlement (UE) 2017/746. Si la finalité prévue est essentiellement déterminée par des sources de données provenant de DM, la législation applicable est le règlement (UE) 2017/745.

### 1.3.Résumé de la démarche de qualification

Ainsi, pour résumer simplement la démarche décrite dans le guide, un logiciel sera qualifié de DM ou DMDIV s'il présente les critères cumulatifs suivants :

- Répondre à la définition d'un logiciel ;
- Être destiné à une utilisation à des fins médicales au sens de la définition du DM ou du DMDIV. Il doit permettre, par exemple, un diagnostic, une aide au diagnostic, un traitement ou une aide au traitement ;
- Faire une action autre que le stockage, un archivage, une communication, ou une simple recherche;
- Effectuer une action au bénéfice d'un seul patient ;
- Effectuer une action sur les données entrantes, telle qu'une analyse afin de fournir une information médicale nouvelle.

Il faudra ensuite s'intéresser à l'origine des données qui sont traitées ou analysées par ce logiciel pour déterminer s'il sera un DM ou un DMDIV.

Certains éléments ont plus d'importance que d'autres dans la démarche de qualification :

*Tableau 1 : Impact de différents éléments sur la qualification d'un logiciel*

<b>Éléments ayant un impact important dans la qualification</b>	<b>Éléments n'ayant pas d'impact dans la qualification</b>
La nature du logiciel : celle-ci correspond-elle à la définition d'un DM ?	Le lieu d'utilisation : un logiciel utilisé à l'hôpital n'est pas forcément un DM alors qu'une montre portée par un patient à son domicile peut l'être
La finalité : doit avoir une finalité médicale	Le risque associé à son utilisation : un logiciel non-DM peut faire l'objet de risques

La revendication du fabricant (l'usage prévu)	Le fait d'utiliser des données de santé : des logiciels non-DM peuvent traiter des données de santé
---	---

La finalité pour laquelle le logiciel est destiné à être utilisé est, et reste, le facteur critique pour déterminer les obligations en matière de conformité réglementaire. C'est l'objectif visé qui détermine, en premier lieu, si un logiciel est considéré comme un SaMD. En ce qui concerne les applications dites de santé ou autres applications liées au bien-être (liées à la forme physique, au régime alimentaire, aux habitudes de sommeil ou à la santé mentale), il est difficile de tracer une ligne claire entre un logiciel classique et un SaMD.

Par exemple, une application qui permet à l'utilisateur de surveiller ses habitudes alimentaires à des fins de contrôle du poids sera considérée comme un simple logiciel de santé. En revanche, la même application pourrait être considérée comme un DM si la surveillance effectuée est ensuite utilisée pour la prévention de maladies telles que les troubles métaboliques. Un autre exemple serait une application logicielle autonome, présentée par son fabricant comme une méthode naturelle de contrôle des naissances et dans laquelle l'utilisateur entre certains paramètres (premier jour des menstruations, température basale du corps, etc.) afin d'obtenir la fenêtre de fertilité. Ici cette application serait qualifiée de DM car elle est destinée à prévenir la grossesse ou à faciliter la conception, qui sont considérées comme des finalités médicales.

Le tableau suivant met en évidence certaines de ces distinctions à travers plusieurs exemples dont certains sont tirés du site de l'ANSM [9] :

*Tableau 2 : Exemples de solutions logicielles DM versus non-DM*

<b>Dispositif Médical</b>	<b>Non Dispositif Médical</b>
Prévention ou diagnostic de maladies ou de traumatismes	Éducation médicale du patient (par exemple, donner des conseils généraux sur la santé)
Traitement ou soulagement d'une maladie ou d'une blessure (par exemple, donner des instructions pour soulager des symptômes tels que des acouphènes)	Suivi de la condition physique générale (par exemple, un tracker d'exercice physique), de la santé générale et du bien-être général (par exemple, un journal du bien-être)
Aide à la décision ou prise de décision (par exemple, en ce qui concerne les mesures thérapeutiques)	Communication ou fonctions de recherche simples (par exemple, trouver un certain spécialiste des soins de santé)

Aide à la conception et suivi de grossesse	Stockage et affichage de données médicales (par exemple, poids ou graisse corporelle) sans aucune modification ou analyse
Télésurveillance du patient avec notion d’alertes	Améliorer l'observance d'un traitement chez un patient

Le MDCG-2019-11 intègre la notion de “*modules*” pour permettre la coexistence de briques DM et non DM dans une solution. Les logiciels peuvent être divisés en un certain nombre d'applications, chacune de ces applications étant corrélée à un module. Certains de ces modules peuvent avoir une finalité médicale, d'autres non. Ces modules peuvent être destinés à couvrir de nombreux besoins, par exemple :

- Collecter et maintenir les données administratives du patient ;
- Conserver dans le dossier l'historique médical du patient ;
- Facturation et autres fonctions comptables ;
- Fournir un lien avec les systèmes de prescription de médicaments (avec un lien possible avec les points de distribution de médicaments) ;
- Fournir un système d'aide à la prise de décision médicale.

Dans ce cas, les modules ayant une finalité médicale doivent être conformes aux exigences de la réglementation sur les dispositifs médicaux et doivent porter le marquage CE. Les modules non médicaux eux, n’y sont pas soumis. Le fabricant a l'obligation d'identifier les limites et les interfaces des différents modules. Les limites des modules soumis à la réglementation sur les dispositifs médicaux doivent être clairement identifiées par le fabricant en fonction de l'utilisation prévue.

Si les modules médicaux sont destinés à être utilisés en combinaison avec d'autres modules de l'ensemble de la structure logicielle, d'autres dispositifs ou équipements, il faut vérifier la compatibilité de l'ensemble des modules. Les différents systèmes doivent être sûrs et ne pas compromettre les performances ou influencer les modules ayant une finalité médicale. Il est également important de noter que des évolutions et mises à jour d'une application avec de nouvelles fonctionnalités peuvent faire passer la frontière de non DM à DM.

Après avoir détaillé la démarche de qualification d’un logiciel en tant que DM ou DMDIV, voyons maintenant comment déterminer sa classe en détaillant les règles de classification présentées dans les règlements.

## **2. Classification : à quelle classe appartient mon logiciel selon le règlement applicable ?**

Selon l'ancienne directive européenne 93/42/CEE relative aux dispositifs médicaux, la plupart des logiciels étaient classés comme des dispositifs médicaux de classe I et donc soumis à l'auto-certification CE. Depuis l'entrée en vigueur du nouveau règlement, la tendance s'est inversée : en raison des nouvelles règles de classification, un nombre beaucoup plus important de DM sont de classe de risque IIa ou plus. Ces logiciels sont soumis à des exigences réglementaires plus strictes et l'obtention du marquage CE nécessitera l'intervention d'un organisme notifié, avec un niveau d'examen croissant en fonction de la classe déterminée.

### **2.1. Classification d'un logiciel selon le MDR 2017/745**

Les règles de classification prennent en compte l'invasivité, la durée d'utilisation du dispositif et son caractère actif ou non actif. Les logiciels sont considérés comme des dispositifs actifs selon le MDR qui précise dans l'Article 2 paragraphe 4 que *“Les logiciels sont aussi réputés être des dispositifs actifs”* c'est à dire *“tout dispositif dont le fonctionnement dépend d'une source d'énergie autre que celle générée par le corps humain à cette fin ou par la pesanteur et agissant par modification de la densité de cette énergie ou par conversion de celle-ci”* [5]. Les logiciels peuvent donc être classés dans les quatre classes de risque.

Les dispositifs médicaux sont répartis en différentes classes de risque allant de la classe I à la classe III en fonction de la destination des dispositifs et des risques qui leur sont inhérents :

- Classe I : classe à faible degré de risque ;
- Classe IIa : classe à degré moyen de risque ;
- Classe IIb : classe à risque potentiel élevé ;
- Classe III : classe à risque potentiel très sérieux, classe de risque la plus élevée.

Le fabricant attribue la classe de risque de son dispositif en s'appuyant sur les règles de classification établies à l'Annexe VIII du MDR. Ces règles sont regroupées comme suit :

- règles 1 à 4 : dispositifs non invasifs ;
- règles 5 à 8 : dispositifs invasifs regroupant les DM invasifs de type chirurgical et invasifs de type non chirurgical ;
- règles 9 à 13 : dispositifs actifs ;
- règles 14 à 22 : règles particulières.

Les logiciels étant considérés comme des dispositifs actifs, les règles 9 à 13 seront applicables. La règle 22 sera aussi pertinente car applicable aux systèmes en “circuit fermé”.

Avant de rentrer plus en détail dans la classification, le MDR précise quelques règles d’application notamment la règle 3.3 de l’Annexe VIII qui concerne les logiciels, et peut être divisée en deux points:

- “*Le logiciel commandant un dispositif ou agissant sur son utilisation relève de la même classe que ce dispositif*” clarifie le régime applicable aux logiciels pilotant ou influençant l'utilisation d'un dispositif ;
- “*Si le logiciel est indépendant de tout autre dispositif, il est classé en tant que tel*”. Cette règle concerne les logiciels autonomes, SaMD ou “standalone software”<sup>1</sup>.

Cette seconde partie de la règle 3.3 s’applique lorsqu’un logiciel a, d'une part, sa propre finalité et, d'autre part, entraîne ou influence l'utilisation d'un dispositif médical à des fins médicales. Il sera alors classé indépendamment du dispositif qu’il pilote, en fonction de son propre usage prévu. Dans ce cas, toutefois, la classe de risque ne doit pas être inférieure à la classe de risque du DM avec lequel il est combiné. Le MDCG 2019-11 illustre cette règle 3.3 de l’Annexe VIII par un exemple, celui d’un logiciel d'analyse d'images de mélanome destiné à être utilisé avec un scanner à lumière laser. Le laser est considéré comme une classe IIa. Le logiciel "*pilote ou influence l'utilisation*" du scanner à lumière laser car il prend le contrôle du scanner en lui permettant d'exécuter des programmes pour la détection de mélanomes. Ici, la règle 3.3 s’applique et le logiciel sera de la même classe que le laser. Cependant, si le logiciel a également une finalité médicale, comme le diagnostic du cancer, il sera alors lui-même classé en classe III sur la base de la règle 11 (voir section Règles de classification).

Enfin, la règle d'application 3.5 de l'Annexe VIII s'applique à tous les dispositifs et stipule que "*Si plusieurs règles ou, dans le cadre d'une même règle, plusieurs sous-règles s'appliquent au même dispositif du fait de la destination de celui-ci, la règle ou la sous-règle qui s'applique est la plus stricte, le dispositif étant classé dans la classe la plus élevée*" [5].

Voyons maintenant en détail les différentes règles de classification. Comme vu précédemment, les logiciels DM sont considérés comme des dispositifs actifs. Il convient donc de prendre en compte les règles 9, 10, 11, 12, 13, 15 et 22 de l'annexe VIII du MDR 2017/745.

---

<sup>1</sup> Logiciel pouvant être exécuté seul, sans que d'autres programmes ou fichiers ne soient nécessaires.

- Règle 9 :

Elle concerne “tous les dispositifs actifs thérapeutiques destinés à fournir ou à transférer de l’énergie [...] les dispositifs actifs destinés à commander ou à contrôler les performances des dispositifs actifs” [5]. Ceux-ci relèvent de la classe IIb. Les appareils classés par cette règle sont principalement des équipements électriques utilisés en chirurgie tels que les lasers ou les appareils destinés à des traitements spécialisés comme la radiothérapie. Les logiciels autonomes destinés à contrôler ou surveiller ces dispositifs, ou à influencer directement leurs performances, sont également classés par cette règle.

- Règle 10 :

Cette règle s’applique aux dispositifs actifs destinés au diagnostic et au contrôle. Ces dispositifs permettent un diagnostic ou un contrôle direct des processus physiologiques tels que la respiration, le rythme cardiaque, les fonctions cérébrales, les gaz du sang, la pression sanguine et la température corporelle. Les logiciels autonomes destinés à contrôler ou surveiller ces dispositifs, ou à influencer directement leurs performances, sont également classés par cette règle. En général, les dispositifs et logiciels destinés au diagnostic et au contrôle relèvent de la classe IIa. Cependant, s’ils permettent un diagnostic ou un contrôle direct des processus physiologiques vitaux ou s’ils sont destinés à poser un diagnostic dans des situations cliniques où le patient est en danger immédiat, dans ce cas ils relèvent de la classe IIb.

- Règle 11 :

Il s’agit de la règle qui s’applique pour les logiciels autonomes. Elle stipule que :

“Les logiciels destinés à fournir des informations utilisées pour prendre des décisions à des fins thérapeutiques ou diagnostiques relèvent de la classe IIa, sauf si ces décisions ont une incidence susceptible de causer:

- la mort ou une détérioration irréversible de l'état de santé d'une personne, auxquels cas ils relèvent de la classe III, ou
- une grave détérioration de l'état de santé d'une personne ou une intervention chirurgicale, auxquels cas ils relèvent de la classe IIb.

Les logiciels destinés à contrôler des processus physiologiques relèvent de la classe IIa, sauf s'ils sont destinés à contrôler des paramètres physiologiques vitaux, lorsque des variations de certains de ces paramètres peuvent présenter un danger immédiat pour la vie du patient, auxquels cas ils relèvent de la classe IIb.

Tous les autres logiciels relèvent de la classe I.” (Annexe VIII, Chapitre III, paragraphe 6.3 du MDR)

Cette règle est une nouveauté apportée par le règlement. Selon la directive, la plupart des logiciels se retrouvaient être de classe I. Maintenant, certains pourront appartenir à la classe III. La règle 11 peut être divisée en trois sous-règles qui s'appliquent en fonction de la finalité du logiciel :

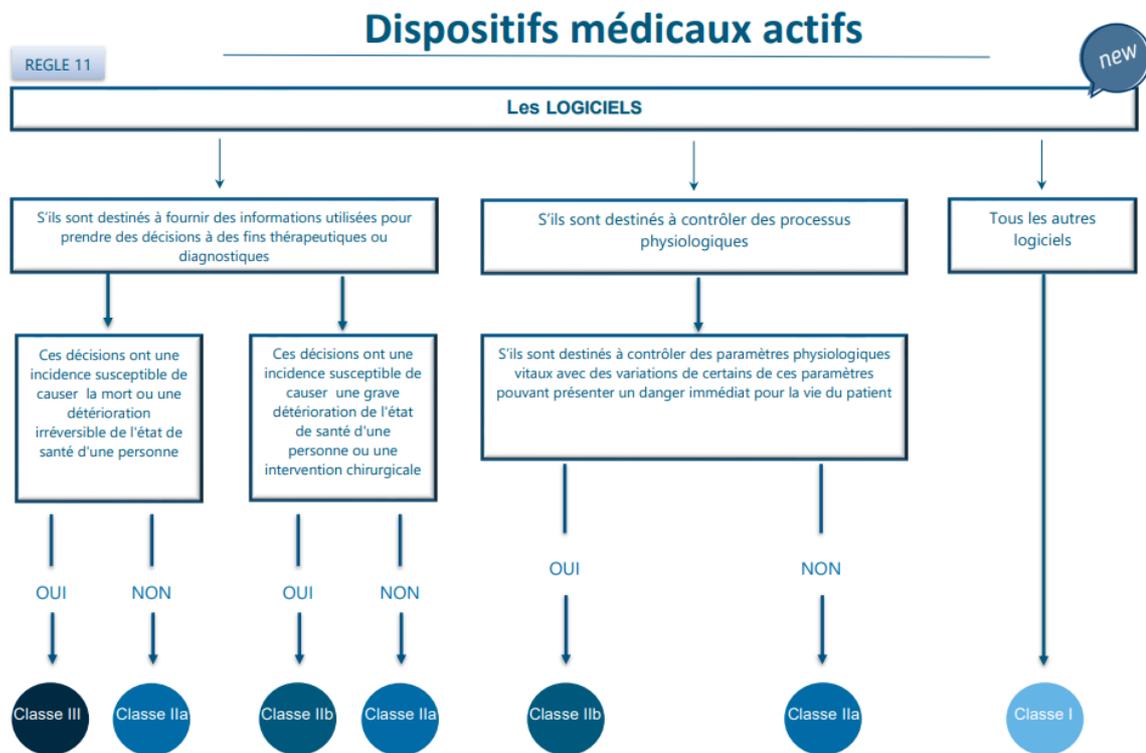
- La première phrase concerne les logiciels destinés à fournir des informations qui sont utilisées pour prendre des décisions à des fins diagnostiques ou thérapeutiques ;
- La deuxième phrase concerne les logiciels destinés à surveiller des processus ou des paramètres physiologiques ;
- La dernière phrase s'applique pour toutes les autres utilisations.

Le libellé "*destinés à fournir des informations utilisées pour prendre des décisions à des fins thérapeutiques ou diagnostiques*" décrit en termes très généraux le mode d'action qui caractérise la majorité des logiciels DM. De ce fait, elle s'applique à la plupart des logiciels ayant une finalité médicale et ils seront donc de classe IIa. Il existe deux exceptions à la première partie de la règle 11 qui visent à appliquer une classification des risques basée sur l'importance des informations fournies et sur l'impact potentiel d'une décision incorrecte prise à l'aide de ces informations. Si ces décisions peuvent entraîner :

- la mort ou une détérioration irréversible de l'état de santé d'une personne,
  - une grave détérioration de l'état de santé d'une personne ou une intervention chirurgicale,
- alors le logiciel appartiendra à une classe de risque plus élevée.

Il est intéressant de noter que la règle 11 reflète les orientations réglementaires élaborées au niveau international dans le cadre de l'International Medical Device Regulators Forum (IMDRF). Il s'agit d'un groupe volontaire réunissant des pays du monde entier, qui vise à accélérer l'harmonisation et la convergence de la réglementation internationale des DM. Les notions de l'importance des informations et de l'état de santé prises en compte dans les exceptions de la règle 11 proviennent d'un de leur guide : *Software as a Medical Device : Cadre possible pour la catégorisation des risques et les considérations correspondantes* [10].

Entreprise Europe Network présente dans son guide "48 réponses pour réussir le marquage CE des Dispositifs Médicaux" [11] un arbre de décision spécifique à cette règle 11. Les 3 sous-règles apparaissent clairement et il est permis de gérer plus facilement les exceptions.



**Figure 3 : Arbre décisionnel de la Règle numéro 11 de classification selon le MDR 2017/745**

Source : *Entreprise europe network : 48 réponses pour réussir le marquage CE des Dispositifs Médicaux*

- La règle 12 ne concerne pas les logiciels car ceux-ci ne peuvent pas administrer et/ou retirer physiquement des substances dans l'organisme.
- La règle 13 stipule que tous les autres dispositifs relèvent de la classe I. C'est le cas lorsqu'aucune règle prise en considération pour un logiciel ne s'applique.
- La règle 15 concerne tout dispositif utilisé pour la contraception ou la prévention de maladies sexuellement transmissibles. Ces DM relèvent de la classe IIb.

Enfin, la règle 22 encadre les systèmes en circuit fermés. Il s'agit de dispositifs thérapeutiques actifs dotés d'une fonction de diagnostic intégrée qui détermine la prise en charge du patient. On peut citer par exemple certains systèmes d'Intelligence Artificielle (IA) tels que le pancréas artificiel, les défibrillateurs automatisés externes ou les dispositifs de stimulation cérébrale profonde. Ces DM relèvent de la classe III.

Afin d'aider et d'orienter les fabricants dans leur démarche de classification, l'Annexe IV du MDCG 2019-11 fournit à titre indicatif, des exemples de classification pour illustrer l'application des règles du MDR :

- Un dispositif de thérapie cognitive qui comprend une fonction de diagnostic destinée à communiquer avec un logiciel pour déterminer le suivi d'une thérapie, comme par exemple un

logiciel qui adapte un traitement pour la dépression en fonction du retour d'information du diagnostic, sera de classe III conformément à la règle 22. Cependant, si un spécialiste établit lui-même la thérapie cognitive nécessaire sur la base des résultats fournis par le logiciel, alors dans ce cas, il appartiendra à la classe IIa selon la règle 11.

- Une application mobile destinée à analyser le rythme cardiaque d'un utilisateur, à détecter des anomalies et à en informer un médecin devrait être classée dans la classe IIIb conformément à la règle 11, si les informations fournies par le logiciel sont uniquement destinées à guider le médecin dans son diagnostic.
- Un logiciel destiné à effectuer un diagnostic à partir d'analyse d'images qui servira à prendre des décisions de traitement chez les patients souffrant d'un accident vasculaire cérébral aigu sera classé dans la classe III selon la règle 11.
- Une application qui vise à favoriser la conception en suivant et prévoyant l'ovulation en fonction des données de santé saisies par l'utilisatrice appartiendra à la classe I selon la règle 11.

## **2.2. Classification d'un logiciel selon l'IVDR 2017/746**

Pour les dispositifs médicaux de diagnostic *in vitro*, toutes les règles d'implémentation et les 7 règles de classification de l'Annexe VIII d' l'IVDR doivent être prises en compte. Les logiciels peuvent appartenir à toutes les classes définies dans le règlement. Celles-ci vont de A à D :

- La classe A (classe de risque la plus faible) : faible risque pour le patient / pas de risque de santé publique ;
- Classe B : risque modéré pour le patient / pas de risque de santé publique ;
- Classe C : risque élevé pour le patient / pas de risque ou risque de santé publique modéré ;
- Classe D (classe de risque la plus élevée) : risque élevé pour le patient / haut risque de santé publique.

Tout d'abord, le règlement présente des règles d'application et notamment la règle 1.4 qui précise que *“Le logiciel commandant un dispositif ou agissant sur son utilisation relève de la même classe que le dispositif. Si le logiciel est indépendant de tout autre dispositif, il est classé en soi.”* (Règlement (UE) 2017/746 ; Annexe VIII 1.4)

La finalité prévue du logiciel est également l'élément sur lequel doit se baser le fabricant lorsqu'il parcourt les règles de classification. Contrairement au MDR, l'IVDR n'inclut pas une règle de classification spécifique aux logiciels. Les différentes règles sont basées sur la criticité de l'objectif et de la destination du DMDIV. Elles précisent, selon la spécificité ou la pathologie recherchée, à quelle classe appartiendra le DMDIV.

- Règle 1 :

Elle s'applique aux dispositifs conçus pour le diagnostic d'agents pathogènes transmissibles dans le sang, les cellules, tissus ou organes. Il s'agit par exemple de tests de détection du virus de l'immunodéficience humaine, le virus T-lymphotrope humain (HTLV), Hépatite B. Si un logiciel intervient dans le diagnostic d'un agent transmissible, alors il appartiendra à la classe D.

- Règle 2 :

Cette règle s'applique aux produits destinés à déterminer les groupes sanguins ou tissulaires (système Rhésus, détermination de groupes sanguins, immuno compatibilité...). Tout logiciel intervenant dans un de ces diagnostic fera partie de la classe C.

- Règle 3 :

La troisième règle concerne les dispositifs destinés au diagnostic d'agent infectieux, le dépistage prénatal, le pronostic, le monitoring ou diagnostic du cancer, ainsi que la surveillance des traitements médicamenteux. Ceux qui seront de classe C.

- Règle 4 :

Elle s'applique aux dispositifs destinés à l'autodiagnostic, ceux qui relèvent de la classe C, à l'exception des dispositifs destinés à :

- La détection des grossesses ;
- Aux tests de fertilité ;
- A la détermination du taux de cholestérol ;
- A la détection de la présence de glucose, d'érythrocytes, de leucocytes et de bactéries dans les urines.

Ceux qui relèvent de la classe B.

- Règle 5 :

Cette règle définit les produits de classe A : il s'agit des dispositifs à usage général de laboratoire n'ayant pas de caractéristiques critiques.

- Règle 6 :

Les dispositifs non concernés par les règles de classifications ci-dessus relèvent de la classe B.

- Règle 7 :

Enfin, les dispositifs destinés à des contrôles sans valeur assignés quantitative ou qualitative relèvent de la classe B.

Il existe un guide spécifique sur les règles de classification définies par l'IVDR : le MDCG 2020-16. Les différentes règles y sont détaillées et des conseils sont donnés sur leur application afin d'aider et d'orienter les fabricants. Quelques exemples de classification de DMDIV sont également donnés par le MDCG 2019-11 :

- Le logiciel installé sur un analyseur ELISA (enzyme-linked immunosorbent assay) entièrement automatisé, qui permet de déterminer la concentration d'HbA1c humaine dans le sérum à partir des résultats obtenus avec un ELISA HbA1c humain, dans le but de dépister, diagnostiquer et surveiller les patients diabétiques, doit faire partie de la classe C selon la règle 3.
- Le logiciel destiné à l'interprétation des lectures automatisées de tests immunologiques en ligne pour la confirmation et la détermination des anticorps au VIH-1, au VIH-1 groupe O et au VIH-2 dans le sérum et le plasma humains, appartiendra à la classe D selon la règle 1.

La qualification d'un logiciel est un choix qui peut se révéler stratégique pour une entreprise. C'est avant tout le fabricant qui détermine si son logiciel sera un dispositif médical s'il a les capacités de s'orienter vers un marquage CE médical ou si son logiciel sera un simple logiciel de bien-être ou de mode de vie. [12] Les développeurs et les fabricants de nouveaux logiciels autonomes doivent se familiariser avec le système de classification prévu par le MDR et l'IVDR. Sous certaines conditions, les SaMD déjà sur le marché de l'UE et classés comme dispositifs médicaux de classe I en vertu de la Directive 93/42/EEC devront se conformer aux nouvelles règles à partir du 26 mai 2024.

L'obtention du marquage CE devient plus complexe et plus longue depuis la mise en application des règlements. Il convient de procéder à une évaluation minutieuse du logiciel, en tenant compte de son usage prévu et de ses différentes fonctions. Il est primordial de bien définir la classe de son SaMD car c'est à partir de cette information que le fabricant pourra identifier les exigences réglementaires à appliquer. Cela aura un impact sur la suite du projet et la partie de développement du logiciel. Reste à suivre les règles spécifiques aux dispositifs médicaux, notamment sur les exigences générales de sécurité et de performances cliniques et sur l'évaluation de la conformité.

### **3. Évaluation de la conformité d'un logiciel DM ou DMDIV**

Après avoir abordé la question de la qualification d'un logiciel en tant que DM ou DMDIV en fonction de sa finalité puis les différentes règles de classifications et comment les appliquer, nous allons voir quels sont les impacts réglementaires ainsi que la marche à suivre pour mettre sur le marché un SaMD.

Les logiciels et applications sont considérés comme tout dispositif médical. Toutes les exigences des règlements leur sont applicables. Les logiciels doivent démontrer un rapport bénéfice risque favorable et le maintenir dans le temps.

Comme l'explique l'ANSM, si un logiciel est qualifié de DM ou DMDIV, son éditeur devient fabricant de DM ou DMDIV, ce qui le contraint, pour pouvoir commercialiser son logiciel, à :

- **Démontrer la conformité aux exigences essentielles** applicables aux DM ou DMDIV de son application conformément aux procédures prévues dans les Règlements européens correspondants.
- **Réaliser une analyse de risque et constituer une documentation technique.** La démonstration de conformité s'appuie sur des normes harmonisées. Les éléments de preuves de conformité à ces normes sont à décrire dans la documentation technique réglementaire.
- **Mettre en place un système de vigilance** qui soit apte à gérer les incidents déclarés, les actions de sécurité ou la diffusion de versions logicielles correctives vers les utilisateurs.
- **Mettre en place un système de surveillance « post mise sur le marché »**, base d'un système de gestion du risque tout au long du cycle de vie du DM ou DMDIV.
- **Mettre en place une démarche qualité** indispensable pour réaliser ces opérations.
- **Respecter les obligations de déclaration et de communication des nouveaux produits mis sur le marché** auprès des autorités compétentes. [13]

Les logiciels suivent donc le même parcours de mise sur le marché que tous les dispositifs médicaux. Pour être mis sur le marché, les dispositifs au-delà de la classe I pour les DM et de la classe A pour les DMDIV, nécessitent une évaluation de la conformité par un organisme tiers, appelé Organisme Notifié (ON). L'ON évalue la conformité du dispositif aux exigences réglementaires selon la procédure appropriée et délivre le certificat CE de conformité qui, en complément de l'apposition du marquage CE, est nécessaire à la libre circulation du dispositif dans l'union Européenne. Pour les DM de classe I et DMDIV de classe A, considérés comme à faible risque, le fabricant reste le seul acteur de la certification du dispositif : on parle d'auto-certification.

### **3.1. La mise en conformité**

#### **3.1.1. Les procédures d'évaluation de la conformité**

La conformité d'un dispositif médical aux exigences des règlements est évaluée par l'ON en amont de sa mise sur le marché. Pour cela, l'ON suit une ou plusieurs procédures décrites dans le MDR et l'IVDR et appelées « procédures d'évaluation de la conformité ». Les deux règlements prévoient les mêmes procédures d'évaluation de la conformité. Elles sont décrites dans les annexes IX à XI :

- Annexe IX : Évaluation de la conformité sur la base d'un système de gestion de la qualité et de l'évaluation de la documentation technique ;
- Annexe X : Évaluation de la conformité sur la base de l'examen de type ;
- Annexe XI : Évaluation de la conformité sur la base de la vérification de la conformité du produit pour le MDR, et Évaluation de la conformité sur la base de l'assurance de la qualité de la production pour l'IVDR.

L'annexe IX est composée de 3 chapitres, applicables ou non en fonction de la classe du dispositif :

- Chapitre I : système de management de la qualité (SMQ). Le fabricant fait évaluer son SMQ par un ON ;
- Chapitre II : évaluation de la documentation technique ;
- Chapitre III : dispositions administratives mentionnant l'obligation de mise à disposition sur demande des autorités compétentes du SMQ, de la documentation technique et des décisions et rapports des ON.

Dans l'annexe X, l'ON vérifie que le dispositif, sa documentation technique et les processus qui lui sont associés sont conformes au règlement. Il s'appuie notamment sur un échantillon représentatif de la production (types). En sus, le dispositif devra se conformer à l'évaluation décrite dans l'annexe XI. Celle-ci repose sur la vérification de la conformité des produits (série) au type qui a été établi pour un dispositif conformément à l'annexe X.

L'article 52 du MDR et l'article 48 de l'IVDR exposent les procédures, ou combinaison de procédures, à utiliser en fonction de la classe de risque du dispositif. Les différentes possibilités sont exposées dans le tableau 3 :

**Tableau 3 : Procédures d'évaluation de la conformité applicables selon la classe du DM ou du DMDIV**

Classe du DM ou DMDIV		Procédures et Annexes applicables	
<b>DM</b>	I	Déclaration de conformité UE	
	IIa	Annexe IX Chap. I, III + DT	Annexe XI
	IIb	Annexe IX Chap. I, III + DT	Annexe X + Annexe XI
	III	Totalité de l'Annexe IX	Annexe X + Annexe XI
<b>DMDIV</b>	A	Déclaration de conformité UE	
	B	Annexe IX Chap. I, III + DT	
	C	Annexe IX Chap I, III + DT	Annexe X + Annexe XI
	D	Annexe IX Chap. I, II, III	Annexe X + Annexe XI

DT = Documentation Technique

### 3.1.2. Démonstration de la conformité

Les deux piliers de la démonstration de conformité d'un dispositif sont la documentation technique et le système de management de la qualité.

- **La documentation technique** : démonstration de la sécurité et de la performance

La documentation technique est l'élément central qui permet d'attester de la conformité des dispositifs médicaux aux exigences qui leur sont applicables et de justifier ainsi le marquage CE. Cette documentation regroupe toutes les informations sur le dispositif durant son cycle de vie : depuis sa conception jusqu'à sa mise sur le marché, en passant par les étapes de production et de recueil des informations post-commercialisation. Le contenu de la documentation technique est détaillé dans l'Annexe II : Documentation technique et l'Annexe III : Documentation technique relative à la surveillance après commercialisation du MDR et de l'IVDR. Elle comprend notamment :

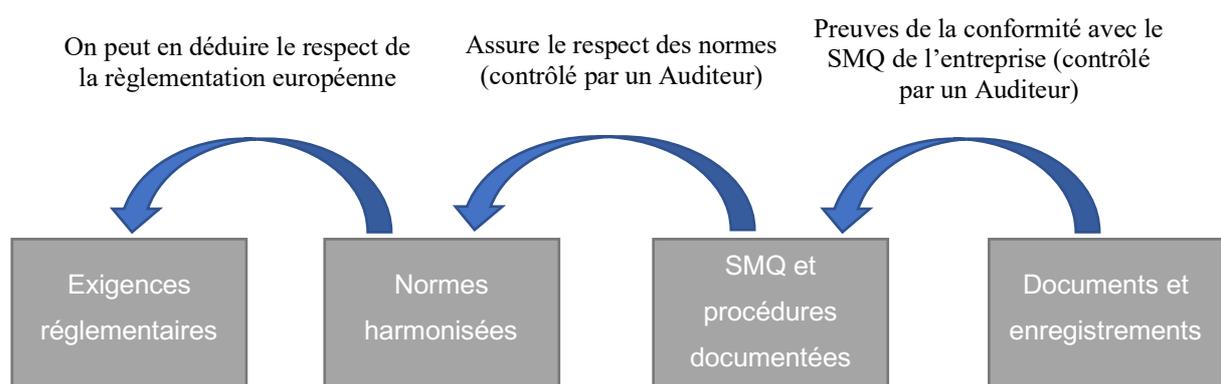
- Les informations sur la conception et la fabrication
- Les exigences générales en matière de sécurité et de performances
- L'analyse bénéfiques/risques et gestion de risques
- Vérification et validation du produit

- **Le système de management de la qualité**

Le fabricant doit mettre en œuvre un système qualité approuvé pour la conception, la fabrication, l’inspection finale des produits et les essais. Ce système de management de la qualité doit permettre de démontrer la capacité à reproduire le produit conformément à la documentation technique, au type et à ce que le fabricant a défini comme exigences essentielles. Les fabricants peuvent choisir la méthode de démonstration de la conformité réglementaire et pour cela ils peuvent s’appuyer sur l’application de normes harmonisées, guides ou recommandations.

Par exemple, la norme applicable en matière de système de management de la qualité pour les DM et DMDIV est la norme ISO 13485. Celle-ci a été réécrite et publiée en 2016, en tenant compte de l’IVDR et du MDR. Être certifié ISO 13485 est un moyen pour le fabricant de prouver qu’il est en phase avec les exigences réglementaires. En effet, comme l’explique le considérant (22) du MDR et le considérant (20) de l’IVDR *“Compte tenu du rôle important de la normalisation dans le domaine des dispositifs médicaux, le respect des normes harmonisées définies dans le règlement (UE) no 1025/2012 du Parlement européen et du Conseil [14] devrait être un moyen pour les fabricants de prouver qu’ils respectent les exigences générales en matière de sécurité et de performances et les autres exigences légales, notamment celles en matière de gestion de la qualité et des risques, énoncées dans le présent règlement.”* Ainsi, si le fabricant choisit d’appliquer les normes harmonisées, les produits bénéficient d’une présomption de conformité et toutes les procédures pour l’obtention du marquage CE seront plus simples.

La relation entre les exigences réglementaires et le système de management de la qualité est illustrée dans un article de Johner Institute sur les normes harmonisées [15].



**Figure 4 : Les normes harmonisées aident à prouver la conformité avec les réglementations de l'UE**

Source : Johner Institute

Prenons un exemple pour illustrer ces relations :

- Exigences réglementaires : le MDR impose que les logiciels soient développés et fabriqués conformément à l’état de l’art ;

- La norme harmonisée correspondante est IEC 62304 - Logiciels de dispositifs médicaux ;
- SMQ et procédures : la procédure de développement du logiciel et le plan de développement du logiciel nécessitent une révision du code ;
- Documents et enregistrements : revue de code documentée le jour X par la personne Y avec le résultat Z.

L'IEC 62304 est une norme qui aborde le développement d'un logiciel dispositif médical et son cycle de vie. La plupart du temps, elle est utilisée en addition avec d'autres normes harmonisées applicables aux SaMD.

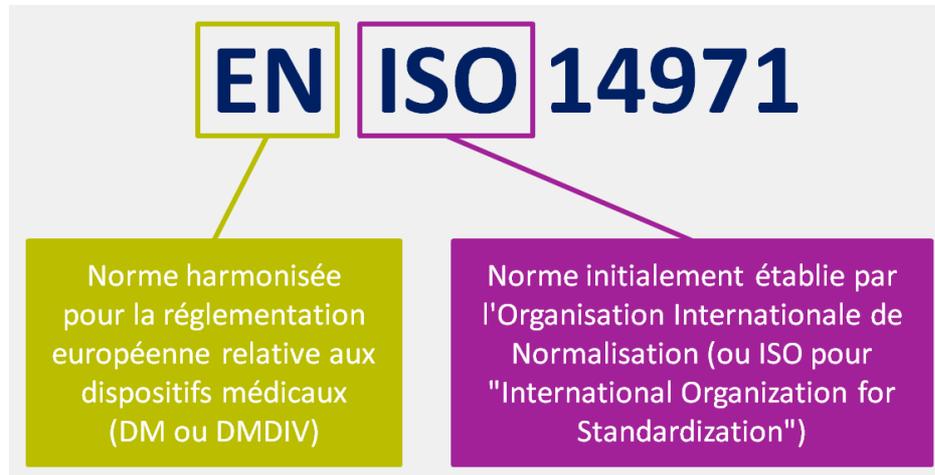
- **Les normes harmonisées applicables aux logiciels dispositifs médicaux**

Outre les exigences communes aux DM et DMDIV, certaines exigences sont spécifiques aux logiciels. Ces exigences sont décrites dans l'Annexe I, Chap. II du MDR et de l'IVDR :

- MDR 17.1 / IVDR 16.1. Les dispositifs comportant des systèmes électroniques programmables, notamment des logiciels, ou les logiciels qui sont des dispositifs à part entière sont conçus de manière à garantir la répétabilité, la fiabilité et les performances eu égard à leur utilisation prévue.
- MDR 17.2 / IVDR 16.2. Pour les dispositifs qui comprennent des logiciels ou pour les logiciels qui sont des dispositifs à part entière, ces logiciels sont développés et fabriqués conformément à l'état de l'art compte tenu des principes du cycle de développement, de gestion des risques, y compris la sécurité de l'information, de vérification et de validation.
- MDR 17.3 / IVDR 16.3. Les logiciels visés à la présente section qui sont destinés à être utilisés en combinaison avec des plateformes informatiques mobiles sont conçus et fabriqués en tenant compte des caractéristiques spécifiques de la plateforme mobile (par exemple, taille et rapport de contraste de l'écran) et des facteurs externes liés à leur utilisation (variation du niveau sonore ou de la luminosité dans l'environnement).
- MDR 17.4. / IVDR 16.4. Les fabricants énoncent les exigences minimales concernant le matériel informatique, les caractéristiques des réseaux informatiques et les mesures de sécurité informatique, y compris la protection contre l'accès non autorisé, qui sont nécessaires pour faire fonctionner le logiciel comme prévu. [5][6]

Le meilleur moyen pour un fabricant d'être conforme à ces exigences est d'appliquer les normes harmonisées applicables aux logiciels. En effet, la mise en œuvre d'une norme dite harmonisée confère aux fabricants une présomption de conformité aux exigences réglementaires relevant de cette norme.

La Commission Européenne assure le maintien de listes de normes harmonisées pour la mise en œuvre de la réglementation sur les dispositifs médicaux. Les mises à jour de ces listes sont régulièrement publiées dans le Journal Officiel de l'Union Européenne (JOUE). Ces normes applicables aux DM et DMDIV et aux logiciels dispositifs médicaux viennent à l'appui de la réglementation existante [13].



*Figure 5 : Harmonisation des normes ISO pour la réglementation Européenne relative aux DM et DMDIV*

*Source : mauricenavarro.com – Consultant qualité & logiciel pour dispositifs médicaux*

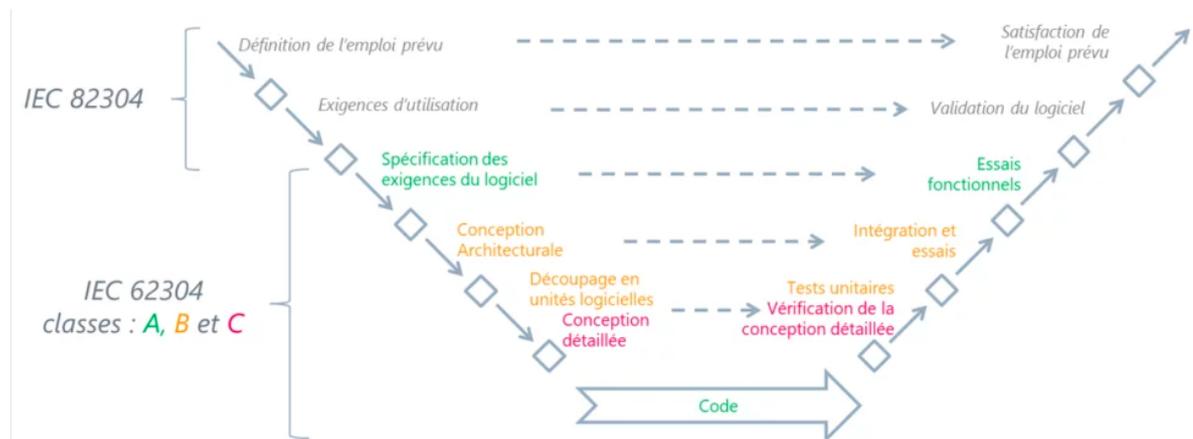
Voyons les différentes normes applicables au processus de développement d'un logiciel. En fonction de la typologie du logiciel qui sera développé, c'est à dire s'il s'agit d'un logiciel standalone (autonome) ou un logiciel intégré (hardware), une ou deux normes seront applicables à la partie développement.

#### **La norme EN 62304 : Logiciels de dispositifs médicaux — Processus du cycle de vie du logiciel.**

Cette norme définit les exigences du cycle de vie des logiciels dispositifs médicaux. Elle est applicable quel que soit le type de logiciel développé : hardware ou standalone. L'ensemble des processus, activités et tâches décrit par la norme constitue un cadre commun pour les processus du cycle de vie des logiciels dispositifs médicaux [16]. Le cycle de vie d'un logiciel comprend le développement et la validation/vérification du logiciel, la maintenance, la résolution des problèmes, la gestion des risques et la gestion de la configuration [17]. La norme IEC 62304 introduit 3 classes de sécurité du logiciel, allant de A (la moins critique) à C (la plus critique). Plus la criticité est élevée, plus le cycle de vie du logiciel de dispositif médical à mettre en œuvre devra être complet. Les classes de sécurité du logiciel se définissent suivant la gravité des conséquences d'une défaillance du logiciel :

- Classe A : Aucune blessure ou atteinte à la santé n'est possible
- Classe B : Une blessure non-grave est possible
- Classe C : Le décès ou une blessure grave est possible. Ici, toutes les exigences de la norme seront applicables.

**IEC 82304 : Logiciels de santé.** Elle s'applique à la sécurité et à la sûreté des produits logiciels de santé destinés à être commercialisés sans matériel dédié (logiciels autonomes). Elle couvre le cycle de vie complet y compris la conception, le développement, la validation, l'installation, la maintenance et l'élimination des produits logiciels de santé. L'IEC 62304 est directement appelée par l'IEC 82304 et les deux normes se complètent. Elles peuvent être représentées sous la forme d'un cycle en V :



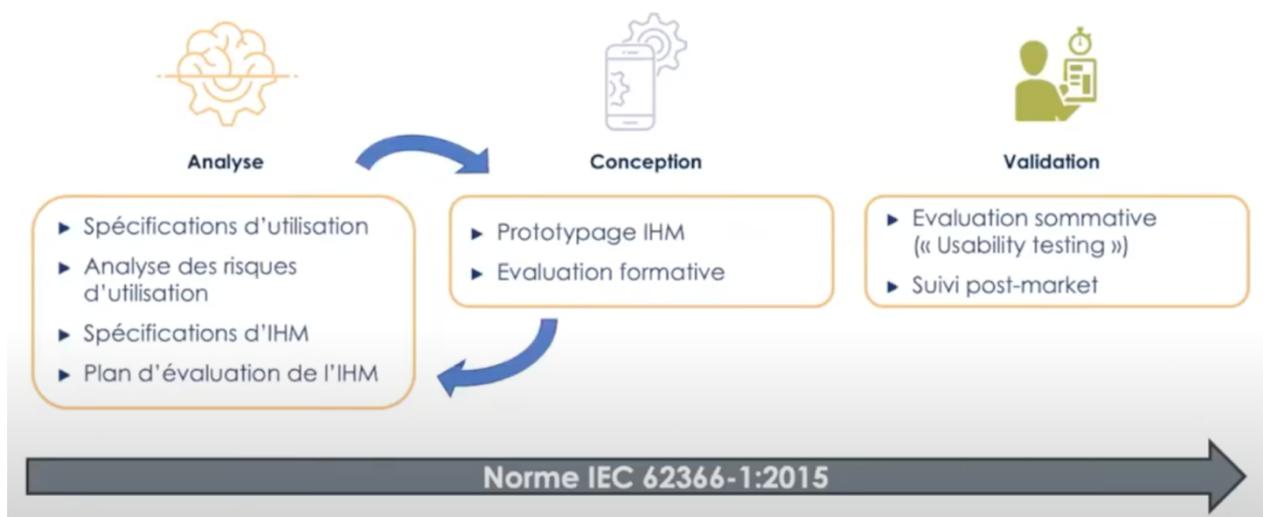
**Figure 6 : Schéma du cycle en V de l'IEC 62304 et de l'IEC 82304**

Source : <https://www.qualitiso.com/iec-82304-1-norme-logiciels-de-sante/>

La norme 62304 part du principe que les données d'entrée du produit sont déjà existantes, il faudra traduire ces données produites en exigences logiciels. Elle n'est pas concernée par la partie définition de la donnée d'entrée et validation du logiciel puisque le produit pour lequel s'applique la norme 62304 sera un logiciel intégré. Les parties spécifications du produit, validation et post market sont apportées par la norme 82304 qui est destinée aux logiciels qui sont eux même des DM ou DMDIV. Il faudra dans ce cas bien définir les spécifications du produit en tant que dispositif médical. C'est notamment durant cette phase que sera déterminée l'utilisation prévue du logiciel qui servira par la suite à le qualifier de dispositif médical ou non. L'étape de validation du logiciel DM ou DMDIV permettra de s'assurer qu'il réponde bien à son utilisation prévue et ait la performance attendue. C'est à cette étape que sera réalisée l'évaluation clinique.

**La norme EN ISO 14971 : Dispositifs médicaux — Application de la gestion des risques aux dispositifs médicaux.** Cette norme traite du processus de gestion des risques nécessaire pour assurer la sécurité et la sûreté des DM et des DMDIV. Initialement établie à l'attention des fabricants de dispositifs médicaux, l'emploi de cette norme s'est étendu aux logiciels de santé non qualifiés de dispositifs médicaux. Elle décrit un processus de gestion des risques applicable tout au long du cycle de vie. Pour les dispositifs médicaux incorporant du logiciel et pour les logiciels dispositifs médicaux en soi, la norme EN ISO 14971 permet de couvrir les risques de sécurité et les risques de cybersécurité (ou sûreté) du logiciel [18]. La norme est également applicable aux logiciels de santé qui ne sont pas qualifiés de dispositifs médicaux. En effet, la norme IEC 82304 renvoie vers la norme EN ISO 14971, notamment pour la gestion des risques de conception et développement du logiciel.

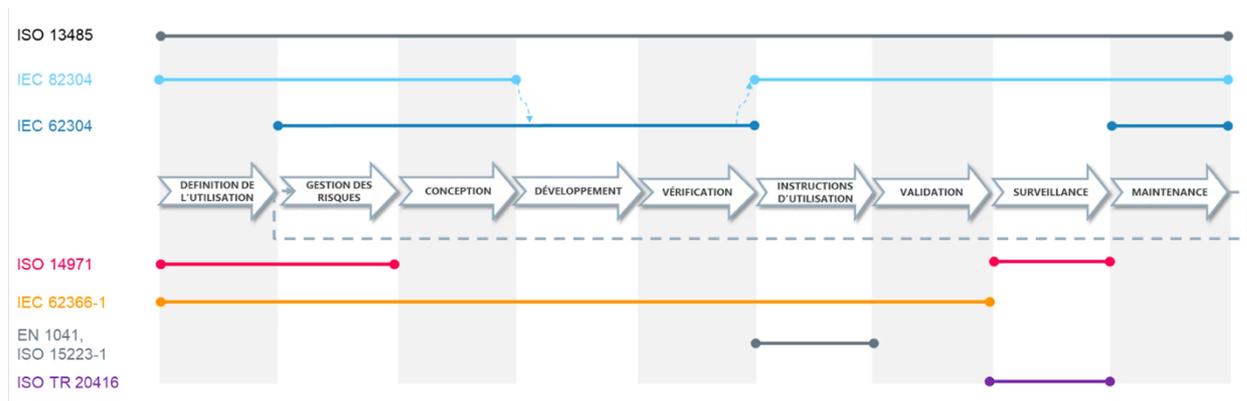
**La norme EN 62366 : Dispositifs médicaux — Application de l'ingénierie de l'aptitude à l'utilisation aux dispositifs médicaux.** Cette norme indique comment mettre au point des interfaces utilisateur qui limitent les risques liés à l'utilisation du dispositif. Le fabricant réalise une analyse préliminaire du produit qu'il veut développer. Dans la phase d'analyse, l'objectif est de décrire le futur usage du DM ou DMDIV ainsi que les caractéristiques utilisateurs. Le but est d'obtenir des scénarios d'utilisation décomposés en tâches. Ces scénarios d'utilisations vont ensuite permettre de faire apparaître des dangers possibles, qui pourraient survenir au cours de l'utilisation du dispositif par son utilisateur. Il sera ensuite possible d'identifier ces risques et de mettre en place des mesures de réduction de risques en appliquant la norme EN ISO 14971. Puis un prototypage du produit sera réalisé afin de pouvoir être évalué. L'objectif est de définir le design du produit et d'affiner l'analyse de risques. Il faudra pour cela tester des hypothèses de conception, les challenger par des utilisateurs en explorant les différents usages (erreurs, incompréhensions, besoins non-couverts...). Le but sera de concevoir un produit simple, sûr et efficace. Il s'agit de l'évaluation formative qui est réalisée pendant la phase de conception. Enfin, le fabricant réalisera une évaluation sommative pendant la phase de validation du logiciel. L'objectif est de démontrer la maîtrise du risque en testant les scénarios les plus critiques dans un protocole de test utilisateur défini par un cadre bien précis afin de satisfaire les exigences réglementaires.



**Figure 7 : Résumé de la norme IEC 62366-1**

Source : Youtube : Experts Medtech Webinars and Trainings – Sécurité d'utilisation et de conception des logiciels médicaux : les erreurs à ne pas commettre  
IHM = Interface Homme Machine

Les produits logiciels de santé, qu'il s'agisse ou pas de dispositifs médicaux, fournissent, stockent et gèrent des informations importantes pour la mise en œuvre de soins et l'adéquation des traitements proposés aux patients. Ces normes permettent aux fabricants de démontrer la conformité de leur dispositif aux exigences réglementaires. Elles se complètent entre elles et permettent ainsi de couvrir entièrement le cycle de vie d'un logiciel.



**Figure 8 : Normes applicables à un logiciel DM ou DMDIV autonome tout au long de son cycle de vie**

Source : <https://www.qualitiso.com/iec-82304-1-norme-logiciels-de-sante/>

### 3.2. Évaluation clinique des logiciels

Pour tous les dispositifs, la documentation technique comprend une évaluation clinique. Cette évaluation est un processus obligatoire, quelle que soit sa classe. Ce processus vise à collecter et évaluer les données cliniques du dispositif afin de vérifier sa sécurité et sa performance, en démontrant le respect des exigences générales associées dans le règlement, et d'attester d'un rapport bénéfique/risque acceptable.

On entend par données cliniques toutes les informations relatives à la sécurité ou à la performance du dispositif (Art. 2, point 48. du MDR). Elles peuvent être obtenues de plusieurs façons :

- analyse critique des données de la littérature avec preuve de l'équivalence entre le dispositif évalué et le dispositif auquel les données de la littérature se rapportent ;
- données propres au dispositif évalué : investigation clinique impliquant une utilisation du dispositif évalué sur un ou plusieurs participants humains. Cette investigation clinique est obligatoire pour certaines classes de dispositifs notamment ceux de classe III.

L'Article 2 (51) du MDR et l'Article 2 (36) de l'IVDR définissent une « preuve clinique » comme *“les données cliniques et les résultats de l'évaluation clinique / des performances relatifs à un dispositif, dont le volume et la qualité sont suffisants pour permettre d'évaluer, en connaissance de cause, si le dispositif est sûr et offre le ou les bénéfices cliniques attendus lorsqu'il est utilisé conformément à la destination prévue par le fabricant”*. L'objectif de l'évaluation clinique est donc de :

- Définir la balance bénéfices/risques au regard des solutions alternatives thérapeutiques ;
- Définir les bénéfices cliniques à travers des investigations cliniques réalisées sur le produit : significatifs, mesurables, des résultats en termes de bénéfice pour le patient...

Aussi, le fabricant ne peut revendiquer aucune allégation si elle n'est pas issue de l'évaluation clinique. Chaque indication et chaque bénéfice clinique revendiqué doivent être évalués individuellement et bénéficier de preuves cliniques pour les étayer. Un logiciel dispositif médical

autonome qui a une finalité médicale propre doit faire l'objet d'une évaluation clinique dédiée. L'Annexe XIV des Règlements donne une méthodologie globale pour la réalisation d'une évaluation clinique mais elle n'est pas propre aux logiciels. Des guides spécifiques à l'évaluation clinique des logiciels DM ou DMDIV sont disponibles pour aider les fabricants :

- MDCG 2020-1: Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software
- IMDRF (International Medical Device Regulators Forum) : Software as a Medical Device (SaMD): Clinical Evaluation

Ces guides donnent des indications sur la méthodologie à suivre pour réaliser une évaluation complète d'un logiciel dispositif médical. Le guide le plus récent, le MDCG 2020-1, prend en compte certains concepts décrits dans l'IMDRF dans le but d'obtenir une harmonisation mondiale. Il est important de préciser que seuls les logiciels pour lesquels le fabricant revendique une finalité médicale, et ayant donc un bénéfice clinique, nécessitent des preuves cliniques dans le cadre de leur évaluation clinique. On parle ici des logiciels autonomes. En revanche, pour les logiciels qui n'ont pas eux-mêmes une finalité médicale, comme par exemple un logiciel destiné à piloter ou influencer un dispositif médical, les preuves cliniques seront fournies dans l'évaluation clinique du dispositif et non du logiciel lui-même [19].

Le processus d'évaluation clinique d'un logiciel DM ou DMDIV décrit par l'IMDRF et le MDCG-2020-1 se décompose en 3 principes clés :

- **La validité scientifique** : cette notion est spécifique aux logiciels. Le fabricant doit s'assurer de la validité clinique de l'association entre les données de sortie du logiciel et la finalité médicale revendiquée. Il doit y avoir une correspondance entre les résultats donnés par le logiciel et la situation clinique. Cette association doit être démontrée par des recherches bibliographiques, des guidances reconnues, une revue de la littérature scientifique ou bien par des données cliniques propres au fabricant en réalisant une évaluation clinique. Par exemple, un logiciel qui détecte l'arythmie cardiaque en analysant le son d'auscultation obtenu par un stéthoscope numérique nécessite de démontrer une association clinique valide de l'association entre les sons cardiaques anormaux et l'arythmie cardiaque [19].
- **Validité technique et analytique** : le fabricant doit vérifier que le logiciel répond de manière fiable, précise et cohérente à son objectif prévu en utilisation réelle. Cela signifie qu'il doit démontrer la capacité du logiciel à générer de manière précise, fiable et exacte le résultat prévu, à partir des données d'entrée. Les résultats doivent être conformes aux spécifications établies.
- **Validation des performances cliniques** : évaluation de la sécurité et des performances cliniques du logiciel de dispositif médical permettant de démontrer que les utilisateurs peuvent obtenir des résultats cliniquement pertinents grâce à une utilisation prévisible et fiable du logiciel (obtenir

les bénéfiques cliniques revendiqués). Le fabricant doit fournir les données cliniques qui supportent les performances et la sécurité de son logiciel. Les preuves peuvent être obtenues en testant le logiciel, ou un dispositif équivalent, dans la population cible, dans les conditions d'utilisation réelles et pour l'utilisation prévue. La méthodologie appliquée doit être appropriée aux caractéristiques du dispositif et à l'usage prévu et peut comprendre des essais précliniques, une enquête clinique ou une étude des performances cliniques.

Pour illustrer ce processus, plusieurs exemples sont donnés par le MDCG 2020-1. Prenons l'exemple d'un logiciel indépendant, destiné à la détection automatique d'organes et de structures anatomiques dans des tomodensitogrammes<sup>2</sup> avec une précision équivalente à celle d'un radiologue. Le fabricant revendique que le logiciel :

- détecte les anévrismes de l'aorte abdominale sur les scanners abdominaux,
- détecte les fractures par compression sur les vertèbres,
- détecte les kystes du foie.

**Validité scientifique** : elle peut être établie en réalisant une revue de littérature :

- Les formes et les tailles standards de l'anatomie sont bien établies.
- Les techniques de segmentation sur des images en coupes transversales ont de bonnes corrélations avec la taille et la forme réelles.

Dans ce cas, l'association clinique et donc la validité clinique peut être établie.

**Validité technique et analytique** : le fabricant devra réaliser des tests de vérification et de validation des performances techniques de base telles que l'affichage, la modification, le nivellement des fenêtres des images, les mesures, y compris la confirmation de la précision, de la sensibilité et de la fiabilité du logiciel conformément aux performances attendues.

**Validation des performances cliniques** : l'évaluation de l'usabilité<sup>3</sup> dans la population cible associée à la validité scientifique et à la validité technique donnent des résultats suffisants pour démontrer la conformité du logiciel aux exigences générales de sécurité et de performances. Dans les cas où des données sont disponibles, une analyse rétrospective peut être effectuée. Cependant, si les données ne représentent pas la variabilité des paramètres d'entrée pour la performance clinique de l'algorithme de segmentation, les données manquantes pourraient être générées dans une investigation prospective.

---

<sup>2</sup> Images prises par un ordinateur et un appareil à rayons X. Ils permettent d'obtenir des images plus détaillées des os et des organes de tissus mous que les radiographies ordinaires. (<https://www.nshealth.ca/sites/nshealth.ca/files/patientinformation/ff1104.pdf>)

<sup>3</sup> L'utilisabilité, ou encore aptitude à l'utilisation est définie par la norme ISO 9241-11 comme « le degré selon lequel un produit peut être utilisé, par des utilisateurs identifiés, pour atteindre des buts définis avec efficacité, efficacité et satisfaction, dans un contexte d'utilisation spécifié »

Cette étape d'évaluation clinique d'un logiciel est complexe et doit donc être anticipée par le fabricant dès le début du développement de son projet afin de prévoir au mieux les coûts et la durée de réalisation. La sécurité, l'efficacité et les performances du logiciel DM ou DMDIV doivent être surveillées activement et en permanence par le fabricant. L'évaluation clinique est un processus continu qui sera constamment mis à jour avec les données de surveillance après commercialisation.

### **3.3. La surveillance après commercialisation et vigilance**

Une fois que le produit est sur le marché, le fabricant doit continuer de recueillir des données sur les performances en situation réelle pour mieux comprendre les besoins du client. Cela permettra de s'assurer que le produit répond à leurs besoins, et de surveiller la sécurité, l'efficacité et les performances du produit en situation réelle. Ces données sur les performances dans le monde réel permettent au fabricant d'identifier et de corriger les éventuels problèmes, d'anticiper les futures extensions de fonctionnalités, de répondre aux demandes des utilisateurs ou d'améliorer l'efficacité du dispositif. La surveillance après commercialisation impose aux fabricants d'être pro-actif dans la collecte des données relatives à leur dispositif. Ces collectes sont à distinguer des actions réactives comprenant la vigilance et les réclamations. Les données collectées peuvent toucher la qualité, les performances et la sécurité du dispositif pendant toute sa durée de vie.

L'objectif de la collecte de ces données est de réaliser une synthèse des résultats après les avoir analysés. La conclusion sur l'analyse de ces données doit être rendue disponible dans des rapports de surveillance après commercialisation pour les DM de classe I et DMDIV de classe A et B et dans les Periodic Safety Update Report (PSUR) pour les DM et DMDIV de classe supérieure. Les rapports de surveillance après commercialisation doivent être mis à jour selon les besoins. Les PSUR doivent être mis à jour au moins une fois par an pour les DM de classe IIb et III et les DMDIV de classe C et D, et selon les besoins et au moins tous les deux ans pour les DM de classe IIa.

Le niveau de connectivité propre aux DM ou DMDIV logiciels facilite l'accès aux données de performances en vie réelle, qui peuvent être utilisées à des fins multiples, y compris pour :

- la détection et la correction rapide des dysfonctionnements ;
- la détection d'une mauvaise utilisation systématique ;
- la compréhension des interactions entre les utilisateurs ;
- pour effectuer une surveillance continue de la performance clinique ;
- pour améliorer l'efficacité ;
- pour développer les revendications pour les versions futures.

Les dispositifs logiciels sont mis sur le marché avec des performances cliniques initialement revendiquées et validées. Le suivi des données de performance en situation réelle peut aider à formuler des hypothèses sur les fonctionnalités futures et ainsi de nouvelles utilisations prévues des SaMD.

La qualification réglementaire d'un logiciel est indispensable et doit être réalisée à la genèse du projet car celle-ci aura un impact sur toute la phase de développement du logiciel et sur sa mise sur le marché. Le choix du périmètre du marquage CE appartient au fabricant. Il doit se demander quelle(s) fonctionnalité(s) du produit entrent dans la définition d'un dispositif médical et pour quelles indications. Comme décrit précédemment, certaines solutions n'ont pas de finalité médicale et ne sont donc pas concernées par les règlements européens. Le cadre réglementaire varie en fonction de la nature du projet et des technologies utilisées pour le traitement et/ou le stockage des données personnelles et de ses utilisateurs finaux. Une solution qui ne sera ni un DM ni un DMDIV sera néanmoins soumise à d'autres sujets réglementaires notamment liés au traitement des données de santé, à leur hébergement et à la cybersécurité. En effet, l'utilisation du numérique en santé amène de nouveaux défis quant à la protection des données de santé. Une réglementation très stricte est alors mise en place dans le déploiement de logiciels ou applications digitales de santé. C'est dans ce contexte que la France vient structurer et faire évoluer le cadre législatif et réglementaire du numérique en santé.

## **II. Panorama de la réglementation française du numérique en santé**

### **1. Contexte général**

#### **1.1. La e-santé en France**

Les logiciels et les applications dans le domaine de la santé connaissent depuis quelques années une forte croissance. Poussée par un écosystème d'acteurs extrêmement riche et dynamique, la France est donc amenée à revoir sa stratégie pour créer un environnement plus propice au déploiement de la e-santé. Le gouvernement a identifié la e-santé et l'exploitation des données de santé comme une filière émergente prioritaire et souhaite les développer de manière encadrée. C'est pourquoi a été créée l'ASIP Santé (Agence des systèmes d'information partagés de santé) en 2009, aujourd'hui devenue l'Agence du Numérique en Santé (ANS). Il s'agit d'une agence gouvernementale française chargée de la santé numérique, ou e-santé. Elle a pour rôle d'accompagner la transformation numérique du système de santé aux côtés de tous les acteurs concernés et élabore un cadre en définissant les réglementations et les référentiels à suivre [20].

Qu'entend-on lorsqu'on parle de "e-santé" ? La e-santé est définie par l'Organisation Mondiale de la Santé (OMS) comme "l'utilisation rentable et sûre des technologies de l'information et des

communications à l'appui de la santé” [21]. Cette définition regroupe des domaines comme la télémédecine, la prévention, le maintien à domicile, le suivi d’une maladie chronique à distance (diabète, hypertension, insuffisance cardiaque...), les dossiers médicaux électroniques et les applications.

Sur la base des différents services identifiés par l’ANS [22], le périmètre de la e-santé pourrait être divisé en 4 grandes catégories :

- Les logiciels métiers destinés aux professionnels de santé tels que les logiciels d’aide à la prescription, les dossiers médicaux électroniques etc. Ils organisent les échanges d’informations entre la médecine de ville et l’hôpital, ou entre services au sein d’un même hôpital.
- La télémédecine, définie par la HAS comme “une forme de pratique médicale à distance fondée sur l’utilisation des technologies de l’information et de la communication”. Elle recouvre notamment la téléconsultation, la téléexpertise et la télémagerie [23].
- La santé mobile, ou m-santé, qui recouvre un large univers d’objets connectés ou d’applications logiciels en rapport avec la santé ou le bien-être. Elle offre de nouvelles possibilités pour améliorer la surveillance des maladies chroniques et permettre au patient d’être acteur de sa prise en charge.
- Logiciels permettant l’analyse de l’information, grâce à l’utilisation de l’intelligence artificielle. On y retrouve les logiciels d’aide à la décision, de détection d’anomalies (en radiologique ou sur des lames) ou encore des solutions de simulation et de modélisation à des fins d’analyse médico-économiques ou de recherche.

La e-santé, ou santé numérique, recouvre donc un ensemble très vaste de techniques et de services, impliquant un large éventail d’acteurs et couvrant de nombreux domaines. Elle a pour ambition de faciliter le dialogue entre les acteurs et les professionnels de santé et d’impliquer davantage le patient dans son parcours de soin et apparaît de plus en plus comme la solution aux défis de notre système de santé. Cependant, l’utilisation du numérique en santé doit concilier le principe de précaution et le principe d’innovation. C’est dans ce contexte que le plan “Ma santé 2022” vient structurer et faire évoluer le cadre législatif et réglementaire du numérique en santé en France. Il est essentiel de comprendre l’écosystème mis en place par l’État depuis quelques années à travers la feuille de route du numérique en santé.

## **1.2 Une accélération du virage du numérique en santé**

Notre système de santé connaît depuis quelques années une mutation qui s’est concrétisée avec la présentation en 2018 d’une politique de transformation de notre système de santé : “Ma santé 2022”. Portée par le Ministre des solidarités et de la santé, une feuille de route nationale du numérique en

santé a vu le jour en avril 2019, et traduit un engagement collectif de mise en œuvre du numérique en santé [24]. Elle vient fixer les cinq grandes orientations du virage du numérique en santé [25] :

#### 1 - Renforcer la gouvernance du numérique en santé :

Cette transformation est pilotée par la Délégation ministérielle du Numérique en Santé (DNS), rattachée directement à la ministre des Solidarités et de la santé. L'ANS est chargée de la mise en œuvre opérationnelle de la stratégie définie par la DNS.

#### 2 - Intensifier la sécurité et l'interopérabilité des systèmes d'information en santé :

Améliorer l'identification et l'authentification des acteurs de santé est une condition indispensable à la sécurité des systèmes d'information de santé. Pour cela, les professionnels seront identifiés grâce à des référentiels nationaux et les patients devront avoir un identifiant unique tout au long de leur parcours de soin : l'Identité Nationale de Santé (INS). Aussi, la majeure partie des solutions sur le marché étaient des solutions propriétaires et donc incompatibles avec le Dossier Médical Partagé. Afin que tous les systèmes puissent communiquer et échanger des informations, il est nécessaire d'utiliser un langage commun : c'est l'objectif de l'interopérabilité.

#### 3 - Accélérer le déploiement des services numériques socles :

La feuille de route présente des services permettant d'échanger et de partager les données de santé en toute confiance :

- Le dossier Médical Partagé (DMP) déjà en place sera amélioré pour stocker toutes les données qu'il est utile de partager, entre le patient et les professionnels qui le prennent en charge. Lancé en janvier 2022, le DMP a été rebaptisé Mon Espace Santé et chaque citoyen ne s'y opposant pas bénéficie d'un espace ouvert.
- Des messageries sécurisées de santé (MSSanté) seront développées pour sécuriser l'échange d'information de santé entre professionnels.
- La e-prescription sera déployée pour simplifier et sécuriser le circuit de transmission de l'ordonnance depuis la prescription jusqu'à la dispensation par le pharmacien.

#### 4 - Déployer au niveau national des plateformes numériques de santé :

Ces plateformes sont des espaces numériques fiables et simples d'accès dans lesquels des applications destinées aux usagers ou aux professionnels de santé sont proposées :

- L'espace Numérique de Santé permet à chaque citoyen, de choisir et d'accéder à des services numériques de santé dans un cadre sécurisé.
- Les professionnels peuvent quant à eux accéder à une plateforme de bouquets de services numériques.

- Le Health Data Hub, plateforme en cours de déploiement, rassemble les données de santé afin de les analyser à grande échelle dans le but de faire avancer la recherche.

#### 5 - Stimuler l'innovation et favoriser l'engagement des acteurs :

Des grands programmes d'investissement concourent aux objectifs de la politique nationale pour aider les acteurs à s'inscrire dans le virage numérique et à développer des solutions s'intégrant dans l'écosystème.

La feuille de route du numérique en santé a donc à la fois pour objectif de soutenir et structurer l'innovation. Durant ces 3 dernières années, cette feuille de route a été le cadre des actions collectives menées par tous les acteurs de l'écosystème (acteurs publics, privés, associations de patients, soignants et établissements, entreprises du numérique...). Une nouvelle feuille de route du numérique en santé 2023 - 2027 a été récemment publiée le 17 mai 2023 et définit les prochaines grandes orientations stratégiques.

Afin d'encourager l'émergence de ces nouvelles solutions en France, l'État s'est engagé dans une démarche de co-construction de la politique de e-santé avec l'ensemble des acteurs de l'écosystème. Les industriels, qui développent des outils et services numériques, sont des partenaires essentiels et incontournables au déploiement de cette politique de la e-santé. Ainsi, afin de montrer leur volonté à prendre part à ce changement, les industriels et éditeurs volontaires ont signé une charte dans laquelle ils s'engagent à favoriser le développement et la modernisation du système de soins. Cette charte "Engagé pour la e-santé" fixe les engagements respectifs des pouvoirs publics, d'une part, et des industriels, d'autre part. En janvier 2022, c'est plus de 350 industriels qui sont signataires de la charte [26]. On y retrouve des start-up, mais aussi des grands noms de l'industrie pharmaceutique comme Abbott France, Pfizer, Novartis ou encore Roche. En adhérant à cette charte, les industriels s'engagent à respecter l'ensemble de ses engagements notamment celui de développer des systèmes d'information, services et outils numériques conformes aux référentiels socles (éthique, sécurité, interopérabilité) et services socles décrits dans la doctrine du numérique en santé.

De fait, une des premières actions de cette démarche de co-construction a été la publication de la doctrine technique du numérique en santé. Élaborée après plusieurs mois de concertation publique entre l'ANS et les industriels, elle fournit le cadre de référence dans lequel devront s'inscrire les outils et services numériques d'échange et de partage de données dans les prochaines années. En respect des engagements pris par l'ANS, ce document est mis à jour tous les ans. La nouvelle version de la doctrine a été mise en ligne début 2022.

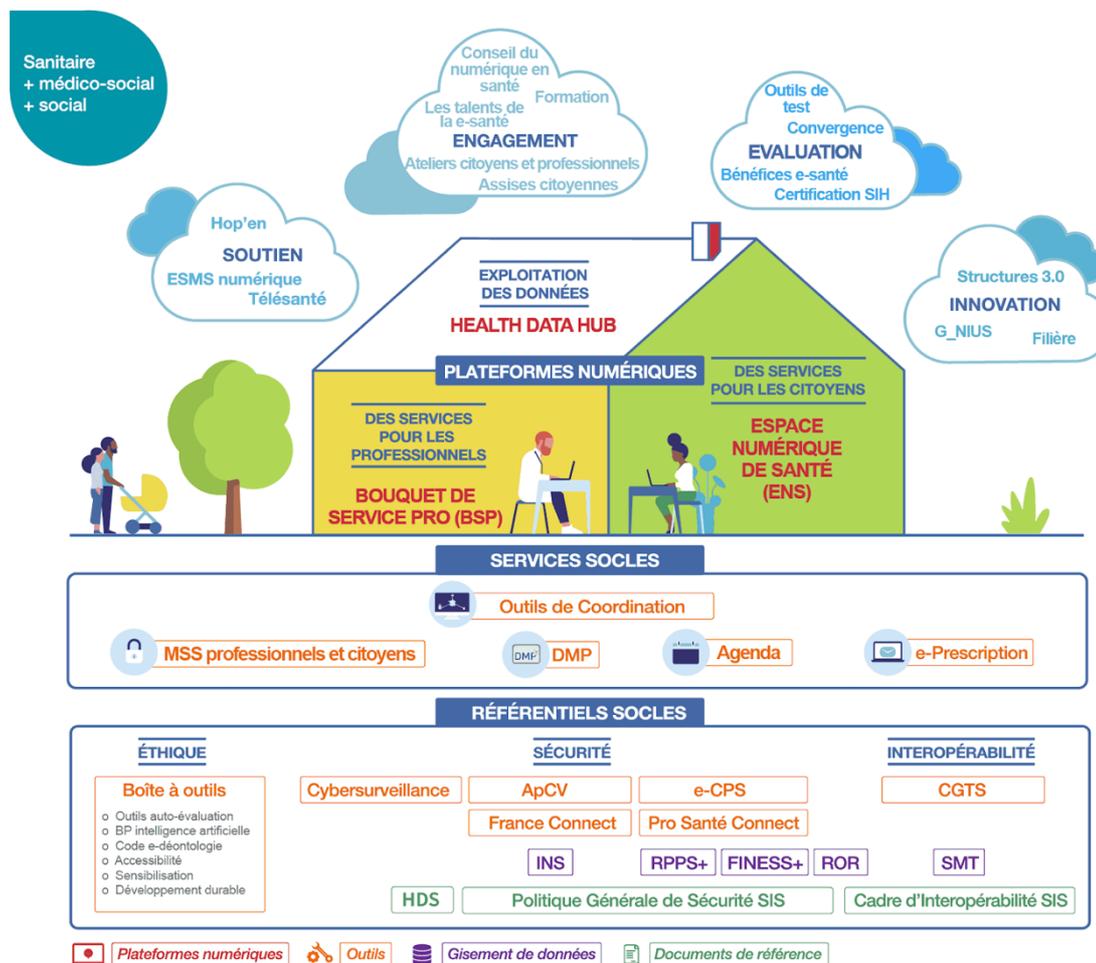
### 1.3 La doctrine du numérique en santé

Cette doctrine s'adresse à tous ceux qui souhaitent développer des projets de services numériques, notamment les industriels et les éditeurs. Elle est également destinée aux usagers de ces services, soit les professionnels de santé et les patients [27]. Elle est applicable à l'ensemble des services numériques manipulant des données de santé et utilisés sur le territoire français. Elle n'a pas de valeur réglementaire, en revanche les référentiels qui en découlent sont ou ont vocation à être rendus opposables. L'État rend opposable les référentiels prioritaires dans le cadre prévu par la loi, comme le référentiel sur l'identification électronique (début 2022), celui sur Pro Santé Connect (2022) et celui sur l'identité nationale de santé (2021). A travers la doctrine, l'État met à disposition de l'écosystème du numérique en santé le cadre technique de référence qui repose sur trois piliers fondateurs : l'éthique, la sécurité et l'interopérabilité. Ce cadre technique de référence comprend :

- **Les référentiels socles** : constitués par un ensemble de documents de référence, de bases de données de références nationales et d'outils.
- **Les services socles** : le dossier médical partagé qui devient une brique fondamentale de Mon Espace Santé, les messageries sécurisées de santé, la e-prescription et des outils de coordination.
- **Les plateformes numériques nationales** : Mon Espace Santé, volet destiné aux usagers, le Bouquet de services aux professionnels qui cible les professionnels de santé ainsi que le Health Data Hub.

Parallèlement à ce cadre technique, l'État a mis en place des leviers pour réguler le numérique en santé et accompagner les acteurs :

- La plateforme en ligne Convergence, qui permet aux éditeurs de services numériques d'évaluer la conformité de leur solution aux différents principes de la doctrine.
- Un programme de financement afin d'accompagner et d'inciter les acteurs à se mettre en conformité : le Ségur du Numérique.
- La plateforme G\_NIUS qui oriente et informe les acteurs de la santé numérique par la mise à disposition de guides.



**Figure 9 : La maison de la e-santé**

Source : Agence du Numérique en Santé

L'ensemble est représenté sous la forme d'une « maison de la e-santé ». Cette image de la maison permet d'illustrer le concept des fondations, qui correspondent aux référentiels et services socles. L'idée est que certains éléments sont indispensables à implémenter dans les solutions numériques (les bases de la maison) afin de permettre la construction solide et sécurisée de l'écosystème.

L'enjeu pour les fabricants souhaitant commercialiser une solution numérique auprès des patients ou des professionnels de santé va être de prendre en compte les différentes exigences et de mettre en conformité leurs solutions. Une étude des référentiels et guides rendus opposables par l'ANS est donc indispensable afin de comprendre le cadre réglementaire, et d'anticiper lors du développement cette mise en conformité pour pouvoir déployer et intégrer leur dispositif dans les outils des clients.

Les réglementations qui découlent de la feuille de route ministérielle définie au profit de l'accélération du numérique en santé sont classées selon leur fonctionnalité [28] :

- Le domaine de la sécurité : on y retrouve la réglementation liée aux services de connexion sécurisée (Application carte vitale (ApCV), e-CPS, Pro Santé Connect), le Règlement Général Sur La Protection Des Données (RGPD), la réglementation concernant les répertoires, annuaires et référentiels du domaine médical (ROR, RPPS+,FINESS+), la réglementation concernant l'hébergement des données de santé (HDS), la réglementation concernant l'Identité Nationale de

Santé (INS), la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) et la réglementation applicable aux dispositifs médicaux.

- Le domaine de l'interopérabilité : il se compose du Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS) qui fixe les règles d'une informatique de santé communicante. Il couvre l'interopérabilité technique et l'interopérabilité des contenus métiers.
- Le domaine des services socles : il regroupe l'ensemble des services comme le dossier médical partagé (DMP) qui est en fait le carnet numérique de santé, la e-Prescription qui consiste à dématérialiser le circuit de l'ordonnance et enfin la messagerie sécurisée de santé professionnels et citoyens (MSSanté).

Voyons maintenant le cadre ainsi que les exigences réglementaires présentées dans ces différents référentiels socles. Ne seront détaillés que les référentiels opposables à ce jour par le catalogue de l'ANS [29].

## **2. Les référentiels et services socles**

### **2.1 La sécurité et la protection des données de santé**

La protection des données médicales constitue un enjeu majeur aussi bien pour les établissements de santé, les éditeurs de logiciel et les patients. Avec l'essor des dispositifs médicaux connectés et la multiplication des cas de vulnérabilité avérés, la cybersécurité est devenue la première préoccupation des fabricants de DM ou DMDIV connectés. En effet, la principale caractéristique des dispositifs connectés est leur capacité à communiquer des données personnelles de santé. Ces données peuvent être utilisées par exemple pour l'aide au diagnostic, ou pour le suivi patient. Pour rappel, selon la CNIL, une donnée de santé est une donnée à caractère personnel qui concerne la santé physique ou mentale d'un individu aussi bien passée, présente que future [30]. Entrent dans cette notion trois catégories de données :

- celles qui sont des données de santé par nature : antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc.
- - celles, qui du fait de leur croisement avec d'autres données, deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne : croisement d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques...), croisement de la tension avec la mesure de l'effort, etc.
- celles qui deviennent des données de santé en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical.

Tous les outils numériques, objets connectés et dispositifs médicaux sont susceptibles d'utiliser, de traiter ou de stocker des données médicales à caractère personnel. Les fabricants doivent donc respecter un cadre de sécurité strict pour assurer la protection des données personnelles et des données de santé des patients.

### 2.1.1 Le Règlement Général sur la Protection des Données (RGPD)

En 2018, l'Union européenne a adopté le Règlement (UE) 2016/679 : Règlement Général sur la Protection des Données (RGPD), qui vise à renforcer la cybersécurité dans toute l'UE. Tous les organismes sont concernés par le RGPD, quels que soient leur taille, leur pays d'implantation ou leur activité. En effet, le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors qu'elle est établie sur le territoire de l'Union européenne, ou que son activité cible directement des résidents européens [31]. Par exemple, une société établie en France, qui exporte l'ensemble de ses produits au Maroc pour ses clients moyen-orientaux, doit respecter le RGPD.

Le RGPD s'étend à toutes données personnelles et impacte significativement le secteur médical. Le règlement impose l'obtention du consentement explicite des patients avant d'utiliser leurs informations médicales. De plus, le RGPD exige des éditeurs de logiciel de santé qu'ils prennent des mesures de sécurité appropriées, telles que le chiffrement et la sauvegarde régulière des données. Bien que non directement applicables aux fabricants de dispositifs médicaux, les principes de base du RGPD font que ces derniers sont fortement impactés. En effet les dispositifs médicaux doivent être conçus de manière à pouvoir respecter ses exigences du RGPD, puisqu'ils sont, pour une grande partie, voués à être utilisés par des organismes qui eux sont pleinement contraint par ce règlement (laboratoire d'analyse, hôpitaux, etc...).

Le RGPD vient donc renforcer la sécurité et la protection des données dans l'UE. La France se distingue par la mise en place d'un cadre spécifique à l'hébergement de ces données. Celui-ci a pour objectif de renforcer la protection des données de santé à caractère personnel et de construire un environnement de confiance autour de la e-santé et du suivi des patients.

### 2.1.2 L'hébergement des données de santé

Du fait de la nature sensible des données de santé à caractère personnel, leur accès et leur hébergement nécessitent une vigilance particulière en termes de sécurité. L'État encadre et fixe un cadre rigoureux concernant les pratiques liées à l'hébergement des données de santé. En 2006, un agrément « hébergeur de données de santé » est instauré en France. Depuis 2018, la certification Hébergeur de Données de Santé (HDS) remplace peu à peu l'agrément qui était délivré par le

ministère [32]. Les hébergeurs de données peuvent déposer une demande de certification HDS auprès de tout organisme de certification approuvé par le COFRAC (Comité Français d'Accréditation). Les modalités d'hébergement de données de santé à caractère personnel sont encadrées par l'article L.1111-8 du code de la santé publique (CSP) qui précise que "Toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, doit être agréée ou certifiée à cet effet" [33].

La procédure de certification repose sur une évaluation de conformité au référentiel de certification. L'hébergeur choisit un organisme certificateur qui procède à un audit en deux étapes pour évaluer la conformité de l'hébergeur aux exigences du référentiel. Il vérifie notamment l'équivalence des éventuelles certifications ISO 27001 ou ISO 20000 déjà obtenues par l'hébergeur. Le décret n°2018-137 du 26 février 2018 définit six activités d'hébergement soumises à la certification :

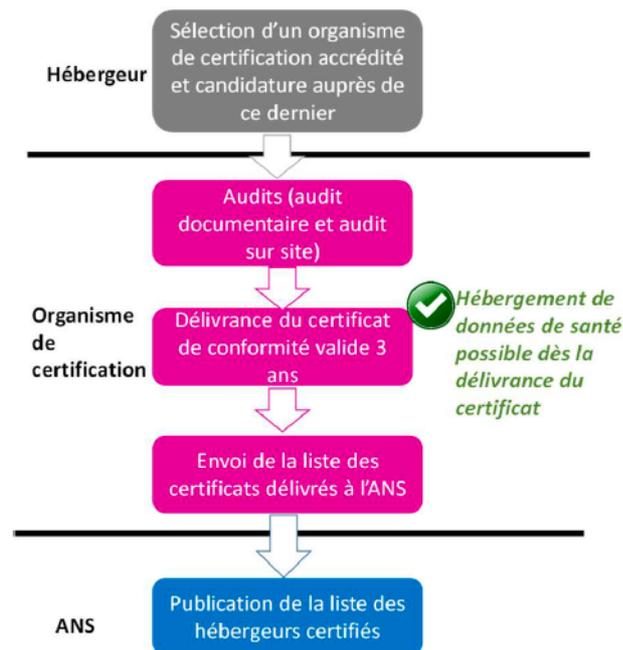
1. La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
2. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;
3. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
4. La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
5. L'administration et l'exploitation du système d'information contenant les données de santé ;
6. La sauvegarde des données de santé.

Deux types de certificats peuvent être délivrés en fonction du type d'activité réalisé par l'hébergeur:

- Le certificat hébergeur d'infrastructure physique pour la mise à disposition d'une infrastructure physique et matérielle. Il concerne les deux premières activités ;
- Le certificat hébergeur infogéreur pour la mise à disposition d'une infrastructure virtuelle, plateforme logicielle ou de sauvegarde externalisée. Il concerne les quatre autres activités.

Un hébergeur de données peut être certifié sur les six activités et donc obtenir les deux certificats. Des audits sur site et documentaire seront réalisés afin de démontrer la conformité de l'hébergeur au référentiel de certification. Une fois l'audit réussi, l'organisme sera certifié pendant 3 ans. Des audits de surveillance annuels devront être réalisés pour assurer le maintien de la certification.

## La procédure de certification



**Figure 10 : Étapes de la procédure de certification Hébergeur de Données de Santé**

Source : <https://industriels.esante.gouv.fr/produits-et-services/hds-certification-hebergeur-de-donnees-de-sante>

L'ANS met à disposition une liste des hébergeurs certifiés sur son site internet précisant les activités d'hébergement couvertes pour chaque hébergeur [34].

La question de l'hébergement des données de santé doit se poser dès les prémices du projet. En effet, tous les organismes publics ou privés qui hébergent, exploitent le Système d'Information (SI) de santé, ou réalisent des sauvegardes pour le compte d'un établissement de santé ou d'un tiers doivent être certifiés HDS [35]. La certification est également nécessaire dans le cadre d'un groupement hospitalier. Seules exceptions des services d'archivages informatiques qui ne sont pas concernés par ces obligations ainsi que les établissements de santé qui gèrent leur propre SI de santé n'ont pas la nécessité d'être certifiés HDS. Les acteurs concernés par la certification sont donc :

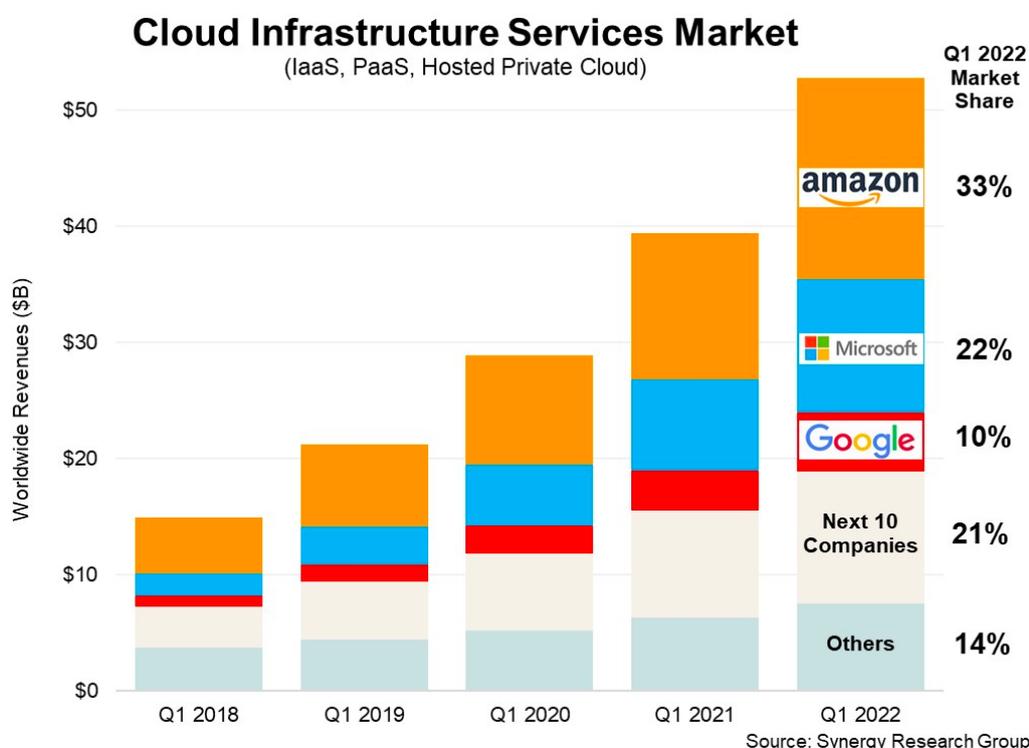
- Les hébergeurs mettant à disposition des datacenters hébergeant les données de santé ;
- Les éditeurs qui exploitent et maintiennent le SI de santé de leurs clients ;
- Toute solution qui exploite des données personnelles de santé.

Un éditeur ou un fabricant d'une solution traitant des données de santé devra donc soit être lui-même certifié HDS soit avoir recours à un sous-traitant certifié HDS. Les modalités de recours à la sous-traitance pour l'hébergement des données de santé et notamment les clauses que doit contenir le

contrat entre l'hébergeur et le client sont définies dans l'article R.1111-11 du décret. Ainsi, doivent figurer dans le contrat entre le fabricant et le sous-traitant :

- l'indication du périmètre du certificat de l'hébergeur ;
- la description des prestations réalisées ;
- l'indication des lieux d'hébergement ;
- les mesures mises en œuvre pour garantir le respect des droits des personnes concernées par les données de santé.

A l'heure actuelle, le marché des services d'hébergement est largement dominé par les géants américains avec en tête Amazon qui possède 33% du marché mondial en 2022 suivi de Microsoft et Google [36].



**Figure 11 : Répartition du marché des services d'hébergement cloud**

Source : Synergy research group - Huge Cloud Market Still Growing at 34% Per Year;  
Amazon, Microsoft & Google Now Account for 65% of the Total

L'Europe occupe une part très faible du marché et cela peut poser un problème du point de vue de la souveraineté numérique, en particulier depuis l'instauration du Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Il s'agit d'une loi entrée en vigueur aux États-Unis le 23 mars 2018. Le CLOUD Act permet au gouvernement des États-Unis de demander l'accès aux données des hébergeurs et de leurs clients. Une pratique contraire au RGPD, et donc aux lois européennes. Cette problématique a été rencontrée dans le cadre de l'hébergement des données du Health Data Hub, groupement d'intérêt public qui rassemble des acteurs, dont une grande majorité d'administrations

(CNAM, CNRS, Haute Autorité de santé...). Cette infrastructure est destinée à faciliter le partage des données de santé issues de sources variées afin de favoriser la recherche. C'est Microsoft Azure, la solution de cloud computing de Microsoft, qui a été sélectionnée pour héberger cette base de données de santé. Un choix lourdement critiqué à plusieurs niveaux. Le gouvernement a pour volonté de migrer vers un nouvel hébergeur mais cette migration ne semble pas envisageable avant 2025 notamment dû à des écarts importants concernant les fonctionnalités de sécurité qui ne répondent pas aux besoins du Health Data Hub [37].

Le choix d'un hébergeur de données de santé est donc tout sauf anodin pour un fabricant de solution logicielle en santé. Aussi, l'hébergement des données de santé n'est pas la seule mesure à respecter afin de garantir la protection de ces données sensibles. L'ANS a établi une politique de sécurité fixant un cadre de référence pour les systèmes d'information de santé. Cette politique fait partie des concepts fondamentaux définis dans la doctrine du numérique en santé.

### 2.1.3 La politique générale de sécurité des systèmes d'information de santé (PGSSI-S)

L'essor du nombre de solutions numériques sur le marché de la santé s'accompagne d'une augmentation des menaces et des risques liés à ces nouveaux outils comme des détournements, modifications ou perte des données. Ces menaces peuvent avoir un gros impact sur la prise en charge des patients et l'activité des professionnels de santé. Il est donc nécessaire d'assurer la sécurité de ces données. Face à ces enjeux, l'État a confié à l'ANS l'élaboration et la publication de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S), cadre devant être respecté par tous les acteurs de la santé, du social et du médico-social pour sécuriser les systèmes d'information de santé. Cette politique a pour objectif d'aider les porteurs de projet dans la définition des niveaux de sécurité attendus. Ainsi, les industriels pourront préciser les niveaux de sécurité proposés dans leurs offres et appliquer les bonnes pratiques afin de répondre aux obligations générales de sécurité fixées par l'État. Une fois appliquée, la PGSSI-S a pour ambition de :

- Mettre à disposition des usagers un système de santé numérisé qui réponde aux exigences des soins et assure la protection de leurs données ;
- Assurer aux responsables de systèmes d'information de santé, la conformité des SIS au cadre juridique et aux bonnes pratiques de sécurité ;
- Équiper les structures de solutions conformes aux exigences de sécurité propres à l'écosystème santé, social et médico-social ; [27]

Cette politique s'applique à tout système d'information utilisé en santé, manipulant des données de santé que celles-ci soient à caractère personnel, directement ou indirectement nominatives (ex. logiciel de professionnel de santé, dispositifs médicaux connectés, base de données de santé

publique, etc.). Ces exigences doivent être prises en compte dès la phase de conception d'un projet ou d'une solution. La PGSSI-S regroupe des référentiels thématiques et des guides pratiques, qui rappellent aux différents acteurs des systèmes d'information de santé les exigences pour être en conformité avec la réglementation en vigueur. Les référentiels et guides comportent généralement une notion de paliers à atteindre : un palier minimal et des paliers progressifs, permettant aux porteurs de projet d'améliorer progressivement la sécurité de leurs projets jusqu'au palier cible défini. A ce jour, tout le corpus documentaire n'est pas opposable, seuls certains référentiels le sont. Les guides quant à eux, sont des bonnes pratiques qu'il est recommandé d'appliquer. D'autres référentiels sont néanmoins destinés à être rendus opposables par arrêté du ministre chargé de la santé. A ce jour, l'ANS a établi 5 référentiels et 6 guides techniques, disponibles sur leur site internet.

*Tableau 4 : Synthèse du corpus documentaire de la PGSSI-S*

<p style="text-align: center;"><b>Référentiels</b></p> <p style="text-align: center;">Objectif d'opposabilité</p>	<p style="text-align: center;"><b>Guides</b></p> <p style="text-align: center;">Objectif d'accompagnement</p>
<ul style="list-style-type: none"> <li>• Identification électronique des acteurs des secteurs sanitaires, médico-social et social (personnes morales)</li> <li>• Identification électronique des acteurs des secteurs sanitaires, médico-social et social (personne physique)</li> <li>• Identification électronique des usagers</li> <li>• Imputabilité : gestion de preuve et traçabilité</li> <li>• Force probante des documents de santé</li> </ul>	<ul style="list-style-type: none"> <li>• Mise en place d'accès Wifi</li> <li>• Accès par application web ou mobile pour des tiers</li> <li>• Protection de l'intégrité des données stockées</li> <li>• Sauvegarde des SI de santé</li> <li>• Destruction sécurisé des données</li> <li>• Plan de continuité informatique</li> <li>• Interventions à distance</li> </ul>

La PGSSI-S cible les entreprises et les fabricants dans le but de les orienter dans leurs choix sur la sécurité et le développement de leurs nouvelles offres ainsi qu'aux porteurs de projet dans la définition des niveaux de sécurité à mettre en œuvre. La consultation des référentiels publiés et la prise en compte des différentes exigences permettra aux fabricants d'ajuster leurs solutions afin de proposer aux structures de santé des outils et des solutions conformes à la PGSSI-S. Celle-ci s'adresse également aux structures de santé, du social et médico-social dans la définition de leur politique de sécurité de leur système d'information.

Le corpus documentaire de la PGSSI-S comprend 3 référentiels :

- Un référentiel d'identification électronique, divisé en 3 volets : un destiné aux personnes physiques acteurs de santé, un deuxième destiné aux personnes morales et un dernier qui vise l'identification des usagers.

- Un référentiel d'imputabilité des systèmes d'information.
- Un référentiel de force probante des documents de santé.

Le référentiel d'identification électronique est le premier à avoir été rendu opposable par arrêté ministériel depuis mars 2022. Néanmoins tous les référentiels ont vocation à être rendus obligatoires.

### 2.1.3.a) Référentiel d'identification électronique

Rendu opposable par un arrêté du 28 mars 2022 [38], ce référentiel définit des exigences sur les connexions à des services numériques traitant des données de santé. Dans ce référentiel, la locution identification électronique, reprise du vocabulaire du Règlement européen eIDAS n°910/2014 du 23 juillet 2014, désigne le processus utilisé par une personne physique ou morale pour s'identifier et s'authentifier auprès d'un système d'information. L'article 3 du Règlement eIDAS définit l'identification électronique comme *“le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale”* [39]. Cette notion d'identification est différente de la notion d'authentification qui elle est définie par le même Règlement comme *“un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique”*. L'identification correspond au fait de communiquer une identité alors que l'authentification consiste à prouver cette identité.

Le référentiel d'identification de l'ANS définit un moyen d'identification électronique comme un *“dispositif matériel et/ou immatériel contenant un identifiant personnel et utilisé pour s'authentifier sur un service numérique”* [40]. Les moyens d'identification électroniques peuvent être associés à des niveaux de garantie en fonction du niveau de sécurité qu'il offre : garantie faible, substantiel ou élevé. (ref) Un couple identifiant / mot de passe ou encore une application mobile d'identification électronique sont des exemples de moyens d'identification électronique.

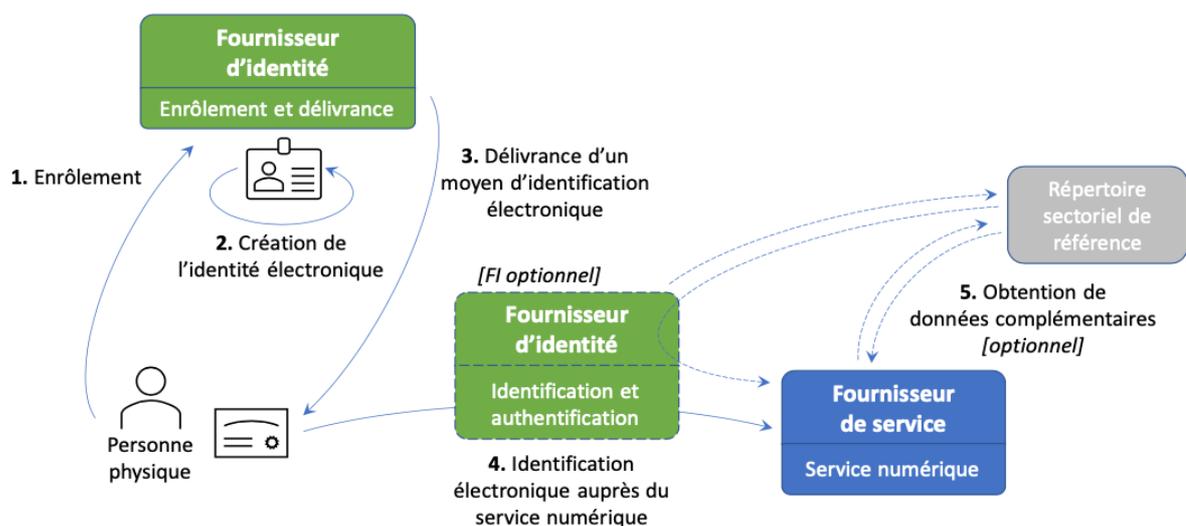
L'ANS considère l'identification et l'authentification des professionnels et usagers du système de santé comme un pilier de la e-santé. Il est établi que les pratiques en matière de connexion aux différents outils numériques sont susceptibles d'impacter très fortement la sécurité des données de santé. Le référentiel vient normaliser le niveau de garanties attendu en termes d'identification électronique pour tous les utilisateurs de services d'e-santé. Celui-ci est découpé en trois volets dédiés respectivement aux différentes catégories d'utilisateurs des services numériques en santé : les usagers, les professionnels de santé et les structures. Il s'applique à tous les outils, systèmes d'information et services numériques concourant à des activités de prévention, de diagnostic, de soin, de prise en charge, de suivi ou d'interventions nécessaires à la coordination de plusieurs de ces activités, à condition que ceux-ci traitent des données à caractère personnel au sens de l'article 4 du

RGPD. Toutefois, le référentiel précise que les logiciels qualifiés de DM ou DMDIV sont exclus du périmètre d'application puisqu'ils font l'objet d'une réglementation spécifique qui leur est propre et dans laquelle des mesures de sécurité sont déjà prises en compte [40].

En règle générale, les exigences posées par le référentiel concernent l'utilisation de mots de passe forts, de second facteurs d'authentification et se base sur des informations d'identification des utilisateurs vérifiées et issues des répertoires de référence (INS, RPPS, FINESS). En effet, le référentiel impose l'usage des identifiants nationaux pour les professionnels de santé, à savoir :

- Le numéro RPPS ;
- Ou le numéro ADELI, utilisé de façon transitoire jusqu'à son remplacement définitif par l'identifiant RPPS pour les professions encore enregistrées dans ADELI.

Ces identifiants nationaux constituent l'identité électronique des professionnels de santé. Un moyen d'identification électronique (tel que l'application mobile e-CPS ou encore les cartes CPS) sera délivré au professionnel de santé par le fournisseur d'identité. Un fournisseur d'identité est une entité qui délivre un moyen d'identification électronique à une personne physique ou morale qui a demandé ce moyen et dont elle a établi une identité électronique fiable. La plateforme IGC-Santé est l'Infrastructure de Gestion des Clés cryptographiques (IGC) opérée par l'ANS. Elle fait office de fournisseur d'identité et délivre des certificats d'authentification de logiciels permettant ensuite aux professionnels de santé de s'authentifier, de signer ou de chiffrer les informations transmises. Après avoir obtenu un moyen d'identification électronique auprès d'un fournisseur d'identité, la personne physique pourra alors utiliser ce moyen pour s'identifier et s'authentifier auprès d'un service numérique. Les processus liés à l'identification électronique d'une personne physique peuvent être représentés par le schéma suivant :



**Figure 12 : Processus d'identification électronique d'une personne physique**

Source : ANS - Référentiel d'identification électronique des personnes physiques

Les industriels développant des solutions numériques doivent donc prendre en compte les exigences décrites dans le référentiel afin d'intégrer ces moyens techniques d'identification électronique dans leurs solutions. Le référentiel décrit des paliers successifs de sécurité à atteindre entre le 1er juin 2022 et le 31 décembre 2025. Le respect des exigences étant obligatoire pour les acteurs concernés, si celles-ci ne sont pas respectées, un plan d'action devra être mis en place afin de pouvoir être conforme aux exigences du référentiel en respectant les délais imposés. Pour certains éditeurs, la mise en conformité au référentiel nécessite de gros investissements de la part des équipes. C'est pourquoi l'ANS prévoit un délai d'implémentation pour les services sensibles pour lesquels les exigences sont les plus strictes.

### 2.1.3.b) Référentiel d'imputabilité

Pour définir l'imputabilité, le référentiel de l'ANS s'appuie sur la définition donnée par la norme ISO 27000 qui décrit l'imputabilité comme "*la responsabilité d'une entité par rapport à ses actions et ses décisions*" [41]. On peut également parler "d'audit trail". En d'autres termes, elle vise à s'assurer que chaque action faite sur un logiciel est attribuée de façon univoque à l'utilisateur ou la machine l'ayant effectuée. Cette traçabilité est réalisée grâce à des traces correspondant à un ensemble de données générées pour refléter une action sur le logiciel ainsi que son contexte d'occurrence. Par exemple, des traces sont créées lors de la connexion à l'application, le dépôt d'un document dématérialisé ou la modification d'un paramètre, et la trace générée contiendra le type d'action, l'auteur de l'action, la date et heure de l'action et les données concernées. La mise en place de ce dispositif de traçabilité permet de répondre au besoin d'apporter la preuve qu'une information n'a été consultée ou modifiée que dans le cadre d'une action légitime. Ainsi, le logiciel produit des preuves électroniques qui pourront être fournies dans le cadre d'une éventuelle action en justice.

Le référentiel décrit 4 paliers apportant un niveau croissant d'assurance sur la fiabilité des traces générées et donc de l'action réalisée. Chaque palier présente les mesures à mettre en place en termes de prérequis, de traçabilité et de documentation du logiciel. Les exigences minimales décrites dans le palier 1 sont notamment :

- La mise en place de mesure d'identification conforme au référentiel ;
- La mise en place d'une gestion des identités, c'est à dire du cycle de vie des personnes et l'impact sur la création de compte utilisateurs et les autorisations associées ;
- La génération de tracer enregistrant les actions faites sur des données à risques ;
- La possibilité d'extraire ces traces. [42]

Les paliers suivants viennent renforcer ces exigences en imposant des critères de plus en plus précis et exigeants. Plus les données traitées par un logiciel seront sensibles et plus le palier applicable sera élevé. Ajouté à ces exigences de traçabilité, un dernier référentiel définit les mesures à mettre en place afin de garantir l'authenticité des documents de santé.

### 2.1.3.c) Référentiel force probante des documents de santé

Ce référentiel répond aux exigences des articles L.1111-25 à 31 du CSP [43] traitant des conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel, créés ou reproduits sous forme numérique. Le référentiel force probante des documents de santé de l'ANS entend par force probante le "niveau de confiance que l'on peut accorder à un document ou une donnée" [44]. Il fixe des conditions de reconnaissance de cette force probante pour les documents de santé qu'ils soient numérisés ou nativement numériques.

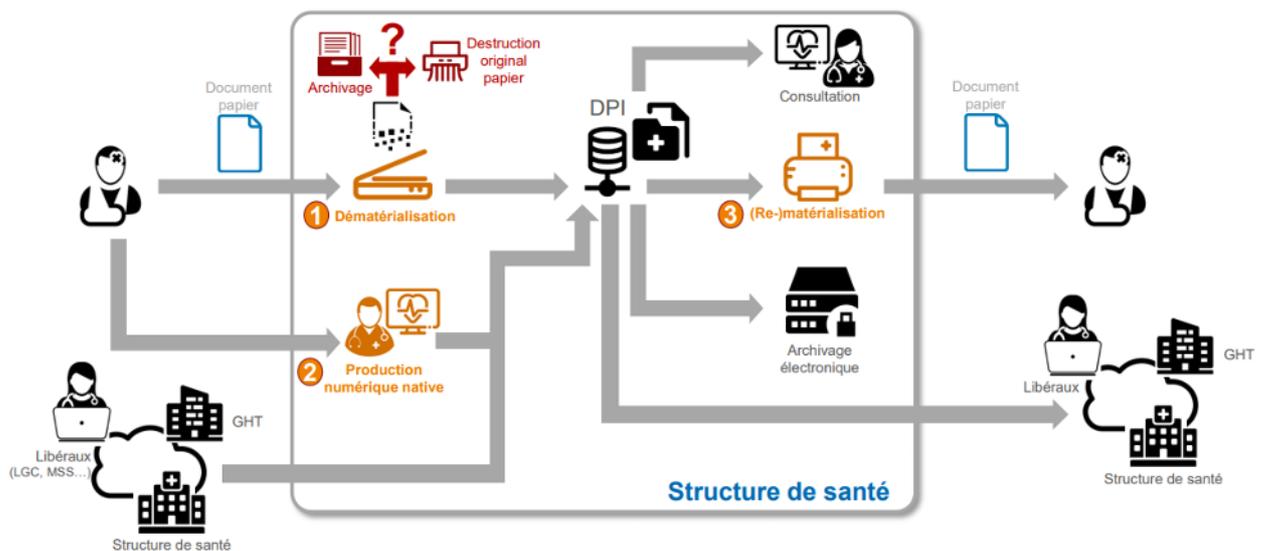


Figure 13 : Flux de documents dans les SI de santé

Source : Webinaire force probante des documents de santé – ANS

Dans un système d'information de santé, comme par exemple au sein d'un centre hospitalier, différents acteurs produisent, partagent, échangent et conservent une grande quantité de documents comportant des données de santé à caractère personnel. Ces documents peuvent être au format papier ou numérique et passer d'un format à l'autre au cours du parcours de soin du patient. Prenons d'abord le cas des documents au format papier qui sont numérisés en vue d'être sauvegardés dans le dossier patient informatisé (DPI). Il faudra s'assurer que leur dématérialisation soit faite dans des conditions maîtrisées et par des personnes disposant du document d'origine. Un autre type de flux est celui des documents nativement numériques, créés au sein d'une structure de santé. Ces documents peuvent également provenir d'autres structures (médecins libéraux, autre GHT). Ils seront stockés au sein du DPI et pourront être consultés, archivés ou exportés vers d'autres structures de santé via des flux électroniques. Enfin, on retrouve les documents dits sortants, qui sont au format numérique et seront imprimés pour être remis au patient.

On a donc l'établissement d'une chaîne entre la production d'un document et sa réception par son destinataire. La finalité du référentiel force probante est de pouvoir s'assurer qu'à un instant T, lorsqu'un

professionnel de santé ou un patient reçoit un document, que celui-ci contient un certain nombre d'informations qui permettent au destinataire d'affirmer que le document qu'il a entre les mains est fiable. Il y a un double enjeu à assurer la force probante des documents de santé :

- En cas de conflit juridique, lors d'un litige mettant en cause l'intégrité d'un document, les responsables du système d'information devront apporter la preuve de la fiabilité de leur dispositif.
- Dans les échanges quotidiens au sein de la sphère santé afin d'assurer dans le temps la continuité et la qualité de la prise en charge des patients.

Le référentiel de l'ANS est constitué d'un ensemble de documents : un document introductif et des annexes. Ces annexes détaillent les mécanismes techniques et procédures organisationnelles à mettre en œuvre en fonction des cas d'usages (numérisation de documents de santé, création de documents nativement numériques...). Il y est décrit les mécanismes de protection à mettre en place sous forme de paliers successifs.

Un grand nombre de logiciels permettent de produire des documents nativement numériques. Ceux-ci doivent ainsi disposer de propriétés permettant de répondre aux enjeux suivants :

- Identification de l'émetteur ;
- Intégrité et non répudiation ;
- Pérennité dans le temps ;
- Portabilité ;
- Traçabilité.

L'ensemble de ces éléments contribuent à la force probante du document. Par ailleurs, que le document soit au format papier ou numérique, il peut être exigé qu'il soit signé. Lorsqu'il est imposé de faire signer un professionnel de santé, la signature signifie que celui-ci valide le contenu du document (ex: certificats décès, naissance, arrêt de travail, etc.). C'est principalement grâce à la signature de ces documents par un professionnel de santé qu'on leur donnera de la force probante. Des mesures organisationnelles, juridiques et techniques doivent être mises en œuvre et être documentées pour répondre à cette exigence dans le cadre de la dématérialisation des documents comportant des données de santé.

La signature et le cachet électroniques sont encadrés par le Règlement européen « eIDAS » n°910/2014 du 23 juillet 2014. Ce texte s'applique depuis le 1er juillet 2016 ; il fixe les bases de la mise en œuvre, de la valeur juridique et de la reconnaissance de 3 niveaux de mise en œuvre pour les signatures électroniques :

- La signature électronique dite « simple » ;
- La signature électronique avancée ;
- La signature électronique qualifiée.

Dans son référentiel, l'ANS a mis en place un système de paliers à respecter en fonction de la catégorie de document. Ces paliers vont de 1 à 3, le palier 1 correspondant aux exigences les plus faibles.

La PGSSI-S assure donc la sécurité d'un système de santé en mettant en place des exigences d'identification et d'authentification des professionnels et structures médicales, des systèmes de traçabilité des actions faites sur les logiciels et des moyens permettant de s'assurer de l'authenticité des documents de santé peu importe leur provenance et leur format. Un dernier élément reste à prendre en compte afin de garantir une sécurité complète du parcours de soin : l'identification des patients.

#### 2.1.4 L'identité Nationale de Sante (INS)

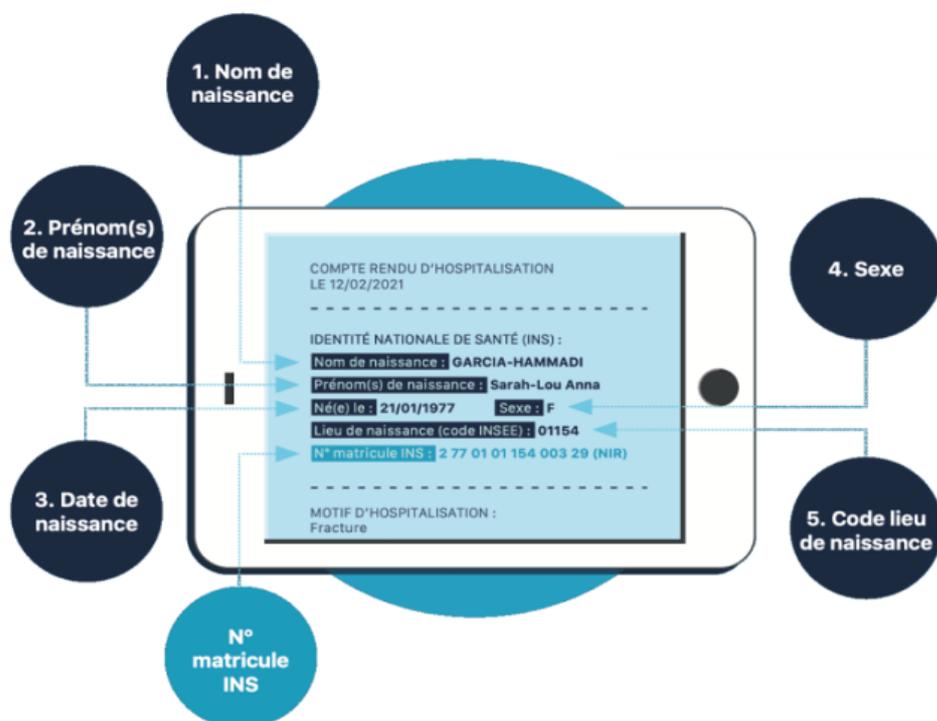
La bonne identification de l'utilisateur, tout au long de son parcours de santé, repose sur l'utilisation d'une identité unique et pérenne. C'est l'objectif de l'identité nationale de santé. Pour reprendre l'exemple donné dans la doctrine du numérique en santé, une patiente pourrait être enregistrée de façon différente auprès des professionnels de santé qu'elle consulte : Sarah-Lou GARCIA chez son médecin traitant, Sarah GARCIA HAMMADI à l'hôpital, Sarah-Lou HAMMADI dans son laboratoire de biologie... Jusqu'à présent, les professionnels de santé n'enregistraient pas les usagers de façon identique dans leurs logiciels. Cela pouvait entraîner un risque de rattacher une donnée de santé à un autre usager (collision de données) pouvant conduire à l'administration de mauvais médicaments ou, inversement, de créer un nouveau dossier alors qu'il y en a déjà un existant, et passer à côté d'une information essentielle. C'est dans l'objectif d'éviter ces erreurs d'identité que, depuis le 1er janvier 2021 (Décret n°2017-412 du 27 mars 2017), toutes les données de santé doivent être référencées avec l'INS [45]. Elle permet de référencer les données de santé avec une identité unique partagée par l'ensemble des professionnels de santé. L'INS vise également à faciliter et à sécuriser les échanges et le partage de données de santé entre l'ensemble des acteurs intervenant dans la prise en charge des patients. Cette identité est constituée :

- D'un numéro unique à chaque individu : le matricule INS qui correspond au NIR (Numéro d'Identification au Répertoire des personnes physiques)<sup>4</sup> ou au NIA (Numéro Identifiant Attente). Ce matricule INS correspond au numéro de sécurité sociale lorsque l'utilisateur est lui-même l'assuré. Lorsque l'utilisateur est différent de l'assuré, dans le cas d'un enfant par exemple, le matricule INS sera différent du numéro de sécurité sociale servant au remboursement des soins. Ce matricule est systématiquement associé aux traits d'identité stricts tels que définis dans le RNIV (Référentiel National d'Identito Vigilance) :
- Le nom de naissance ;
- La liste des prénoms de naissance ;

---

<sup>4</sup> Le NIR est un numéro attribué à la naissance pour toute personne née en France ou au moment de l'inscription auprès de la sécurité sociale pour toute personne née à l'étranger. Dans certaines situations, lorsque le patient ne dispose pas d'un NIR, il peut se voir attribuer un Numéro Identifiant d'Attente (NIA) par la CNAV.

- La date de naissance ;
- Le sexe ;
- Le code INSEE correspondant au lieu de naissance de l'utilisateur.



**Figure 14 : Identité Nationale de Santé**

Source : ordre des Pharmaciens –

<https://www.ordre.pharmacien.fr/les-communications/focus-sur/les-actualites/identite-nationale-de-sante-de-quoi-s-agit-il>

La mise en place de l'INS est obligatoire d'un point de vue réglementaire. Les industriels doivent fournir à leurs clients des solutions INS-compatibles, c'est-à-dire capables de gérer cette identité. Pour cela, ils doivent suivre le référentiel mis à disposition par l'ANS qui décrit les conditions et modalités d'utilisation de l'INS [46]. Ce référentiel se décline en 2 documents :

- Le référentiel national d'identitovigilance (RNIV) à destination des professionnels et établissements intervenant dans la prise en charge sanitaire ou médico-social, découpé en un volet commun à l'ensemble des secteurs et en trois volets spécifiques (établissements de santé, structures non hospitalières, acteurs libéraux). Il vient fixer les exigences et recommandations en termes d'identification des usagers avec, par exemple, la nécessité de valider au moins une fois l'identité du patient à l'aide d'une pièce d'identité à haut niveau de confiance (passeport, carte d'identité française, etc.).
- Le guide d'implémentation à destination des éditeurs de logiciels, qui spécifie les modalités d'appels au téléservice INSi (Identifiant National de Santé intégré) et les modalités de référencement des données de santé avec l'INS. Ce guide permet aux éditeurs d'intégrer l'INS à leur logiciel déjà existant ou lors du développement d'une nouvelle solution [47].

Selon le référentiel, afin d'intégrer l'INS à leurs solutions les fournisseurs de logiciels doivent :

- Intégrer le téléservice INSi : faire appel à ce service à partir des solutions permet d'obtenir ou de vérifier l'INS d'une personne grâce aux bases de référence de l'état civil.
- Implémenter l'INS dans les logiciels : les solutions doivent permettre de gérer l'identité selon les bonnes pratiques d'identitovigilance.
- Pouvoir diffuser l'INS : les solutions doivent être capables de recevoir et véhiculer l'INS dans tous les flux informatisés en respectant les standards d'interopérabilité en vigueur.

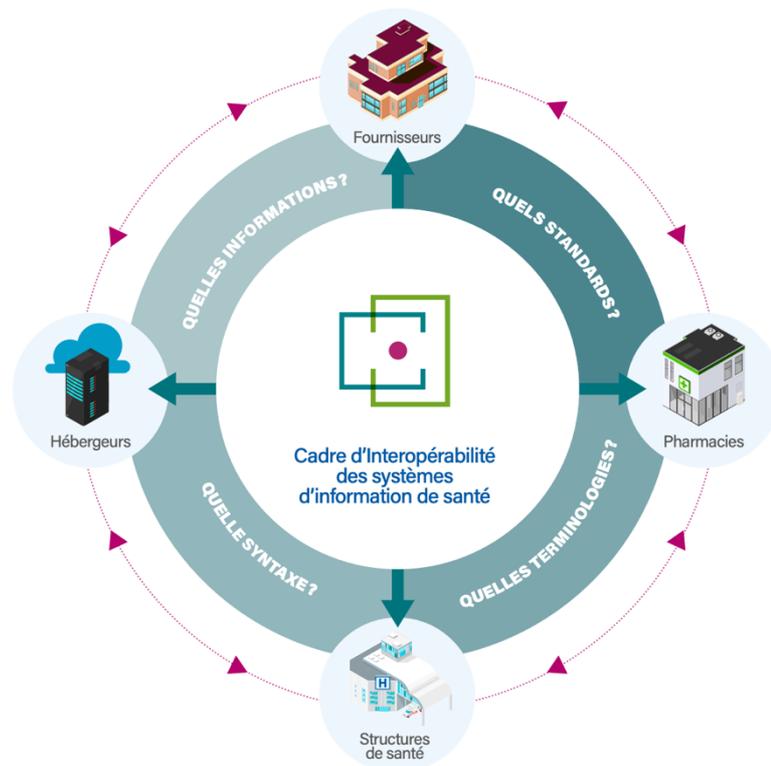
Cette notion d'interopérabilité est essentielle et fait partie des missions de l'ANS. La PGSSI-S et les conditions d'hébergement des données de santé permettent de créer un environnement sécurisé par la mise en œuvre de règles et de bonnes pratiques. Une fois les données de santé sécurisées, leur échange et leur partage entre les différents professionnels de santé doit pouvoir se faire de manière simple. Pour que cette communication soit possible, il faut que tous les acteurs et surtout, tous leurs systèmes d'informations parlent le même langage.

## **2.2 Le cadre d'interopérabilité des systèmes d'information de santé (CI-SIS)**

### 2.2.1 Pourquoi l'interopérabilité en santé est-elle importante ?

L'interopérabilité est la capacité d'un système d'information à communiquer avec d'autres systèmes d'information, même s'ils ont été développés par des fabricants différents, sans multiplier les efforts de développements. Elle est garante de l'échange et du partage d'informations entre deux systèmes n'ayant pas forcément la même finalité. L'interopérabilité est le « langage commun » pour produire et exploiter les données de santé échangées [27]. Dans le domaine de la e-santé, la faculté d'échanger des données est fondamentale, puisqu'elle conditionne la bonne coordination des soins et le suivi des patients. Devoir ressaisir une donnée à la main, ne pas pouvoir faire de statistiques car les données sont "non-structurées", ne pas pouvoir connecter son logiciel de prise de rendez-vous en ligne à son logiciel métier, devoir payer pour de nouvelles interfaces... Ces différents cas peuvent être rencontrés régulièrement par les professionnels de santé et illustrent le manque d'interopérabilité dans notre système d'information en santé. Ces insuffisances en matière d'interopérabilité constituent un frein à la bonne utilisation des logiciels, et par conséquent un parcours de soin moins efficient pour le patient.

En effet, tous les professionnels n'utilisent pas les mêmes logiciels et il existe de nombreuses variantes suivant le fournisseur. Pour suivre un patient correctement, les données de tous ces logiciels doivent pouvoir être mises en commun. Prenons l'exemple d'un médecin recevant de nouveaux résultats d'analyses biologiques d'un patient par voie numérique. Sans l'interopérabilité, pour avoir une courbe d'évolution du cholestérol, le médecin doit pointer à la main les différentes données sur l'ensemble des comptes rendus dont il dispose pour ses patients. La structuration apportée par l'interopérabilité permettrait à son logiciel métier de produire automatiquement ce type de courbe d'historique.



**Figure 15 : Cadre d'Interopérabilité des systèmes d'information de santé**

Source : Pourquoi la France se dote-t-elle d'un cadre d'interopérabilité en santé ? - ASIP Santé

L'interopérabilité s'appuie sur des standards ou des normes adoptés d'une manière consensuelle. Elle peut être appréhendée suivant de multiples points de vue selon qu'on l'aborde sous l'angle de l'utilisateur et du besoin métier (processus, sémantique et information échangée), ou sous l'angle des systèmes au niveau applicatif (fonctions) et/ou technique (intégration technique). Tous ces points de vue se complètent et il ne peut y avoir d'interaction entre les systèmes sans que chacun d'eux soit précisément défini ainsi que les procédures communes appliquées par l'ensemble des systèmes interagissant entre eux [48]. L'interopérabilité se divise donc en deux notions :

- L'interopérabilité « technique » c'est-à-dire l'interconnexion entre deux systèmes, s'appuyant sur l'utilisation d'interfaces définies, de normes et de protocoles partagés dans le respect des exigences de sécurité et de confidentialité des données personnelles de santé ;
- L'interopérabilité « sémantique » permet de s'assurer qu'une donnée est interprétée de la même manière dans tous les systèmes. Pour cela, l'interopérabilité sémantique s'appuie sur des vocabulaires communs, permettant de standardiser les concepts de la santé [27].

Un système sera interopérable s'il peut traiter un message sur le plan technique (le recevoir, l'enregistrer, le transférer...) mais également comprendre son contenu sur le plan sémantique pour pouvoir interpréter sa signification. Prenons l'exemple du compte-rendu de biologie médicale :

- l'interopérabilité technique permet l'échange et le partage des comptes-rendus de biologie médicale ;

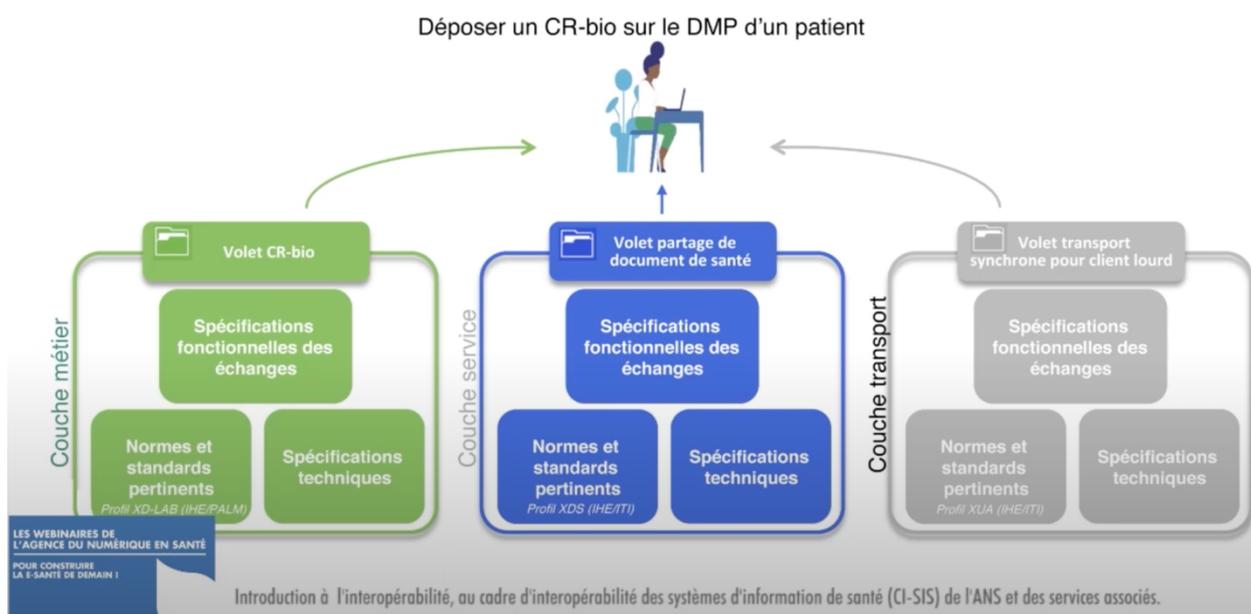
- l'interopérabilité sémantique permet aux systèmes de traiter les données de biologie (courbe, tableau, alerte...), en codant les analyses réalisées avec la terminologie LOINC (Logical Observation Identifiers Names and Codes) codant les examens de biologie médicale et leur résultats.

### 2.2.2 Le cadre d'interopérabilité mis en place par l'ANS

L'ANS a établi un cadre d'interopérabilité des systèmes d'information de santé (CI-SIS). Il contient des spécifications standards que peuvent utiliser les éditeurs pour proposer aux professionnels de santé des interfaces interopérables et donc communicantes. Ce cadre a initialement été créé en 2009 afin de favoriser le partage d'informations entre l'hôpital et la ville dans la perspective du déploiement du DMP. Il s'est ensuite étendu à d'autres champs [49].

Le CI-SIS s'appuie sur des normes et standards internationaux matures et stables. Pour l'aider à construire ce cadre d'interopérabilité, l'ANS a consulté les représentants des professionnels de santé et du médico-social ainsi que les éditeurs des systèmes d'information de santé. Le CI-SIS est constitué d'un volet de spécifications syntaxiques (structuration et format des données) et sémantiques (jeux de valeurs et terminologies de référence). Ces volets sont organisés et répartis en trois couches :

- Couche Métier, dont les volets spécifient les contenus métiers échangeables afin de classer ensemble les différents types d'informations médicales, par exemple volet compte rendu de rétinographie, volet vaccination, volet compte rendu d'anesthésie, etc.;
- Couche Service, pour définir les modalités d'échanges et de partage pour communiquer les contenus avec efficacité et en toute sécurité (volet partage de documents de santé, volet gestion d'agendas partagés, etc.);
- Couche Transport, dont les volets spécifient les moyens de transport de l'information.



**Figure 16 : Exemple d'articulation des volets du CI-SIS**

Source : Webinaire ANS | Introduction à l'interopérabilité, au CI-SIS de l'ANS et des services associés

Prenons l'exemple d'un dépôt de compte rendu de biologie médicale sur le DMP du patient. Cette action va faire intervenir un volet de chaque couche :

- Couche transport : le volet "*transport synchrone pour client lourd*" qui va spécifier techniquement comment se connecter au DMP et comment coder l'insertion en fournissant les éléments d'identité de l'utilisateur ;
- Couche service : volet "*partage de document de santé*" qui précise comment déposer le document sur le DMP ;
- Couche métier : volet "*compte rendu de biologie*" qui décrit comment exprimer de manière technique et universelle les différents résultats présentés dans le compte rendu.

L'utilisation prioritaire de normes internationales du domaine sanitaire dans le CI-SIS est l'occasion pour les éditeurs utilisant ce référentiel, de proposer des produits compatibles avec les autres systèmes appliquant également le CI-SIS. Pour le professionnel de santé, la mise en place de ces cadres devrait lui permettre de disposer, à terme, d'un environnement et de systèmes performants, à moindre coût et de meilleure qualité dans lequel il peut avoir confiance au quotidien.

Afin d'aider les industriels dans la mise en conformité de leur solution et les guider dans les différents parcours (PGSSI-s, hébergement des données et INS) l'ANS et la délégation ministérielle au numérique en santé (DNS) ont mis en place la plateforme G-NIUS : guichet national de l'innovation du numérique en santé. La plateforme aide à décrypter les réglementations grâce à des contenus pratiques et des mises en relation avec les acteurs clés de la e-santé. Elle propose des parcours guidés sur tous les thèmes réglementaires abordés précédemment. Elle permet également d'identifier les financements dont une solution logicielle peut bénéficier.

En effet, l'État a mis en œuvre un programme de financement destiné à encourager l'équipement numérique des acteurs de l'offre de soins en solutions logicielles respectant les exigences techniques et fonctionnelles précédemment développées : le Ségur du Numérique en santé. Ce dispositif prend la forme, à travers un système de référencement et de financement, d'un mécanisme d'achat pour compte au bénéfice des acteurs de l'offre de soins : établissements de santé, professionnels de santé, et établissements et services médico-sociaux. Il permet de prendre en charge financièrement la prestation de passage à une solution disposant d'un référencement Ségur. Ce financement est versé aux fournisseurs éligibles, car distribuant des solutions logicielles référencées Ségur par l'ANS, en contrepartie de la réalisation des prestations de mise à jour logicielle réalisées auprès de leurs clients [50]. C'est ainsi 2 milliards d'euros d'investissements qui seront consacrés au numérique en santé. Les éditeurs devront se conformer au référentiel d'exigences minimales recensant les exigences techniques et fonctionnelles qui doivent être satisfaites pour qu'un logiciel soit éligible au référencement et fournir les preuves associées à chaque exigence. Ce programme favorise donc l'accélération du déploiement de la feuille de route du

numérique en santé en exigeant la conformité aux volets du CI-SIS, l'implémentation de l'INS ou encore l'identification électronique des professionnels de santé via Pro Santé Connect. Pour les industriels, il leur permet de mettre en avant leurs solutions en figurant dans la liste des services référencés sur le site de l'ANS et également d'être plus attractif pour leurs clients grâce au financement à l'équipement.

Ces référentiels socles et documents de référence établis par l'ANS ont donc pour objectif de créer un écosystème sécurisé autour du partage et du stockage des données de santé. Le rôle des industriels est d'intégrer ces moyens techniques dans leurs solutions afin d'être conforme réglementairement. La prise en compte de ces différentes exigences sera détaillée à travers un exemple dans la troisième partie de ce travail.

### **III. Illustration du positionnement réglementaire : exemples de logiciels et applications**

Avec des fonctionnalités de plus en plus étendues, la question du statut de ces logiciels est un point à étudier de près par les fabricants. Comme développé précédemment, tous les logiciels et applications utilisés dans le champ de la santé ne relèvent pas nécessairement du statut de DM ou de DMDIV. La qualification d'une solution logicielle ou d'une application est un exercice indispensable qui doit être réalisé aux prémices d'un projet. Cette analyse réglementaire doit se faire au cas par cas en suivant la démarche du MDCG 2019-11 décrite dans la première partie de ce travail. Voyons comment appliquer cette démarche de qualification à travers plusieurs exemples.

#### **1. Exemples de qualification de logiciels selon la méthodologie du MDCG 2019-11**

##### **1.1. Algorithme de prédisposition au syndrome de Down**

Le MDCG 2019-11 présente dans son ANNEXE II [8] quelques exemples de qualification de logiciels. L'un d'eux est l'exemple d'un algorithme destiné à fournir des informations statistiques sur la prédisposition au syndrome de Down (trisomie 21) au cours du premier et du deuxième trimestre de la grossesse. Le logiciel analyse les données d'entrée qui sont le dosage de marqueurs sériques obtenus après une prise de sang et la mesure de la clarté nucale lors d'une échographie. L'algorithme fournit ensuite aux cliniciens ou obstétriciens un score de risque représentant la probabilité que le fœtus soit porteur de trisomie 21. Selon le score de risque obtenu, le logiciel suggère si des tests supplémentaires sont nécessaires ou non pour confirmer les mutations génétiques. Prenons les différentes étapes du logigramme et appliquons-les à ce logiciel :

- Étape 1 : Le produit est-il un « logiciel » selon la définition du MDCG 2019-11 ?

Pour rappel, la définition d'un logiciel donnée dans le MDCG 2019-11 est “*un ensemble d'instructions qui traite les données d'entrée et crée des données de sortie*”. Ici, les données d'entrée sont le dosage de marqueurs sériques et la mesure de la clarté nucale et la donnée de sortie est le score de risque.

Réponse : oui.

- Étape 2 : Est-ce un logiciel au sens du « MDR Annex XVI device », un accessoire pour un dispositif médical conformément à l'Art 2(2) du MDR ou de l'IVDR ou un « logiciel conduisant ou influençant l'utilisation d'un dispositif médical (hardware) » ?

Le logiciel n'entre dans aucune des catégories présentées.

Réponse : non.

- Étape 3 : Le logiciel effectue-t-il une action sur les données autre que le stockage, l'archivage, la communication, une simple recherche ou une compression ?

Ici, le logiciel calcule un score de risque à partir des données d'entrée, il effectue une action qui n'est pas seulement un stockage, une communication ou une simple recherche d'informations. Réponse : oui.

- Étape 4 : L'action est-elle au bénéfice de patients individuels ?

Le risque de score obtenu est un résultat propre au bénéfice d'un seul patient.

Réponse : oui.

- Étape 5 : Est-ce que la finalité de cette action est médicale au sens de l'article 2(1) des Règlements UE 2017/745 ou UE 2017/746 ?

Le logiciel a une “*finalité de diagnostic*” selon le MDR et il “*fournit des informations concernant la prédisposition à une affection ou à une maladie*” selon l'IVDR.

Réponse : oui.

Enfin, pour déterminer sa qualification en DM ou DMDIV, il faudra s'intéresser à la source des données traitées par le logiciel. Les données jugées déterminantes pour le calcul du score de risque sont celles des marqueurs sériques et sont obtenues depuis un dispositif médical de diagnostic *in vitro*. Les données reçues par le logiciel provenant d'un DMDIV, le logiciel sera donc classé selon le Règlement UE 2017/746 IVDR.

Après avoir déterminé à quel règlement répond le logiciel, il faut se référer aux règles de classifications pour déterminer sa classe. Ici, le logiciel sera classé selon la règle 3.1) de l'Annexe VIII de l'IVDR car

il est destiné “au dépistage de troubles congénitaux chez l'embryon ou le fœtus”. Le logiciel relèvera alors de la classe C.

## 1.2. Logiciel d'analyse d'images uPath HER2

Développé par Roche Diagnostic France, le logiciel uPath enterprise software est une solution de pathologie basée sur une interface web pour la visualisation, la gestion et le partage de lames de verre numériques. Il est compatible avec les scanners à lames et permet la communication avec les algorithmes logiciels de scores de coloration et d'interprétation développés par Roche [51]. Une des solutions d'analyse algorithmique d'images disponible sur uPath permet d'assister le médecin dans l'évaluation et le suivi des patientes atteintes du cancer du sein. Cette solution permet l'évaluation semi quantitative de la protéine HER2 présente dans un tissu mammaire fixé dans le formol et inclus en paraffine. L'image de la lame est analysée par l'algorithme avant l'évaluation par le médecin pathologiste et permet d'obtenir un calcul rapide du score HER2. Le logiciel offre aussi une possibilité de visualisation superposée nette grâce à une mise en surbrillance de la membrane colorée positive pour une visualisation facile. Lorsque le médecin a terminé l'étude d'un cas, le logiciel lui permet de générer un rapport officiel, sous forme de PDF, contenant un récapitulatif des résultats. Il offre également une vue globale des cas patients ainsi qu'une collaboration facile grâce à l'option de gestion et de partage de ces cas entre médecins [52]. Suivons les étapes décrites dans le MDCG 2019-11 pour ce logiciel :

- Étape 1 : Le produit est-il un « logiciel » selon la définition du MDCG 2019-11 ?

Le logiciel uPath crée une donnée de sortie, le calcul du score HER2, à partir de la donnée d'entrée qui est l'image de la lame de tissu.

Réponse : oui.

- Étape 2 : Est-ce un logiciel au sens du « MDR Annex XVI device », un accessoire pour un dispositif médical conformément à l'Art 2(2) du MDR ou de l'IVDR ou un « logiciel conduisant ou influençant l'utilisation d'un dispositif médical (hardware) » ?

uPath HER2 n'entre dans aucune de ces catégories.

Réponse : non.

- Étape 3 : Le logiciel effectue-t-il une action sur les données autre que le stockage, l'archivage, la communication, une simple recherche ou une compression ?

Les actions effectuées par uPath HER2 ne sont ni un simple stockage, ni une communication ou une simple recherche d'informations.

Réponse : oui.

- Étape 4 : L'action est-elle au bénéfice de patients individuels ?

L'analyse algorithmique du tissu et donc le résultat est propre au bénéfice d'un seul patient.

Réponse : oui.

- Étape 5 : Est que la finalité de cette action est médicale au sens de l'article 2(1) des Règlements UE 2017/745 ou UE 2017/746 ?

Le logiciel permet de fournir des informations sur l'état pathologique des patientes à partir d'un échantillon provenant du corps humain, ici l'analyse du tissu mammaire. Celui-ci a donc une finalité de diagnostic au sens du Règlement UE 2017/746 et sera donc qualifié de DMDIV.

Ce logiciel suit la règle de classification numéro 3.h) de l'Annexe VIII du règlement IVDR et relève de la classe C car il est destiné "à être utilisé dans le dépistage ou le diagnostic du cancer".

### 1.3. Le cas des Middlewares

Il s'agit de solutions destinées au dialogue et à l'échange entre les automates et le système d'information des laboratoires (SIL). Ce sont des logiciels positionnés de manière stratégique qui apportent des fonctionnalités qui ne sont pas traditionnellement supportés par les SIL. Leur but est d'optimiser tout ou partie des processus de laboratoire (production, traçabilité, validation...). Appliquons les étapes de l'arbre décisionnel à un middleware :

- Étape 1 : Le produit est-il un « logiciel » selon la définition du MDCG 2019-11 ?

Un middleware entre bien dans la définition suivante "*un ensemble d'instructions qui traite les données d'entrée et crée des données de sortie*". Le logiciel reçoit des données d'entrée depuis le SIL comme par exemple les informations liées au patient, aux tubes analysés, des règles de routage etc. et il transmet des données de sortie : résultats d'analyses, traçabilité des tubes, suivi de l'activité etc.

Réponse : oui.

- Étape 2 : Est-ce un logiciel au sens du « MDR Annex XVI device », un accessoire pour un dispositif médical conformément à l'Art 2(2) du MDR ou de l'IVDR ou un « logiciel conduisant ou influençant l'utilisation d'un dispositif médical (hardware) » ?

Les middlewares n'entrent dans aucune de ces catégories.

Réponse : non.

- Étape 3 : Le logiciel effectue-t-il une action sur les données autre que le stockage, l'archivage, la communication, une simple recherche ou une compression ?

Le middleware n'exploite et n'analyse pas les données qui lui sont transmises. Il sert de point d'échange entre les automates et le SIL pour transmettre les données sans avoir lui-même une finalité médicale. Pour être qualifié de DM ou DMDIV, un logiciel doit permettre, un diagnostic, une aide au diagnostic, un traitement ou une aide au traitement. Il doit fournir une information médicale nouvelle contribuant au diagnostic ou au traitement du patient. L'analyse par l'arbre décisionnel s'arrête à cette étape pour les middlewares et ceux-ci ne seront donc pas qualifiés de DM ni de DMDIV.

## **2. Exigences à prendre en compte pour la mise sur le marché français d'une solution logicielle**

### **2.1. Diagnostic réglementaire**

Voyons maintenant la démarche à suivre afin d'identifier les sujets réglementaires mis en place par l'ANS et opposables auxquels peut être soumis un service ou un produit logiciel.

Dans un premier temps, il faut définir dans quel cadre s'inscrit le service numérique : dans le champ de la santé ou dans le champ du loisir et du bien-être ? En fonction de la typologie des données utilisées, collectées et traitées, cela déterminera quel cadre appliquer. Comme développé précédemment, le fait de traiter des données de santé à caractère personnel est précisément encadré afin de sécuriser l'accès à ces données et garantir leur confidentialité. Le fabricant devra donc se conformer au RGPD ainsi qu'à la mise en place d'un hébergement sécurisé conforme au référentiel HDS. En revanche, si le logiciel développé entre dans le champ du loisir et du bien-être alors le fabricant ne sera pas concerné par la réglementation qui régit le traitement des données de santé.

Le deuxième point à prendre en compte est : qui accède aux données de santé personnelle du logiciel ? Est-ce uniquement l'utilisateur ? Ou bien un ensemble de professionnels de santé a également accès à ces données ? Il convient de distinguer si l'utilisateur, et donc le patient, est le seul à accéder aux données de santé qu'il saisit dans le produit ou le service, ou si des tiers peuvent également y accéder. Si les données sont amenées à être consultées par des professionnels de santé, le fabricant devra mettre en place un dispositif d'authentification forte garantissant l'identité des professionnels. Il doit pour cela prendre connaissance des différents référentiels d'identification établis par l'ANS et plus particulièrement celui qui concerne l'identification électronique des acteurs des secteurs sanitaires, médico-social et social (le référentiel personne physique). Comme détaillé précédemment, le référentiel présente une liste d'exigences minimales à respecter pour garantir une identification sécurisée des professionnels de santé. Si la solution logicielle propose également un accès pour le patient, il faudra prendre en compte le volet identification électronique des usagers et appliquer les différentes exigences relatives à leur identification.

Le fait de traiter des données de santé personnelles et de contribuer aux actions de prise en charge d'un patient nécessite que celui-ci puisse être identifié sans ambiguïté. Dans ce cas, la solution logicielle sera concernée par l'intégration et l'utilisation de l'INS.

Enfin, si le service doit envoyer ou recevoir des données provenant d'autres services numériques, à vocation à s'intégrer dans les outils métier existant des professionnels de santé ou encore est une étape dans un parcours de santé alors celui-ci doit être interopérable afin de pouvoir communiquer avec d'autres outils numériques.

## **2.2. Exemple illustratif : solution de prescription connectée à domicile**

Roche Diagnostics France et la start-up normande Deigma ont conçu ensemble une plateforme numérique interopérable, associée à une application mobile, qui permet de moderniser la prise en charge des prélèvements biologiques réalisés par les Infirmier Diplômé d'État (IDE) à l'extérieur des laboratoires, au domicile des patients par exemple.

Habituellement, les laboratoires de biologie médicale doivent attendre d'avoir reçus les prélèvements pour les enregistrer dans leur système d'information, et cela provoque des pics d'activité intense. Avec cette solution, les informations relatives au prélèvement (date, identité du préleveur, identité du patient, liste des examens depuis la photo de l'ordonnance...) sont digitalisées par l'IDE et transmises automatiquement et en temps réel aux laboratoires et à leur middleware [53]. Cela simplifie ainsi la tâche des IDE qui n'ont plus à renseigner ces informations à la main, et allège significativement la charge administrative du secrétariat des laboratoires. Cela permet également de réduire le délai pré-analytique ainsi que le risque d'erreur humaine, de renforcer la fiabilité des informations transmises et une meilleure traçabilité des prélèvements. L'utilisation se fait en plusieurs étapes :

1/ L'IDE scanne un QR code sur le sachet ou la boîte du prélèvement avec son application mobile pour horodater le prélèvement et s'identifier comme préleveur.

2/ L'IDE associe au dossier l'identité du patient en scannant un QR code.

3/ L'IDE peut compléter le dossier avec différents éléments : photo de l'ordonnance, mutuelle, code-barre du tube, informations cliniques du prélèvement... Le logiciel détecte automatiquement les examens réalisés depuis la photo de l'ordonnance.

4/ Toutes ces informations sont ensuite automatiquement intégrées dans le SIL. La prescription est créée alors que les prélèvements sont toujours au domicile du patient.

Appliquons le diagnostic réglementaire à la solution Deigma :

- Celle-ci traite des données de santé à caractère personnel : toutes les informations relatives au prélèvement. L'hébergement de l'application permettant la numérisation de ces données doit donc être fait sur un serveur habilité, c'est-à-dire certifié HDS.
- L'IDE est un professionnel de santé et doit s'identifier comme préleveur sur l'application. Celle-ci doit donc bénéficier d'un système d'identification conforme au référentiel d'identification électronique des personnes physiques.
- L'application contribue aux actions de prise en charge dans le parcours de soin du patient, il est donc nécessaire d'intégrer et d'utiliser l'INS pour pouvoir identifier de manière sûre le bon patient et communiquer ses informations entre les membres de l'équipe de soin. Ici, l'application est capable d'associer l'identité du patient au dossier en scannant l'INS sous forme de QR code présent sur la prescription.
- Enfin, des échanges de données étant faits avec d'autres systèmes d'information, l'application doit être interopérable. Cela permet par exemple, l'intégration automatique dans le SIL de toutes les informations transmises depuis l'application.

## Conclusion

La santé est aujourd'hui l'une des industries les plus transformatrices mais aussi l'une des plus exigeantes. La part du numérique ne cesse de croître dans ce secteur et, grâce à ses avancées, le patient devient progressivement acteur de sa santé et peut aujourd'hui vérifier par lui-même son état grâce à des dispositifs connectés à des applications ou rendant eux même des résultats. La médecine personnalisée devient un nouveau modèle pour les industries pharmaceutiques dans lequel la e-santé prend tout son sens. Le numérique a également envahi le quotidien des professionnels de santé. Que ce soit dans les cabinets des médecins, les pharmacies, les laboratoires de biologie ou encore à l'hôpital, l'informatique se manifeste à tous les niveaux.

Cependant, un tel marché en pleine expansion nécessite la mise en place d'un cadre réglementaire clair et défini. Cyberattaques, fuites de données et systèmes incompatibles ne sont que quelques exemples de situations préjudiciables qui ont conduit à des adaptations réglementaires. Nous avons pu voir au travers de cette thèse qu'au niveau européen, les logiciels sont maintenant pris en compte dans les règlements relatifs aux DM et DMDIV. Des guides et normes spécifiques sont établis afin d'accompagner les acteurs dans la mise en conformité de leurs solutions. La France dispose désormais d'une doctrine du numérique permettant aux acteurs d'avoir un document de référence définissant une vision stable et détaillée du cadre de la e-santé.

La compréhension et la mise en application de ces réglementations est essentielle pour les industriels afin de mettre sur le marché des solutions conformes. Cependant, la prise en compte des réglementations va plus loin que le simple fait d'avoir une solution qui respecte les exigences demandées. En effet, l'enjeu est également commercial et concurrentiel : les industriels qui intègrent dans leurs projets les points réglementaires auront un avantage sur le marché. Leurs solutions seront choisies de préférence par les clients. D'autant plus que l'État met en avant les solutions conformes en publiant par exemple sur son site internet l'utilisation effective du téléservice INSi ou encore en tenant à jour la liste des hébergeurs certifiés HDS. De plus, l'Etat lance la prise en charge anticipée des dispositifs médicaux numériques. Le décret du 30 mars 2023 en précise les modalités et permet dès maintenant aux éditeurs de déposer leur candidature. Ce parcours permet d'accélérer l'obtention d'un remboursement par l'Assurance Maladie pour certaines solutions numériques de santé dites matures, c'est à dire bénéficier d'un marquage CE conformément aux règlements 2017/745 ou 2017/746 et respecter les exigences des référentiels opposables de l'ANS.

Les entreprises spécialisées ou se lançant dans les dispositifs médicaux, en particulier dans le numérique, rencontrent de nombreux challenges. Au-delà de la recherche et développement, la première marche à

franchir concerne l'approche qualité et réglementaire. Il est essentiel de construire une stratégie réglementaire dès les premiers stades de développement du produit, en accord avec les objectifs de son entreprise. Le réglementaire peut être utilisé comme un guide complet et efficace pour mettre sur le marché un dispositif médical sûr et performant pour les usagers, et ne doit pas être vu, uniquement, comme une contrainte.

## Références

- [1] S. Price, « Global digital healthcare market to surpass \$234.5bn by 2023 », *Health Europa*, 11 octobre 2019. <https://www.healtheuropa.com/digital-healthcare-market-234-5bn-2023/94032/> (consulté le 8 janvier 2023).
- [2] « E-santé: 1,79 milliard d'euros levés en France en 2022, trois fois plus qu'en 2021 (Karista) - TICpharma ». <https://www.ticpharma.com/story?ID=2223&story=2223> (consulté le 30 avril 2023).
- [3] F. Barbabella, M. G. Melchiorre, S. Quattrini, R. Papa, et G. Lamura, « How can eHealth improve care for people with multimorbidity in Europe? ».
- [4] N. Vollmer, « Article 9 EU règlement général sur la protection des données (EU-RGPD) », 22 août 2022. <https://www.privacy-regulation.eu/fr/9.htm> (consulté le 8 janvier 2023).
- [5] « RÈGLEMENT (UE) 2017/ 745 DU PARLEMENT EUROPÉEN ET DU CONSEIL - du 5 avril 2017 - relatif aux dispositifs médicaux, modifiant la directive 2001/ 83/ CE, le règlement (CE) no 178/ 2002 et le règlement (CE) no 1223/ 2009 et abrogeant les directives du Conseil 90/ 385/ CEE et 93/ 42/ CEE ».
- [6] « RÈGLEMENT (UE) 2017/ 746 DU PARLEMENT EUROPÉEN ET DU CONSEIL - du 5 avril 2017 - relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/ 79/ CE et la décision 2010/ 227/ UE de la Commission ».
- [7] A. S. R. S. Rao et J. A. Vazquez, « Identification of COVID-19 can be quicker through artificial intelligence framework using a mobile phone-based survey when cities and towns are under quarantine », *Infection Control & Hospital Epidemiology*, vol. 41, n° 7, p. 826-830, juill. 2020, doi: 10.1017/ice.2020.61.
- [8] « MDCG 2019-11 : Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR ». Consulté le: 8 janvier 2023. [En ligne]. Disponible sur: [https://health.ec.europa.eu/system/files/2020-09/mdc\\_mdgc\\_2019\\_11\\_guidance\\_qualification\\_classification\\_software\\_en\\_0.pdf](https://health.ec.europa.eu/system/files/2020-09/mdc_mdgc_2019_11_guidance_qualification_classification_software_en_0.pdf)
- [9] « Le logiciel ou l'application santé que je vais mettre sur le marché relève-t-il du statut de dispositif médical (DM) ou de dispositif médical de diagnostic in vitro (DM DIV)? », *ANSM*. <https://ansm.sante.fr/documents/referance/le-logiciel-ou-lapplication-sante-que-je-vais-mettre-sur-le-marche-releve-t-il-du-statut-de-dispositif-medical-dm-ou-de-dispositif-medical-de-diagnostic-in-vitro-dm-div> (consulté le 30 avril 2023).
- [10] « 2014 - Software as a Medical Device Possible Framework.pdf ». Consulté le: 11 février 2023. [En ligne]. Disponible sur: <https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf>
- [11] « entreprise europe network - Nouveau guide sur les dispositifs médicaux ». Consulté le: 1 mai 2023. [En ligne]. Disponible sur: [https://www.entreprise-europe-sudouest.fr/ckfinder/userfiles/public/03%20FAQ%20%E2%80%93%20FICHES%20TECHNIQUES%20%E2%80%93%20GUIDES/FICHES%20-%20FAQ%20-%20GUIDES/Nouveau%20guide%20sur%20les%20dispositifs%20m%C3%A9dicaux\\_25%20janvier%202021\\_FR.pdf](https://www.entreprise-europe-sudouest.fr/ckfinder/userfiles/public/03%20FAQ%20%E2%80%93%20FICHES%20TECHNIQUES%20%E2%80%93%20GUIDES/FICHES%20-%20FAQ%20-%20GUIDES/Nouveau%20guide%20sur%20les%20dispositifs%20m%C3%A9dicaux_25%20janvier%202021_FR.pdf)
- [12] « Mon logiciel est-il un dispositif médical en vertu du règlement européen ? », *DeviceMed.fr*, 21 juin 2021. <https://www.devicemed.fr/dossiers/reglementation/mon-logiciel-est-il-un-dispositif-medical-en-vertu-du-reglement-europeen/27626> (consulté le 12 février 2023).

- [13] « Je qualifie mon logiciel ou mon application de DM ou DMDIV, quelles sont les conséquences et la marche à suivre pour commercialiser mon produit ? - ANSM ». <https://ansm.sante.fr/documents/referance/je-qualifie-mon-logiciel-ou-mon-application-de-dm-ou-dmdiv-quelles-sont-les-consequences-et-la-marche-a-suivre-pour-commercialiser-mon-produit> (consulté le 13 février 2023).
- [14] « Règlement (UE) no 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision no 1673/2006/CE du Parlement européen et du Conseil Texte présentant de l'intérêt pour l'EEE ».
- [15] « Manufacturers Use Harmonized Standards ». <https://www.johner-institute.com/index.php?id=96> (consulté le 20 février 2023).
- [16] 14:00-17:00, « IEC 62304:2006 - Logiciels de dispositifs médicaux - Processus du cycle de vie du logiciel », *ISO*. <https://www.iso.org/fr/standard/38421.html> (consulté le 22 février 2023).
- [17] L. Keutzer et U. S. Simonsson, « Medical Device Apps: An Introduction to Regulatory Affairs for Developers », *JMIR mHealth and uHealth*, vol. 8, n° 6, p. e17567, juin 2020, doi: 10.2196/17567.
- [18] M. Navarro, « Qu'est-ce que la norme EN ISO 14971 ? », *mauricenavarro.com*. <https://www.mauricenavarro.com/articles/qu-est-ce-que-la-norme-en-iso-14971/> (consulté le 24 février 2023).
- [19] « MDCG 2020-1 : Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software ». Consulté le: 26 février 2023. [En ligne]. Disponible sur: [https://health.ec.europa.eu/system/files/2020-09/md\\_mdcg\\_2020\\_1\\_guidance\\_clinic\\_eva\\_md\\_software\\_en\\_0.pdf](https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2020_1_guidance_clinic_eva_md_software_en_0.pdf)
- [20] « L'ANS au cœur de la transformation numérique en santé », *esante.gouv.fr*. <http://esante.gouv.fr/lagence> (consulté le 6 mars 2023).
- [21] « WHO EMRO | eHealth | Health topics », *World Health Organization - Regional Office for the Eastern Mediterranean*. <http://www.emro.who.int/health-topics/ehealth/> (consulté le 6 mars 2023).
- [22] « Ce que la e-santé fait pour vous », *esante.gouv.fr*. <http://esante.gouv.fr/ce-que-la-e-sante-fait-pour-vous> (consulté le 6 mars 2023).
- [23] « Avec la télémédecine, une prise en charge rapide de vos patients », *Haute Autorité de Santé*. [https://www.has-sante.fr/jcms/p\\_3106483/fr/avec-la-telemedecine-une-prise-en-charge-rapide-de-vos-patients](https://www.has-sante.fr/jcms/p_3106483/fr/avec-la-telemedecine-une-prise-en-charge-rapide-de-vos-patients) (consulté le 7 mars 2023).
- [24] « Stratégie nationale », *esante.gouv.fr*. <http://esante.gouv.fr/strategie-nationale> (consulté le 7 mars 2023).
- [25] « Feuille de route stratégique du numérique en santé ». Consulté le: 7 mars 2023. [En ligne]. Disponible sur: [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/Dossier\\_virage\\_numerique\\_masante2022.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/Dossier_virage_numerique_masante2022.pdf)
- [26] « Charte engagé pour la e santé-12-01-22.pdf ». Consulté le: 8 mars 2023. [En ligne]. Disponible sur: [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/Charte%20engage%CC%81%20pour%20la%20e%20sante%CC%81-12-01-22.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/Charte%20engage%CC%81%20pour%20la%20e%20sante%CC%81-12-01-22.pdf)

- [27] « Doctrine du numérique en santé ». Consulté le: 8 mars 2023. [En ligne]. Disponible sur: [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/doctrine-du-numerique-en-sante\\_version-2022\\_vf.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/doctrine-du-numerique-en-sante_version-2022_vf.pdf)
- [28] « Sujets de réglementation (page 2/2) | G\_NIUS ». <https://gni.us.esante.gouv.fr/fr/reglementation/fiches-reglementation?title=&page=1> (consulté le 1 mai 2023).
- [29] « Nos offres de produits et services pour les industriels | Portail Industriels ». <https://industriels.esante.gouv.fr/nos-offres-de-produits-et-services-pour-les-industriels> (consulté le 12 mars 2023).
- [30] « Qu'est-ce qu'une donnée de santé ? | CNIL ». <https://www.cnil.fr/fr/quest-ce-que-une-donnee-de-sante> (consulté le 12 mars 2023).
- [31] « RÈGLEMENT (UE) 2016/ 679 DU PARLEMENT EUROPÉEN ET DU CONSEIL - du 27 avril 2016 - relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/ 46/ CE (règlement général sur la protection des données) ».
- [32] *Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel*. 2018.
- [33] « Article L1111-8 - Code de la santé publique - Légifrance ». [https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI000033862549](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033862549) (consulté le 12 mars 2023).
- [34] « Liste des hébergeurs certifiés », *esante.gouv.fr*. <http://esante.gouv.fr/offres-services/hds/liste-des-herbergeurs-certifies> (consulté le 12 mars 2023).
- [35] « HDS », *Agence du Numérique en Santé*. <http://esante.gouv.fr/produits-services/hds> (consulté le 1 mai 2023).
- [36] « Huge Cloud Market Still Growing at 34% Per Year; Amazon, Microsoft & Google Now Account for 65% of the Total | Synergy Research Group ». <https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues> (consulté le 15 mars 2023).
- [37] « Stéphanie Combes dévoile le programme de rentrée du Health Data Hub ». <https://www.ticpharma.com/story/2044/stephanie-combes-devoile-le-programme-de-rentree-du-health-data-hub.html> (consulté le 15 mars 2023).
- [38] « Arrêté du 28 mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé - Légifrance ». <https://www.legifrance.gouv.fr/jorf/id/JORFARTI000045457994#JORFARTI000045457994> (consulté le 28 mars 2023).
- [39] « Règlement européen « eIDAS » n°910/2014 du 23 juillet 2014 ». Consulté le: 30 mars 2023. [En ligne]. Disponible sur: <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR>
- [40] « PGSSI-S - Référentiel d'identification électronique - Acteurs des secteurs sanitaire, médico-social et social [personnes physiques] ».
- [41] 14:00-17:00, « ISO/IEC 27000:2009 », *ISO*. <https://www.iso.org/fr/standard/41933.html> (consulté le 28 mars 2023).

- [42] « PGSSI-S : Référentiel d'imputabilité v1.0 ».
- [43] « Section 4 : Conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique (Articles L1111-25 à L1111-31) - Légifrance ». [https://www.legifrance.gouv.fr/codes/section\\_lc/LEGITEXT000006072665/LEGISCTA000033861544/](https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000033861544/) (consulté le 28 mars 2023).
- [44] « Référentiel force probante des documents de santé ».
- [45] *Décret n° 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé*. 2017.
- [46] *Arrêté du 27 mai 2021 portant approbation des modifications apportées au référentiel « Identifiant national de santé »*.
- [47] « Référentiel INS », *esante.gouv.fr*. <https://esante.gouv.fr/produits-services/referentiel-ins> (consulté le 2 avril 2023).
- [48] K. Bourquard et A. Coat, « Une démarche d'élaboration de cadres d'interopérabilité ou de sécurité pour les systèmes d'information en santé », *Pratiques et Organisation des Soins*, vol. 40, n° 4, p. 283-296, 2009, doi: 10.3917/pos.404.0283.
- [49] S. Sacconi, J. Mehl, C. Lenain, F. Lofaso, et J. Taytard, « E-Santé et innovation thérapeutique », *Med Sci (Paris)*, vol. 35, p. 42-45, mars 2019, doi: 10.1051/medsci/2019052.
- [50] « Financement à l'équipement - Ségur du numérique en santé », *Agence de services et de paiement (ASP)*. <https://www.asp-public.fr/aides/segur-du-numerique-en-sante-financement-lequipement> (consulté le 30 avril 2023).
- [51] « Roche uPath entreprise software », *Diagnostics*. <https://diagnostics.roche.com/fr/fr/solutions-digitales/upath-roche-enterprise-software-diagnostics.html> (consulté le 4 avril 2023).
- [52] « uPath HER2 (4B5) image analysis », *Diagnostics*. <https://diagnostics.roche.com/fr/fr/solutions-digitales/upath-roche-enterprise-software-diagnostics/upath-her2-4b5-image-analysis.html> (consulté le 4 avril 2023).
- [53] J. Mourain, « Newsletter Spectra Diagnostic N°21 », *Spectra Diagnostic*, 1 août 2022. <https://spectradiagnostic.com/2022/08/01/newsletter-spectra-diagnostic-n21/> (consulté le 1 mai 2023).

## SERMENT DE GALIEN

*Je jure, en présence de mes maîtres de la Faculté, des conseillers de l'Ordre des pharmaciens et de mes condisciples :*

- ❖ D'honorer ceux qui m'ont instruit dans les préceptes de mon art et de leur témoigner ma reconnaissance en restant fidèle à leur enseignement.*
- ❖ D'exercer, dans l'intérêt de la santé publique, ma profession avec conscience et de respecter non seulement la législation en vigueur, mais aussi les règles de l'honneur, de la probité et du désintéressement.*
- ❖ De ne jamais oublier ma responsabilité et mes devoirs envers le malade et sa dignité humaine, de respecter le secret professionnel.*
- ❖ En aucun cas, je ne consentirai à utiliser mes connaissances et mon état pour corrompre les mœurs et favoriser des actes criminels.*

*Que les hommes m'accordent leur estime si je suis fidèle à mes promesses.*

*Que je sois couvert d'opprobre, méprisé de mes confrères, si j'y manque.*