



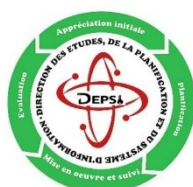
REPUBLIKAN'I MADAGASIKARA
Fihavanana - Tanindrazana - Fandrosoana
MINISTÈRE DE LA SANTÉ PUBLIQUE

POLITIQUE DE GOUVERNANCE DES DONNÉES DE SANTÉ

MADAGASCAR - MINISTÈRE DE LA SANTÉ PUBLIQUE

2024

L'élaboration du présent document a été coordonnée par le Service de l'Observatoire National de la Cybersante (SONC) auprès de la Direction des Etudes, de la Planification et du Système Information (DEPSI), avec l'appui technique et financier de Data-FI.



Ensemble pour des informations de qualité,
décisions pertinentes, résultats probants



Sponsored by the United States

Data.FI
Data for Implementation

TABLE DES MATIÈRES

TABLE DES MATIÈRES	i
SIGLES ET ABRÉVIATION	iv
GLOSSAIRE	v
PRÉFACE	vii
INTRODUCTION	1
Contexte :	1
Vision :	2
Objectif principal :	2
Portée de la politique de gouvernance des données :	2
Classification des données de santé	2
Parties prenantes et bénéficiaires de la politique	2
CADRE LÉGAL ET RÉGLEMENTAIRE EN MATIÈRE DE GOUVERNANCE DES DONNÉES DE SANTÉ	4
Cadre juridique :	4
Cadre juridique international :	4
Cadre juridique national :	4
Lois et réglementations pour la gouvernance des données de santé :	5
Politique de gouvernance des données de santé :	5
Droits des personnes et éthiques	5
Droits des personnes en matière de protection des données de santé :	5
Mise en place de mécanismes de recours efficaces en cas de violation des droits :	6
Éthiques soulevées par l'utilisation des données de santé, notamment en matière de recherche, d'intelligence artificielle et de profilage :	6
Assurer une utilisation équitable et non discriminatoire des données de santé :	6
CADRE DE GOUVERNANCE DES DONNÉES DE SANTÉ	8
Politiques, normes et directives clés en matière de gestion de données :	8
▪ Collecte des données :	8
▪ Outils de collecte et de communication des données :	8
▪ Traitement des données :	8
▪ Durée de conservation et période d'expiration :	8
▪ Archivage et partage des données :	9
▪ Utilisation des données :	9

Politiques relatives à la gestion de la qualité des données (y compris l'assurance de la qualité des données).....	9
POLITIQUE RELATIVE À L'ACCÈS, AU PARTAGE ET À LA SÉCURITÉ DES DONNÉES DE SANTÉ.....	10
Protection des données personnelles :	10
Accès et partage des données :	10
Sécurité des données :	10
POLITIQUE RELATIVE AUX INFRASTRUCTURES TECHNOLOGIQUES POUR LA GOUVERNANCE DES DONNÉES DE SANTÉ	11
Choix des solutions technologiques appropriées pour mettre en place un système d'information sanitaire national intégré :	11
Hébergement et gestion des serveurs :	11
Interopérabilité des systèmes :	11
Cybersécurité :	12
POLITIQUE RELATIVE À LA STRUCTURE ORGANISATIONNELLE DE LA GOUVERNANCE DES DONNÉES	13
Structure responsable de la gouvernance des données de santé à Madagascar :	13
Rôles et responsabilités des différents acteurs impliqués dans la gouvernance des données de santé	13
Au sein des établissements de santé	14
Professionnels de la santé et les secteurs public et privé	14
Informaticiens :	14
Au niveau institutionnel	14
Ministère de la Santé Publique :	14
Ministère du Développement Numérique :	14
Ministère de la Justice :	14
Organisme de contrôle et de suivi :	15
Au niveau des structures spécialisées.....	15
Unité de Gouvernance Digitale :	15
Commission Malagasy de l'Informatique et des Libertés :	15
Comités d'éthique de la recherche :	15
Les autres acteurs	15
Partenaires techniques et financiers :	15
Société civile, y compris les ordres professionnels de santé et les sociétés savantes :	16
Citoyens/usagers :	16
Le secteur privé :	16
Sensibilisation des professionnels de la santé et du grand public aux enjeux de la protection des données de santé :	16

Mécanismes de suivi et d'évaluation de la politique de gouvernance des données de santé :.....	16
CONCLUSION	17
RÉFÉRENCES BIBLIOGRAPHIQUES.....	18
ANNEXE I. LISTE DES CONTRIBUTEURS PAR ORDRE ALPHABÉTIQUE	19

SIGLES ET ABRÉVIATION

CHRD	Centre Hospitalier de Référence de District
CHRR	Centre Hospitalier de Référence Régionale
CHU	Centre Hospitalier Universitaire
CMIL	Commission Malagasy de l'Informatique et des Libertés
CS	Centre spécialisé
CSB	Centre de Santé de Base
DAJ	Direction des Affaires Juridiques
DEPSI	Direction des Études, de la Planification et du Système d'Information
DHRD	Direction des Hôpitaux des Régions et des Districts
DRSP	Direction Régionale de la Santé Publique
HIPAA	Health Insurance Portability and Accountability Act
IA	Intelligence artificielle
INSTAT	Institut National de la Statistique
MNDPT	Ministère du Développement numérique, des Postes et des Télécommunications
MSANP	Ministère de la Santé Publique
ONG	Organisation non gouvernementale
POS	Procédure opérationnelle standard
PSRSIS	Plan Stratégique de Renforcement du Système d'Information Sanitaire
PTF	Partenaires techniques et financiers
RGPD	Règlement Général sur la Protection des Données
SDSP	Service du District de la Santé Publique
Sida	Syndrome d'immunodéficience acquise
SIS	Système d'information sanitaire
SNSD	Stratégie Nationale en Santé Digitale
TIC	Technologies de l'information et de la communication
UGD	Unité de Gouvernance Digitale
VIH	Virus de l'immunodéficience humaine

GLOSSAIRE

Accord de non-divulgation : Contrat légal entre deux ou plusieurs parties qui s'engagent à préserver la confidentialité de certaines informations sensibles. Dans le contexte médical, ces informations peuvent inclure des données de patients, des protocoles de recherche, des formulations de médicaments ou des technologies médicales innovantes. Cet accord de non-divulgation vise à protéger ces informations confidentielles tout en permettant la collaboration nécessaire entre les professionnels de santé, les chercheurs ou les institutions médicales.

Anonymisation : Consiste à modifier le contenu ou la structure des données afin de rendre très difficile, voire impossible l'identification des personnes (physiques ou morales) ou des entités concernées.

Archivage des données : Processus de conservation des données qui ne sont plus activement utilisées, mais qui doivent être stockées de manière sécurisée pour des raisons légales, historiques ou de conformité.

La **cohérence** des données qui se rapporte à l'absence de contradictions ou d'incompatibilités internes au sein des ensembles de données. Des données cohérentes assurent une correspondance logique entre différentes parties des informations enregistrées. Les données cohérentes ne se contredisent pas et sont logiquement cohérentes.

Complétude : Degré auquel les données sont complètes et ne comportent pas de lacunes. La complétude des données mesure la présence de toutes les informations requises sans omissions. Des données complètes incluent tous les éléments nécessaires, garantissant une représentation exhaustive du sujet ou du processus concerné.

Conformité numérique : Processus par lequel une organisation s'assure que ses activités numériques respectent les lois, réglementations, et normes en vigueur, notamment en matière de protection des données et de cybersécurité. Vise à réduire les risques juridiques, à protéger les données sensibles et à maintenir la confiance des parties prenantes.

Confidentialité : Principe de protection des informations sensibles garantissant que seules les personnes autorisées puissent consulter, divulguer ou utiliser ces données, avec une divulgation ou non-divulgation de renseignements personnels fondée sur le principe selon lequel ces informations ne doivent pas être divulguées sans le consentement de la personne concernée, sauf si cela est nécessaire pour protéger cette personne ou la société.

Consentement : Conformité, approbation ou toute manifestation préalable d'une personne concernée qui a librement, sans ambiguïté et expressément déclaré ou indiqué clairement, par oral ou par écrit, ses souhaits concernant la collecte, le traitement, l'utilisation, le partage ou le stockage de ses données relatives à la santé. Le consentement est considéré comme éclairé lorsqu'une personne concernée reçoit des informations dans un format accessible et à un niveau approprié pour son éducation et sa compréhension des risques, des avantages et des utilisations prévues de ses données.

Cybercriminalité : Désigne tout acte illégal commis au moyen d'un système ou d'un réseau informatique ou de tout autre réseau physique connexe ou en relation avec un système d'information.

Disponibilité : Capacité d'un système ou d'une ressource à être accessible et opérationnel lorsque cela est requis, assurant que les utilisateurs peuvent accéder aux données et services nécessaires sans interruption.

Données de santé (également appelées données liées à la santé) : Données liées à l'état de santé général, tant physique que mental, d'un individu ou d'un groupe concerné.

Données : Éléments d'information bruts et non interprétés, pouvant se présenter sous diverses formes (textes, chiffres, images, sons, etc.), utilisés pour représenter des faits, des événements ou des concepts. Lorsqu'elles sont traitées ou analysées, elles constituent la matière première pour créer des informations et des connaissances.

Fiabilité : Toutes les données sont collectées en utilisant la même méthodologie. Elle concerne, entre autres :

L'intégrité : Les données intègres sont protégées contre les accès non autorisés, la corruption et la perte. L'intégrité des données garantit leur protection contre toute altération non autorisée, préservant ainsi la précision, la cohérence et la validité. Des données intègres demeurent intactes et non altérées.

Intelligence artificielle : Domaine de l'informatique qui vise à créer des machines capables de simuler l'intelligence humaine.

Ligne directrice : Normes et conduites à adopter en conformité avec les politiques de gouvernance des données adoptées pour orienter les décisions futures.

Une seule santé « One Health » : L'approche Une seule santé « One Health » est une stratégie intégrée qui reconnaît l'interconnexion entre les santés humaine, animale et environnementale. Elle vise à optimiser la santé globale par des efforts de collaboration entre divers secteurs.

Précision : Les données sont exactes et sans erreurs.

Promptitude : Capacité à disposer de données collectées régulièrement, mises à jour et de manière opportune. Elle inclut deux aspects : la fréquence qui tient compte de la disponibilité régulière pour éclairer les décisions de gestion des programmes. L'actualité se réfère au degré auquel les données sont à jour et reflètent l'état actuel des choses. L'actualité des données mesure la fraîcheur et la pertinence temporelle des informations enregistrées. Des données actualisées reflètent des événements récents et sont adaptées aux besoins actuels des utilisateurs.

Protection des données : « Application systématique d'un ensemble de garanties institutionnelles, techniques et physiques qui préservent le droit à la vie privée en ce qui concerne la collecte, le stockage, l'utilisation et la divulgation de données personnelles et collectives ».

Pseudonymisation : Méthode de désidentification des données consistant à retirer les informations permettant d'identifier directement une personne et à les remplacer par d'autres identifiants (pseudonymes) ne présentant aucun lien apparent avec les identifiants d'origine. Les données personnelles sont ainsi dissociées des éléments d'identification de sorte qu'elles ne puissent plus être attribuées à une personne précise sans recourir à des informations supplémentaires relatives au processus de désidentification, telles qu'une clé de correspondance reliant les identités aux pseudonymes.

Validité : La validité des données fait référence à la mesure dans laquelle les données collectées ou utilisées reflètent avec précision la réalité qu'elles sont censées représenter. En d'autres termes, des données valides sont des données qui sont **exactes, pertinentes et appropriées** par rapport à l'objectif pour lequel elles sont collectées. Les données doivent couvrir tous les aspects pertinents du phénomène étudié. La validité se rapporte aussi à la capacité des données ou des résultats à être généralisés au-delà du contexte dans lequel elles ont été collectées. Pour que les données soient valides, elles doivent être correctement collectées, mesurées et interprétées en fonction de leur finalité, sans biais ni erreurs majeures.

PRÉFACE

La République de Madagascar connaît actuellement une transformation numérique majeure, marquée par une augmentation considérable des données de santé. Au niveau du secteur de la santé, une attention particulière a été accordée à l'amélioration de la qualité des soins, qui est de plus en plus observée à travers ces données et la mise en œuvre de la santé digitale, comme en témoignait la récente validation de sa nouvelle stratégie nationale en santé digitale. À Madagascar, la population considère la santé comme une richesse fondamentale, ce qui souligne l'importance d'une gouvernance rigoureuse des données de santé pour éclairer les décisions en matière de santé publique. Les avancées technologiques et les innovations dans le traitement de l'information ouvrent des perspectives inédites pour améliorer la prise en charge des patients, mais elles soulèvent également des enjeux complexes en matière de protection de la vie privée, de sécurité des données et d'éthique.

Ce document sur la politique de gouvernance des données de santé a pour objectif d'établir un cadre structuré et clair pour la gestion de ces informations sensibles et essentielles. Il est le fruit d'une réflexion approfondie et d'une collaboration étroite entre divers acteurs, publics et privés du secteur de la santé, avec l'appui de ses partenaires techniques et financiers. Le but est de définir des orientations politiques explicites garantissant la transparence, la sécurité des données, l'accès équitable et la qualité des soins de santé, tout en respectant les droits des individus et les exigences légales et réglementaires en vigueur.

Il sera une ressource précieuse pour les professionnels de la santé, les gestionnaires de données et les responsables stratégiques, en les guidant dans le paysage complexe de la gouvernance des données de santé. Ensemble, nous pouvons construire un avenir où l'innovation en soins de santé est soutenue par une gestion rigoureuse des données, garantissant ainsi des bénéfices durables pour les individus et les communautés que nous servons.

Nous tenons à exprimer notre profonde reconnaissance à tous ceux et celles qui ont participé à la création de cette politique. Leur savoir-faire, leur dévouement et leur engagement ont été décisifs dans la concrétisation de ce projet. Puissent ces lignes inspirer des pratiques exemplaires et nourrir une réflexion continue sur la gouvernance des données de santé.

INTRODUCTION

CONTEXTE :

En 2020, aucun pays à faible revenu ne disposait d'une entité gouvernementale dédiée à la gouvernance des données. En 2025, 35 % d'entre eux en avaient mis une en place — chiffre qui reste bien inférieur aux 81 % observés dans les pays à revenu élevé¹.

À Madagascar, au cours du premier semestre de 2024, 15 % de la population malagasy ont accès à Internet, selon l'Institut National de la Statistique (INSTAT) (2024). Cependant, l'accès aux services de santé digitale demeure limité dans les zones rurales et reculées. La pénétration de la téléphonie mobile est plus élevée : environ 50 % de la population utilise un téléphone mobile, ce qui offre des perspectives importantes pour le développement des services de santé mobile (mHealth)². Madagascar présente une fracture numérique marquée entre les zones rurales et urbaines et se classe au 18^e rang parmi les 19 principaux pays africains selon l'indice de développement des technologies de l'information et de la communication (TIC) de l'Union internationale des télécommunications³. L'opérationnalisation des autorités de protection des données n'est pas encore effective. L'existence de financements et d'appuis techniques de la part des partenaires, l'engagement de l'État en faveur du renforcement du système de gouvernance, ainsi que les avancées technologiques et le développement des compétences constituent autant d'opportunités à saisir.

Des initiatives telles que le projet de connectivité rurale financé par la Banque Mondiale visent à améliorer l'accès à Internet dans les zones rurales. De plus, des programmes de formation en santé digitale sont en cours de déploiement afin de renforcer les compétences des professionnels de la santé dans ces régions.

Dans le secteur de la santé, l'alignement des partenaires techniques et financiers (PTF) sur les orientations du Ministère de la Santé Publique (MSANP) conformément aux stratégies définies dans le Plan Stratégique de Renforcement du Système d'Information Sanitaire (PSRSIS) et de la Stratégie Nationale en Santé Digitale (SNSD), reste encore à consolider. Nous faisons face à plusieurs défis. D'une part, il est nécessaire d'opérationnaliser la Commission Malagasy de l'Informatique et des Libertés (CMIL) en appui au secteur de la santé ainsi que la disponibilité de responsables de la gouvernance des données et d'utilisateurs de données qualifiés. Pour garantir la conformité réglementaire, il est essentiel de mettre en place une coordination efficace et une responsabilisation des acteurs, ainsi que leur adhésion aux cadres normatifs et réglementaires. D'autre part, nous devons veiller à l'interopérabilité effective des plateformes existantes et à l'harmonisation des outils et des plateformes de collecte et de gestion des données. Par ailleurs, l'accessibilité permanente aux données ainsi que la fluidité de cet accès nécessitent des améliorations, sans pour autant négliger leur sécurisation.

Une gouvernance efficace des données de santé est essentielle au renforcement du système de santé à Madagascar. Il est aujourd'hui nécessaire de réduire la charge de travail des professionnels et d'éliminer les redondances dans la collecte des données. Il importe également d'harmoniser les différents systèmes pour qu'ils mesurent les mêmes indicateurs finaux, et de renforcer la communication et les échanges de données entre les plateformes. La mise en place d'une gouvernance adaptée permet

¹ GovTech Dataset - World Bank Data Catalog

² INSTAT Madagascar. (2024). Enquête nationale sur l'accès à Internet et les technologies de l'information et de la communication. Institut national de la statistique, Madagascar.

³ Étude de base sur la numérisation des services publics dans les pays africains, JICA, mars 2022

en effet de favoriser une prise de décision éclairée, tout en garantissant la sécurité, l'intégrité et la qualité des données, ainsi qu'en prévenant leur perte.

Pour relever ces défis, il est nécessaire de mobiliser les ressources humaines et matérielles, de renforcer les capacités en matière de gouvernance des données et de santé digitale, de numériser les registres, de sécuriser les données personnelles, et d'harmoniser les processus de collecte. De plus, il faut assurer la qualité des données, soutenir l'opérationnalisation de l'observatoire de cybersanté, simplifier la collecte de données, garantir la transparence et l'équité d'accès, ainsi que l'opérationnalisation de la CMIL.

VISION :

Garantir une gestion sécurisée, **éthique** et **innovante** pour une utilisation **équitable** des données de santé et un accès aux **soins de qualité** pour la santé de la population malagasy grâce aux avancées de la **santé numérique**.

OBJECTIF PRINCIPAL :

Renforcer la gouvernance des données de santé pour une planification et une gestion efficace du système de santé malagasy.

PORTÉE DE LA POLITIQUE DE GOUVERNANCE DES DONNÉES :

Les types de données de santé collectées peuvent inclure des données cliniques, épidémiologiques, administratives, de recherche et de santé publique ainsi que des informations logistiques, financières, matérielles, humaines et démographiques. Ces données sont produites et utilisées à différents niveaux du système de santé et présentent des degrés variables de sensibilité.

Classification des données de santé

Afin d'adapter les règles d'accès, de partage et de sécurité, les données de santé sont classées selon leur niveau de sensibilité, ce qui permet de définir des exigences minimales de protection :

- Données identifiables : Données permettant d'identifier directement ou indirectement une personne. Leur accès est strictement limité aux personnes dûment autorisées, des mesures de sécurité renforcées doivent être appliquées, et le partage est fortement restreint.
- Données pseudonymisées : Données pour lesquelles les éléments d'identification ont été remplacés par des identifiants indirects. Leur accès est contrôlé et le partage peut être autorisé selon certaines conditions clairement définies, notamment à des fins de recherche ou d'analyse.
- Données agrégées : Données regroupées ne permettant pas l'identification d'individus. L'accès est élargi et le partage est possible, sous réserve du respect des règles en vigueur.
- Données publiques : Données ne présentant aucun risque pour la confidentialité ou la vie privée. L'accès est libre, conformément aux dispositions légales et réglementaires en vigueur.

Les exigences de sécurité, de confidentialité et de gouvernance doivent être proportionnées au niveau de sensibilité des données, et clairement définies dans les procédures opérationnelles.

Parties prenantes et bénéficiaires de la politique

Les entités et parties prenantes impliquées dans la mise en œuvre de la politique de gouvernance des données comprennent notamment : les professionnels de santé, les secteurs public et privé, le Ministère de la Santé, l'Unité de Gouvernance Digitale (UGD), la CMIL, les comités d'éthique de la recherche, les

organismes de certification, le Ministère du Développement Numérique, le Ministère de la Justice, les partenaires techniques et financiers (PTF), ainsi que la société civile, y compris les ordres professionnels de santé et les sociétés savantes.

Les utilisateurs finaux des données, tels que les établissements de santé, les chercheurs, les responsables de la santé publique, les décideurs politiques et les personnes concernées par les données, sont également couverts par la présente politique, dans le respect du niveau de sensibilité des données qu'ils utilisent.

CADRE LÉGAL ET RÉGLEMENTAIRE EN MATIÈRE DE GOUVERNANCE DES DONNÉES DE SANTÉ

CADRE JURIDIQUE :

Le cadre juridique de la gouvernance des données de santé est constitué par les lois et règlements nationaux ainsi que par les engagements internationaux auxquels le pays s'est souscrit. Il est essentiel de respecter ces exigences pour garantir la légalité et la conformité des pratiques de gestion des données de santé.

Cadre juridique international :

La Convention de MALABO (Guinée équatoriale), adoptée le 27 juin 2014, est un traité de l'Union africaine visant à renforcer la cybersécurité et la protection des données à caractère personnel en Afrique. Elle établit un cadre juridique destiné à favoriser la coopération entre les États membres dans la lutte contre la cybercriminalité et la protection des informations personnelles.

Cadre juridique national :

Bien qu'ils demeurent insuffisants, plusieurs textes législatifs et réglementaires (lois, décrets, etc.) sont déjà en vigueur et doivent être pris en considération, notamment ceux relatifs à la protection des données personnelles, à la confidentialité des informations de santé et aux réglementations sectorielles spécifiques. Il s'agit, entre autres, des textes suivants :

- Loi n° 2003-011 du 3 septembre 2003 sur le Statut général des fonctionnaires (confidentialité des documents) ;
- Loi n° 2005-040 du 15 décembre 2005 sur la lutte contre le VIH/sida et la protection des droits des personnes vivant avec le VIH/sida ;
- Loi n° 2011-002 du 15 juillet 2011 modifiée et complétée par le Décret n° 2022-2024 du 30 janvier 2023 portant sur le Code de la Santé ;
- Loi n° 2014-006 du 17 juillet 2014 modifiée et complétée par la Loi n° 2016-031 du 15 juillet 2016 portant sur la lutte contre la cybercriminalité ;
- Loi n°2014-025 du 5 novembre 2014 sur la signature électronique ;
- Loi n°2014-026 du 5 novembre 2014, fixant les principes généraux relatifs à la dématérialisation des procédures administratives ;
- Loi n° 2014-038 du 9 janvier 2015 sur la protection des données à caractère personnel ;
- Loi n°2016-031 du 15 juillet 2016 modifiant et complétant certaines dispositions de la Loi n°2014-006 du 17 juillet 2014 sur la lutte contre cybercriminalité ;
- Décret n° 2017-530 du 4 juillet 2016 portant sur la réorganisation et le fonctionnement de la commission « Droit et VIH » ;
- Décret n° 2023-1541 du 6 décembre 2023 portant attributions, organisation et fonctionnement de la Commission Malagasy de l'Informatique et des Libertés « CMIL » et traitements des données à caractère personnel.
- Décret n° 2012- 0632 du 13 juin 2012 portant sur le code de déontologie médicale.

- Décret n° 2023-1356 du 11 octobre 2023 portant sur la création, l'organisation, le fonctionnement, et la composition de la Plateforme nationale « Une seule santé » à Madagascar.

Les lois actuellement en vigueur nécessitent des mises à jour pour s'adapter aux réalités contemporaines et aux évolutions technologiques. En outre, le projet de réforme du Code de la santé n'intègre pas encore la protection des données de santé. Dans ce contexte, il est essentiel de mettre en place un cadre juridique permettant de protéger les droits des personnes, de garantir une utilisation équitable des données et de promouvoir des valeurs de santé à l'ère numérique. Les acteurs concernés incluent les patients, les agents de santé, les gestionnaires de données, les administrateurs du système de santé et les utilisateurs de données en dehors du secteur de la santé.

Les parties prenantes concernées comprennent notamment les patients, les professionnels de santé, les gestionnaires de données, les administrateurs du système de santé ainsi que les utilisateurs de données extérieurs au secteur de la santé.

LOIS ET RÉGLEMENTATIONS POUR LA GOUVERNANCE DES DONNÉES DE SANTÉ :

Madagascar ne dispose d'aucun cadre législatif et réglementaire spécifique sur la protection des données de santé, y compris la santé numérique. Toutefois, des initiatives doivent être entreprises pour élaborer une législation dédiée, inspirée des normes internationales telles que le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne et la Health Insurance Portability and Accountability Act (HIPAA) des États-Unis d'Amérique, qui établit des principes fondamentaux pour la gestion des données personnelles, y compris les données de santé.

L'élaboration d'un projet de cadre législatif et réglementaire sur la protection des données de santé est nécessaire. Il est impératif d'adopter un arrêté interministériel et de mettre en œuvre la stratégie nationale de la santé digitale, incluant les réglementations sur l'accès et le consentement des patients, les normes strictes encadrant le stockage, le traitement et la transmission des données sensibles ainsi que les exigences de cryptage et de contrôles d'accès rigoureux.

POLITIQUE DE GOUVERNANCE DES DONNÉES DE SANTÉ :

Afin de garantir la conformité de la politique de gouvernance des données de santé avec les lois nationales et internationales, il est nécessaire d'élaborer un document décrivant les lignes directrices relatives à l'accès et au partage des données.

La Commission Malagasy de l'Informatique et des Libertés (CMIL) intervient en tant qu'autorité de régulation en matière de protection des données personnelles. En cas d'infraction, la Direction des Affaires Juridiques (DAJ) du Ministère peut saisir la CMIL, tandis que la Direction en charge du système d'information sanitaire (SIS) supervise la mise en œuvre de la politique de gouvernance des données.

DROITS DES PERSONNES ET ÉTHIQUES

Droits des personnes en matière de protection des données de santé :

Les droits des personnes sont cruciaux pour garantir la confidentialité des informations médicales. Les principaux droits incluent :

Droit à l'information : Les personnes doivent être informées sur la collecte et l'utilisation de leurs données de santé, y compris les objectifs, les destinataires et la durée de conservation.

Droit d'accès : Les personnes peuvent consulter et obtenir une copie de leurs données de santé détenues par les professionnels de la santé.

Droit de rectification : Les personnes peuvent demander la correction des informations inexactes ou incomplètes concernant leur état de santé.

Droit à l'effacement : Les personnes peuvent demander la suppression de leurs données lorsque celles-ci ne sont plus nécessaires ou ont été traitées illégalement, avec certaines exceptions.

Droit à la portabilité : Les personnes peuvent recevoir leurs données de santé dans un format structuré et demander leur transfert à un autre responsable de traitement.

Droit d'opposition : Les personnes peuvent s'opposer au traitement de leurs données dans certaines situations, comme pour le marketing direct.

Droit à la sécurité : Les données doivent être protégées contre les accès non autorisés et les violations.

Droit à la réparation : En cas de violation, les personnes peuvent demander réparation par des plaintes ou actions en justice.

Droit au consentement : Le traitement des données de santé nécessite généralement le consentement éclairé de la personne, sauf exceptions prévues par la loi.

Mise en place de mécanismes de recours efficaces en cas de violation des droits :

Pour garantir des recours efficaces en cas de violation des droits, il est nécessaire de définir les cas de violation, d'établir une plateforme sécurisée pour signaler ces violations, de mettre en place des procédures d'enquête et de recours et de sensibiliser les parties prenantes sur leurs droits. La mise en place d'un système judiciaire **impartial** et **équitable** conditionne l'efficacité de ces mécanismes.

Éthiques soulevées par l'utilisation des données de santé, notamment en matière de recherche, d'intelligence artificielle et de profilage :

L'utilisation des données de santé soulève plusieurs enjeux éthiques majeurs, en particulier dans les domaines de la recherche, de l'intelligence artificielle (IA) et du profilage. Il est impératif de veiller à ce que la collecte des données soit strictement liée aux objectifs poursuivis, et de ne recueillir des données personnelles identifiables ou sensibles qu'en cas de nécessité absolue. Il convient également de recourir à des mécanismes sécurisés pour la collecte, le stockage et la diffusion des données, de définir clairement les usages inappropriés et de mettre en place des dispositifs de contrôle, de consentement et de responsabilisation afin de garantir une utilisation éthique des données de santé, respectueuse des droits des personnes. Lors de la collecte, les données personnelles devraient être identifiables et codées, mais pour des besoins spéciaux, elles peuvent être déchiffrées ou identifiées.

Assurer une utilisation équitable et non discriminatoire des données de santé :

Pour garantir une utilisation équitable et non discriminatoire des données de santé, il est essentiel d'assurer une représentation équitable dans les données de toutes les personnes et de toutes les communautés, quelles que soient leurs caractéristiques sociales (par exemple, l'âge, le sexe, la race, l'orientation sexuelle, le statut de réfugié) ou économiques (par exemple, le niveau de revenu, la profession), et un accès équitable à la valeur sanitaire générée par les données.

Il est essentiel de prendre en compte les besoins spécifiques des groupes les plus vulnérables et de s'efforcer de lutter contre la discrimination et d'identifier les cas où certains biais peuvent être introduits. Des mécanismes de rétroaction doivent être mis en place afin que les personnes et les communautés impliquées à chaque étape de la collecte, de l'analyse et de l'utilisation des données sachent comment elles sont utilisées. Les personnes doivent également avoir des droits sur leurs données et être capables de prendre des décisions appropriées pour elles-mêmes.

Afin d'assurer la mise en œuvre de l'ensemble de ces actions, il est nécessaire de rendre disponibles les documents cadres, comme les lignes directrices relatives à l'accès et au partage des données, la Stratégie Nationale en Santé Digitale (SNSD) ainsi que les procédures opérationnelles standardisées (POS). Ces documents doivent être mis à la disposition des utilisateurs des données, des administrateurs du système de santé et de gestion des données dans le domaine de la santé ainsi que des professionnels de santé chargés de la collecte des données ou de la prestation des soins (médecins, agents communautaires, etc.). Il faut également éduquer le public pour connaître ses droits sur ses données.

Il est également essentiel de sensibiliser le public afin qu'il connaisse ses droits en matière de données personnelles.

CADRE DE GOUVERNANCE DES DONNÉES DE SANTÉ

POLITIQUES, NORMES ET DIRECTIVES CLÉS EN MATIÈRE DE GESTION DE DONNÉES :

La mise en place d'une gouvernance rigoureuse est essentielle pour assurer une gestion optimale des données, qui sont essentielles à la prestation des soins, à la recherche médicale et à la gestion des systèmes de santé. Pour une gestion efficace, il est nécessaire de disposer de cadres robustes et de politiques claires pour assurer la collecte, le traitement et l'utilisation appropriés des données. Le cycle de vie des données sanitaires comprend plusieurs étapes : la création, la collecte, le traitement, l'utilisation et l'archivage des informations.

Les outils utilisés pour chaque étape incluent des systèmes de gestion de bases de données pour la collecte, des logiciels d'analyse pour le traitement, et des serveurs sécurisés pour l'archivage. Les défis associés incluent la garantie de l'interopérabilité entre différents systèmes et la protection contre les cyberattaques.

▪ **Collecte des données :**

La collecte de données en santé implique plusieurs sources clés, chacune fournissant des informations essentielles pour divers objectifs. Les données individuelles, obtenues à partir des sites communautaires — notamment via les Agents Communautaires (AC), reconnus comme producteurs de données à part entière dans le cadre de gouvernance —, des Centres de Santé de Base (CSB), des Centres Hospitaliers de Référence de District (CHRD), des Centres Hospitaliers de Référence Régionale (CHRR), des Centres Hospitaliers Universitaires (CHU), des Centres Spécialisés (CS), des laboratoires et des formations sanitaires privés, sont analysées selon l'approche Une seule santé « One Health » pour optimiser les soins et les politiques de santé.

Les données logistiques, en ressources humaines, financières, matérielles, et démographiques sont également collectées à partir de ces mêmes sources ainsi que des Services du District de la Santé Publique (SDSP) et les Directions Régionales de la Santé Publique (DRSP) et de l'Institut National de la Statistique (INSTAT). Ces informations soutiennent la gestion opérationnelle, l'allocation des ressources, et la planification stratégique dans le secteur de la santé.

▪ **Outils de collecte et de communication des données :**

Des outils électroniques sont utilisés pour la gestion des patients, la collecte, la communication et le traitement des données de santé, adaptés aux différents niveaux de la pyramide sanitaire. Toutefois, il convient de souligner que les outils de collecte de données ne se limitent pas aux dispositifs électroniques, mais englobent également des outils physiques, qui peuvent jouer un rôle important dans certains contextes de gestion des données de santé.

▪ **Traitement des données :**

Le traitement des données en santé repose sur des méthodes structurées pour garantir leur qualité, leur sécurité et leur utilité. Une fois collectées, ces données sont analysées pour identifier des tendances, maintenir la qualité et la sécurité des informations, et soutenir la prise de décision. Ce processus permet d'optimiser les interventions en santé, de planifier efficacement les ressources et de conduire des recherches fondamentales pour améliorer les pratiques et les politiques de santé.

▪ **Durée de conservation et période d'expiration :**

La durée de conservation des données doit être déterminée en fonction des objectifs spécifiques, des exigences légales et des besoins opérationnels. Les données analytiques sont souvent conservées plusieurs années pour permettre des analyses approfondies et assurer une traçabilité historique, tandis que les données de gestion quotidienne peuvent avoir des périodes de conservation plus courtes.

▪ **Archivage et partage des données :**

Les données doivent être archivées lorsqu'elles ne sont plus activement utilisées, mais doivent être conservées pendant au moins dix ans pour des raisons légales, historiques ou de conformité. Cet archivage se fait sur des serveurs numériques protégés pour les données numériques et dans des entrepôts dédiés pour les documents physiques. Il est important de préparer les données pour un partage sécurisé et conforme aux politiques de confidentialité, tout en contrôlant strictement l'accès aux seules parties autorisées.

▪ **Utilisation des données :**

Les responsables de l'utilisation des données doivent garantir la transparence, obtenir le consentement des personnes concernées, assurer la sécurité des informations et respecter le cadre et la loi. Les utilisateurs de données, quel que soit leur niveau de responsabilité, doivent s'appuyer sur une analyse rigoureuse pour orienter leurs décisions.

L'utilisation des données de santé inclut également le plaidoyer auprès des Partenaires Techniques et Financiers (PTF). Les données agrégées et validées issues du DHIS2 et des rapports de routine peuvent être mobilisées à des fins de plaidoyer pour appuyer la mobilisation des ressources et l'alignement des PTF sur les priorités nationales de santé, dans le respect des règles de confidentialité et de partage en vigueur.

Entité	Rôles et responsabilités
DRSP	• Gestion et collecte des données sanitaires au niveau régional • Utilisation des données pour la prise de décision régionale, le suivi des programmes et la rédaction de rapports à destination des PTF opérant au niveau régional • Appui aux formations sanitaires et sites communautaires de la région dans le rapportage et la qualité des données • Transmission et utilisation des données des sites communautaires (AC) pour la supervision et la planification régionale
SDSP	• Gestion et collecte des données sanitaires au niveau district • Utilisation des données pour la planification des activités du district, la supervision des formations sanitaires et la coordination avec les sites communautaires • Transmission et valorisation des données issues des AC pour la gestion des programmes au niveau district

POLITIQUES RELATIVES À LA GESTION DE LA QUALITÉ DES DONNÉES (Y COMPRIS L'ASSURANCE DE LA QUALITÉ DES DONNÉES)

Les politiques relatives à la gestion de la qualité des données sont des directives et des procédures mises en place pour assurer que les données respectent les standards de qualité attendus selon les différentes dimensions de la qualité de données. Les sept dimensions essentielles à considérer sont : la complétude, la promptitude, la précision, la validité, la fiabilité, l'intégrité et la confidentialité. Ces critères assurent et visent à garantir que les données sont complètes, disponibles en temps opportun, exactes, conformes aux normes, cohérentes, fiables et protégées contre les accès non autorisés tout au long de leur cycle de vie.

POLITIQUE RELATIVE À L'ACCÈS, AU PARTAGE ET À LA SÉCURITÉ DES DONNÉES DE SANTÉ

PROTECTION DES DONNÉES PERSONNELLES :

Pour garantir une gestion transparente et respectueuse des données personnelles, il est essentiel de fournir des informations claires et accessibles, expliquant les types de données collectées, les raisons de la collecte, les traitements prévus et les droits des personnes, en utilisant un langage simple. Le consentement doit être obtenu explicitement par une action claire de l'individu, avec la possibilité de le retirer à tout moment sans affecter les traitements antérieurs. Il est aussi important d'offrir des options spécifiques pour des finalités précises, de former le personnel sur le consentement et la communication, d'informer régulièrement les personnes des mises à jour, et de mettre en place des mécanismes de rétroaction pour répondre aux questions et préoccupations.

ACCÈS ET PARTAGE DES DONNÉES :

Le partage des données de santé doit se faire avec un consentement éclairé du patient. Ce consentement doit respecter les règles, lois et normes nationales, avec des accords contractuels définissant les responsabilités des tiers en matière de sécurité. Les données doivent être partagées uniquement pour des finalités spécifiques et clairement définies. Il est essentiel de limiter le partage pour protéger la vie privée. Les données doivent être utilisées uniquement à des fins éthiques.

SÉCURITÉ DES DONNÉES :

La sécurité des données repose sur trois dimensions essentielles, à savoir : (i) la confidentialité, (ii) l'intégrité et (iii) la disponibilité. Afin de garantir ces principes, des évaluations régulières des risques, des tests de sécurité, le respect des réglementations nationales en vigueur, ainsi que la documentation des mesures techniques et organisationnelles et la formation continue du personnel sont indispensables.

Toute faille de sécurité ou incident affectant la confidentialité, l'intégrité ou la disponibilité des données doit faire l'objet d'un signalement obligatoire dans les meilleurs délais, conformément aux procédures établies. L'autorité compétente désignée (par exemple le MSANP, la CMIL ou toute autre instance nationale habilitée) est responsable de la conduite de l'enquête, de l'évaluation de l'impact, et de la détermination et du suivi des mesures correctives appropriées.

POLITIQUE RELATIVE AUX INFRASTRUCTURES TECHNOLOGIQUES POUR LA GOUVERNANCE DES DONNÉES DE SANTÉ

CHOIX DES SOLUTIONS TECHNOLOGIQUES APPROPRIÉES POUR METTRE EN PLACE UN SYSTÈME D'INFORMATION SANITAIRE NATIONAL INTÉGRÉ :

Madagascar rencontre des défis significatifs en matière d'infrastructures technologiques dans le secteur de la santé, avec des disparités marquées entre les zones urbaines et rurales. Pour surmonter ces obstacles et mettre en place un système d'information sanitaire national intégré, il est vital d'adopter des solutions technologiques en ligne qui respectent les normes internationales et qui reflètent les priorités du Ministère de la Santé Publique. En particulier, l'adoption d'infrastructures numériques sécurisées, couplée à l'utilisation de protocoles de communication standards, permettra une meilleure intégration des données de santé à travers le pays. Cette démarche facilitera l'interopérabilité des systèmes et assurera une continuité des soins et de la gestion des informations à tous les niveaux de la pyramide sanitaire.

HÉBERGEMENT ET GESTION DES SERVEURS :

L'état actuel des infrastructures technologiques à Madagascar montre que les équipements et la connectivité restent rudimentaires et vulnérables. Pour remédier à cette situation, il est essentiel de mettre en place des politiques rigoureuses concernant l'hébergement et la gestion des serveurs. Ces politiques devraient promouvoir l'utilisation de centres de données sécurisés au niveau national, avec des options de sauvegarde régulière et une redondance adéquate pour éviter les pertes de données. À long terme, la mise en place de sites de secours est nécessaire pour assurer la résilience des données. À court terme, à titre de mesure transitoire, la migration vers des serveurs cloud hybrides, qu'ils soient publics ou privés, doit être envisagée afin d'améliorer la résilience, la disponibilité et la sécurité du système d'information sanitaire. Des critères stricts de sélection doivent être définis pour le choix des prestataires de services cloud, en veillant à leur conformité aux standards internationaux en matière de sécurité des données, de protection de la vie privée et de gestion des infrastructures.

Dans l'hypothèse d'un retour à un hébergement sur site, des vérifications rigoureuses et préalables doivent être réalisées afin de s'assurer que les infrastructures nationales disposent des capacités techniques, des ressources humaines, et des mécanismes de sécurité nécessaires pour répondre aux besoins actuels et futurs du pays. Ces vérifications doivent notamment porter sur la fiabilité du matériel, la sécurité physique et logique, la redondance, les mécanismes de sauvegarde et de reprise après incident, ainsi que la conformité aux normes internationales applicables.

Toute décision relative au mode d'hébergement doit s'appuyer sur une analyse de risques documentée, validée par l'entité en charge du système d'information sanitaire.

INTEROPÉRABILITÉ DES SYSTÈMES :

Pour favoriser l'interopérabilité des systèmes, la présente politique est établie dans le but de garantir que tous les systèmes de santé, qu'ils soient publics ou privés, puissent communiquer et échanger des données de manière transparente. L'adoption de standards ouverts et de formats de données universels est indispensable pour permettre une intégration fluide. De plus, il est nécessaire de mettre en place des mécanismes de contrôle pour surveiller l'interopérabilité des systèmes, en s'assurant que les données circulent de manière fluide et sécurisée à travers tous les niveaux de la pyramide sanitaire.

L'instauration de cette interopérabilité se déroulera en deux phases : d'abord, une interopérabilité interne sera établie au sein des structures du système de santé, puis, une fois celle-ci consolidée, l'interopérabilité externe avec les autres secteurs sera mise en œuvre.

CYBERSÉCURITÉ :

La sécurité des données de santé doit être au cœur de toute politique technologique. Le développement d'une infrastructure technologique robuste doit s'accompagner de politiques strictes en matière de cybersécurité. Cela inclut le chiffrement des données, l'application de contrôles d'accès rigoureux, la conduite d'audits réguliers, et l'utilisation de solutions de cybersécurité avancées. Il est également important de former le personnel aux meilleures pratiques en matière de sécurité des données pour minimiser les risques de violations. Les mécanismes de sécurité mis en place doivent être conformes aux normes et réglementations en vigueur, garantissant ainsi la protection des données de santé tout au long de leur cycle de vie.

En somme, la mise en place de ces politiques relatives aux infrastructures technologiques permettra, non seulement d'améliorer la gestion des données de santé à Madagascar, mais aussi, de jeter les bases pour des initiatives futures, telles que l'intégration de l'intelligence artificielle et du *machine learning*, qui promettent de révolutionner la santé publique dans le pays. La valorisation et l'application des POS existantes sont essentielles pour assurer la sécurité et la gestion adéquate des données de santé. En respectant et en mettant à jour régulièrement ces POS, le Ministère de la Santé Publique garantira une gestion efficace et sécurisée des informations sanitaires, tout en se préparant aux défis et opportunités futures.

POLITIQUE RELATIVE À LA STRUCTURE ORGANISATIONNELLE DE LA GOUVERNANCE DES DONNÉES

STRUCTURE RESPONSABLE DE LA GOUVERNANCE DES DONNÉES DE SANTÉ À MADAGASCAR :

À Madagascar, la gestion des données de santé est principalement supervisée par le Ministère de la Santé Publique (MSANP), qui établit les politiques nationales de santé et coordonne les systèmes d'information sanitaire. L'Institut National de la Statistique (INSTAT) collabore avec le MSANP pour la collecte et l'analyse des données de santé. En plus de ces organismes, des structures locales, des agences, des organisations non gouvernementales (ONG), ainsi que d'autres ministères, comme celui du Développement Numérique, des Postes et des Télécommunications (MNDPT) et le Ministère de la Justice peuvent également être impliqués dans la gouvernance des données de santé. La complexité du domaine implique la participation de nombreux acteurs avec des rôles spécifiques.

Pour optimiser les rôles et les responsabilités des structures de gouvernance, il est proposé de créer un comité national de gouvernance des données de santé, qui fonctionnerait comme un observatoire. Ce comité multisectoriel regrouperait des représentants des différentes entités mentionnées précédemment. Il pourrait être intégré :

- au sein de la Commission Malagasy de l'Informatique et des libertés (CMIL), dont l'opérationnalisation est en cours ;
- au sein de l'UGD, en précisant néanmoins les rôles que cette dernière pourrait jouer dans ce cadre.

Par ailleurs, il est important de spécifier le rôle de l'observatoire de la cybersanté qui est implanté au sein du Ministère de la Santé Publique. La création d'un groupe de travail sur la santé « Task Force santé » qui sera rattachée à la CMIL ou sera constituée en dehors de la CMIL est suggérée et doit être discutée.

RÔLES ET RESPONSABILITÉS DES DIFFÉRENTS ACTEURS IMPLIQUÉS DANS LA GOUVERNANCE DES DONNÉES DE SANTÉ

La bonne gouvernance des données repose sur une répartition claire des rôles et responsabilités entre les différents acteurs impliqués dans leur traitement, leur gestion et leur utilisation. À ce titre :

- Le responsable du traitement est l'entité qui détermine les finalités et les modalités d'utilisation des données et en assume la responsabilité. Ce rôle est généralement assuré par le MSANP ou par l'établissement de santé concerné.
- Le gestionnaire des données est chargé, au niveau opérationnel, de la collecte, de la saisie, de la gestion ainsi que du contrôle de la qualité des données.
- Tout utilisateur des données est tenu de respecter les règles d'accès, de confidentialité et de sécurité définies par la présente politique.
- La supervision de la gestion et de la gouvernance des données est assurée à tous les niveaux de la pyramide sanitaire — central, régional, district, formation sanitaire et communautaire. Elle vise à garantir le respect des normes et procédures en vigueur, à renforcer la qualité des données et à promouvoir une utilisation responsable, sécurisée et conforme des informations de santé.

Ces responsabilités doivent être explicitement définies et attribuées au sein de chaque structure, afin de garantir une application cohérente et effective des principes de gouvernance des données.

Cela signifie concrètement qu'à chaque niveau de la pyramide sanitaire, un responsable identifié assure la supervision des activités de gestion des données relevant de son niveau, rend compte au niveau supérieur et appuie les niveaux subordonnés. Cette chaîne de supervision est continue et documentée.

Au sein des établissements de santé

PROFESSIONNELS DE LA SANTÉ ET LES SECTEURS PUBLIC ET PRIVÉ :

Ils garantissent la conformité des systèmes d'information en respectant les normes et réglementations pour assurer la sécurité et la confidentialité des données.

INFORMATIENS :

Ce sont les facilitateurs de la vie des usagers. Ils appuient et rendent possible l'exploitation des données et assistent les usagers. Ils transforment les besoins en solutions centrées sur l'utilisateur, de la conception à l'évaluation, tout en collaborant étroitement avec les fournisseurs de services et de logiciels pour garantir une mise en œuvre efficace et alignée sur les objectifs stratégiques.

AU NIVEAU INSTITUTIONNEL

Ministère de la Santé Publique :

Le Ministère de la Santé Publique joue un rôle central dans la gouvernance des données de santé. Il est responsable de s'assurer que les systèmes de santé respectent les droits des patients, favorisent l'innovation tout en garantissant la sécurité des données, et facilitent la coordination entre les différents acteurs du secteur pour améliorer la qualité des soins et l'accès à l'information. Il est également responsable de la sensibilisation et de l'éducation sur les politiques de données de santé pour garantir leur compréhension et adhésion. À travers ses démembrements, que ce soit au niveau central, régional ou district, jusqu'au niveau des formations sanitaires et communautaires, le Ministère de la Santé Publique est l'organe principal chargé de la gestion des données de santé. Il veille à ce que le processus de collecte, de stockage, d'analyse et d'utilisation des données se fasse en respectant les normes techniques et administratives, en continu, respectant l'éthique et tenant compte du désenclavement géographique.

Ministère du Développement Numérique :

C'est l'institution nationale chargée principalement d'appuyer le développement des activités liées à la digitalisation des secteurs nationaux. Il assure la promotion de la politique nationale, guide la transformation numérique, développe le partage du savoir et l'amélioration de la gouvernance digitale. Au niveau du secteur santé, il sert de facilitateur technique et opérationnel que le secteur santé peut solliciter en fonction des services.

Ministère de la Justice :

Le Ministère de la Justice veille à ce que les infractions aux réglementations sur les données de santé soient correctement sanctionnées, ce qui contribue à la protection des droits des individus et à la crédibilité du système. Il contribue à l'élaboration, la révision et l'amélioration des lois et règlements sur la gestion des données de santé, en veillant à ce que le cadre juridique s'adapte aux évolutions technologiques et aux exigences de protection des données.

Organisme de contrôle et de suivi :

Cet organisme est chargé de certifier que les systèmes d'information de santé répondent aux normes de sécurité établies. Il assure également un rôle clé dans l'audit, l'évaluation et la validation des compétences, des systèmes, des produits ou des processus selon les normes établies avec les différentes entités concernées (MSANP, CMIL, UGD etc.). Il délivre un certificat attestant que le produit, le service ou le système respecte les normes et les exigences définies. Il veille sur l'évolution technologique et de l'environnement global de la santé digitale et promeut une amélioration continue.

AU NIVEAU DES STRUCTURES SPÉCIALISÉES

Unité de Gouvernance Digitale :

Il s'agit d'une unité créée pour la gouvernance digitale en collaboration avec tous les ministères et institutions nationales dans l'objectif d'améliorer la qualité et l'accessibilité des services publics via la digitalisation et la simplification des procédures. Dans le domaine de la gouvernance des données, l'UGD sera responsable de la « conformité digitale », qui implique le respect des réglementations, des normes et des meilleures pratiques numériques. L'UGD supervisera l'orientation nationale sur la gouvernance des données, l'interopérabilité, l'implémentation des solutions technologiques, et coordonnera les partenaires tout en renforçant la communication et la sensibilisation des différents acteurs. Il appuie le MSANP dans la mise en œuvre de la santé digitale et sert d'organe consultatif technique.

Commission Malagasy de l'Informatique et des Libertés :

En cours d'opérationnalisation, la CMIL est l'autorité chargée de la protection des données personnelles, y compris les données de santé, selon la loi. La CMIL veille à ce que les organisations respectent les législations locales sur la collecte, le traitement et la conservation des données personnelles, garantissant ainsi la confidentialité et la sécurité des informations. La CMIL protège les droits individuels, assure le respect des libertés et droits fondamentaux, et sensibilise le public et les organisations à la vie privée. Il conseille, assiste, surveille les tendances et peut imposer des sanctions en cas de non-conformité.

Comités d'éthique de la recherche :

Ce comité est chargé d'évaluer des projets de recherche impliquant des données de santé humaine pour s'assurer qu'ils respectent les principes éthiques.

Les autres acteurs

Partenaires techniques et financiers :

Les partenaires techniques et financiers (PTF) veillent à aligner leur soutien avec les politiques nationales de santé en collaborant avec les entités responsables au sein du Ministère de la Santé Publique pour renforcer l'efficacité des systèmes de gouvernance des données de santé. Ils apportent une expertise technique, partagent des innovations, et financent des initiatives essentielles, telles que le développement d'infrastructures, l'acquisition de matériel, et la formation des professionnels de santé. Enfin, les PTF renforcent les capacités locales pour garantir une appropriation durable des systèmes de gouvernance des données.

Société civile, y compris les ordres professionnels de santé et les sociétés savantes :

Toute la société civile, y compris les sociétés savantes et l'ordre professionnel (médecins, infirmiers, sage-femme, etc.), contribue activement à la sensibilisation et à l'éducation sur les enjeux liés aux données de santé en informant les membres et le public des bonnes pratiques et des politiques en vigueur. Ils veillent également à ce que leurs membres respectent les normes et règlements en matière de gestion des données en mettant en place des mécanismes de contrôle et de suivi pour garantir la conformité. La société civile participe également à l'information, éducation et communication auprès des usagers et appuie le respect des conformités.

Citoyens/usagers :

Les citoyens jouent un rôle clé dans la gouvernance des données de santé en donnant un consentement éclairé et en participant aux décisions concernant l'utilisation de leurs données. Ils sont également responsables de protéger leur vie privée et de collaborer pour influencer les politiques de manière éthique et équitable.

Le secteur privé :

Le secteur privé joue un rôle significatif dans la gouvernance des données sanitaires à travers l'appui au développement des technologies et les innovations pour la collecte, le stockage, l'analyse et l'utilisation des données de santé, la fourniture de services de formation et de support, le renforcement du partenariat, la sensibilisation des acteurs et la veille technologique.

SENSIBILISATION DES PROFESSIONNELS DE LA SANTÉ ET DU GRAND PUBLIC AUX ENJEUX DE LA PROTECTION DES DONNÉES DE SANTÉ :

La sensibilisation des professionnels de la santé et du grand public aux enjeux liés à la protection des données de santé passe par la mise en œuvre d'une campagne visant à informer sur les bonnes pratiques de gestion de l'information sanitaire et les risques associés aux brèches de gestion. Cette démarche comprend notamment l'élaboration et la mise en œuvre d'un plan de renforcement des capacités pour assurer une meilleure gestion et protection des données de santé. Un dispositif de suivi et d'évaluation est également mis en place pour mesurer l'efficacité des actions entreprises et en garantir l'amélioration continue.

MÉCANISMES DE SUIVI ET D'ÉVALUATION DE LA POLITIQUE DE GOUVERNANCE DES DONNÉES DE SANTÉ :

Afin d'assurer une gouvernance optimale des données de santé, il est essentiel d'opérationnaliser un observatoire central chargé de veiller au respect des normes et de promouvoir les meilleures pratiques. Des audits périodiques permettront de vérifier le respect et la conformité aux réglementations en vigueur, d'identifier les éventuels écarts et de formuler des recommandations concernant les ajustements nécessaires. Ces audits fourniront notamment des informations sur la conformité des systèmes et des infrastructures, la sécurité des données, la qualité des informations, la planification stratégique ainsi que l'impact des dispositifs mis en place sur la performance du système de santé. Enfin, des évaluations régulières, qu'elles soient annuelles ou semestrielles, permettront de mesurer l'efficacité des politiques mises en œuvre et d'ajuster les stratégies en fonction des résultats obtenus.

CONCLUSION

La politique de gouvernance des données de santé à Madagascar est un cadre essentiel pour assurer la sécurité et la qualité des données dans le secteur de la santé. En mettant en place des structures organisationnelles solides, des infrastructures technologiques adaptées, et des lignes directrices claires en matière de collecte, de partage et de protection des données, le pays se positionne pour répondre efficacement aux défis actuels tout en préparant le terrain pour les innovations futures. La mise en œuvre de cette politique exigera une collaboration étroite de tous les acteurs concernés et une détermination constante à améliorer les procédures de gouvernance. En gérant de manière éthique et transparente les données, Madagascar pourra améliorer l'équité d'accès et la qualité des soins de santé, tout en renforçant la confiance des citoyens dans le système de santé national.

RÉFÉRENCES BIBLIOGRAPHIQUES

INSTAT Madagascar. (2024). Enquête nationale sur l'accès à Internet et les technologies de l'information et de la communication. Institut national de la statistique, Madagascar.

Étude de base sur la numérisation des services publics dans les pays africains, JICA, mars 2022

DAMA DMBOK, Data Management Body of Knowledge, 2nd Edition

<https://www.who.int/publications/i/item/9789240081949>

<https://www.unicef.fr/politique-de-protection-des-donnees-personnelle>

<https://healthdataprinciples.org/fr/principles>

https://www.oecd.org/fr/publications/gouvernance-des-donnees-de-sante-a-l-ere-du-numerique_37ef3797-fr.html

<https://wdr2021.worldbank.org/fr/stories/gouvernance-des-donnees>

<https://www.talend.com/fr/resources/guide-gouvernance-donnees/>

<https://www.zucisystems.com/be/blog/quelle-est-la-gouvernance-des-donnees-quelle-est-son-importance/>

Textes législatifs et réglementaires : <https://cnlegis.gov.mg/>

Bruns, D. E., & Ashwood, E. R. (2015). Fundamentals of Molecular Diagnostics (2nd ed.). Elsevier Health Sciences.

ANNEXE I. LISTE DES CONTRIBUTEURS PAR ORDRE ALPHABÉTIQUE

ANDRIAMAHEFA Rindra, Data.FI, Palladium International

ANDRIAMAROFARA Haja, Banque Mondiale

ANDRIAMIRADOMANANTSOA Tiana Voahirana, Équipe managériale régionale, DRSP Vakinankaratra

ANDRIANAIVORAVELONA M. Jaona, Spécialiste S&E USAID IMPACT

ANDRIANARIJONA Onitiana Oliva Heroïne, Assistant technique, DGR

ANDRIANARIMALALA Manantsoa Lovaniaina, Spécialiste principal en TI, MCGL

ANDRIANIRINA Rijanarivo Alfa, Conseiller technique en santé numérique, ONG Pivot

ANDRIANJAFY Fetrarivo Harizo, Adjoint technique, SONC

ANDRIANJANAKA Christian, S&E, UNICEF

ANDRINIAINA Zafimaherisoa Rosin, Équipe technique, SEMIDSI

BANGAGNE Yemdame, Spécialiste de la santé, UNICEF

EUGÈNE Marie Yolande B., Directeur Pays, Data.FI, Palladium International

JACQUIT Edinho, Équipe technique LA2M

NYANDWI Alphonse, Spécialiste des TIC, UNICEF

RABEMANANJARA Rija, Directeur, DEPSI

RABEMILA Josia Hasiniaina, Responsable informatique à la Clinique privé Médico-chirurgicale SANTE PLUS Antsirabe, Représentant AHPM

RABIBIZAKA Urbain, Gestionnaire des données, PNLP, MSANP

RAFANOMEZANTSOA Heritiana Narindra, Assistant technique auprès de la DGFS

RAFIDIMANANTSOA Tahina Nomenjanahary, Assistant technique, DAJ

RAHARINARIVO David Heritiana, Chargé d'études, DAJ

RAKOTOARIMINO Nomenjanahary, Équipe technique SSSD

RAKOTOARISOA Fefimanambatra Leonardo, Équipe technique, SEMIDSI/DEPSI

RAKOTOARISON Daniel Elysé, Chef de service SEMIDSI

RAKOTOARIVELO Miarana, Équipe technique, SEMIDSI

RALANTOMAHEFA Richard, Data.FI, Palladium International

RAMAROSON Emile, Chef de division du suivi-évaluation, PNLT

RAMBOANASOLONDRAINIBE Joelson, Directeur Technique, Data.FI, Palladium International

RAMINOSOA Tantely, Conseiller principal du SIGS, USAID ACCESS

RANAIVOSON Harinjaka Fortuna, spécialiste en base de données, Unité de coordination des projets (UCP), MSANP

RANDRIAMANGA Tolotra Nantenaina Assistant technique de la DHRD

RANDRIAMBOAVONJY Rado, Analyste en santé numérique, UNICEF

RANDRIAMIALY Lalatina Larissa Chef du SSSD

RANDRIAMORASATA Tojoniaina Josoa, Équipe technique, SONC

RANDRIANANTOANDRO Mijoro Arisoa, Chef de service, SONC

RANDRIANARIJAONA Tojo Andry, Gestionnaire des données, DPEV, MSANP

RANDRIANAVALONA Harimisa, Chef de division du suivi-évaluation, PNLP

RANOROSOA Livamalala Fortunat, Équipe technique, DHRD

RASOAMANANJARA Marie Claudia, Équipe technique SONC

RASOLO RANAIVONIRINA Mamisoa, Assistant technique en charge du SIS, DEPSI

RASOLOHARIVOLOLONA Alice Responsable de la base de données Hospitalière, SSSD

RATSIMANDRESY Vonindravola, Équipe technique, SEMIDSI

RAZAFIMAHATRATRA Fenohasina Lova, Équipe technique, SEMIDSI

RAZAFINDRAKOTO Hasimbola Andry, Équipe technique, SONC

RAZAFINDRANALEFONA Jean Philippe, Équipe technique SONC

RAZAFINDRANOVA Hary Mampionona Muriel, Équipe technique SSSD

RAZAKANDRETSA Solange, Assistante technique de la DEPSI

RAZANAMIARANA Voahirantsoa Pâquerette, Chef de division du suivi et de l'évaluation du Programme national de lutte contre les IST/SIDA, PNLIS

TATAMO ARIMALALA Cynthia, TIC, DVSSER



REPUBLIKAN'I MADAGASIKARA

Fahavanan' - Tanindrazana - Fandriamandriamandriana

MINISTÈRE DE LA SANTÉ PUBLIQUE



Sponsored by the United States