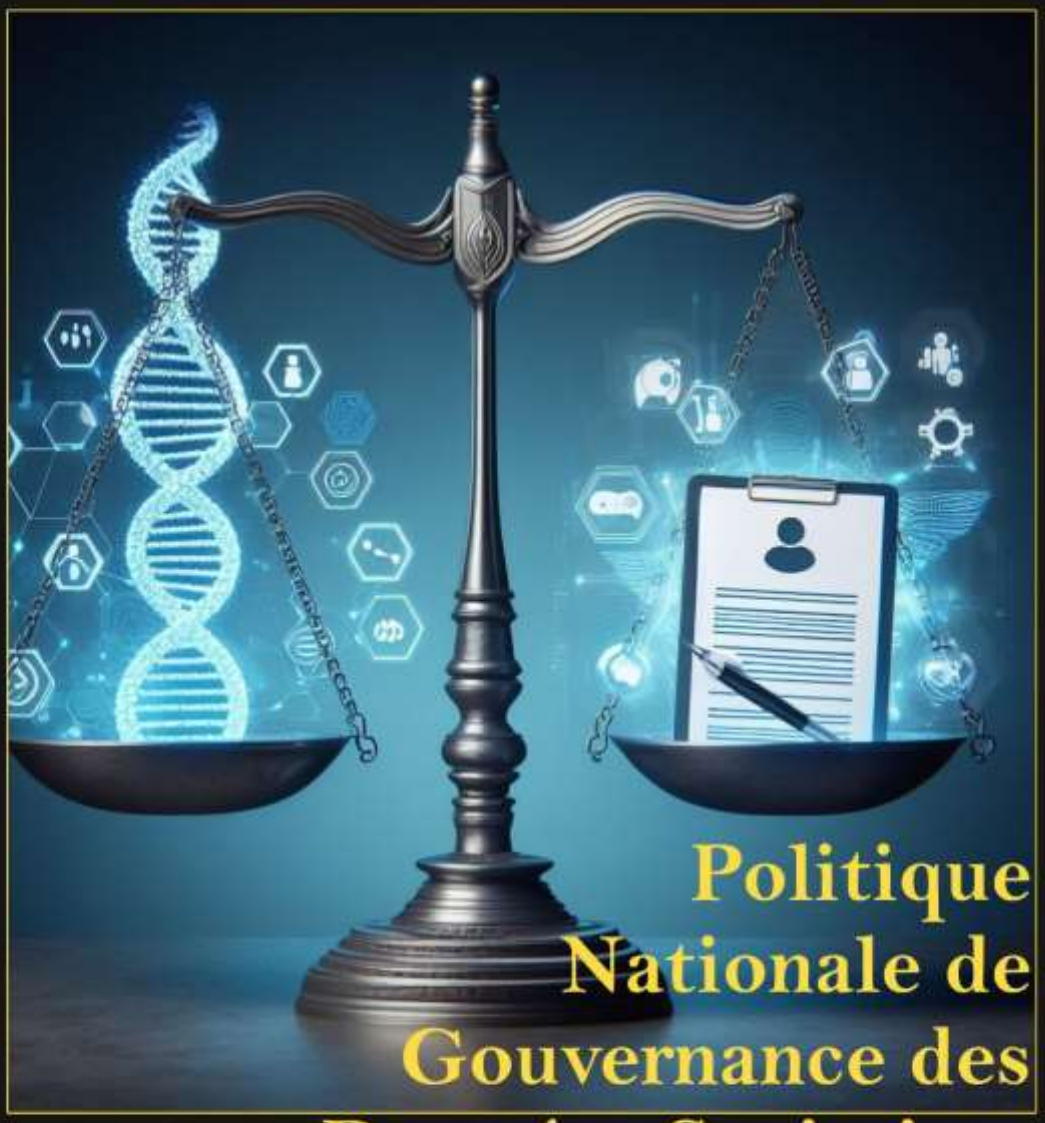
RÉPUBLIQUE DU BURUNDI

MINISTÈRE DE LA SANTÉ PUBLIQUE
ET DE LUTTE CONTRE L SIDA

DIRECTION GÉNÉRALE DES SERVICES DE SANTÉ ET DE LA LUTTE CONTRE LE SIDA

PROGRAMME DE GESTION INFORMATIQUE DU SECTEUR DE LA SANTÉ



Politique Nationale de Gouvernance des Données Sanitaires

2024 - 2027

USAID
FROM THE AMERICAN PEOPLE

cHiSU

TABLE DES MATIERES

SIGLES ET ABRÉVIATION

API	Application Programming Interface
ASS	Annuaire des Statistiques Sanitaires
BSS	Behavioural Surveillance System
BPS	Bureaux Provinciaux de Santé
CDA	Clinical Document Architecture
CDS	Centre de Santé
CHISU	Country Health Information System and data Use
CIM	Classification Internationale des Maladies
CNIL	Commission Nationale de l'Informatique et des Libertés
CNTS	Centre National de Transfusion Sanguine
COUSP	Centre des Opérations des Urgences de Santé Publique
DHIS	District Health Information Software
DQA	Data Quality Assessment
EAC	East African Community
EDS	Enquête Démographique de Santé
EDSB	Enquête Démographique de Santé au Burundi
FHIR	Fast Healthcare Interoperability Resources
HL7	Health Level seven
HTTPS	Hypertext Transfer Protocol Secure
FPEV	Femmes les Plus Exposées au VIH
FOSA	Formations Sanitaires
IBBS	Integrated Biological and Behavioral Survey
IRA	Infection Respiratoire Aigue
IST	Infections Sexuellement Transmissibles
HANDISSR	Etude sur la Santé sexuelle et Reproductive des Jeunes et Adultes handicapés à Bujumbura – Burundi
HPEV	Hommes les Plus Exposées au VIH
HTTPS	HyperText Transfert Protocol Secure
MSPLS	Ministère de la Santé Publique et de la Lutte Contre le Sida
MTN	Maladies Tropicales Négligées
NEPAD	Nouveau Partenariat Africain pour l'Aide au Développement

ODD	Objectifs de Développement Durable
OMD	Objectifs du Millénaire pour le Développement
OMS	Organisation Mondiale de la Santé
ONG	Organisation Non Gouvernementale
PLACE	Priorities for Local AIDS Control Efforts
PNLS/IST/HV	Programme National de Lutte contre le SIDA/ Infections Sexuellement Transmissibles/ Hépatite Virale
PNS	Politique Nationale de Santé
RDQA	Routine Data Quality Assessment
RGPD	Règlement Général sur la Protection des Données
SIDA	Syndrome d'Immuno Déficience Acquise
SIS	Système d'Information Sanitaire
SNIS	Système National d'Information Sanitaire
SSD	Solid State Drive
TI	Technologies de l'information
TB	Tuberculose
TPB+	Tuberculose Pulmonaire Bactériologiquement Confirmée
TB/TTF	Tuberculose toute forme confondue
TB/VIH	Tuberculose/Virus d'Immunodéficience Humaine
UDI	Usagers de Drogues Injectables
USAID	United States Agency for International Development
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VIH	Virus d'Immunodéficience Humaine
VIH/SIDA	Virus de l'Immunodéficience Humaine/Syndrome d'Immunodéficience acquise
VPS	Virtual Private Servor
WHO	World Health Organization
Wi-Fi	Wireless Fidelity

GLOSSAIRE

Chiffrement

C'est l'opération qui consiste à transformer un message à transmettre, dit « message clair », en un autre message, inintelligible pour un tiers, dit « message chiffré », en vue d'assurer le secret de sa transmission. Chiffrer c'est noté le message en un code conventionnel et secret. Seul celui qui possède la clé sera en mesure de lire le message. Il est synonyme de cryptage.

Cryptage

Le cryptage en informatique est la conversion de données lisibles en un format codé illisible pour les protéger. Il utilise des algorithmes et des clés pour garantir la confidentialité, l'intégrité et la non-répudiation des données. En effet, il existe deux principaux types de cryptage : symétrique et asymétrique. Le cryptage est utilisé pour protéger les données sensibles, sécuriser les communications et authentifier les utilisateurs et les appareils. C'est un outil essentiel pour la sécurité des données informatiques.

Données personnelles sensibles

Les informations personnelles sensibles sont des données soumises à des directives de protection strictes et comprennent des détails très intimes sur des personnes, tels que leur affiliation politique, croyance religieuse, conviction philosophique, race ou l'appartenance ethnique, orientation sexuelle, données de santé, données biométriques, antécédents criminels, etc.

Hébergement dédié

L'hébergement dédié consiste à louer auprès d'un hébergeur web un serveur complet qu'il est ensuite possible de configurer selon ses besoins (choix du système d'exploitation, choix de la configuration et des applications, …)

Hébergement VPS

L'hébergement VPS (Serveur Virtuel Privé) est un système hybride à mi-chemin entre l'hébergement mutualisé et l'hébergement dédié. Le VPS consiste en effet à créer plusieurs serveurs virtuels sur un même serveur réel via des technologies logicielles de virtualisation qui peuvent être redémarrées indépendamment et évoluer sur des systèmes d'exploitation distincts.

Hébergement cloud

Contrairement à l'hébergement mutualisé, l'hébergement dédié et l'hébergement VPS, l'hébergement cloud ne repose pas sur un serveur mais sur une multitude de serveurs et le client paye pour ce qu'il utilise et permet une flexibilité accrue.

Hébergement mutualisé

L'hébergement mutualisé consiste à se partager à plusieurs un seul et même serveur.

Informations privées

Les informations privées sont définies comme toute donnée personnelle considérée comme confidentielle en raison de son caractère intime. Cela inclut les informations relatives à la santé ou à la vie sexuelle d'un individu, les dossiers médicaux, les informations financières sensibles, les mots de passe, les identifiants de connexion, les correspondances privées, etc. Il se peut qu'une personne ne puisse pas prétendre à une attente légitime de confidentialité si l'information concernée est déjà accessible au public.

Informations relatives à la santé

Les informations personnelles sur la santé sont une catégorie d'informations qui fait référence aux dossiers et aux antécédents médicaux d'un individu, qui sont protégés par la loi sur la portabilité et la responsabilité en matière d'assurance maladie. Elles comprennent principalement des ensembles d'indicateurs médicaux, tels que les résultats de tests, les diagnostics, les antécédents médicaux personnels ou familiaux, les points de données appliqués à un ensemble d'informations démographiques pour un patient particulier.

Système de santé

L'Organisation mondiale de la santé (OMS) définit les systèmes de santé comme "la totalité des organisations, institutions et ressources consacrées à la production d'actions visant principalement à améliorer, maintenir ou restaurer la santé".

PREFACE

Le présent document de politique de gouvernance des données sanitaires définit les principes, les normes et les pratiques pour la gestion efficace des données dans notre système de santé. Dans un monde de plus en plus numérisé et axé sur les données, une gouvernance solide des données est cruciale pour garantir la confidentialité, la sécurité, le partage et l'intégrité des informations sanitaires.

Cette politique reflète l'engagement du Ministère de la Santé Publique et de Lutte contre le SIDA (MSPLS) envers la performance du système d'information sanitaire, en mettant l'accent sur la protection de la vie privée des patients, la conformité aux réglementations en vigueur et l'amélioration continue des processus et des systèmes. Elle a été élaborée en tenant compte des meilleures pratiques du secteur, des recommandations des organismes de réglementation et des besoins spécifiques du MSPLS.

Nous sommes convaincus que cette politique servira de cadre solide pour tous les acteurs impliqués dans la collecte, le stockage, le traitement et l'utilisation des données sanitaires. Elle vise à garantir la qualité, l'accès, la sécurité, le partage et l'utilisation des données afin que chaque individu puisse bénéficier des avancées de la santé numérique de manière sécurisée, éthique et équitable, tout en facilitant l'accès approprié aux données pour soutenir la prise de décision clinique et l'amélioration des soins aux patients.

Nous encourageons tous les membres du personnel à lire attentivement cette politique, à en comprendre les principes et les exigences, et à les mettre en pratique dans leur travail quotidien. Ensemble, nous pouvons garantir que les données sanitaires sont gérées de manière responsable, éthique et sécurisée, dans l'intérêt supérieur de nos patients et de notre Ministère.

Nous tenons à remercier toutes les parties prenantes qui ont contribué à l'élaboration de cette politique, ainsi que celles qui s'engagent à la mettre en œuvre et à la faire respecter. Ensemble, nous pouvons maintenir des normes élevées de gouvernance des données sanitaires et fournir des soins de qualité supérieure à ceux que nous servons.

LE MINISTRE DE LA SANTÉ PUBLIQUE

ET DE LA LUTTE CONTRE SIDA

Dr Lydwine BARADAHANA

I. INTRODUCTION

I.1 CONTEXTE

L'accès à la santé et la promotion du bien-être de tous est la volonté du Gouvernement du Burundi, en témoignent les engagements pris à travers les ratifications et déclarations faites dans le cadre de la mise en œuvre des Objectifs de Développement Durable (ODD) dont la déclaration d'Astana sur les Soins de Santé Primaires durables, la Stratégie Sanitaire du Nouveau Partenariat Africain pour l'Aide au Développement (NEPAD) et le Sommet d'Abuja sur le Paludisme. Dans le cadre de la Vision 2050 de la Communauté de l'Afrique de l'Est (EAC), le Burundi s'est engagé à contribuer à l'amélioration de la nutrition, de permettre à tous de vivre en bonne santé et de promouvoir le bien-être de tous à tout âge. Depuis l'année 2014, le Burundi a initié le processus de renforcement de son système d'information sanitaire pour améliorer la collecte, l'analyse, la gestion et l'utilisation des données de santé. Cela inclut des initiatives visant à moderniser les dossiers médicaux à travers la digitalisation, mettre en place un système national de gestion de l'information sanitaire par utilisation du DHIS2 (District Health Information Software 2) et à améliorer la surveillance épidémiologique. Ainsi, la digitalisation a permis une augmentation exponentielle de la production et de l'utilisation des données sanitaires. Cette disponibilité accrue de données actualisées offre d'énormes avantages aux praticiens, aux décideurs politiques et aux personnes qui cherchent à améliorer la santé publique. En même temps, une faible gouvernance des données de santé risque d'exacerber les inégalités en matière de santé, de perpétuer les préjugés et la discrimination à l'égard des communautés marginalisées, et de porter atteinte à la santé individuelle et aux droits humains.

La vision du Burundi « **un pays émergent en 2040 et pays développé en 2060** » témoigne de la volonté du gouvernement, d'une part à concrétiser les engagements pris ; d'autre part, à améliorer les conditions de vie/bien-être et la réduction des inégalités dans la population. Pour mettre le pays sur cette nouvelle trajectoire, cette vision d'émergence sera basée sur un « Modèle de développement axé sur l'action publique, la planification et une coordination forte visant la transformation structurelle, le développement du secteur privé et l'exploitation du potentiel économique dont dispose le pays. Cette ambition implique une synergie d'actions pour augmenter les infrastructures sanitaires en vue d'une accessibilité physique facile, renforcer la chaîne d'approvisionnement des médicaments, augmenter les ressources humaines, investir dans la formation très pointue et dans les équipements de haute technologie, améliorer les capacités du système de santé afin de bien répondre aux besoins sanitaires de la population.

La politique de gouvernance des données vise à établir un cadre de travail clair et cohérent pour la gestion des données au sein d'une organisation, en garantissant leur qualité, leur protection et leur utilisation optimale, tout en respectant les exigences réglementaires en matière de protection des données.

Ainsi, dans le but de renforcer la gouvernance des données sanitaires au Burundi, le Ministère de la Santé Publique et de la Lutte contre le SIDA en collaboration avec les partenaires au développement élabore ce présent document de politique de gouvernance des données sanitaires afin de garantir une utilisation efficace et sécurisée de ces dernières.

I.2. PROFIL EPIDEMIOLOGIQUE

Le profil épidémiologique du pays reste dominé par les maladies transmissibles qui constituent les principales causes de morbi-mortalité, particulièrement chez les femmes et les enfants de moins de cinq ans. Il sied de citer notamment le paludisme, le VIH/Sida/IST, la tuberculose, les hépatites virales, les maladies tropicales négligées et les infections respiratoires aiguës (IRA). En effet, le paludisme demeure un problème majeur de santé publique et compte parmi les principales priorités nationales en matière de santé. Selon les données du SNIS, le paludisme est la première cause de morbi-mortalité avec une incidence de 503 pour 1000 habitant en 2022 [Rapport de l'Annuaire Statistique (ASS) 2023] ; il représente 46% des motifs de consultation dans les formations sanitaires (FOSA). La prévalence du paludisme chez les enfants de moins de 5 ans est passée de 17% (enquête sur les indicateurs du paludisme Burundi 2012) et elle est estimée à 27% selon les données de la troisième enquête démographique de santé du Burundi (EDSB III ,2016-2017).

La tuberculose (TB) constitue toujours un important problème de santé publique et sévit sous forme endémo-épidémique. L'incidence notifiée en 2021 est de 34 cas pour 100 000 habitants pour les TPB+ et 55 cas pour 100 000 habitants pour les TTF (annuaire statistique). La proportion de TPB+ représente 63%.
La coïnfection TB/VIH reste une préoccupation (la prévalence du VIH chez les patients tuberculeux est de 6% selon la même source).

L'infection à VIH se présente sous forme d'épidémie généralisée avec un taux de prévalence globale de 0,9% au sein de la population générale âgée de 15 à 49 ans (EDSB III 2016-2017). Selon la même source, l'épidémie à VIH a une tendance à la féminisation avec une séroprévalence 1,2% chez la femme contre

0,6% chez l'homme dans la même tranche d'âge. L'épidémie est plus concentrée en milieu urbain avec une prévalence de 2,5 % contre 0,7 % pour le milieu rural. (EDSB III 2016-2017). Malgré la séroprévalence du VIH dans la population générale de 15-49 ans soit faible (0,9%), certaines catégories de populations ont des séroprévalences relativement élevées. En effet, elle est de 7% chez les personnes vivant avec un handicap (HANDISSR 2019), 3% chez les hommes en uniforme, 3% les pêcheurs (BSS 2011) contre 0,66 % en 2022 et les prisonniers (BSS 2011).

En plus, l'analyse comparée des données de 3 catégories de populations ; les femmes les plus exposées au VIH (FPEV), les usagers de drogues injectables (UDI), les hommes les plus exposés au VIH (HPEV) de 2013 (PLACE) à 2021 (IBBS 2021) montre des prévalences plus élevées de manière disproportionnée en 2021. En effet, la prévalence chez les FPEV était de 21,30% en 2013 (PLACE), alors qu'elle est de 30,9% en 2021(IBBS 2021). La prévalence du VIH chez les UDI était de 10,2% en 2017, alors qu'elle est de 15,3% (IBBS 2021). Pour les HPEV, la prévalence était de 4,60% en 2013 (PLACE 2013) et à 5,96% en 2021 (IBBS 2021). Les hépatites virales constituent un problème de santé publique majeur dans le monde

Au Burundi, selon les estimations de l'OMS, la prévalence de l'hépatite virale B est de 2,3% dans la population générale et de 0,5% chez les personnes de moins de 5 ans et celle de l'hépatite C est plus importante de l'ordre de 3,6%.

Selon quelques études parcellaires réalisées au cours des 2 dernières décennies au niveau du pays, la prévalence de l'hépatite B oscillerait entre 5% et 10% et celle de l'hépatite C est plus importante, proche des 10% et augmente avec l'âge.

Quant à l'étude IBBS de 2021, la prévalence de l'hépatite virale B chez les consommateurs de drogues injectables est de 4,6% et celle de l'hépatite virale C est de 3,1%. Selon le rapport du PNLS/IST/HV de 2022, les données recueillies auprès du CNTS, montrent un taux de positivité de l'hépatite virale B qui s'élève à 1,9% et celui de l'hépatite virale C à 2%.

Les Maladies Tropicales Négligées dont on dispose les données épidémiologiques sont : la schistosomiase (1,13%), les helminthiases 12.5% (l'ascaridiose (8,9%), l'ankylostomiase (1,7%) et la trichocéphalose (3,9%) selon l'enquête menée par le programme en 2021-2022, le trachome et la lèpre. Pour les autres MTN (la rage, la tæniase/ la cysticercose, l'ulcère de Buruli, la Trypanosomiase humaine africaine, la gale, le pian, la filariose lymphatique, le mycétome...), les données épidémiologiques restent méconnues malgré les cas sporadiques rapportés par les FOSA.

I.3. IMPORTANCE D'UNE GOUVERNANCE DE DONNEES

La gouvernance des données est un ensemble de processus, rôles, règles, normes et métriques permettant d'assurer une utilisation efficace et efficiente des informations, dans le but d'aider les institutions à atteindre leurs objectifs. Elle définit les procédures et les responsabilités garantissant la qualité et la sécurité des données au sein d'une institution ou d'une organisation. Elle définit également qui peut effectuer quelle action, sur quelles données, dans quelle situation et selon quelle méthode. On peut citer quelques éléments d'importance de gouvernance de données :

- ✓ **Une compréhension commune des données** : la gouvernance des données offre une vue cohérente des données et une terminologie commune, tout en laissant aux unités opérationnelles la flexibilité dont elles ont besoin ;
- ✓ **Une meilleure qualité des données** : la gouvernance des données crée un plan assurant l'exactitude des données, leur exhaustivité et leur cohérence ;
- ✓ **Une carte des données** : la gouvernance des données offre une fonctionnalité avancée de compréhension de l'emplacement de toutes les données liées aux entités clés, facteur indispensable de l'intégration des données ;
- ✓ **Une conformité à tous les niveaux** : la gouvernance des données offre une plate-forme permettant de répondre aux exigences réglementaires nationales ou internationales ;
- ✓ **Une meilleure gestion des données** : la gouvernance des données apporte une dimension humaine dans ce monde des données fortement automatisé. Elle établit des codes de conduite et des bonnes pratiques en matière de gestion des données afin de répondre aux besoins et inquiétudes dans tous les domaines (données, technologies, sécurité, conformité) et autres aspects juridiques.

II. VISION ET OBJECTIFS

La vision et les objectifs de la politique de gouvernance des données sanitaires sont fondamentaux pour guider l'approche nationale de gestion des données de santé. Cette politique encapsule l'engagement du gouvernement du Burundi à utiliser la santé numérique comme catalyseur pour améliorer la santé et le bien-être de sa population. Elle reconnaît que les données sanitaires sont un élément clé de la stratégie pour atteindre la couverture sanitaire universelle et pour réduire les inégalités en matière d'accès aux soins de santé.

Cette section décrit la vision aspirante qui motive la politique et les objectifs spécifiques qui encadrent sa direction stratégique

II.1 VISION

« **Garantir la qualité, l'accès, la sécurité et l'utilisation des données afin que chaque individu puisse bénéficier des avancées de la santé numérique de manière sécurisée, éthique et équitable** ».

II.2 OBJECTIFS DE LA POLITIQUE

La politique de gouvernance des données sanitaires se fixe trois objectifs fondamentaux :

1. Confidentialité et sécurité des données sanitaires pour préserver la vie privée et la confiance des individus.
2. Utilisation des données pour informer les décisions politiques, améliorer les soins de santé, favoriser la recherche et promouvoir des interventions efficaces.
3. Accès équitable aux données et bénéfices pour toutes les populations, indépendamment de leur origine, statut socio-économique ou situation géographique.

Ces objectifs se déclinent en huit principes directeurs qui guident la gouvernance des données de santé.

1. **Qualité des données** : Assurer la collecte, le stockage et la gestion des données sanitaires de manière à garantir leur qualité, leur exactitude et leur intégrité.

2. **Interopérabilité** : Faciliter l'interopérabilité entre les différents systèmes de santé, permettant un échange efficace et sécurisé des données entre les institutions sanitaires.

3. Encourager l'innovation et **la recherche médicale** : Faciliter l'utilisation des données sanitaires pour la recherche médicale, tout en respectant les principes d'éthique et en assurant la confidentialité des patients.

4. **Faciliter le partage et l'utilisation éthique des données** : Établir des directives claires pour l'utilisation et le partage éthique des données sanitaires, équilibrant le besoin de confidentialité avec le potentiel des données pour améliorer les résultats de santé, soutenir la recherche et informer les interventions de santé publique.

5. **Sécurité des données** : Mettre en place des mesures de sécurité robustes pour protéger les données sanitaires contre les accès non autorisés, les fuites et les cybermenaces.

6. **Assurer la confidentialité et la vie privée des informations sanitaires** : Assurer la conformité aux réglementations nationales et internationales en matière de protection des données de santé. Garantir la confidentialité et protéger les informations médicales contre l'accès et l'utilisation non autorisés, en veillant à ce que seules les personnes autorisées aient accès à des données sensibles tout en respectant les droits des patients à la confidentialité et à la vie privée.

7. **Prise de Décision Informée** : Fournir des données de santé fiables et pertinentes pour soutenir la prise de décision informée au niveau des soins de santé individuels, de la gestion hospitalière et des politiques de santé publique.

8. **Collaboration Intersectorielle** : Encourager la collaboration entre les différents secteurs, y compris les secteurs publics et privés, pour maximiser l'utilisation des données sanitaires et améliorer les résultats de santé globaux. Auditer, surveiller et mettre en œuvre des mécanismes d'audit et de surveillance pour évaluer régulièrement la conformité aux politiques de gouvernance des données et identifier les domaines nécessitant des améliorations. Mettre en place des processus efficaces pour gérer le cycle de vie des données, de la collecte à l'archivage, en passant par la mise à jour et la suppression.

Source : *Gouvernance des données en santé, Transform Health, 2022*

III. PORTÉE DE LA POLITIQUE DE GOUVERNANCE DES DONNEES

Tous les intervenants dans le système de santé au Burundi ont la responsabilité de prendre soins des données générées par le MSPLS, de respecter cette politique et toutes les lois applicables en matière de protection de données personnelles.

III.1. TYPES DE DONNEES SANITAIRES COUVERTS

Cette politique s'applique à toutes les données de santé collectées, traitées, générées, stockées, transmises et partagées au sein du système de santé du Burundi. Cela inclut, sans s'y limiter, les données générées par les établissements sanitaires, les données de recherche liées à la santé ainsi que les données collectées par des applications et des dispositifs de santé numérique.

La définition des types de données couverts par cette politique se trouve en ***annexe 1.***

III.2. ENTITES ET PARTIES PRENANTES IMPLIQUEES DANS LA POLITIQUE DE GOUVERNANCE DES DONNEES

La gouvernance des données sanitaires implique une variété d'entités et de parties prenantes, chacune jouant un rôle spécifique dans la gestion, la protection et l'utilisation des données. Toutes les parties prenantes intervenant dans le domaine de la santé à tous les niveaux sont concernées par cette politique de gouvernance des données.

Une liste non exhaustive d'entités et des parties prenantes est présentée en ***annexe 2.***

IV. CADRE DE GOUVERNANCE DES DONNÉES SANITAIRES

Le cadre de gouvernance des données définit les rôles et responsabilités stratégiques, tactiques et opérationnels en matière de processus, gestion, analyse et utilisation des données au sein du MSPLS selon les niveaux de la pyramide sanitaire. Ces niveaux sont reliés entre eux par des relations de fonctionnement hiérarchique.

1. Le niveau central : le niveau central comprend le Cabinet du Ministre, le Secrétariat Permanent, le Secrétariat Exécutif Permanent du Conseil National de Lutte contre le SIDA, l'Inspection Générale de la Santé Publique et de la Lutte contre le Sida, quatre Directions Générales centrales (Services de Santé, Ressources, Planification et Offre des soins). En outre, il comprend 4 Directions Générales à gestion personnalisées, les programmes nationaux intégrés de santé, les administrations personnalisées de l'Etat et les hôpitaux nationaux.

2. Le niveau intermédiaire : le niveau intermédiaire est un niveau déconcentré du Ministère. Il comprend 18 Bureaux Provinciaux de Santé (BPS) qui ont pour mission de veiller à la mise en œuvre de la politique sanitaire dans leur zone de responsabilité.

3. Le niveau périphérique : le niveau périphérique est composé de 49 districts sanitaires autour desquels gravitent des hôpitaux et les CDS et constitue le niveau opérationnel du système de santé. Il a le rôle de coordonner l'action sanitaire et d'encadrer les activités communautaires.

4. Le niveau communautaire : le volet communautaire comprend les relais communautaires qui sont les associations locales, les agents de santé communautaire, les comités de santé, les accoucheuses traditionnelles et les guérisseurs traditionnels, etc. Ces relais ont pour rôle d'assurer certaines prestations au niveau communautaire et servent de pont entre la communauté et le centre de santé. De façon opérationnelle, les prestations offertes au niveau communautaire sont sous la responsabilité du Centre de Santé.

Le cadre définit la politique pour la collecte des données, le circuit, la sécurité et le partage de l'information ainsi que les ressources nécessaires pour le fonctionnement du système d'information aux différents niveaux du système de santé.

IV.1. **POLITIQUES RELATIVES A LA GESTION ET LA QUALITE DES DONNEES SANITAIRES**

IV.1.1 COLLECTE ET SAISIE DES DONNEES

De la provenance des données

Les données sanitaires proviennent du recueil quotidien (au niveau de la communauté et des formations sanitaires) et des études et enquêtes. La collecte des données des événements inhabituels est définie par le COUSP.

Des outils de collecte des données

Les outils de collecte des données dont dispose le système national d'information sanitaire sont de trois types :

- ✓ Les outils pour la collecte des données individuelles. Il s'agit des registres primaires d'enregistrement des patients et les fiches de stocks des intrants ;
- ✓ Les outils pour la collecte des données agrégées. Il s'agit des canevas de rapport et des fiches de pointage standards ;
- ✓ Les outils électroniques de gestion du patient, de rapportage ou de traitement des données.

Les registres individuels et les canevas de rapports standards sont conçus en fonction des services offerts à chaque niveau de pyramide sanitaire.

IV.1.2 DE L'ENREGISTREMENT DES DONNEES.

- ✓ Les données des FOSA digitalisées doivent être collectées via les registres électroniques. Les rapports agrégés devraient être générés automatiquement par l'outil électronique utilisé et transférés automatiquement dans la plateforme nationale DHIS2.
- ✓ Pour les FOSA non-digitalisées, les données collectées via les registres physiques standardisés dans les différents services doivent être consignées dans un rapport journalier, hebdomadaire, mensuel, trimestriel, semestriel ou annuel.
- ✓ Le responsable de la FOSA a la responsabilité d'organiser des réunions mensuelles avec les prestataires de service et le chargé du SIS pour vérifier la qualité du remplissage des outils de collecte. Pendant la réunion, il procède à la vérification de la complétude des registres, des fiches de collecte des données. Le chargé du SIS fournit également une orientation et veille au respect des directives pour le remplissage correct des outils.

IV.1.3. DE L'ANALYSE DES DONNEES, PARTAGE ET TRANSMISSION DU RAPPORT

Les données sur les maladies à potentiel épidémique et les évènements de santé publique sont analysés et transmis dans DHIS2 à un rythme journalier. Les données de routine rapportées sont analysées sur un rythme mensuel à travers le DHIS2 et se fait en équipe en utilisant les rapports papiers pour les formations sanitaires non digitalisées. Pour ces dernières, un exemplaire du rapport est systématiquement rempli et photocopié : une copie est transmise au niveau supérieur, l'originale est gardée et classée. Ces rapports seront rassemblés dans un classeur annuel.

IV.2. DE L'ASSURANCE QUALITE DES DONNEES

La qualité des données comprend tous les éléments d'une bonne information qui influent sur la prise de décision aux besoins des décideurs et des autres utilisateurs. La qualité des données est constituée des dimensions suivantes : l'intégrité, la complétude, la cohérence, l'exactitude, la rapidité de transmission et d'accessibilité à temps réel des données (promptitude), la possibilité d'agrégation des données et de l'interprétation de l'information, la traçabilité, la sécurité et la confidentialité des données. (*Définition des dimensions de la qualité des données en* ***annexe 3***).

Le personnel impliqué dans la gestion des données doit évaluer la qualité des données sur une base trimestrielle en utilisant les outils destinés à cet effet tels que WHO Data Quality Tool, RDQA Tool, DQA Tool, ...

IV.3 POLITIQUES RELATIVES A LA SECURITE, LA CONFIDENTIALITE ET LE PARTAGE DES DONNEES

IV.3.1 DE LA SECURITE DES DONNEES NUMERIQUES

La sécurité des données consiste à protéger les informations numériques contre tout accès non autorisé, toute corruption ou tout vol le long de leur cycle de vie. Les données doivent être sécurisées selon les réglementations nationales et internationales.

En effet :

- ✓ L'accès aux données sera réservé aux utilisateurs autorisés avec des privilèges appropriés (lecture seule, insertion, modification / suppression), des mécanismes garantissant l'intégrité des données concernant l'exploitation, le stockage, l'archivage, le codage et les transmissions

de données en empêchant les manipulations non autorisées ou malveillantes ainsi que les défaillances technologiques.

- ✓ Tous les appareils informatiques connectés au réseau de l'institution doivent exécuter un antivirus à jour conformément aux normes de l'institution ou doivent être protégés par d'autres moyens appropriés. Pour ce qui est des antivirus, les paramètres ne doivent pas être modifiés d'une manière qui réduit l'efficacité du logiciel. Au fait, le paramétrage par défaut du logiciel garantit un très bon niveau de sécurité ; cependant les paramètres avancés de ces logiciels favorisent une protection optimale en fonction de certains besoins spécifiques.

IV.3.2 DE LA CONFIDENTIALITE DES DONNEES

La confidentialité des données est un processus qui consiste à :

- ✓ Ne pas divulguer à des personnes non expressément autorisées à les recevoir ;
- ✓ Ne pas utiliser les données qu'à des fins prévues par les attributions de l'utilisateur ;
- ✓ Prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité matérielle des données.

Ainsi, la notion de confidentialité utilise les mécanismes de la sécurité des données et de la traçabilité des données. Il est donc indispensable de définir au préalable avant le déploiement de toute application exploitant des données, les principes de confidentialité à appliquer par rapport aux données manipulées. De plus, tout individu ayant accès aux données confidentielles doit respecter les principes de confidentialité et d'éthique professionnelle.

Cette procédure est applicable à toutes les institutions sanitaires du pays. Elle sera appliquée par tous les prestataires au niveau de la FOSA. Elle sera communiquée à tout nouveau staff avant de lui donner accès aux dossiers des patients. Une version signée sera gardée dans le dossier du personnel afin d'attester que celui-ci en a été informé.

IV.3.3 DU STOCKAGE ET ACCESSIBILITE DES DONNEES

Le stockage des données est le processus de conservation des informations d'une manière qui permet de les récupérer, de les traiter et de les analyser ultérieurement. Il fait généralement appel à des supports numériques ou physiques tels que des disques durs, SSD ou des serveurs.

Tous les documents contenant des informations sur les patients (dossiers patient, données de laboratoire, registres, cahiers ou formes de compilation, Quick soft, OpenClinic, SIDA Info et autres outils

électroniques…) doivent être conservés dans un endroit sûr, accessible uniquement au personnel autorisé et fermé à clé en dehors des heures de service.

Toutes les bases de données et outils électroniques contenant des données de patients doivent être protégées par des mots de passe.

Le serveur qui héberge la base de données doit également faire l'objet de mesures de sécurité (physique et électronique). Les outils électroniques de collecte de données tels que : Quick Soft Application, OpenClinic, SIDAInfo, … doivent créer leurs backups automatiques sur une base journalière et les encrypter avec un mot de passe. De plus, ces outils électroniques doivent avoir un système de gestion des utilisateurs qui force ces derniers à s'authentifier avant d'accéder aux données.
Chaque membre du personnel devant avoir accès aux données stockées sur Quick Soft Application, OpenClinic, SIDAInfo, DHIS2 et autres systèmes, doit avoir un compte d'accès *(nom d'utilisateur et un mot de passe personnalisé*). Ce compte sera désactivé au cas où cette personne ne serait plus affiliée à l'institution, ou quand ses fonctions ne nécessiteraient plus l'accès aux dossiers des patients**.** Cette désactivation sera documentée et datée dans la liste tenue mensuellement par l'administrateur du système au niveau de la formation sanitaire.
Tous les ordinateurs ayant les dossiers des patients doivent être dotés d'un antivirus à jour et de système de détection d'intrusion et ils doivent être protégés par des mots de passe.
Ces ordinateurs seront programmés pour passer en mode « veille » après cinq minutes de temps d'inactivité.
Les ordinateurs seront placés de façon que les écrans ne puissent pas être vus par les personnes non autorisées.

IV.3.4 DE L'ACCES ET STOCKAGE DES DONNEES DE RECHERCHE

Les données de recherche seront mises à disposition publique lorsque cela est possible et approprié tout en respectant les principes de confidentialité et d'éthique.
La création de portails en ligne dédiés permettra de faciliter l'accès aux données de recherche pour les chercheurs, les praticiens de la santé et les décideurs. Ces portails devront être conçus de manière à garantir la sécurité et la confidentialité des données.

IV.3.5 DE LA SAUVEGARDE DE DONNEES (BACKUP)

La stratégie de sauvegarde 3-2-1 doit être adoptée pour toutes les données de santé. Cette stratégie met l'accent sur la redondance et la protection contre les scénarii potentiels de perte de données. Une description de cette stratégie est présentée comme ci-après :

3 copies : Conserver au moins trois copies des données. Les copies originales sur l'appareil principal, deux copies de sauvegarde supplémentaires sur différents types de supports ;

2 types de supports différents : Stocker les copies de sauvegarde sur deux types de supports différents pour atténuer les risques liés aux points de défaillance uniques ;

1 copie hors site : Conserver une copie des données hors site dans un emplacement physiquement séparé. Cela protège les données contre des événements tels que des catastrophes naturelles qui pourraient affecter l'emplacement principal.

IV.3.6 DU CLASSEMENT DES DOSSIERS MEDICAUX ET DES REGISTRES PHYSIQUES (GESTION DES ARCHIVES)

Les dossiers doivent être classés soit par :

- ✓ *Ordre alphabétique* selon le nom : La classification des dossiers par ordre alphabétique est simple et nécessite peu de formations. Ce procédé est utilisé par beaucoup d'établissements sanitaires surtout quand le nombre de patients vus au cours de l'année n'est pas élevé ;

- ✓ *Numéro* : Dans la classification numérique, chaque personne reçoit un numéro unique qui l'identifie et les dossiers sont classés selon la séquence numérique. Toutes les composantes du dossier reçoivent le même numéro et sont plus facilement regroupées. Il permet une extension plus facile et plus rapide. Cependant, cette méthode requiert un index pour retrouver les dossiers quand la personne ne revient pas avec la carte portant son numéro ;

- ✓ *Famille* : Tous les dossiers des membres d'une même famille sont regroupés ensemble. Cela permet à la personne qui fournit les soins de penser et de questionner sur l'état de santé des autres membres de la famille ;

- ✓ *Ordre chronologique* : La classification chronologique se fait par date selon l'ordre d'arrivée des dossiers. Il est facile à utiliser puisqu'il ne nécessite pas de formations spéciales pour le

personnel qui doit avoir la date de classement pour retrouver rapidement un dossier. Cette méthode est surtout utilisée pour le classement temporaire des dossiers médicaux.

Quelle que soit la méthode choisie par une institution, l'important est que l'on puisse retrouver un dossier en moins de cinq minutes.

De plus, il faut bien conserver les registres car ils contiennent des informations très utiles sur l'état de santé de la population desservie par l'établissement. Les registres remplis seront gardés dans un endroit sec, à l'abri des intempéries et sous clé. Voir **annexe 5** pour plus de détails.

IV.3.7 DE LA DUREE DE CONSERVATION DES DOSSIERS MEDICAUX

L'Organisation Mondiale de la Santé (OMS) n'a pas établi de norme universelle sur la durée de conservation des dossiers médicaux. Cependant, Les dossiers médicaux doivent être conservés aussi longtemps que nécessaire pour assurer la continuité des soins, la recherche, l'enseignement, la planification, l'évaluation et la gestion des services de santé.

Au Burundi, à partir des bureaux de chaque niveau du système sanitaire, l'archivage sera fait sur les outils informatiques (disque dur externe, petit serveur et autres supports de sauvegarde).

Un espace d'archivage et de documentation doit être installé dans les établissements sanitaires pour la conservation des dossiers médicaux et fiches remplis. Les dossiers médicaux et les fiches seront conservés pour une durée de 20 ans à compter à partir de la dernière information enregistrée dans le dossier ; ces délais (y compris le délai de 20 ans) constituent des durées minimales. Chaque établissement sanitaire peut élaborer une politique de conservation plus contraignante en fonction des pathologies concernées.

Quand ces délais sont atteints, la décision de destruction du dossier médical est prise par le Directeur de l'établissement sanitaire et Conseil de direction après avis de l'autorité hiérarchique.

IV.4. POLITIQUE RELATIVE A LA PROTECTION DES DONNEES PERSONNELLES

Les informations personnelles se réfèrent aux :

- ✓ Informations qui peuvent être utilisées pour distinguer ou retracer l'identité d'une personne, telles que son nom, son numéro de sécurité sociale, ses données biométriques, etc., seules ou combinées à d'autres informations personnelles comme la date et le lieu de naissance ;

- ✓ Autres informations pouvant être liées à un individu, comme les informations médicales, éducatives, financières et d'emploi.

Tout intervenant dans le système de santé doit respecter les 5 principes de protection des données personnelles ci-après :

- ✓ Le principe **de finalité** : le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime ;
- ✓ Le principe **de proportionnalité et de pertinence** : les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier ;
- ✓ Le principe d'une **durée de conservation limitée** : il n'est pas possible de conserver des informations des personnes physiques dans un fichier pour une durée indéfinie. Une durée de conservation précise doit être fixée en fonction du type d'information enregistrée et de la finalité du fichier ;
- ✓ Le principe de **sécurité et de confidentialité** : le responsable du fichier doit garantir la sécurité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations ;
- ✓ Le principe du respect des **droits de la personne.**

IV.5 POLITIQUE RELATIVE A L'HEBERGEMENT ET LA GESTION DES SERVEURS

Dans le contexte de la digitalisation croissante des services de santé, le MSPLS reconnaît l'importance fondamentale de l'hébergement sécurisé et efficace des données de santé. Cette section présente les directives strictes et les standards requis pour les environnements d'hébergement des serveurs, afin de garantir la protection, la confidentialité et l'intégrité des données de santé des citoyens.

IV.5.1 DU CHOIX DE L'ENVIRONNEMENT D'HEBERGEMENT

Le MSPLS donne la priorité à l'hébergement sur site ou à l'utilisation de serveurs dédiés pour les données et les applications informatiques de santé. Les systèmes d'information de santé doivent être hébergés préférentiellement sur des serveurs dédiés ou des environnements cloud national, afin de minimiser les

risques de sécurité et d'assurer un contrôle complet sur les ressources et les données. Cette approche offre un meilleur contrôle sur la sécurité physique et logique, l'accès au réseau et les pratiques de gestion des données.

L'hébergement partagé est fortement déconseillé pour les données sensibles ou critiques. Dans des cas exceptionnels où l'hébergement partagé est utilisé, des mesures de sécurité renforcées doivent être mises en place.

IV.5.2 DE LA CONFORMITE REGLEMENTAIRE

Tous les environnements d'hébergement doivent se conformer aux législations nationales et aux standards internationaux en matière de protection des données de santé.

IV.5.3 DE LA GESTION DES ACCES

L'accès aux données hébergées doit être strictement contrôlé et limité au personnel autorisé, avec une authentification forte et un enregistrement détaillé de ces accès.

IV.5.4 PLAN DE CONTINUITE D'ACTIVITE ET DE RECUPERATION APRES SINISTRE

Un plan de continuité d'activité doit être mis en place, assurant la disponibilité continue des services de santé en cas d'incident affectant l'environnement d'hébergement.

Des stratégies de sauvegarde régulières et des plans de récupération après sinistre sont requis pour garantir la restauration rapide des données en cas de perte ou d'endommagement.

IV.5.5 DU SUIVI ET EVALUATION CONTINUE

Un suivi continu de la performance et de la sécurité des environnements d'hébergement doit être mise en œuvre, avec des rapports périodiques pour évaluer la conformité aux directives établies. Les rétro-informations des utilisateurs et les analyses de tendances technologiques doivent être régulièrement recueillis pour informer les mises à jour de la politique d'hébergement.

IV.6 POLITIQUES RELATIVES AU PARTAGE DES DONNEES

Les données doivent être partagées dans un but bien précis dans le respect des lois nationales (recherche, analyse, audit, …). Ce partage sera autorisé par la direction de l'établissement sanitaire.

La quantité et la nature des données partagées seront toujours le strict minimum nécessaire :

- ✓ Les données qui seront transmises sur un support portable (Laptop, External Drive, Flash Drive, cellulaire…) ou par voie électronique devront être agrégées, anonymisées et/ou encryptées ;

- ✓ Pour rendre les données anonymes, toutes les variables relatives aux données personnelles seront encodées ou encryptées de façon irréversible;
- ✓ Au cas où les données protégées par les mots de passe seront partagées par courriel, le mot de passe ne sera pas partagé par mail ;
- ✓ Des audits mensuels sur des ordinateurs choisis au hasard permettront de supprimer au besoin les fichiers avec des données de patients qui ne sont plus utiles ou nécessaires ;
- ✓ Un registre devra être tenu dans chaque établissement sanitaire pour documenter les partages de données effectuées, incluant la date, le destinataire, la nature des données partagées et le but (Voir l'**annexe 6).**

IV.7 POLITIQUE RELATIVE A L'INTEROPERABILITE DES SYSTEMES

L'interopérabilité fait référence à la capacité de différents systèmes d'information, appareils et applications d'accéder, d'échanger, d'intégrer et d'utiliser de manière coordonnée des données, à travers de multiples organisations, environnements et localisations géographiques, afin de fournir des services rapides et transparents.

Dans le contexte des données de santé, l'interopérabilité permet le partage sécurisé et efficace des dossiers électroniques, des résultats de laboratoire, des images diagnostiques et d'autres données liées à la santé entre les professionnels de santé autorisés, les patients et les parties prenantes concernées, y compris les entités non liées aux soins de santé dans des circonstances spécifiques.

IV.7.1 DES NORMES D'INTEROPERABILITE

IV.7.1.1 DE LA NORMALISATION

Le MSPLS adopte des normes mondiales reconnues, telles que FHIR, HL7, CDA et CIM-10/11 comme base pour une représentation et une communication cohérente des données entre les différents systèmes. Les systèmes informatiques de santé utilisés dans le pays doivent se conformer à ces normes internationales d'interopérabilité pour assurer une base commune d'échange de données. Ils doivent aussi mettre en œuvre des protocoles de sécurité robustes pour la protection des données échangées, conformément aux lois nationales et internationales sur la protection des données.

IV.7.1.2 DE L'HARMONISATION DES DONNEES

En collaboration avec les parties prenantes, le MSPLS élaborera et mettra en œuvre des dictionnaires et vocabulaires nationaux de données afin de garantir une terminologie cohérente et de minimiser l'ambiguïté dans les données échangées.

IV.7.1.3 DES SPECIFICATIONS TECHNIQUES

Des spécifications techniques relatives à la sécurité des données, à la confidentialité et aux protocoles d'authentification doivent être établies pour garantir un échange sûr et fiable des données de santé.

IV.7.1.4 DE L'OUVERTURE ET LA TRANSPARENCE

Le MSPLS privilégie les API ouvertes et les solutions open-source pour une large accessibilité et une intégration au sein de l'établissement de santé, favorisant l'innovation et la concurrence.

IV.7.2 DE LA PLATEFORME D'INTEROPERABILITE DES SYSTEMES

Pour renforcer l'efficacité et la cohérence des systèmes, le MSPLS développera une plateforme d'interopérabilité centralisée. Cette plateforme facilitera l'échange sécurisé et efficace de données entre différentes applications et plateformes de collecte, de rapportage et de gestion des données sanitaires.

IV.7.3 DE L'ECHANGE DE DONNEES SANITAIRES AVEC LES AUTRES SECTEURS

Dans le contexte de l'interopérabilité des systèmes au Burundi, il est essentiel de reconnaître et de réguler l'échange de données entre le secteur de la santé et les autres secteurs. Ces échanges doivent être gérés avec une attention particulière à la sécurité, à la confidentialité et à l'intégrité des données.

IV.7.4 ECHANGE DE DONNEES POUR LES BESOINS ADMINISTRATIFS ET FISCAUX

Les applications informatiques de santé doivent être configurées pour transmettre automatiquement les informations relatives aux factures aux autres entités conformément aux exigences légales et réglementaires en vigueur. Cet échange doit se limiter aux données nécessaires aux fins de conformité fiscale et administrative excluant toute information d'identification personnelle des patients, sauf dans des circonstances légalement justifiées et avec des garanties de confidentialité appropriées.

IV.8 POLITIQUE RELATIVE A LA CYBERSECURITE

La cybersécurité est un ensemble de processus, d'outils et de cadres visant à protéger les réseaux, les appareils, les programmes et les données des cyberattaques. Les cybercriminels lancent de telles attaques pour pirater le système informatique et obtenir un accès non autorisé à des systèmes informatiques, interrompre des opérations des institutions, modifier, manipuler ou voler des données ou réaliser de l'espionnage.

Toute entité intervenant dans le domaine de la santé numérique doit protéger les systèmes informatiques du piratage ou des cyberattaques en appliquant les principes fondamentaux de la cybersécurité (*prévention, détection, réaction, sensibilisation et gouvernance*).

V. MÉCANISME DE SUIVI ET ÉVALUATION DE LA POLITIQUE DE GOUVERNANCE DES DONNÉES SANITAIRES

Dans le but d'assurer le suivi et l'évaluation de la mise en œuvre de cette politique de gouvernance des données sanitaires, une approche axée sur les résultats s'avère indispensable. Les lignes qui suivent décrivent les aspects fonctionnels et organisationnels à prendre en compte dans le cadre du suivi-évaluation de la mise en œuvre de la politique de gouvernance des données à tous les niveaux de la pyramide sanitaire du Burundi. En effet, le système de suivi-évaluation devra à terme permettre au MSPLS de :

- ✓ Mesurer l'état d'avancement de la mise en œuvre de la politique de gouvernance des données afin de prendre des décisions conséquentes ;
- ✓ Partager les expériences et valoriser les bonnes pratiques en matière de gouvernance des données sanitaires dans le but d'améliorer les actions futures ;
- ✓ Disposer à temps des informations sur les performances de la mise en œuvre de la politique de gouvernance des données.

L'opérationnalisation du système de suivi et évaluation comprendra la mise en place d'un système de collecte de données à tous les niveaux de la pyramide sanitaire ainsi qu'un système de diffusion et de partage des informations sur la mise en œuvre de la présente politique.

V.1. ROLES DES PARTIES PRENANTES AU SYSTEME DE SUIVI-EVALUATION

Les principaux acteurs impliqués dans le système de suivi-évaluation et leurs rôles sont les suivants :

- ✓ **Responsables au niveau central :** Pilotage, collecte, documentation des indicateurs et transfert d'information vers les décideurs ;
- ✓ **Sous-groupe thématique « Digitalisation » :** proposition de décisions et transfert des informations aux directions ;
- ✓ **Le chargé du SIS à tous les niveaux :** collecte de données, transmission et partage des informations sur la mise en œuvre de la politique.

V.2. INDICATEURS DE PERFORMANCE

Les indicateurs de performance retenus pour évaluer l'efficacité de la politique de gouvernance des données sont définis ci-après :

1. **Proportion d'adoption des normes de gouvernance des données** : Mesure le pourcentage d'entités et de directions du MSPLS qui ont adopté les normes et les meilleures pratiques de gouvernance des données recommandées par la politique.

2. **Conformité réglementaire** : Évalue le degré de conformité des entités et de directions du MSPLS aux lois et réglementations nationales et internationales en matière de protection des données.

3. **Sécurité des données** : Mesure le nombre d'incidents de sécurité des données et leur gravité pour évaluer l'efficacité des mesures de sécurité mises en place.

4. **Qualité des données** : Evalue la précision, la cohérence et l'exhaustivité des données collectées et gérées par les entités et de directions du MSPLS.

5. **Transparence et accès aux données** : Mesure la facilité avec laquelle les données sont accessibles au public et la transparence des processus de collecte.

6. **Engagement des parties prenantes** : Evalue le degré d'engagement, de satisfaction et de collaboration des parties prenantes dans le processus de gouvernance des données.

7. **Efficacité opérationnelle** : Evalue l'impact de la politique de gouvernance des données sur l'efficacité opérationnelle des entités et des directions du MSPLS, y compris la réduction des coûts, l'amélioration de la productivité et la prise de décision plus éclairée.

8. **Innovation et utilisation des données** : Mesure le niveau d'innovation et d'utilisation des données pour favoriser l'innovation technologique et améliorer les services de santé.

9. **Confiance des décideurs et autres parties prenantes** : Evalue le niveau de confiance des décideurs et parties prenantes dans la manière dont les données sont gérées et utilisées par les entités du MSPLS.

10. **Impact social et économique** : Evalue l'impact global de la politique de gouvernance des données sur la société et l'économie, y compris son rôle dans la promotion de l'inclusion sociale, de l'équité et du développement durable.

La combinaison de ces métriques permettra d'évaluer de manière holistique l'efficacité de la politique de gouvernance des données.

V.3. FREQUENCE D'EVALUATION DE LA POLITIQUE DE GOUVERNANCE DES DONNEES

La fréquence d'évaluation de cette politique de gouvernance des données sera déterminée en tenant compte de plusieurs facteurs clés :

- ✓ **Maturité de la politique et des processus** : Si la politique et les processus de gouvernance des données sont bien établis et matures, des évaluations moins fréquentes peuvent être appropriées. Il est utile d'effectuer des suivis périodiques tous les six mois, surtout au début de la mise en œuvre de la politique, pour s'assurer qu'elle fonctionne comme prévu et pour identifier rapidement les ajustements nécessaires. Par la suite, une évaluation annuelle sera suffisante, à moins qu'il n'y ait des événements particuliers comme des incidents de sécurité des données ou des changements majeurs dans l'environnement réglementaire ou technologique, qui pourraient nécessiter une évaluation plus fréquente.

- ✓ **Complexité du paysage des données** : Si le paysage des données est complexe, en constante évolution ou sujet à des changements rapides, des évaluations plus fréquentes seront nécessaires pour garantir que la politique reste efficace et pertinente.

- ✓ **Évolution de la réglementation** : Si les réglementations liées à la protection des données ou à d'autres aspects de la gouvernance des données sont sujettes à des changements fréquents, cela nécessitera des évaluations plus fréquentes pour assurer la conformité continue.

- ✓ **Incidents de sécurité des données ou non-conformité** : Tout incident de sécurité des données majeur ou toute non-conformité significative nécessitera une évaluation immédiate de la politique pour identifier les lacunes et mettre en œuvre des mesures correctives.

- ✓ **Demandes des parties prenantes et des intervenants clés** : Les demandes des parties prenantes internes et externes pourront influencer la fréquence des évaluations si elles expriment des préoccupations ou des besoins spécifiques.

V.4. RETRO INFORMATION

Des mécanismes de rétro information sont essentiels pour garantir l'efficacité continue et l'adaptation aux besoins changeants d'une politique de gouvernance des données.

Voici quelques mécanismes de rétroaction les plus couramment utilisés :

- ✓ **Système de signalement des problèmes** : Mettre en place un système permettant aux utilisateurs de signaler les problèmes liés à la gouvernance des données, tels que des erreurs de données, des lacunes dans la sécurité ou des préoccupations concernant la confidentialité.

- ✓ **Revues régulières** : Réaliser des revues régulières de la conformité aux politiques et aux normes de gouvernance des données, ainsi que des examens de la qualité des données pour identifier les problèmes et les opportunités d'amélioration.

- ✓ **Enquêtes auprès des parties prenantes** : Collecter des commentaires auprès des parties prenantes internes et externes, y compris les utilisateurs et les partenaires, sur leur expérience avec la gouvernance des données et sur les domaines à améliorer.

- ✓ **Tableaux de bord de suivi des performances** : Mettre en place des tableaux de bord pour assurer le suivi des performances des indicateurs clés de la gouvernance des données.

- ✓ **Formation et sensibilisation** : Organiser des sessions de formation et de sensibilisation pour les utilisateurs sur les politiques et les meilleures pratiques de gouvernance des données.

En intégrant ces mécanismes de rétroaction dans le cadre de la politique de gouvernance des données, le MSPLS s'assurera d'une gestion efficace et évolutive des données sanitaires, tout en répondant aux besoins changeants et aux défis émergents.

VI. CONCLUSION

La politique de gouvernance de données en santé 2024-2027 est l'aboutissement d'un travail collectif de l'ensemble des acteurs impliqués dans le système d'information sanitaire au Burundi. Elle prend en compte les acquis et les projections en matière de digitalisation et propose des normes politiques de référence dans l'élaboration des procédures opérationnelles standards. Un plan de mise en œuvre de cette politique qui sera élaboré précisera les actions concrètes pour suivre les indicateurs de performance objectivement vérifiables de cette politique de gouvernance de données sanitaires.

VII. REFERENCES BIBLIOGRAPHIQUES

1. La sécurité des données personnelles, les guides de la CNIL - Édition 2018 https://www.techopedia.com/definition/14221/personal-health-information-phi
2. Le règlement général sur la protection des données – RGPD 24 mai 2016
3. https://piwikpro.fr/blog/quest-ce-que-les-pii/
4. https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi https://www.ibm.com/fr-fr/topics/pii
5. https://www.hayesconnor.co.uk/news-resources/news/what-is-misuse-of-private-information/
6. https://www.ibm.com/fr-fr/topics/cybersecurity
7. Loi n° 1 /10 du 16 mars 2022 portant prévention et répression de la cybercriminalité au Burundi
8. https://www.talend.com/fr/resources/guide-gouvernance-données
9. PNS 2023-2027
10. Vision 2040-2060
11. Etude prévalence VIH, des Hépatites virales B et C des personnes travaillant dans la communauté des pêcheurs sur le littoral le Lac TANGANYIKA au BURUNDI

VIII. ANNEXES

Annexe 1 : Types de données couverts par la politique de gouvernance des données

Types de données	Description
Données Personnelles de Santé	Données d'identification personnelle telles que le nom, le prénom, la date de naissance, l'adresse, etc.
Antécédents Médicaux	Informations sur les conditions médicales passées, les traitements, les traitements, les diagnostics, les interventions chirurgicales antérieures, les allergies, etc.
Données Biométriques	Mesures physiques telles que la pression artérielle, la fréquence cardiaque, la taille, le poids, etc.
Résultats de Tests Médicaux	Résultats de tests de laboratoire, d'imagerie médicale, de tests de diagnostic, etc.
Prescriptions et médicaments	Informations sur les prescriptions médicales, les médicaments prescrits, les doses, les instructions d'utilisation, etc.
Données génétiques	Informations liées au code génétique d'un individu, souvent utilisées dans le contexte de la génomique médicale.
Données de soins infirmiers	Informations sur les soins infirmiers, les suivis médicaux, les vaccinations, etc.
Données d'assurance santé	Informations relatives à la couverture d'assurance santé, aux réclamations, aux paiements, etc.
Données administratives et démographiques	Informations administratives sur les patients, y compris les données démographiques, l'histoire des visites médicales, etc.
Données de télémédecine	Informations générées à partir de consultations médicales à distance, comprenant des données audio, vidéo et autres données électroniques.
Données de recherche médicale	Informations utilisées dans le cadre de projets de recherche médicale, y compris les données épidémiologiques, les données cliniques, etc.
Données de santé mentale et infantile	Informations sur la santé mentale et infantile, les diagnostics psychiatriques, les traitements, etc.
Données de santé publique	Informations utilisées pour surveiller et contrôler les maladies au niveau de la population, les statistiques épidémiologiques, etc.
Données liées à la sécurité des patients	Informations sur les incidents de sécurité des patients, les erreurs médicales, les réclamations, etc.
Données de formation sanitaire	Informations liées à la formation sanitaire, aux certifications, aux compétences, etc.

Annexe 2 : Principales entités et parties prenantes impliquées dans la gouvernance des données sanitaires.

Structures sanitaires : Les hôpitaux, les cliniques, les laboratoires et autres institutions de santé sont directement impliqués dans la collecte, le stockage et l'utilisation des données sanitaires.

Professionnels de la santé : Les médecins, les infirmiers, les pharmaciens et d'autres professionnels de la santé sont des acteurs clés dans la gestion quotidienne des données de santé, fournissant des informations et accédant aux dossiers médicaux.

Responsables informatiques : Les départements informatiques ont la responsabilité de mettre en œuvre et de maintenir les systèmes d'information de santé, en veillant à leur sécurité, à leur intégrité et à leur disponibilité. Ces professionnels sont chargés de garantir la confidentialité des données de santé et de mettre en place des mesures de sécurité appropriées pour protéger les informations sensibles.

Gestionnaires de données : Les responsables de la gestion des données sont chargés de superviser les politiques et les procédures de gestion des données, de garantir leur conformité et de mettre en œuvre les meilleures pratiques.

Patients et public : Les patients et le public ont un intérêt direct dans la gestion transparente, éthique et sécurisée de leurs propres données de santé. Ils sont également impliqués dans la prise de décisions concernant l'utilisation de leurs informations.

Autorités sanitaires : Les agences gouvernementales de santé publique peuvent être impliquées dans la collecte et l'analyse de données à l'échelle de la population, ainsi que dans la formulation de politiques basées sur ces données.

Organismes de recherche en santé : Les institutions de recherche médicale peuvent utiliser des données sanitaires dans le cadre de projets de recherche, avec la nécessité de respecter des protocoles éthiques stricts.

Fournisseurs de technologies de l'information (TI) : Les entreprises fournissant des solutions technologiques, telles que des systèmes d'information médicale, sont des parties prenantes importantes pour assurer la fonctionnalité et la sécurité des outils utilisés.

Assureurs et organismes de gestion des réclamations (les courtiers) : Les compagnies d'assurance et les organismes de gestion des réclamations peuvent utiliser des données sanitaires pour évaluer les risques, gérer les réclamations et établir des politiques.

Éducateurs en santé : Les éducateurs en santé peuvent utiliser des données sanitaires dans le cadre de programmes de sensibilisation et d'éducation, contribuant à des pratiques de santé plus informées.

Gouvernement : Le gouvernement peut jouer un rôle dans la création de politiques et de réglementations globales en matière de santé et de protection des données.

Les partenaires au développement : Les partenaires au développement peuvent être impliqués dans les programmes de santé basées sur des données.

Annexe 3 : les dimensions de la qualité des données

Dimension de la qualité des données	Définition opérationnelle
Exactitude	Aussi appelée validité. Les données exactes sont considérées comme étant correctes : les données mesurent ce qu'elles doivent mesurer. Des données exactes minimisent les erreurs (par exemple, parti pris de l'enregistrement ou de la personne qui conduit l'interview, erreur de transcription, erreur d'échantillonnage) au point de les rendre négligeables.
Fiabilité	Les données générées par le système d'information d'un programme sont basées sur des protocoles et procédures qui ne changent pas en fonction de la personne qui les utilise, du moment et de la fréquence de leur utilisation. Les données sont fiables parce qu'elles sont mesurées et collectées de manière cohérente.
Précision	Cela signifie que les données sont assez détaillées. Par exemple, un indicateur requiert la connaissance du nombre d'individus qui ont reçu de l'assistance et des analyses du VIH et reçu les résultats de leurs tests, selon le sexe de la personne. Un système d'information manque de précision s'il n'a pas été conçu pour enregistrer le sexe de l'individu qui a reçu l'assistance et les analyses.
Exhaustivité	L'exhaustivité signifie qu'un système d'information duquel on tire les résultats est inclusif de manière appropriée : Il représente la liste *exhaustive* des personnes ou unités éligibles et pas juste une fraction de la liste.
Opportunité	Des données sont dites opportunes quand elles sont à jour (actuelles), et quand l'information est disponible à temps. L'opportunité est affectée par : (1) le rythme auquel le système d'information du programme est mis à jour ; (2) le rythme de changement des activités réelles du programme ; et (3) quand l'information est réellement utilisée ou requise.
Intégrité	Les données sont intègres quand le système utilisé pour les générer est protégé de tout parti pris ou manipulation délibérés pour des raisons politiques ou personnelles.
Confidentialité	La confidentialité signifie que les clients sont assurés que leurs données seront conservées en conformité avec les normes nationales et/ou internationales en matière de données. Cela signifie que les données personnelles ne sont pas divulguées et que les données contenues sur des supports papier et électroniques sont traitées avec un niveau de sécurité approprié (par exemple, gardés dans des armoires fermées et des fichiers protégés par des mots de passe).

Annexe 4 : Sécurité du réseau

1. Réseaux locaux : Les administrateurs du site sont responsables de tenir un inventaire des appareils et des utilisateurs en s'assurant que les ordinateurs accédant aux bases de données se trouvant sur un réseau privé où aucun autre appareil ne sont connectés. Si plusieurs utilisateurs doivent partager le même accès internet, c'est-à-dire les invités, les serveurs, le Wi-Fi, etc., ceux-ci doivent se trouver sur un segment de réseau ou un réseau virtuel (VLAN) distinct.

2. Accès à l'ordinateur : Les administrateurs du site sont chargés de garantir que seuls les ordinateurs sécurisés se connectent au système d'information sanitaires, dont :

a. Le compte administrateur de l'appareil n'est pas utilisé.
b. L'appareil se verrouille après cinq minutes d'inactivité.
c. Les périphériques de stockage USB ont été désactivés.
d. Le cryptage du disque dur a été activé.
e. Un logiciel antivirus est installé et à jour.

3. Logiciel antivirus : Tous les ordinateurs clients se connectant au système d'information sanitaire doit disposer d'un logiciel antivirus à jour fonctionnant sur les appareils utilisés pour accéder à la base de données. Les établissements sanitaires doivent garantir que le logiciel antivirus est actif pour identifier et traiter les menaces, notamment les virus, chevaux de Troie, logiciels espions et autres logiciels malveillants.

4. Environnement d'application sécurisé : vérifier que l'application qui est utilisée dans établissement sanitaire est conforme aux meilleures pratiques en matière de qualité logicielle et de sécurité. L'administrateur système veillera à ce que le serveur soit à jour avec les derniers correctifs de sécurité.

5. Environnement d'hébergement sécurisé : Des connexions HTTPS sont utilisées pour maintenir l'échange d'informations entre les appareils clients et le système crypté de manière sécurisée. De plus, le serveur chiffre le lecteur de disque pour garantir que les données sont chiffrées au repos et ne peuvent être lues que par des administrateurs système autorisés.

6. Données confidentielles cryptées : les applications doivent crypter automatiquement les données confidentielles (biométriques et informations personnelles identifiables) dans la base de données. Cette protection supplémentaire garantit que les données confidentielles ne sont visibles que par les utilisateurs autorisés via l'interface Web. Les administrateurs système n'ont pas accès à ces données.

7. Reprise après sinistre : Les applications de santé sont hébergées dans un environnement de serveur sécurisé. La perte de données est très peu probable en raison de la réplication continue se produisant au sein de l'environnement d'hébergement. Le système peut être récupéré après une panne catastrophique du serveur en quelques heures, au lieu de quelques jours. Les sauvegardes cryptées sont stockées dans plusieurs dossiers sécurisés en ligne, garantissant ainsi la continuité en cas de panne catastrophique sur un seul emplacement.

Annexe 5 : Gestion des archives

a. Conservez les dossiers papier à l'écart des climatiseurs, des chauffages et des sources d'eau.

b. Installez des portes et des fenêtres dans tous les bureaux et zones de stockage de dossiers avec des serrures solides.

c. Gardez les classeurs et autres zones de stockage de documents verrouillés à tout moment lorsqu'ils ne sont pas utilisés.

d. Étiquetez tous les fichiers, dossiers et boîtes afin que leur contenu, leurs dates et leur étendue soient clairs.

e. N'autoriser l'accès aux zones de stockage des dossiers qu'à un petit nombre de personnel qualifié.

f. Supervisez tous les visiteurs externes chaque fois qu'ils se trouvent dans les bureaux ou dans les zones de stockage des dossiers.

g. Effectuer des inspections régulières de sécurité et des installations pour tous les espaces de travail ou zones de stockage de dossiers.

h. Détruisez les enregistrements dès qu'ils ne sont plus nécessaires.

i. Conserver une documentation complète sur tous les dossiers détruits.

Annexe 6. Accord de partage de données de l'organisation

Toutes les données soumises à cet accord de partage de données sont fournies dans le but d'aider le MSPLS et ses partenaires à identifier des problèmes de santé publique et à formuler des réponses appropriées. Les actions de partage de données doivent à tout moment être conformes aux lois et aux politiques et réglementations locales applicables. De plus, cette politique est soumise au règlement sanitaire international de l'Organisation mondiale de la santé (http://www.who.int/ihr/en/).

1. Résumé

Destinataire des données	[Organisation/Institution recevant les données]
Durée de l'accord	[Ajouter]
Données à partager	Préciser

2. Justification de la demande de données (Préciser le motif de la demande et l'utilisation y relatif)

…… …….. …….

Je comprends que je peux avoir accès à des informations privées et/ou sensibles sur des individus, des établissements sanitaires et des communautés. En signant cette déclaration, j'indique ma compréhension de mes responsabilités et de mon engagement à maintenir la confidentialité de ces ensembles de données.

3. SIGNATAIRES

Propriétaire de données	**Bénéficiaire des données-**
Entité :	Entité :
Nom :	Nom :
Signature :	Signature :
Date :	Date :

Annexe 7 : Plan de mise en œuvre de la politique de gouvernance des données de santé

Introduction

Les données de santé sont des informations personnelles sensibles liées à la santé des individus ; elles constituent une cible attrayante pour les cyberattaques en raison de leur valeur et de leur sensibilité. La gouvernance des données de santé vise à trouver le juste équilibre entre la protection de la vie privée des individus et la facilitation de l'accès contrôlé aux données à des fins de recherche, d'innovation et d'amélioration des soins.

La politique de gouvernance des données de santé :

- ✓ garantit la mise en place de mesures de sécurité et de confidentialité appropriée pour protéger ces données contre tout accès non autorisé, toute divulgation ou utilisation abusive ;
- ✓ intègre des protocoles de sécurité robustes, tels que le chiffrement, l'authentification et la détection des intrusions, pour prévenir les violations de données et les atteintes à la sécurité. Cela contribue à éviter les conséquences néfastes telles que l'usurpation d'identité, le vol d'informations médicales confidentielles et les dommages à la réputation des institutions de santé ;
- ✓ établit des mécanismes d'accès contrôlé, tels que des consentements éclairés et des protocoles de partage des données, qui permettent de garantir que les données sont utilisées de manière responsable, conforme aux normes éthiques et réglementaires ;
- ✓ assure la conformité aux réglementations en vigueur, réduisant ainsi les risques juridiques et les sanctions potentielles liées à la non-conformité.

L'objectif global de ce plan est de décrire les actions concrètes à mettre en œuvre pour doter des capacités de gestion et de management de la politique de gouvernance des données de santé aux entités du MSPLS concernées. De façon spécifique, le document établit un calendrier de mise en œuvre des activités ayant obtenu un consensus de toutes les parties prenantes avec des responsabilités définies.

Différentes entités du MSPLS participant à la mise en œuvre de la politique de gouvernance des données

Gouvernement : Le gouvernement peut jouer un rôle dans la création de politiques et de réglementations globales en matière de santé et de protection des données.
Les partenaires au développement : Les partenaires au développement peuvent être impliqués dans les programmes de santé basées sur des données.
Structures sanitaires : Les hôpitaux, les cliniques, les laboratoires et autres institutions de santé sont directement impliqués dans la collecte, le stockage et l'utilisation des données sanitaires.
Professionnels de la santé : Les médecins, les infirmiers, les pharmaciens et d'autres professionnels de la santé sont des acteurs clés dans la gestion quotidienne des données de santé, fournissant des informations et accédant aux dossiers médicaux.
Responsables informatiques : Les départements informatiques ont la responsabilité de mettre en œuvre et de maintenir les systèmes d'information de santé, en veillant à leur sécurité, à leur intégrité et à leur disponibilité. Ces professionnels sont chargés de garantir la confidentialité des données de santé et de mettre en place des mesures de sécurité appropriées pour protéger les informations sensibles.
Gestionnaires de données : Les responsables de la gestion des données sont chargés de superviser les politiques et les procédures de gestion des données, de garantir leur conformité et de mettre en œuvre les meilleures pratiques.
Patients et public : Les patients et le public ont un intérêt direct dans la gestion transparente, éthique et sécurisée de leurs propres données de santé. Ils sont également impliqués dans la prise de décisions concernant l'utilisation de leurs informations.
Autorités sanitaires : Les agences gouvernementales de santé publique peuvent être impliquées dans la collecte et l'analyse de données à l'échelle de la population, ainsi que dans la formulation de politiques basées sur ces données.

Organismes de recherche en santé : Les institutions de recherche médicale peuvent utiliser des données sanitaires dans le cadre de projets de recherche, avec la nécessité de respecter des protocoles éthiques stricts.

Fournisseurs de technologies de l'information (TI) : Les entreprises fournissant des solutions technologiques, telles que des systèmes d'information médicale, sont des parties prenantes importantes pour assurer la fonctionnalité et la sécurité des outils utilisés.

Assureurs et organismes de gestion des réclamations (les courtiers) : Les compagnies d'assurance et les organismes de gestion des réclamations peuvent utiliser des données sanitaires pour évaluer les risques, gérer les réclamations et établir des politiques.

Éducateurs en santé : Les éducateurs en santé peuvent utiliser des données sanitaires dans le cadre de programmes de sensibilisation et d'éducation, contribuant à des pratiques de santé plus informées.

Plan de mise en œuvre

Communication stratégique dans le secteur de la santé

1. Ateliers de diffusion de la politique de gouvernance des données de santé ;
2. Production des livrets de la politique de gouvernance des données de santé ;
3. Publication sur site web du MSPLS du document de la politique de gouvernance des données de santé.

Identification des zones pilotes

1. Etablir des critères de choix des zones pilotes ;
2. Identifier les zones pilotes

3. Mise à l'échelle

Formations du personnel dans les zones pilotes à tous les niveaux du MSPLS pour assurer la mise en œuvre technique de la politique de gouvernance des données

1. Elaboration d'un module de formation et formation des formateurs sur la politique de la gouvernance des données ;
2. Formation du personnel dans les zones pilotes ;
3. Supervision post-formation dans des zones pilotes ;
4. Mise en place d'une base de données de suivi de formation sur la politique de gouvernance des données de santé.

Coordination de planification et de suivi-évaluation de la politique de la gouvernance des données

1. Mise en place d'un projet pilote pour tester les politiques, les processus et les outils de gouvernance des données dans un environnement contrôlé (établissements sanitaires réduits) ;
2. Supervisions sur la mise en œuvre de politique dans les établissements sanitaires ;
3. Evaluation Baseline de la politique de gouvernance des données de santé ;
4. Evaluation périodique de la politique de gouvernance des données de santé 2024-2027 ;
5. Evaluation Endline de la politique de gouvernance des données de santé 2024-2027 ;
6. Déploiement de la politique de gouvernance des données à l'échelle nationale ;
7. Suivi des indicateurs de performance (base de données)

Activités du plan

Activité	Référence	Unité	Chronogramme				Cibles	Coût estimatif Fbu	Sources de financement	Occasion d'évaluation	Commentaires
			2024	2025	2026	2027					
Communication stratégique dans le secteur de la santé											
Tenir 4 ateliers de diffusion de la politique de gouvernance des données de santé ;	0	Atelier/région	4				4	20000000	Partenaires	Fin Septembre 2024	
Produire 1450 livrets de la politique de gouvernance des données de santé	0	Livrets	1450				1450	14500000	Partenaires	Fin Septembre 2024	1411 Fosa (publics, privées et agréées)
Effectuer une publication sur site web du MSPLS du document de la politique de gouvernance des données de santé	0	Publication	1				1	0	MSPLS	Fin Septembre 2024	
Identification des zones pilotes											
Etablir des critères de choix des zones pilotes	0	Grille	1				1	0	MSPLS	Fin Septembre 2024	
Identifier les zones pilotes	0	Etablissement sanitaire	20	20				5000000	MSPS et partenaires	Fin Septembre 2024	Mission de visite pour l'identification des zones pilotes
Formations du personnel dans les zones pilotes à tous les niveaux du MSPLS pour assurer la mise en œuvre technique de la politique de gouvernance des données											

Elaborer les modules sur la politique de la gouvernance des données	0	Modules					1	0	MSPLS	Fin Septembre 2024	
Former un pool de 10 formateurs sur la politique de la gouvernance des données	0	Formateurs	10				10	5000000	MSPS et partenaires	Fin Septembre 2024	
Former un pool de 80 personnes dans les zones pilotes	0	Personnes	80				80	20000000	MSPS et partenaires	Fin Septembre 2024	en raison de 4 par établissements sanitaires
Effectuer 4 supervisions post-formations dans des zones pilotes	0	Supervisions	4				4	2000000	MSPS et partenaires	Fin Septembre 2024	
Mettre en place une base de données de suivi de formation sur la politique de gouvernance des données de santé	0	Base de données	1				1	0	MSPS et partenaires	Fin Septembre 2024	
Coordination de planification et de suivi-évaluation de la politique de la gouvernance des données											
Réaliser un projet pilote pour tester les politiques, les processus et les outils de gouvernance des données dans un environnement contrôlé (établissements sanitaires réduits)	0	Etablissements sanitaires	20				1	15000000	MSPS et partenaires	Fin Septembre 2024	
Effectuer 12 supervisions sur la mise en œuvre de politique dans les établissements sanitaires	0	Supervisions	12				12	60000000	Partenaires et MSPLS	Fin 2027	

Réaliser une évaluation périodique de la politique de gouvernance des données de santé 2024-2027	0	Evaluation	1		1		1	30000000	Partenaires et MSPLS	Fin 2025	
Réaliser une évaluation Endline de la politique de gouvernance des données de santé 2024-2027	0	Evaluation	1				1	30000000	Partenaires et MSPLS	Fin 2027	
Mettre à l'échelle la politique de gouvernance des données de santé	0	Etablissement sanitaire			1411		1411	100000000	Partenaires et MSPLS	Fin 2026	Supervisions et évaluations
Constituer une base de données pour le suivi des indicateurs de performance	0	Base de données	1				1	0	MSPS et partenaires	Fin Septembre 2024	
TOTAL BUDGET DE MISE EN ŒUVRE								301 500 000			