Union Africaine

AFRICA CDC
Le Centre africain de prévention et de lutte contre les maladies
Protection de la santé de l'Afrique

UNION AFRICAINE
ÉCHANGE D'INFORMATIONS SUR LA SANTÉ
LIGNES DIRECTRICES ET NORMES

2023

+251 11 551 77 00 africacdc@africa-union.org africacdc@africa-union.org

Table des matières

Acronymes

EDA	Échange de données agrégées
ATS	Admettre le transfert de sortie
SIDA	Syndrome immunodéficitaire acquis
CACP	Consentements avancés de confidentialité des patients
TRA	Traitement antirétroviral
CANEI	Code américain normalisé pour l'échange d'information
SATM	Société américaine des tests et des matériaux
ADUA	Agence de développement de l'Union africaine
UA	Union africaine
DCS	Document de continuité des soins
CDC	Centres pour le Contrôle et la Prévention des catastrophes
ADC	Architecture de documents cliniques
COVID-19	Maladie du coronavirus 2019
DHIS2	Version 2 du logiciel d'information sur la santé du district
INCM	Imagerie numérique et communications en médecine
AUD	Accord d'utilisation des données
CEA	Commission économique pour l'Afrique
DME	Dossier médical électronique
UE	Union européenne
RIRS	Ressources d'interopérabilité rapide des soins de santé
PTF	Protocoles de transfert de fichiers
DSE	Dossier de santé électronique
SIS	Système d'information sur la santé

PSIS	Programme des systèmes d'information sur la santé
EIS	Échange d'informations sur la santé
HL7	Niveau de santé sept
VIH	Virus de l'immunodéficience humaine
HTML	Langage Signalétique Hyper-Text
HTTP	Protocole de transfert hypertexte
IISA	Institut d'ingénierie et de sciences avancées
IIEE	Institut d'ingénieurs en électricité et électronique
GTII	Groupe de travail sur l'ingénierie Internet
RSI	Règlement sanitaire international
RPI	Résumé des patients internationaux
TIC	Technologie de l'information et de la communication
CIM	Classification internationale des maladies
SIMR	Surveillance intégrée des maladies et riposte
IIEE	Institut d'ingénieurs en électricité et électronique
GTII	Groupe de travail sur l'ingénierie Internet
UIT	Union internationale des télécommunications
ISO	Organisation internationale de normalisation
NOJS	Notation d'objet JavaScript
LIMS	Système de gestion des informations de laboratoire
SIL	Système d'information de laboratoire
NCIOL	Noms et codes des identificateurs d'observations logiques
NPPDA	Nouveau partenariat pour le développement de l'Afrique
INNT	Institut national des normes et de la technologie

INSP	Instituts nationaux de santé publique
ISP	Instituts de santé publique
SSP	Surveillance de la santé publique
IPI	Informations personnellement identifiables
PDCP	Protection des données à caractère personnel
CCR	Centres de collaboration régionaux
CER	Communautés économiques régionales
ODD	Objectifs de développement durable
AHS	Algorithme de hachage sécurisé
SMTP	Protocole de transfert de courrier simple
SNOMED-CT	Nomenclature systématisée de la médecine - Terminologie clinique
PAOS	Protocole d'accès aux objets simple
TB	Tuberculose
SCT	Sécurité de la couche de transport
ST	Spécifications techniques
ST	Spécifications techniques
TB	Tuberculose
UN	Les Nations Unies
PDU	Protocole de datagramme utilisateur
GTTAHW	Groupe de travail sur la technologie des applications hypertextes Web
OMS	Organisation Mondiale de la Santé
W3C	World Wide Web Consortium
XML	Langage de balisage extensible
XUA	Profil d'assertion utilisateur

Remerciements

L'équipe du groupe de travail sur l'échange d'informations sur la santé, qui a été organisée par CDC Afrique et avec le soutien des experts techniques de l'Université de Gondar et de PSIS Afrique du Sud, a été responsable de l'élaboration de ce document. Nous tenons à exprimer notre plus profonde gratitude à chacun des membres du groupe de travail, ainsi qu'aux présidents, coprésidents, réviseurs et à tous les autres experts qui ont apporté une contribution importante à la création de ce document. Vous pouvez trouver une liste des membres du groupe de travail ainsi qu'une liste complète des contributeurs à l'annexe 14.

Préface

L'application de la technologie de santé numérique se développe rapidement en Afrique, dans le but d'améliorer la prestation des services de santé et d'atteindre plus efficacement les communautés éloignées et mal desservies. D'autre part, l'absence de lignes directrices et de normes dans l'ensemble du continent rend difficile le partage des données de manière significative sur l'ensemble du continent. C'est pourquoi les Centres africains de contrôle et de prévention des maladies (Africa CDC) ont mis en place un groupe de travail composé de 24 membres afin de fournir une expertise et des conseils pour l'élaboration des lignes directrices et des normes de l'UA en matière de HIE. Les membres du groupe de travail étaient des experts en la matière travaillant en Afrique et au niveau international sur la collecte, l'analyse et l'échange d'informations sur la santé. Certains de ces experts avaient participé à des consultations antérieures sur la définition de la stratégie des systèmes d'information sur la santé d'Afrique CDC. Un président, un coprésident et un secrétaire ont été élus pour impliquer les membres de la tasé force dans différents groupes de travail techniques.

Un président, un coprésident et un secrétaire ont été élus pour engager les membres du groupe de travail. Trois groupes de travail techniques ont été constitués pour diriger la rédaction des trois sections du document :

1. Orientations de la politique HIE
2. Normes HIE
3. Cas d'utilisation de la mise en œuvre

Après plusieurs réunions et consultations virtuelles, un projet de document sur les lignes directrices et les normes HIE de l'UA a été élaboré. La méthodologie employée a consisté à examiner les publications scientifiques et les rapports gouvernementaux sur les lignes directrices et les normes en matière de HIE en Afrique, à examiner les normes d'échange de données complètes et solides connues au niveau international et à incorporer les recommandations des membres du groupe de travail HIE des CDC Afrique.

En outre, le document a fait l'objet d'un examen critique et a été validé par les États membres de toutes les régions de l'UA lors de plusieurs ateliers de validation : Afrique de l'Ouest (l'atelier de validation a eu lieu au Sénégal), Afrique centrale (Congo-Brazaville), Afrique de l'Est (Rwanda), Afrique du Sud (Namibie) et Afrique du Nord (Mauritanie). Des représentants des CDC d'Afrique, des Centres de collaboration régionale (CCR), de l'Organisation mondiale de la santé (OMS), de l'Organisation ouest-africaine de la santé (OOAS), de la Communauté sanitaire de l'Afrique de l'Est, centrale et australe (ECSA) et de la Communauté économique des États de l'Afrique centrale (CEEAS) ont également été invités à participer aux ateliers de validation. Les versions anglaise, française et portugaise du document ont été préparées pour que les participants à l'atelier puissent procéder à un examen critique et assurer l'alignement des lignes directrices et des normes HIE énoncées sur les lignes directrices et les normes nationales existantes des États membres. À la suite de l'exercice de validation, les commentaires et les recommandations des États membres ont été pris en compte et incorporés en conséquence.

Introduction

La 26e Assemblée ordinaire des chefs d'État et de gouvernement de l'UA a créé le CDC Afrique en janvier 2016, et il a été officiellement lancé le 31 janvier 2017 à Addis-Abeba, en Éthiopie. Lors du Sommet spécial sur le VIH et le sida, la tuberculose et le paludisme qui s'est tenu à Abuja, les chefs d'État et de gouvernement de l'Union africaine sont arrivés à la conclusion qu'il était nécessaire de créer cette agence spécialisée (juillet 2013). Son objectif est de relever les défis sanitaires auxquels le continent est actuellement confronté ainsi que le besoin urgent de renforcer les capacités et les capacités des institutions et des partenariats de santé publique en Afrique afin de détecter et de répondre rapidement et efficacement aux menaces de maladies et aux épidémies en utilisant des interventions et des programmes pilotés par des données.

Dans l'exécution de ses opérations quotidiennes, l'organisation s'appuie sur les principes directeurs de leadership, de crédibilité, d'appropriation, de délégation de pouvoir, de diffusion rapide de l'information et de transparence [1]. Il agit comme un forum dans lequel les États membres peuvent discuter et échanger des informations concernant les interventions de santé publique, ainsi que les enseignements tirés de ces interventions. En plus de cela, il est nécessaire de fonctionner dans un cadre qui permet d'obtenir facilement les informations essentielles des manières suivantes :

a) Établir un cadre continental pour le partage des données ;
b) Améliorer la qualité des données ;
c) Développer des éléments de données interchangeables qui préparent les États membres de l'UA à répondre aux urgences ; et
d) Diffuser en temps voulu les informations essentielles aux États membres.

CDC Afrique a élaboré un plan stratégique (2017 - 2021) dans ce cadre à travers un processus consultatif et une évaluation de la situation des cadres politiques de l'UA [1]. Ce plan a été élaboré dans le contexte du cadre. Selon le plan, l'un des piliers fonctionnels des Centres africains de contrôle et de prévention des maladies sera le développement et le renforcement des systèmes d'information qui soutiennent les stratégies de santé publique en Afrique. L'un des objectifs stratégiques primordiaux du pilier fonctionnel est de concevoir et de mettre en œuvre la création d'une plate-forme continentale de partage de données pour les États membres. Cela sera accompli en connectant les instituts nationaux de santé publique (INSP) ou les institutions ayant des fonctions comparables dans chaque pays à un réseau étendu dans le but d'assurer la transmission électronique sécurisée des données et des rapports liés à la santé. Afin d'atteindre cet objectif, il est nécessaire d'élaborer une politique et des normes pour les EIS qui permettront aux systèmes de santé numériques d'être mis en œuvre avec succès sur tout le continent africain.

Objet et portée du document

Ce document propose des politiques et des normes aux États membres de l'UA pour aider à développer et à mettre en œuvre le EIS pour les systèmes de santé numériques sur le continent africain. Alors que les États membres de l'UA peuvent utiliser une combinaison de solutions d'échange sur papier et numériques pour les interactions avec le CDC africain, ce document se concentre sur les données électroniques, l'échange de données et les normes de sécurité pour aider le CDC africain à définir et spécifier un cadre pour guider son , et les États membres de l'UA, le développement et la mise en œuvre à long terme des systèmes de santé numériques. Le dossier comprend :

1. Un ensemble de principes et de lignes directrices sur la politique EIS pour les systèmes de santé numériques ;
2. Un ensemble de principes et de lignes directrices informant les normes EIS pour les systèmes de santé numériques ;
3. Un cadre de mise en œuvre EIS pour les systèmes de santé numériques.

Section A : Politique d'échange d'informations sur la santé de l'Union africaine pour les systèmes de santé numériques

Pour faciliter le EIS pour les systèmes de santé numériques parmi les États membres de l'UA, il est nécessaire de définir la gouvernance et le cadre juridique des politiques et des normes en équilibrant les besoins en matière de confidentialité, de sécurité et de partage des données. Cette section fournit un cadre de politique EIS complet.

Cadre politique

1. Gouvernance

Cette sous-section fournit un ensemble commun de comportements, de politiques et de normes qui permettent la mise en place et la supervision d'une EIS efficace. Il se concentre sur EIS pour les systèmes de santé numériques sur le continent africain afin de relever les défis liés à l'échange d'informations sur la santé entre les INSP ou leurs équivalents à travers le continent.

1.1. Cadre de gouvernance

EIS nécessite souvent des choix techniques et politiques complexes. Il a besoin d'un consensus entre plusieurs parties prenantes. Pour établir et superviser un ensemble commun de comportements, de politiques et de normes qui permettent le EIS pour les systèmes de santé numériques pour les États membres de l'UA, il est nécessaire de développer un cadre de gouvernance du EIS. Un tel cadre favorise le partenariat et la collaboration entre les États membres de l'UA pour assurer la coordination et l'harmonisation des réglementations sur les maladies émergentes et endémiques ainsi que sur les urgences de santé publique. Par conséquent, le cadre de gouvernance vise à servir de principes directeurs du EIS pour les systèmes de santé numériques des États membres de l'UA. Le cadre comprend :

I. Principes de gouvernance des EIS

- Centré sur les États membres de l'UA
- Participation inclusive, représentation adéquate et responsabilités partagées
- Collaboration et/ou partenariat avec les parties prenantes concernées
- Appropriation nationale des informations sur la santé qui facilite l'échange bidirectionnel transparent avec CDC Afrique et les États membres de l'UA

- Renforcer les capacités (par exemple, l'éducation et la formation continues) pour mettre en œuvre le programme EIS dans les États membres de l'UA
- Promouvoir la transparence et la responsabilité publique
- Se conformer aux lois et réglementations des États membres de l'UA
- Promouvoir et soutenir l'innovation

II. Environnement opérationnel

- La politique et les normes de l'UA EIS doivent être l'approche préférée des EIS continentales pour les systèmes de santé numériques.
- Les États membres de l'UA doivent soutenir le EIS avec des incitations fortes pour promouvoir vigoureusement l'adoption.
- Le EIS pour les systèmes de santé numériques des États membres de l'UA doit offrir une flexibilité maximale pour l'innovation et l'adaptation.
- Les États membres de l'UA doivent garantir un pool d'experts pour la mise en œuvre réussie de la politique et des normes de l'UA EIS

III. Leadership

- CDC Afrique établira les conditions fondamentales de la confiance et de l'interopérabilité et veillera à leur respect.
- CDC Afrique doit reconnaître les politiques et normes EIS existantes dans tous les États membres de l'UA et faciliter la coordination et l'harmonisation de ces politiques et normes avec la politique et les normes EIS de l'UA, au besoin.
- Les États membres de l'UA doivent participer pleinement et directement au EIS pour les systèmes de santé numériques et à sa gouvernance.
- Les États membres de l'UA auront des responsabilités partagées avec CDC Afrique dans le EIS pour les systèmes de santé numériques

IV. Responsabilité

- CDC Afrique et les États membres de l'UA doivent surveiller et mettre en évidence l'innovation pour la mise en œuvre réussie de la politique et des normes de l'UA en matière d'EES

- CDC Afrique et les États membres de l'UA doivent lever les obstacles à la gouvernance
- CDC Afrique et les États membres de l'UA doivent fournir une évaluation continue et une amélioration continue de EIS parmi les États membres

V. Organe de gouvernance

- CDC Afrique établira une « Communauté de pratique » (« la CoP ») composée de représentants des États membres de l'UA et d'autres experts bénévoles en la matière en Afrique.
- La CoP supervisera la politique et les normes de l'UA EIS pour les systèmes de santé numériques et transmettra sa recommandation au CDC africain.
- La CoP élit un coordinateur pour superviser les activités quotidiennes de la CoP.
- La CoP aura un secrétariat au sein de la Division de la surveillance et des renseignements sur les maladies du CDC Afrique.
- La CoP se réunira annuellement. La date, l'heure, le lieu et l'ordre du jour de ces réunions sont communiqués à tous les membres au moins un mois à l'avance. En plus de la réunion annuelle, la CoP peut également avoir une réunion d'urgence. Toutes les réunions de la CoP seront supervisées par le coordinateur de la CoP.
- La CoP établira un « groupe de travail technique » (« le GTT ») composé de représentants de la CoP qui sont des professionnels de la santé, des sciences animales ou de l'informatique de la santé en tant qu'organe directeur et décisionnel pour le EIS des systèmes de santé numériques. Les membres du GTT peuvent également inclure des représentants de domaines spécifiques (par exemple les sciences de l'environnement) selon les besoins.
- La CoP élira un président pour superviser les activités quotidiennes du GTT.
- La CoP élit un secrétaire pour assister le président dans la coordination et l'exécution des activités quotidiennes du GTT.
- Les actions du GTT seront soumises à l'examen et à l'approbation de la CoP.
- Le GTT se réunira tous les six mois. La date, l'heure, le lieu et l'ordre du jour de ces réunions doivent être communiqués à tous les membres au moins un mois à l'avance. En plus de la réunion périodique, le GTT peut également tenir une réunion d'urgence, par exemple, lorsqu'il répond à des problèmes de santé publique continentaux. Toutes les réunions du GTT seront supervisées par un président nommé par la CoP.

- Le GTT sera chargé de superviser et d'orienter stratégiquement les EIS des États membres de l'UA pour les systèmes de santé numériques. Le GTT sera également responsable de la durabilité et de l'évolutivité du EIS en matière de technologie et de services. La surveillance doit inclure, mais sans s'y limiter, les domaines suivants :
    a) Développement, révision et approbation des politiques et normes EIS pour les systèmes de santé numériques, accord de participation, accord de partage de données standardisé et cas d'utilisation EIS.
    b) Développement et approbation des fonctions de renforcement des capacités et d'évaluation.
    c) Enregistrement de nouveaux participants (États membres de l'UA) pour l'échange d'informations sur la santé entre les États membres de l'UA.
    d) Spécification et approbation du nouveau EIS pour les types de données des systèmes de santé numériques, les termes de vocabulaire des données et tous les registres de données partagés connexes.
    e) Assurer l'allocation des ressources (avec le soutien d'CDC Afrique), et/ou la formation de sous-comités, pour l'amélioration et l'évolution du système et/ou des processus.
    f) Suivi et résolution des problèmes des participants et escalade de ces problèmes au conseil d'administration d'CDC Afrique où des conseils et des actions de plus haut niveau sont nécessaires.
    g) Sélection et approbation des systèmes de santé numérique CDC Afrique et de la technologie, des équipements, des plateformes et des interconnexions EIS.
    h) Surveiller et évaluer la mise en œuvre de la politique et des normes de l'UA EIS pour les systèmes de santé numériques dans les États membres de l'UA.
    i) Recommander aux États membres d'élaborer leur plan stratégique en tenant compte de la politique et des normes de l'UA EIS.

1.2. Cadre juridique

Afin d'orienter correctement les politiques EIS pour les systèmes de santé numériques, l'élaboration et l'adoption d'un cadre juridique par chaque État membre de l'UA est essentielle. Ce cadre juridique a été établi dans le but de garantir que chaque INSP participant ou son équivalent dans les États membres de l'UA se conformera, à tout moment, à toutes les politiques et normes EIS, ainsi qu'aux lois et réglementations nationales et locales applicables. Cela inclut, mais sans s'y limiter, la protection de la confidentialité et de la sécurité des informations de santé.

Le cadre légal comprend :

I. Stewardship

- Le groupe de travail technique (TWG) pour la politique et les normes EIS (spécifiées à la section 1.1 (v)) doit examiner la politique EIS pour les systèmes de santé numériques tous les deux ans et apporter les modifications appropriées, comme déterminé par le TWG.
- Chaque État membre de l'UA doit déployer des efforts raisonnables pour se tenir au courant de toute modification ou mise à jour et interprétation de toutes les lois et réglementations nationales, étatiques et locales applicables susceptibles d'affecter leur utilisation et leur divulgation des informations sur la santé.
- Chaque État membre de l'UA doit permettre aux documents et messages électroniques d'être équivalents aux documents papier à des fins juridiques ; et la source des documents et messages électroniques doit être traçable.
- Chaque État membre de l'UA accepte les signatures électroniques de confiance comme équivalentes aux remplacements acceptables des signatures manuelles sur papier à des fins juridiques.

II. Partage de données

- CDC Afrique et les États membres de l'UA devraient définir un accord standard de partage de données à utiliser et à signer par CDC Afrique et chaque État membre.
- Conformément aux termes d'un accord standard de partage de données, chaque État membre de l'Union africaine (UA) est tenu de partager par voie électronique des données de santé publique anonymisées et agrégées avec le CDC Afrique, les autres États membres de l'UA, et organisations internationales de santé.
- Chaque État membre de l'UA doit partager des données électroniques identifiables basées sur les cas avec CDC Afrique et les autres États membres de l'UA, comme spécifié dans un accord standard de partage de données.
  Chaque membre d'un État membre de l'UA est tenu, si nécessaire, de demander une dérogation à toute exigence spécifique de la politique de partage de données, mais il est également tenu de fournir un plan pour se conformer éventuellement à cette exigence au fil du temps.

III. Confidentialité et sécurité

- Il est conseillé à chaque État membre de l'UA de légiférer ou de réglementer les comportements qui nuisent aux systèmes de santé publique et/ou à l'intégrité des données et/ou à la confidentialité des données.
- Chaque État membre de l'UA doit définir les protections minimales requises en matière de confidentialité et de sécurité pour les données de santé publique stockées en dehors des frontières de l'État membre (par exemple, dans un environnement cloud).

IV. Domestication

- Chaque État membre de l'UA est responsable de s'assurer qu'il est conforme à la version la plus récente de la présente politique EIS, qui doit être mise à la disposition de tous les États membres de l'UA par l'intermédiaire du CDC Afrique.
- Cette politique EIS entrera en vigueur dès son approbation par la Communauté de pratique (CoP) et sera contraignante une fois que les États membres auront signé un accord de participation avec CDC Afrique.

2. Architecture, rapports et partage d'échange de données Continental

L'architecture conceptuelle continentale EIS pour les systèmes de santé numériques est une architecture de haut niveau qui définit l'échange de données sur la santé en commençant par le système d'information sur la santé au niveau des établissements et en continuant jusqu'au CDC africain, à l'OMS, aux organismes régionaux, aux États membres de l'UA et autres partenaires. Le modèle conceptuel de l'architecture EIS des États membres de l'UA sera discuté dans la section suivante.

2.1. Architecture d'échange de données et interopérabilité

L'architecture EIS des États membres de l'UA pour la santé numérique doit fournir un ensemble commun de plates-formes, de services et de référentiels pour les données de santé publique partagées. Les données contenues dans les référentiels doivent être partitionnées de manière à ce que chaque État membre de l'UA contrôle ses propres données de santé numériques et le moment de toute publication ultérieure de ces données, ou d'un sous-ensemble de ces données, vers les référentiels d'CDC Afrique et/ou d'autres États membres de l'UA. Une fois publiées, les données partagées peuvent être consultées par CDC Afrique et les États membres de l'UA conformément aux accords de partage de données de santé publique signés.

Les services associés pour les EIS des fonctions de santé numérique doivent être basés sur des composants logiciels interopérables et doivent garantir que les données de santé publique des INSP participants ou équivalents sont protégées et contrôlées de manière appropriée. Une représentation schématique de l'architecture est illustrée à la figure 1 ci-dessous.

Figure 1: Modèle conceptuel EIS des États membres de l'UA

La figure 1 montre les flux d'informations à partir d'un système d'information sanitaire au niveau des établissements vers CDC Afrique, l'OMS et les organismes régionaux africains (par exemple, les comités de collaboration régionaux (CCR) et les communautés économiques régionales (CER)). Les chiffres de 1 à 4 identifient les flux d'informations individuels. Les flux numérotés 1 et 2 doivent être facilités par le système de santé numérique des États membres de l'UA englobant le système national d'information sanitaire, la surveillance intégrée des maladies et la réponse (SIMR) et la fonctionnalité du système d'information de laboratoire (SIL).

Les flux numérotés de 2 à 4 seront facilités par le système EIS des États membres de l'UA. Les détails de chacun de ces flux sont décrits dans le tableau 1 ci-dessous.

Tableau 1: Définitions des flux de données du modèle conceptuel EIS des États membres de l'UA

COULER	FROM	TO	PROCESSUS	CONTENU DES DONNÉES	SÉCURITÉ	RÉACTIVITÉ
1	État membre de l'UA SIS /SIMR/LIS	CDC Afrique/OMS/ Organismes régionaux (CCR et CER)	Évaluer Rapport Notifier Coordonner Disséminer	ndicateurs Événements Indicateurs de santé publique Événements de santé publique Réponse de santé publique Constatations pertinentes	Protéger les données Protégez les données et les informations personnelles Protéger les données Protégez les données et les informations personnelles Protégez les données et les informations personnelles Protégez les données et les informations personnelles	1 semaine à 1 mois Un jour 1 semaine à 1 mois Immédiatement Le cas échéant Le cas échéant
2	SIS de 1er niveauinfranational	État membre de l'UA SIS /SIMR/LIS	Détecter Évaluer Agrégat Rapport Coordonner	Tendances des maladies Indicateurs de santé publique Indicateurs de santé publique Indicateurs de santé publique Réponse de santé publique	Protéger les données Protéger les données Protéger les données Protéger les données Protégez les données et les informations personnelles	2 semaines à 1 mois 1 semaine à 1 mois 1 semaine à 1 mois 1 semaine à 1 mois Le cas échéant
3	SIS de 2e niveau infranational	SIS de 1er niveau infranational	Détecter Évaluer Agrégat Rapport Coordonner	Tendances des maladies Indicateurs de santé publique Indicateurs de santé publique Indicateurs de santé publique Réponse de santé publique	Protéger les données Protéger les données Protéger les données Protéger les données Protégez les données et les nformations personnelles	mois 1 semaine à 1 mois 1 semaine à 1 mois 1 semaine à 1 mois 1 semaine à 1 Le cas échéant
4	DSE/SIL/ Communauté	SIS de 2e niveau infranational	Détecter Évaluer Rapport	Donnée clinique Maladie / Décès Résultats de santé Indicateurs de santé publique	Protégez les données et les informations personnelles Protégez les données et les informations personnelles Protégez les données et les informations personnelles Protéger les données	Un jour Un jour Un jour 1 semaine à 1 mois

IIP : Informations personnelles identifiables, SIS : Système d'information sur la santé, DSE : Dossier de santé électronique, SIL : Système d'information de laboratoire, SIMR : Surveillance intégrée des maladies et riposte, CCR : Centres de coordination régionaux, CER : Communautés économiques régionales

Dans le tableau 1, la colonne De indique l'initiateur du flux d'échange de données. Une fois le flux lancé, l'échange de données proprement dit sera bidirectionnel. Chaque flux comprend un ou plusieurs processus (comme indiqué dans la colonne **Processus**). Pour chaque processus répertorié, il existe une exigence correspondante relative **au contenu des données**, à la **sécurité** et à la réactivité .

Bien que le type détaillé de données à déclarer soit indiqué dans le tableau 1, la priorité doit être accordée aux mortalités, aux données cliniques, aux résultats de laboratoire, à la surveillance des maladies à déclaration obligatoire, à la surveillance intégrée des maladies et à la surveillance nationale en temps réel. D'autres rapports tels que la logistique, la génomique des virus et les ressources humaines peuvent également être pris en compte.

La plate-forme EIS des États membres de l'UA pour la santé numérique doit échanger des données sur la base des normes identifiées à la section B - Normes EIS de l'UA pour les systèmes de santé numériques. La plate-forme doit soutenir l'échange de données de santé publique entre les États membres de l'UA et le CDC Afrique pour inclure :

a) Échange de données agrégées

- Des États membres de l'UA
- Basé sur un registre continental des installations et des emplacements
- *Des données agrégées, issues de l'extraction, de la transformation et de l'analyse des données*

b) Échange de données basé sur l'entité (c'est-à-dire, patient basé sur le cas, cas, échantillon de laboratoire)

- Extrait de données basées sur des cas fournies aux États membres de l'UA
- Réductible à des indicateurs agrégés

c) Échange de données hybride (c'est-à-dire un mélange d'échange de données agrégées et basées sur les entités)

- Basé sur une combinaison d'informations agrégées et basées sur des cas
- Au départ, les données peuvent arriver sous forme agrégée, avec des messages transactionnels agrégés et basés sur des cas provenant de systèmes de santé plus avancés des États membres de l'UA.

En plus de construire le EIS continental pour les systèmes de santé numériques, le CDC Afrique fournira une orientation stratégique et promouvra la pratique de la santé publique dans les États membres de l'UA en renforçant les capacités, en promouvant l'amélioration continue de la qualité dans la prestation des services de santé publique et en prévenant les urgences de santé publique. et menaces. Le CDC africain coordonnera et harmonisera les lois et programmes nationaux de santé, ainsi que les meilleurs moyens de partager les informations sur la santé.

Le CDC Afrique, en collaboration et en consultation avec les représentants des États membres, définira un référentiel commun de vocabulaire et de terminologie à utiliser pour le EIS des systèmes de santé numériques. Les États membres de l'UA devront soit adopter ces termes de vocabulaire, soit associer leurs termes utilisés en interne à ces termes pour faciliter l'échange de données partagées. Le vocabulaire médical continental et la terminologie de codage seront sélectionnés et approuvés par le Comité sur la base des contributions des États membres de l'UA.

Avenir de l'architecture d'échange de données

En plus de l'échange de données agrégées et basées sur les entités, comme indiqué ci-dessus, les évolutions futures de l'architecture EIS pour la santé numérique doivent tenir compte de l'échange de données génomiques, vétérinaires et de santé publique au point d'entrée, des liens de données environnementales et des liens de population anonymisés, comme déterminé par le Comité en coordination avec les États membres de l'UA.

2.2. Rapport de données

Les données à déclarer via le EIS des États membres de l'UA pour les systèmes de santé numériques doivent être liées à des cas d'utilisation spécifiques définissant les données à collecter, le contenu de l'échange de données, les vocabulaires associés et les délais de notification. Lorsque des données basées sur des cas sont signalées, le partage de données au niveau continental sera limité conformément à l'accord de partage de données actuel pour permettre des réponses régionales et continentales aux situations de santé publique. Le partage de données peut être destiné à des organisations non gouvernementales qui financent certains traitements (par exemple, la thérapie antirétrovirale) ou au CDC Afrique pour permettre au continent de demander des fonds qui pourraient soutenir un plus grand investissement dans la recherche dans les universités africaines (par exemple, la recherche sur le VIH). De tels accords de partage de données peuvent être conclus au niveau des États membres de l'UA, du CDC Afrique ou à la fois au niveau des États membres de l'UA et du CDC Afrique.

2.3. Accords de propriété et d'utilisation des données

I. Propriété des données

En 2014, l'UA a adopté la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles [2] et, aujourd'hui, de nombreux pays africains ont adopté des lois sur la protection des données [3]. Certains pays ont adopté des lois indépendantes, telles que la loi sud-africaine sur la protection des informations personnelles [4] (POPIA), tandis que d'autres pays, comme le Kenya, ont adopté des lois conformes à la loi générale sur la protection des données de l'UE [5]. Des arguments ont été présentés pour une stricte propriété des données par les patients [6] tandis que d'autres ont présenté des modèles de copropriété [7]. Informations sur les premiers concepts de propriété des données [8] et le concept de propriété des données cliniques [7] est disponible dans les références. Aux fins du EIS pour les systèmes de santé numériques, les États membres de l'UA possèdent leurs propres données et doivent conclure des accords de partage et d'utilisation des données afin de partager des ensembles de données. Les ententes de partage de données sont traitées à la section 2.4.

II. Accord d'utilisation des données

L'accord d'utilisation des données (AUD) peut être défini comme : "un document contractuel utilisé pour le transfert de données qui a été développé par une organisation à but non lucratif, gouvernementale ou privée, où les données ne sont pas publiques ou sont autrement soumises à certaines restrictions sur leur utilisation"[9].

Le AUD est requis en vertu des règles de confidentialité et doit être conclu avant toute utilisation ou divulgation d'un ensemble limité de données à une institution ou à une partie extérieure. Un ensemble de données limité est un ensemble de données dépourvu de certains identifiants directs spécifiés dans la règle de confidentialité. Un ensemble limité de données peut être divulgué à une partie extérieure sans l'autorisation du patient uniquement si le but de la divulgation est à des fins de recherche, de santé publique ou d'opérations de soins de santé et que la personne ou l'entité recevant les informations signe un AUD avec l'entité couverte ou son partenaire commercial [10].

Un ensemble de données limité est toujours des informations de santé protégées (ISP), et pour cette raison, CDC Afrique et les États membres de l'UA doivent conclure un AUD avec tout destinataire d'un ensemble de données limité l'un de l'autre. Au minimum, le AUD doit contenir des dispositions qui traitent des points suivants :

- Établir les utilisations et les divulgations autorisées de l'ensemble limité de données.
- Identifier qui peut utiliser ou recevoir les informations.
- Interdire au destinataire d'utiliser ou de divulguer davantage les informations, sauf dans la mesure permise par l'accord ou autrement autorisée par la loi.
- Exiger que le destinataire utilise les mesures de protection appropriées pour empêcher toute utilisation ou divulgation non autorisée non prévue par l'accord.
- Exiger que le destinataire signale à l'entité visée toute utilisation ou divulgation dont il prend connaissance.
- Exiger que les destinataires s'assurent que tous les agents (y compris les sous-traitants) auxquels ils divulguent les informations accepteront les mêmes restrictions que celles prévues dans l'accord.
- Interdire au destinataire d'identifier les informations ou de contacter les personnes concernées.

En collaboration avec les États membres de l'UA, CDC Afrique doit établir un mécanisme pour suivre l'utilisation des données après le partage des données avec les utilisateurs. En outre, les entités couvertes doivent prendre toutes les mesures raisonnables pour atténuer la violation du AUD par un destinataire, ce qui pourrait impliquer la réparation ou la surveillance du crédit.

III. Qualité, intégrité, utilisation, transparence et responsabilité des données

Pour prendre les meilleures décisions possibles au niveau continental, les données communiquées par les pays doivent être de la meilleure qualité possible. La qualité des données fait référence aux données et aux informations qui répondent à des critères spécifiques pour être adaptées à l'utilisation prévue. En santé publique, les caractéristiques les plus recherchées de la qualité des données sont l'exhaustivité, l'actualité et l'exactitude [11, 12]. Dans le contexte de EIS, l'intégrité des données est une autre dimension importante de la qualité des données pour garantir que les données ne sont pas altérées entre la source et le point d'utilisation. Lorsque les données répondent à ces quatre critères, elles peuvent être utilisées de manière fiable pour prendre des décisions. Des données complètes sont nécessaires pour permettre l'utilisation de techniques épidémiologiques pour calculer l'incidence de la maladie, ainsi que pour mesurer des résultats tels que la guérison, l'invalidité et la mortalité. Des données opportunes sont nécessaires pour que les décisions des décideurs politiques aux niveaux national et continental puissent intervenir sans retard inutile. La précision est cruciale pour garantir que les décisions basées sur les données sont prises avec intégrité. Par conséquent, cette politique vise à garantir que les données de santé partagées par les États membres de l'UA sont complètes, exactes et disponibles pour CDC Afrique et n'ont pas été modifiées ou corrompues de manière non autorisée.

Les exigences suivantes doivent être respectées pour garantir la qualité, l'intégrité, l'utilisation, la transparence et la responsabilité des données :

- Les États membres de l'UA doivent prendre des mesures raisonnables pour garantir que les données partagées via les systèmes de santé numériques sont exactes, complètes et à jour, et n'ont pas été modifiées ou corrompues de manière non autorisée.
- Les États membres de l'UA doivent signaler tous les cas de données à déclarer conformément aux réglementations sanitaires internationales (2005) et au document d'échange d'informations sur la santé de l'Union africaine - Politique et normes pour le système d'information sur la santé (politique actuelle) au CDC Afrique par le biais des normes EIS convenues. Si le ministère national a connaissance d'un cas, il doit être compté et signalé. Tous les détails sur un cas qui ne compromettraient pas la confidentialité doivent être inclus dans le rapport de cas.
- Les États membres de l'UA doivent signaler les cas en temps opportun au CDC Afrique. Chaque cas d'utilisation (par exemple, VIH et COVID-19) doit spécifier un délai raisonnable pendant lequel les États membres peuvent identifier et signaler un cas.

- Les États membres de l'UA doivent communiquer des données exactes au CDC Afrique. Les ministères devraient établir des processus de contrôle de la qualité pour s'assurer que les données qu'ils rapportent sont exactes et qu'elles nécessiteront une correction minimale à une date ultérieure.
- Les États membres de l'UA doivent mettre en œuvre des mesures de sécurité techniques pour se protéger contre tout accès non autorisé aux données transmises sur un réseau de communications électroniques ou stockées dans un dispositif de saisie de données, un dispositif de stockage amovible, un système informatique, un centre de données ou des services cloud.
- Les États membres de l'UA doivent travailler en collaboration pour assurer l'intégrité des données et répondre en temps opportun aux demandes d'examen ou de révision. Chaque INSP participant ou équivalent doit avoir la capacité technique de transmettre les mises à jour et les corrections aux EIS des États membres de l'UA pour les systèmes de santé numériques.
- CDC Afrique communiquera aux institutions participantes en cas d'enregistrements incorrects et en double. Les enregistrements incorrects et en double seront résolus par les institutions participantes.
- Des audits périodiques du EIS des États membres de l'UA pour les données de santé numériques doivent être effectués par CDC Afrique pour l'exactitude, l'exhaustivité, l'actualité et la cohérence des données sur la base des directives normalisées d'évaluation de la qualité des données qui doivent être préparées par CDC Afrique.
- Toutes les divulgations de données par l'intermédiaire du EIS des États membres de l'UA pour la santé numérique et l'utilisation des informations obtenues à partir de celui-ci doivent être conformes à toutes les lois et réglementations nationales, étatiques et locales applicables, et ne doivent pas être utilisées à des fins illégales ou non autorisées (par exemple , exposition d'informations personnellement identifiables, usurpation d'identité et ciblage à des fins de harcèlement).
- Les EIS des États membres de l'UA pour les systèmes de santé numériques doivent fonctionner avec transparence et ouverture.
- CDC Afrique sera responsable de la mise à jour et de la gestion du référentiel de données.
- Les États membres de l'UA sont responsables d'assurer la qualité des données et le partage des données en temps opportun selon un format convenu.

Il est recommandé à chaque État membre de l'UA d'établir une politique de « gestion des archives et de l'information » qui spécifie ce qui suit :

- Quelles données et informations (dossiers) seront collectées par diverses entités (par exemple, hôpital de district, hôpital régional et ministère) au sein du pays.
- Dans quel système d'information les enregistrements seront conservés ; il peut s'agir de systèmes électroniques ou papier.
- Propriété des enregistrements.
- Qui aura accès à la saisie et/ou à la récupération des enregistrements du système d'information.
- Comment l'accès à l'information est tracé, de sorte que l'information existe pour déterminer la cause de la violation ou de l'échec du processus.
- Comment le système d'information sera sécurisé pour protéger la vie privée et la confidentialité des personnes auxquelles ils se rapportent.
- Les registres de durée doivent être conservés par les organismes qui les gèrent.
- Dans quelles conditions un enregistrement peut être expurgé, supprimé ou archivé.
- Quelles sont les méthodes acceptables pour l'élimination des données.
- À quelles fins les enregistrements peuvent être utilisés.

2.4. Données ouvertes

L'Open Data Handbook fournit "des données qui peuvent être librement utilisées, réutilisées et redistribuées par n'importe qui - sous réserve uniquement, au plus, de l'obligation d'attribuer et de partager à l'identique" [13]. La définition complète des données ouvertes [13] fournit des critères supplémentaires, notamment la disponibilité et l'accès, la réutilisation et la redistribution, la participation universelle et l'interopérabilité. Les modèles de données ouvertes peuvent jouer un rôle important dans la création d'un cadre pour fournir des services de données interopérables qui soutiennent le développement d'applications innovantes de santé intelligente bénéficiant de la fusion et du partage de données [14]. Aux fins du EIS, les données non identifiables partagées entre les États membres de l'UA et CDC Afrique seront traitées comme des données ouvertes au sein de cette communauté continentale. L'utilisation des données au-delà de cette communauté doit être spécifiée dans un accord d'utilisation des données (voir la section 2.3).

Inspirés de la science ouverte, il existe des principes directeurs FAIR, qui sont maintenant prônés par les communautés des sciences de l'information [15]. FAIR visait à fournir des lignes directrices pour améliorer la trouvabilité, l'accessibilité, l'interopérabilité et la réutilisation des actifs numériques. FAIR n'est pas égal à Open [16]. Le « A » dans FAIR signifie « Accessible dans des conditions bien définies ». Parfois, il peut y avoir des raisons légitimes et valables de protéger les données et les services générés avec un financement public de l'accès public. Il s'agit notamment de la vie privée, de la sécurité nationale et de la compétitivité.

I. Politique de données ouvertes

Le CDC Afrique doit établir une politique de gestion et de partage des données [17]. Lignes directrices sur la politique de données ouvertes de l'Open Sunlight Foundation [18] seront adoptés par le CDC Afrique pour cet usage.

II. Objectif de la politique de données ouvertes

La politique de données ouvertes doit garantir que les États membres participants identifient, préparent et publient des ensembles de données pertinents, précis et de haute qualité au CDC Afrique en temps opportun. [19]. La politique de données ouvertes offre aux États membres la possibilité de mettre à jour et d'améliorer l'accès aux informations déjà ouvertes, et de spécifier que de nouveaux ensembles de données et enregistrements doivent être collectés et publiés.

III. Types de données pouvant être partagées avec les utilisateurs

Les données de santé publique sont un élément clé du partage. Un guide publié par le Center on Global Health Security en 2017 [20] stipule que le partage des données de santé publique améliore et protège la santé publique. Cela peut aider à atteindre les ODD des Nations Unies, en particulier l'ODD 3 - "permettre à tous de vivre en bonne santé et promouvoir le bien-être de tous à tout âge". CDC Afrique, en accord avec les États membres de l'UA, doit spécifier les données de santé publique à partager entre les États membres de l'UA et CDC Afrique dans un accord de partage de données. Un État membre de l'UA doit avoir la possibilité de demander une dérogation temporaire au partage d'un ensemble particulier de données chaque fois que nécessaire, mais doit également fournir un plan et un calendrier pour pouvoir partager les données particulières.

IV. Principes de partage des données

Le comité scientifique du système mondial de données a publié des principes de partage de données conformes aux politiques de données d'un certain nombre d'initiatives nationales et internationales [21]. Les principes de partage des données dans les pays en développement (principes de partage des données de Nairobi) ont également été publiés [22].

La politique de partage des données du CDC africain doit spécifier les principes de partage des données comme un moyen important d'accroître la capacité des chercheurs, des scientifiques et des décideurs politiques à analyser et à traduire les données en rapports et connaissances significatifs.

Responsabilité

Le partage de données nécessite la confiance et la responsabilité entre les partenaires. La confiance se construit au fil du temps et la responsabilité est développée grâce à de solides accords de partage de données et en veillant à ce que les données soient utilisées aux fins prévues. La politique de partage des données doit permettre la confiance et exiger la responsabilité des participants.

Confidentialité

Le maintien de la vie privée et de la confidentialité des informations des individus nécessite que toutes les données partagées soient rendues anonymes ou protégées contre toute utilisation, accès et divulgation non autorisés dans la mesure du possible. La confidentialité garantit que cette protection a lieu. Afin d'empêcher la divulgation d'informations personnellement identifiables, la politique régissant le partage des données doit stipuler que toutes les données basées sur l'entité qui sont partagées doivent faire l'objet d'une protection stricte. La méthode de collecte des données, en plus de toutes les procédures nécessaires pour le partage des données et les métadonnées, relèvent toutes de la responsabilité des États membres de l'UA. Le CDC Afrique est chargé de s'assurer que chaque source de données fournit des détails concernant les données.

Qualité des données

Les données ouvertes peuvent améliorer la qualité des données en les ouvrant à l'examen par d'autres. La politique de partage des données doit préciser quand les données partagées des États membres de l'UA peuvent être utilisées librement par CDC Afrique et quand elles peuvent être utilisées librement par les autres États membres.

Efficacité

Les données partagées se traduisent par une efficacité accrue en termes de réduction de la duplication des efforts dans la capture et l'acquisition de données. La politique de partage des données doit préciser où les données partagées seront mises à la disposition des utilisateurs.

V. L'accord de partage de données

Il existe des exemples de dispositions incluses dans un accord typique de partage de données [23] et pour les guides de partage des données de santé publique [20]. Un article récent d'Afrique du Sud articule l'utilisation d'un accord de transfert de matériel pour partager des données [24].

L'accord de partage de données d'CDC Afrique doit être un contrat formel qui documente clairement quelles données sont partagées et comment les données peuvent être utilisées. L'accord a deux objectifs. Premièrement, il doit protéger le fournisseur de données, en veillant à ce que les données ne soient pas utilisées à mauvais escient. Deuxièmement, il doit empêcher une mauvaise communication de la part du fournisseur des données et du destinataire des données en établissant les paramètres d'utilisation des données. Chaque membre de l'UA doit conclure un accord de partage de données avec CDC Afrique. Chaque accord fera l'objet de zéro ou plusieurs dérogations temporaires pour les dispositions que l'État membre de l'UA n'est pas en mesure de respecter au moment de la signature. Toutes les renonciations doivent inclure un plan et un délai de résolution. CDC Afrique veillera à ce que toutes ces dérogations soient résolues conformément au plan et au calendrier fournis par les États membres de l'UA.

L'accord de partage de données doit comporter quatre éléments principaux : définir les données à partager, sécuriser les données partagées, se conformer à toutes les exigences légales relatives aux données et spécifier les conditions dans lesquelles les données peuvent être partagées avec des entités externes autres que les participants au partage de données.

Les éléments suivants doivent être inclus dans l'accord de partage de données :

- Durée de l'accord
- Utilisation prévue des données
- Contraintes sur l'utilisation des données
- Confidentialité des données
- Sécurité des données
- Méthodes de partage des données
- Coûts financiers du partage de données
- Tout autre point à décider par CDC Afrique et l'État membre

Un modèle d'accord de partage et d'utilisation des données est joint en annexe 14.

2.5. Politiques de confidentialité et de sécurité des données

Les organisations de santé sont vulnérables aux menaces de sécurité internes et externes en raison de la valeur des informations de santé ; ainsi, la protection des informations sur la santé est un défi [25]. Il est important de noter que la vie privée, la sécurité et la confidentialité établissent la confiance nécessaire à une interopérabilité réussie des systèmes de santé numériques. [26].

Environ 57 % des États membres de l'UA (31) ont soit mis en place une législation sur la protection de la vie privée et des données, soit sont en train de rédiger leur législation sur la confidentialité et la protection des données en ligne. [27]. Cependant, en ce qui concerne les normes de confidentialité et de sécurité des données de santé, les défis suivants ont été observés : manque de cadres juridiques en place pour soutenir la confidentialité et la sécurité des données de santé ; le manque d'organes de gouvernance au niveau national ; mauvaise attitude culturelle envers la confidentialité du patient ; l'existence de lois sur la protection de la vie privée non spécifiques à la santé qui ne peuvent pas être interpolées pour les données de santé [28]. Les actions importantes en matière de confidentialité et de sécurité comprennent l'octroi de l'accès aux données aux utilisateurs au niveau national et continental, l'établissement des protocoles de confidentialité et de sécurité, la compréhension des conditions et des solutions de sécurité actuelles et la sélection des normes appropriées d'identification et d'authentification des patients.

CDC Afrique apprécie l'importance d'établir et de maintenir de solides politiques de confidentialité et de sécurité des données au sein de son organisation et des organisations partenaires, y compris les États membres de l'UA. Les politiques de confidentialité et de sécurité des données permettent aux organisations d'établir des normes, des règles et des réglementations concernant la sécurisation des données, le maintien de la confidentialité et la protection contre les violations potentielles.

Que les informations sur la santé soient sous forme papier ou électronique, les informations personnellement identifiables (IPI) doivent être sécurisées pour protéger à la fois les données et la vie privée du patient. Dans le cas des données électroniques sur la santé publique, alors que la plupart des données quotidiennes sur la santé publique seront anonymisées, l'accès aux IPI sera nécessaire pour soutenir les activités de suivi des cas de santé publique pour les maladies à fort potentiel épidémique d'avoir un impact grave sur la santé publique en raison de à leur capacité à se propager rapidement à l'échelle nationale et internationale (par exemple, choléra, peste, fièvre jaune, fièvre hémorragique virale et COVID-19).

I. Conventions de l'UA

L'Union africaine a adopté une Convention sur la cybersécurité et la protection des données personnelles en juin 2014. La Convention stipule que le mécanisme ainsi établi doit garantir que toute forme de traitement de données respecte les libertés et droits fondamentaux des personnes physiques tout en reconnaissant les prérogatives de l'État et les droits des communautés locales. En outre, la collecte de données doit être entreprise pour des finalités spécifiques, explicites et légitimes,

et ne doit pas être traitée ultérieurement d'une manière incompatible avec ces finalités ; la collecte des données doit être adéquate, pertinente et non excessive au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement ; les données ne sont pas conservées plus longtemps que nécessaire aux fins pour lesquelles les données ont été collectées ou traitées ultérieurement ; les données à caractère personnel sont traitées de manière confidentielle et protégée, notamment lorsque le traitement implique la transmission des données sur un réseau ; le traitement des données personnelles est confidentiel. Ce traitement est effectué uniquement par des personnes opérant sous l'autorité d'un responsable du traitement et uniquement sur instruction du responsable du traitement.

II. Lois, réglementations et autres politiques nationales

Comme spécifié dans la Convention de l'UA sur la cybersécurité et la protection[1] des données personnelles, les politiques de confidentialité et de sécurité des données, y compris celles d'CDC Afrique, doivent être conformes aux lois, réglementations et autres politiques nationales des États membres de l'UA. Chaque État partie s'engage à mettre en place un cadre juridique visant à renforcer les droits fondamentaux et les libertés publiques, notamment la protection des données physiques, et à sanctionner toute atteinte à la vie privée sans préjudice du principe de libre circulation des données personnelles. Les États parties adoptent également les stratégies qu'ils jugent appropriées et adéquates pour mettre en œuvre la politique nationale de cybersécurité, notamment dans le domaine de la réforme et du développement législatifs, de la sensibilisation et du renforcement des capacités, du partenariat public-privé et de la coopération internationale, entre autres. Ces stratégies définissent les structures organisationnelles, fixent les objectifs et les délais pour une mise en œuvre réussie de la politique de cybersécurité et jettent les bases d'une gestion efficace des incidents de cybersécurité et de la coopération internationale. Une législation sur la vie privée et la protection des données existe déjà pour de nombreux États membres de l'UA.

III. Mécanismes assurant la confidentialité, l'intégrité et la disponibilité des données

Les mécanismes suivants doivent être adoptés par CDC Afrique pour garantir la confidentialité, l'intégrité et la disponibilité des données :

- Toujours protéger les données de santé publique des États membres de l'UA.

[1] https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

- Collectez et traitez ce qui est nécessaire et important, et rien d'autre - chaque élément de données doit être justifié.
- Maintenir et préserver les informations et l'infrastructure de gestion et d'échange d'informations associées pour empêcher la corruption et/ou les modifications non autorisées (par exemple, systèmes d'information protégés par mot de passe, restriction d'accès aux utilisateurs autorisés, stockage sécurisé et verrouillé des formulaires papier de collecte de données et des registres des établissements de santé, etc.).)
- Tous les systèmes (c'est-à-dire les serveurs, les ordinateurs personnels/portables et les appareils mobiles) accédant au CDC Afrique doivent inclure des solutions de pare-feu, de protection antivirus et de prévention des pertes de données. Ces systèmes doivent en outre installer les dernières mises à jour disponibles pour leur système d'exploitation respectif, les définitions de virus et la sécurité logicielle.
- Veiller à ce que toutes les données du système national des CDC Afrique et des États membres de l'UA soient anonymisées dans la mesure du possible pour inclure à la fois des données basées sur des indicateurs, des événements et des cas.
- Établir une définition commune des IPI dans tous les États membres de l'UA.
- Limiter l'exposition des IPI aux situations où une telle exposition est jugée critique et nécessaire à l'exécution d'actions de sécurité de santé publique (par exemple, problèmes de sécurité transfrontaliers et/ou urgences de santé publique transfrontalières (c'est-à-dire dans l'intérêt public)).
- Protégez les IPI des patients - nourrissons, enfants, adolescents, adultes, personnes âgées, hommes/femmes, populations clés.
- Crypter fortement tout le contenu des messages de santé publique au repos et en transit.
- Tous les systèmes traitant des données EIS doivent fournir des outils de chiffrement des données (au repos et en transit) et de sauvegarde des données.
- Obtenir l'approbation préalable de l'autorité de contrôle des données des États membres de l'UA avant l'échange de données anonymisées (c'est-à-dire, doit avoir une source approuvée), sur la base d'accords de confidentialité préétablis entre CDC Afrique et les États membres individuels de l'UA.
- Toujours chiffrer les IPI lorsqu'ils sont présents.
- Utilisez toujours des identifiants anonymes et uniques dans la mesure du possible (c'est-à-dire des données anonymisées) ; sécurisez et cryptez séparément tout mappage entre les identifiants uniques anonymes et les identités réelles des patients et restreignez l'accès à ce mappage au seul personnel de confiance et contrôlé.

- Établir des mécanismes pour détecter et informer les autorités compétentes des violations de données et des compromissions d'infrastructure.
- Mettre en place des équipes d'intervention en cas d'urgence informatique (CERT) du CDC africain et des États membres de l'UA ou des équipes d'intervention en cas d'incident de sécurité informatique (CSIRT) pour répondre aux cyber menaces, aux violations de données et aux pannes de système.

IV. Signalement et correction des violations de données

La divulgation et l'acquisition non autorisées de données personnelles à partir d'un système d'information sont qualifiées de « violation de données ». Les États parties doivent investir dans la création d'une législation appropriée pour poursuivre et condamner les cybercrimes qui interceptent ou tentent d'intercepter frauduleusement des données informatisées par des moyens techniques lors d'une transmission privée vers, depuis ou au sein d'un système informatique, utilisent sciemment des données obtenues frauduleusement à partir d'un système informatique et frauduleusement signaler les violations de données et y remédier, comme spécifié dans la Convention de l'UA sur la cybersécurité et la protection

[2]

des données personnelles. En cas de violation de données, les lois et réglementations locales des États membres de l'UA concernés peuvent également être appliquées.

Chaque État membre de l'UA et CDC Afrique s'efforcent de détecter toute circonstance susceptible d'entraîner ou d'entraîner une violation potentielle ou réelle. CDC Afrique est tenu de signaler toute violation des informations de santé protégées aux États membres de l'UA concernés. Tout État membre de l'UA qui a des raisons de croire qu'une violation s'est produite ou pourrait s'être produite doit rapidement signaler ces informations à CDC Afrique. La «découverte» d'une violation potentielle se produit lorsque CDC Afrique est informé par les États membres de l'UA ou d'autres entités d'une violation potentielle ou lorsque CDC Afrique découvre une violation potentielle.

En cas de violation de données de santé publique, les États membres de l'UA ou CDC Afrique (selon le lieu de la violation) doivent s'informer mutuellement dans les 24 heures.

[2] https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Les États membres de l'UA doivent signaler la nature de la violation, décrire le risque potentiel pour les personnes dont les données ont été consultées et divulguées, et préciser les mesures correctives prises pour éviter de futures violations. Pour examiner les rapports de violation de données et fournir des conseils pertinents à l'État membre concerné, CDC Afrique doit établir un comité d'enquête sur les violations composé de membres du personnel d'CDC Afrique de la Division de la surveillance et du renseignement sur les maladies et du Bureau des sciences et des programmes, et d'autres organismes de surveillance des maladies et de santé. experts en systèmes d'information d'États membres sélectionnés. En fonction de la nature et de la gravité de la violation de données signalée, le comité d'enquête sur la violation peut recommander qu'une évaluation des risques/préjudices soit effectuée dans l'État membre concerné par des membres du comité ou d'autres personnes. L'évaluation doit inclure un examen des sauvegardes, des politiques et des pratiques actuelles en matière de confidentialité et de sécurité des données afin d'identifier les risques en cours et les mesures correctives proposées pour empêcher que de futures violations ne se produisent. Ces évaluations doivent être menées dans les 30 à 60 jours suivant le signalement de la violation à CDC Afrique. CDC Afrique conservera toute la documentation concernant les violations, y compris les copies des notifications de violation envoyées conformément à la présente politique.

Section B : Normes EIS de l'Union africaine pour les systèmes de santé numériques

Cette section décrit les normes et technologies actuelles sur les EIS, les normes d'échange de données, les normes de confidentialité et de sécurité et les normes de base communes pour l'interopérabilité.

3. Examen des normes et technologies actuelles liées aux EIS en Afrique

L'Afrique a connu une augmentation constante du déploiement de solutions de santé numériques. La plupart de ces systèmes utilisent des technologies locales, propriétaires et insulaires [29]. Le manque d'interopérabilité, la capacité d'échanger des données, entre des systèmes hétérogènes a été reconnu comme un obstacle majeur à la réalisation des avantages potentiels de la santé en ligne [30]. Les résolutions de l'Assemblée mondiale de la santé sur la cybersanté (WHA:58.28 (2005)) [31], sur la normalisation et l'interopérabilité de la cybersanté (WHA:66.25 (2013)) [32], et sur la cybersanté (WHA:71.20 (2018) [33] et WHA:71.57 (2018) [34]) reconnaissent tous le rôle des systèmes numériques interopérables dans la réalisation des ODD.

Toutes les stratégies, politiques et architectures de santé numérique examinées parmi les pays africains ont mentionné les normes comme un élément clé pour l'interopérabilité et l'amélioration de l'intégration du SIS [Ghana e-health strategy (2010) [35], Stratégie nationale tanzanienne de cybersanté (2019) [36], National Health Normative Standards Framework for Interoperability in e-health in South Africa (2014) [30], Politique de cybersanté du Kenya (2016) [37], Politique nationale de cybersanté du Rwanda (2017) [38] et Architecture e-santé éthiopienne (2018) [39]]. Les défis comprennent les cadres de gouvernance des EIS, les normes réglementaires de e-santé à tous les niveaux des EIS et la coordination nationale et continentale.

Pour que deux ou plusieurs systèmes hétérogènes échangent des données de manière significative, il doit exister une norme mutuelle pour l'échange de données ou la communication entre ces systèmes [40]. Les normes d'échange de données fournissent des directives claires pour des solutions robustes et interopérables [30, 41, 42]. Conscient de cela, le groupe de travail CDC Afrique EIS adopte et recommande des normes d'interopérabilité EIS qui peuvent être utilisées par les États membres de l'UA pour soutenir divers systèmes de santé numériques, la surveillance des maladies et la réponse de l'UA à la pandémie (telle que COVID-19) parmi les États membres de l'UA, CDC Afrique et CCR.

4. Normes d'échange de données

Les recommandations sur les normes d'échange de données pour les systèmes de santé numériques fournies ici s'appliquent directement à des limites spécifiques, comme indiqué dans la figure 1 de la section Politique.

4.1. Directives standard des systèmes

Il n'existe pas de solution numérique unique pour l'Afrique. Au lieu de cela, chaque solution doit être adaptée aux besoins, aux circonstances et aux ressources nationales et continentales. Chaque solution doit prendre en charge une extension progressive vers un système national d'information sur la santé entièrement intégré sans réingénierie substantielle des systèmes hérités [43]. Il n'est pas pratique d'abandonner les systèmes existants ou de n'avoir qu'un seul système en place pour résoudre le problème d'interopérabilité [29]. Dans le même temps, CDC Afrique encourage l'utilisation et l'application des technologies modernes afin de maximiser les avantages à long terme pour les systèmes de santé numériques des États membres de l'UA.

Les pays de l'Union africaine devraient aspirer à une solution numérique plus intégrée, ouverte et flexible [44]. Plus précisément, les biens mondiaux communs ont été reconnus par les entités publiques et privées comme un plan d'action fondamental pour la construction de composants d'infrastructure interopérables, rentables et faciles à utiliser. [45].

Au lieu de nommer des systèmes spécifiques, le CDC africain suggère que les applications/plateformes de surveillance de la santé et des maladies et les systèmes EIS choisis par le CDC africain, les États membres de l'UA, les hôpitaux publics et privés dans les États membres de l'UA et les laboratoires publics et privés de l'UA Les États membres suivent tous les principes et pratiques indiqués à l'annexe 3.

4.2. Protocoles de communication

Il est recommandé aux États membres de l'UA d'adopter les protocoles de communication suivants pour leurs communications nationales avec les systèmes de santé numériques :

- Communication capteur : Institut d'ingénieurs en électricité et électronique (IIEE) 11073-10101 (Nomenclature), IIEE 11073-10201™ (Domain information model) et IIEE 11073-20101™ (Application profile base standard) pour la prise en charge de la communication interopérable entre les dispositifs de détection et les ordinateurs.

- Couche transport : Internet Engineering Task Force (GTII) Internet Protocol (IP) Version 4 [RFC 1812 (routeurs IPv4) et 2474 (IPv4)] et Transmission Control Protocol (TCP) [RFC 793, 1122, 3168, 6093, 6528 et 7414] pour l'interconnexion de réseaux entre les participants et les réseaux locaux. L'utilisation du protocole de datagramme utilisateur (PDU) [RFC 768] n'est pas autorisée pour les communications CDC Afrique EIS.
- Sécurité de la couche transport : Protocole GTII Sécurité de la couche de transport (SCT) Version 1.3 [RFC 8446] pour la sécurisation des services PTF, SMTP (Simple Mail Transfer Protocol) et HTTP (Hypertext Markup Language).

4.3. Normes de messagerie

Les normes d'échange de données complètes et robustes reconnues à l'échelle internationale sont recommandées.

- Pour la messagerie de contenu clinique et de santé publique, les normes de messagerie Health Level Seven (HL7) suivantes sont recommandées :
  - Pour les messages de santé publique : HL7 V2.5.1 est recommandé car il s'agit de la norme administrative et de messagerie clinique la plus largement utilisée pour faciliter l'échange de données de santé sur les données d'admission, les données de sortie/transfert, les commandes et les résultats des tests de laboratoire, les traitements, les observations cliniques, les horaires de rendez-vous et la facturation. informations entre des systèmes de santé hétérogènes. Les principaux avantages de HL7 V2 sont sa rétrocompatibilité et son haut niveau de flexibilité pour s'adapter à tout environnement de soins de santé. Spécifier une seule norme de messagerie HL7 (V2.5.1) éliminera le besoin d'effectuer des conversions entre différents formats HL7.
  - Pour le contenu et la structure cliniques (y compris les résumés cliniques, les notes de sortie, le laboratoire, l'investigation radiologique), utilisez l'architecture de document clinique (ADC) HL7 V3R2. De plus, CDC Afrique recommande le HLT Document de continuité des soins (DCS) pour l'échange d'informations cliniques, y compris les données démographiques des patients, les problèmes, les médicaments et les allergies.
  - Pour échanger des données pour la santé numérique et les communications cloud, utilisez les communications cloud standard IHE ou HL7® Ressources d'interopérabilité rapide des soins de santé (RIRS). RIRS combine les meilleures fonctionnalités de HL7v2, HL7 V3R2 ADC et des normes Web (Extensible

Markup Language (XML), Notation d'objet JavaScript (NOJS), HTTP, Atom et autres). Pour cette raison, le TF recommande que toutes les nouvelles implémentations et améliorations du système de santé numérique utilisent le RIRS comme principal mécanisme d'échange de données.

- Les dernières normes de messagerie HL7 peuvent également être adaptées.

- INCM est utilisé pour partager des images numériques de diagnostic médical entre des équipements d'imagerie et d'autres applications de soins de santé. Il est utilisé pour des choses comme la radiologie, la radiothérapie, l'ophtalmologie, l'échographie, la mammograp EIS numérique, la pathologie, la dentisterie, la dermatologie, la tomodensitométrie, etc. Il présente la structure des données et les règles de partage des images médicales.
- Le profil Échange de données agrégées (EDA) est recommandé par CDC Afrique pour soutenir l'échange d'indicateurs de santé, de données agrégées (du système d'information sanitaire de district version 2 (DHIS2)) et de métadonnées entre les États membres de l'UA [30, 46, 47].
  [See https://wiki.ihe.net/index.php/Aggregate_Data_Exchange].
- Langage de balisage de données et de documents : Utilisez le langage de balisage e-Xtensible (XML) du World Wide Web Consortium (W3C) [voir https://www.w3.org/TR/xml/] pour faciliter le traitement des données échangées et du contenu des documents et pour identifier les sources de données/documents.
- Langage de balisage de page Web : Utilisez le groupe de travail GTTAHW (Web Hypertext Application Technology Working Group) et le langage de balisage hypertexte (HTML) W3C version 5 [voir https://html.spec.whatwg.org] pour la présentation et le développement de pages Web.
- Format d'échange de données : Utilisez Notation d'objet JavaScript (NOJS) [RFC 7159] [voir https://tools.GTII.org/html/rfc7159] pour faciliter le traitement des données échangées et du contenu des documents et pour identifier les sources de données/documents.
- Jeux de caractères de transmission : Utiliser Utiliser le codage Unicode Transformation Format (UTF-8) de l'Organisation internationale de normalisation (ISO) [conformément à la norme ISO/IEC 10646-1:2017]. Cette norme est également conforme au codage CANEI utilisé par HL7 v2.5.1.

Les normes de messagerie ci-dessus correspondent aux différentes catégories de rapports du CDC africain, comme indiqué à l'annexe 4.

4.4. Normes de vocabulaire

Il est conseillé que les normes suivantes servent de base à la spécification de la terminologie et de la nomenclature pour EIS (ces normes couvrent un large éventail de sujets, mais seule une partie de chacune sera applicable pour une utilisation par le CDC africain dans les systèmes de santé numériques, même si une utilisation plus large par les États membres de l'UA est conseillée) :

- Nomenclature systématisée de la médecine - Terminologie clinique (SNOMED-CT) [43, 48] pour coder les termes et les synonymes des résultats cliniques, des symptômes, des diagnostics, des procédures, des produits pharmaceutiques, etc. Il a un mécanisme intégré pour répondre aux extensions locales et aux différentes langues.
- Classification internationale des maladies (CIM-11) pour classer les maladies, les problèmes de santé, les causes de décès, la terminologie clinique et les normes de codage.
- Noms et codes des identificateurs logiques d'observation (NCIOL) pour le codage des rapports d'essais de laboratoire. Les codes NCIOL peuvent être intégrés dans le contenu des messages de données tels que HL7 V2.5.1 et HL7 ADC pour normaliser les rapports de laboratoire tels que la chimie, l'hématologie, la sérologie, la microbiologie et la toxicologie ainsi que les numérations cellulaires, les sensibilités aux antibiotiques et autres.
- RX-Norm fournit des noms normalisés pour les médicaments cliniques et relie son nom à de nombreux vocabulaires de médicaments couramment utilisés dans la gestion des pharmacies et les interactions médicamenteuses.
- Le Manuel diagnostique et statistique des troubles mentaux (DSM) doit être utilisé comme nomenclature à laquelle les cliniciens peuvent se référer pour améliorer les pratiques cliniques et comme langage pour communiquer les informations diagnostiques.

Les normes de vocabulaire ci-dessus correspondent aux différentes catégories de rapports du CDC africain, comme indiqué à l'annexe 5.

4.5. Profil d'intégration

Aux fins de mappage des identifiants locaux aux numéros de sécurité sociale, aux numéros d'identification biométriques ou aux numéros d'identification nationaux, le CDC Afrique conseille la création et la gestion d'un registre des patients contenant des informations conformes à la norme HL7 V3 ATS (Admettre le transfert de sortie) . Les patients ne sont autorisés à partager leurs dossiers médicaux avec l'CDC Afrique que s'ils fournissent un

consentement éclairé [49] et acceptent de participer à l'étude. Cette recommandation est faite par l'CDC Afrique pour protéger la vie privée et la sécurité des patients et est basée sur le profil Consentements avancés de confidentialité des patients (CACP). Les éléments de données qui sont échangés localement sont distincts de ceux qui sont échangés à travers les frontières internationales. Pour l'échange local, les principaux éléments de données qu'il est recommandé de collecter comprennent les informations démographiques sur les patients, les informations sur l'établissement et les informations sur les antécédents du patient, y compris les signes vitaux, les allergies, le statut vaccinal, le cas de diagnostic, le résultat du diagnostic, le traitement et la date et l'heure du rendez-vous. . En ce qui concerne l'échange de données à travers les frontières internationales, les éléments de données consistent en des éléments de données agrégés qui mettent l'accent sur le diagnostic critique des cas conformément à la ligne directrice de l'International Patient Summary (RPI) [voir application au-delà d'une région spécifique ou pays]. Pour l'utilisation secondaire des données, le CDC Afrique suggère de combiner les normes nationales (le cas échéant) avec les normes internationales nouvellement établies (comme indiqué dans la section 4.3). Cette recommandation s'applique aux utilisations secondaires des données à des fins nationales et internationales.

La divulgation d'informations sur les patients à des fins de recherche nécessite que les données soient conservées dans leurs caractéristiques statistiques tout au long du processus de divulgation afin de limiter la quantité d'informations perdues [50]. Par conséquent, le CDC Afrique recommande que les chercheurs en santé publique partagent des fichiers de données plats (y compris la date du service, les établissements de service, le mois et l'année de naissance du patient, le sexe, les résultats des tests, les signes vitaux et les codes de diagnostic associés à la rencontre) avec le organisation. Cette recommandation dépend d'un accord de partage et d'utilisation des données, qui est décrit dans la section politique de la politique de partage et d'utilisation des données. De plus, les chercheurs sont tenus de signer des accords qui protègent la confidentialité de leurs données.

L'CDC Afrique recommande l'utilisation des pratiques standard suivantes pour l'intégration des profils de patients :

- Utilisation d'un format d'identifiant de cas unique afin d'éviter les collisions d'identifiants dans les États membres de l'UA, tous les identifiants de cas partagés avec les CCR et le CDC Afrique doivent inclure un préfixe de pays unique.
- Création de bases de données de registre partagées pour inclure :

    - Participants au système de santé publique (SSP) et codes d'identification uniques ; seuls les États membres de l'UA identifiés et leurs participants désignés devraient avoir accès au registre de santé numérique des États membres de l'UA. Les codes de participant uniques permettent l'anonymisation des messages échangés ou la source et/ou la destination des données.
    - Politiques SSP pour spécifier les transactions autorisées et l'accès aux informations par chaque participant (voir la section A).
    - Données sur le vocabulaire de la santé publique pour soutenir le développement du système de messagerie des États membres de l'UA, le partage avec les utilisateurs potentiels du système de santé numérique et la diffusion des dernières informations sur le vocabulaire et la terminologie.
    - Informations sur la santé publique à partager entre les participants à la santé numérique ou un sous-ensemble de participants SSP désignés (par exemple, l'évolution des épidémies dans les États membres voisins de l'UA).
- Rapport selon l'accord OMS-CDC Afrique : Signaler les maladies sur la base du dernier instrument de décision entre le CDC Afrique et l'OMS :
    - Maladies signalées à l'échelle internationale en vertu de l'actuel Règlement sanitaire international (RSI) [51] (par exemple, variole, poliomyélite due au poliovirus de type sauvage, grippe humaine causée par un nouveau sous-type, le syndrome respiratoire aigu sévère (SRAS)).
    - Maladies à fort potentiel épidémique pouvant avoir de graves répercussions sur la santé publique en raison de leur capacité à se propager rapidement à l'échelle internationale (par exemple, le choléra, la peste, la fièvre jaune, la fièvre hémorragique virale).
    - Les maladies qui sont les principales causes de morbidité et de mortalité dues aux maladies et affections transmissibles dans la Région africaine (par exemple, le paludisme, la pneumonie, les maladies diarrhéiques, la tuberculose, le VIH/SIDA, les décès et blessures maternels).
    - Toute maladie ou affection non transmissible prioritaire dans la région (par exemple, hypertension artérielle, diabète sucré, santé mentale et malnutrition).
- **Consolider les informations des secteurs concernés :** Les informations provenant des secteurs pertinents de l'administration de la région de l'Union africaine concernée sont consolidées par les CCR. Ces secteurs concernés comprennent ceux qui sont responsables de la surveillance et de la notification, les points d'entrée, les services de santé publique, les laboratoires, les cliniques et les hôpitaux, ainsi que d'autres départements gouvernementaux de l'Union africaine et des États membres de l'Union africaine (conformément à l'article 4.2 du RSI).

- **Diffuser les informations aux parties concernées :** Les informations sont diffusées par les CCR aux secteurs concernés de l'administration de la région de l'Union africaine concernée, tels que les responsables de la surveillance et de la notification, les points d'entrée, les services de santé publique, les laboratoires, les cliniques et les hôpitaux, ainsi que d'autres départements gouvernementaux de la région de l'Union africaine. Union africaine et États membres de l'Union africaine (conformément à l'article 4.2 du RSI).
- **Signaler rapidement :** Présenter un rapport dans les vingt-quatre heures suivant l'achèvement d'une analyse des informations de santé publique [exigence de rapidité] en utilisant la méthode de communication la plus efficace parmi celles qui sont disponibles (comme spécifié à l'article 6.1 du RSI). [Il est important de noter que l'évaluation a lieu au niveau du CCR]
- **Signalez les urgences de santé publique de portée internationale :** Signaler tous les événements susceptibles de constituer une urgence de santé publique de portée internationale sur son territoire conformément à l'instrument de décision (conformément à l'article 6.1 du RSI).
- **Signaler la réponse de santé publique aux événements :** Signaler toute mesure sanitaire mise en œuvre en réponse à ces événements (conformément à l'article 6.1 du RSI).
- **Protéger les informations :** Respecter la dignité, les droits de l'homme et les libertés fondamentales des personnes (conformément à l'article 3.1 du RSI).

5. Normes de confidentialité et de sécurité

5.1. Évaluation et audits externes

- CDC Afrique suggère qu'un journal d'audit ou une série de journaux d'audit soit créé et conservé pour que le EIS puisse suivre :
- Tentatives d'accès des participants, réussites et échecs : cela permettra d'identifier les tentatives d'accès non autorisées pour le processus d'audit de sécurité.
- Sources et volumes de messages : cela prendra en charge l'identification des changements dans le volume de trafic de messages statistiques au fil du temps pour le processus d'audit de sécurité et la planification de l'expansion du système.
- Types et volumes de transactions : cela permettra d'identifier les changements dans les niveaux de transactions statistiques au fil du temps pour le processus d'audit de sécurité, la planification de l'expansion du système et la priorisation de l'amélioration du système.
- Modèles d'heure d'accès des participants : cela prendra en charge l'identification de l'utilisation inattendue de EIS en fonction de l'heure de la journée et/ou du jour de la semaine pour le processus d'audit de sécurité.

5.2. Gestion des risques : évaluation et acceptation

CDC Afrique recommande :

a) Utilisation de l'analyse de réseau bayésienne prédictive.
b) Élicitation de l'évaluation de la vie privée des utilisateurs à l'aide de l'approche d'évaluation des menaces, des actifs et des vulnérabilités critiques sur le plan opérationnel (OCTAVE) de l'économie expérimentale.
c) Mise en place d'un contrat d'assurance sécurité de l'information [50].
d) Mesurer le niveau de risque en termes d'une combinaison de la probabilité d'occurrence (probabilité) et du degré d'impact (positif ou négatif) (INNT SP 800-30).

5.3. Norme de sécurité

CDC Afrique recommande les normes techniques suivantes pour la sécurité de l'information :

- Certificats : Certificats numériques ITU-T X.509 à utiliser dans le chiffrement à clé publique pour SCT et S/MIME. À utiliser conjointement avec Public Key Cryptography Standards 7 (PKCS7) Cryptographic Message Syntax [GTII RFC 5652] et Public Key Cryptography Standards 12 (PKCS12) Personal Information Exchange Syntax Standard [GTII RFC 7292].
- Algorithmes de hachage : INNT Secure Hashing Algorithm 2 (AHS-2) pour inclure AHS-256, AHS-384 et AHS-512 pour créer un hachage sécurisé unidirectionnel d'un document ou d'un message ; en conjonction avec PKCS7 pour prendre en charge la traçabilité du contenu vers une source fiable [voir https://csrc.nist.gov/publications/detail/fips/180/4/final].
- Affirmation de l'utilisateur : Profil XUA avec rôle d'utilisateur, autorisation et objectif des cas d'utilisation. Le profil XUA se concentre sur les transactions de services Web qui suivent ITI TF-2 avec un jeton SAML 2.0 contenant l'assertion d'identité [voir https://wiki.ihe.net/index.php/Cross-Enterprise_User_Assertion].
- Contrôles de sécurité et d'accès ISO pour la gestion des privilèges et le contrôle d'accès (ISO/ST22600).
- Guide standard SATM pour l'authentification et l'autorisation des utilisateurs (SATM E1985-98) [50].

Afin de sécuriser avec succès l'échange d'informations sur la santé à tous les niveaux du système de santé, il est impératif que le facteur humain, qui comprend des éléments tels que la formation et la sensibilisation ainsi que la préparation aux catastrophes et les plans de rétablissement, soit pris en considération.

6. Normes fondamentales communes pour l'interopérabilité

6.1. Gestion des normes

6.2. CDC Afrique suggère que chaque État membre forme un groupe de travail au niveau national afin de revoir en permanence ses normes une fois tous les deux ans et de s'assurer que ces normes évoluent de manière à la fois réfléchir EIS et maîtrisée.

Prise en charge des tests des normes d'échange de messagerie

6.3. Afin de vérifier les implémentations de messagerie et les vocabulaires associés, CDC Afrique conseille la création d'un environnement de test de message et le développement d'un outil de validation de message à utiliser par tous les États membres de l'UA participants.

Protocoles et services pour l'interopérabilité

Les domaines de service d'interopérabilité suivants sont essentiels pour réaliser l'interopérabilité des systèmes de santé numériques entre le CDC africain et les États membres de l'UA. Chaque zone de service décrite brièvement ci-dessous doit être conforme à la dernière version de la norme RFC correspondante ou du service équivalent, lorsqu'elle est adoptée par le CDC Afrique. La norme initialement recommandée pour 2022 est identifiée ci-dessous comme référence pour l'évolution de l'interopérabilité dans le temps :

CDC Afrique recommande que les systèmes participants des États membres de l'UA prennent en charge au moins un, et de préférence tous, des protocoles de transfert suivants :

- File Transfer Protocol over Sécurité de la couche de transport (PTF-SCT) pour prendre en charge l'accès sécurisé et le transfert des messages et des fichiers d'informations. Cela fournit une alternative de service possible pour l'échange de données (c'est-à-dire l'encapsulation des messages et/ou des documents du système de santé numérique dans un fichier lisible par machine). Pour 2022, les protocoles GTII actuellement applicables pour PTF-SCT sont RFC 959 (PTF), 2246 (SCT), 2228 (PTF Security Extensions) et 4217 (PTF-SCT).

- Protocole SMTP (Simple Mail Transfer Protocol) sur Sécurité de la couche de transport (SMTP-SCT) pour prendre en charge l'accès sécurisé et le transfert des messages et des fichiers d'informations. Cela fournit une autre alternative de service possible pour l'échange de données (c'est-à-dire l'encapsulation des messages et/ou des documents du système de santé numérique sous la forme d'une pièce jointe sécurisée à un e-mail). Pour 2022, les protocoles GTII actuellement applicables pour SMTP-SCT sont RFC 2246 (SCT), 3207 (SMTP-SCT), 7817 (SMTP-SCT mis à jour) et 8314 (SCT pour le courrier électronique). Un e-mail doit, à son tour, être pris en charge par :
    - Secure/Multipurpose Internet Mail Extensions (S/MIME) pour les pièces jointes sécurisées aux e-mails SMTP et la protection du contenu des données (par exemple, alors que SMTP-SCT assure le cryptage des données en transit, S/MIME fournit une protection supplémentaire pour les données au repos (par exemple, stocké sur un système). CDC Afrique exige uniquement des algorithmes de chiffrement authentifié avec données associées (AEAD) (c'est-à-dire avec des performances de chiffrement élevées). Les systèmes participants des États membres de l'UA doivent également prendre en charge cette norme s'ils prennent en charge SMTP-SCT. Pour 2022, les protocoles GTII actuellement applicables pour S/MIME version 4 sont RFC 5652 (Cryptographic Message Syntax (CMS), 3370 (CMS Algorithms), 5754 (Secure Hashing Algorithm 2 (AHS-2)), 8702 (AHS-3) et 8551 (S/MIME).

    - Simple Object Access Protocol (PAOS) pour prendre en charge l'échange d'informations via SMTP-SCT. Les systèmes de santé numérique des États membres de l'UA doivent prendre en charge cette norme (c'est-à-dire faciliter l'échange de services de système à système à l'aide de SMTP-SCT). Pour 2022, le protocole W3C actuellement applicable est le framework de messagerie PAOS version 1.2 (https://www.w3.org/TR/PAOS12-part1/). Le transfert d'état représentatif (REST) est la norme facultative pour prendre en charge l'échange d'informations sur la santé.
    - Langage de balisage hypertexte (HTML) pour la présentation et le développement de pages Web. Les systèmes de santé numérique des États membres de l'UA doivent prendre en charge cette norme (c'est-à-dire faciliter le développement de pages Web accessibles aux systèmes via SMTP-SCT). Pour 2022, le protocole GTTAHW et W3C actuellement applicable est la version HTML 5 [voir https://html.spec.whatwg.org].

- Protocole de transfert hypertexte sur Sécurité de la couche de transport (HTTP-SCT) pour prendre en charge un accès Web sécurisé aux messages et aux fichiers d'informations et leur transfert. Cela fournit une troisième alternative de service possible pour l'échange de données (c'est-à-dire entre deux systèmes ou entre un utilisateur et une application Web). Pour 2022, les protocoles GTII actuellement applicables pour HTTP-SCT sont RFC 2817 (SCT dans HTTP), 2818 (HTTP-SCT), 7230 (HTTP Syntax & Routing), 7595 (Universal Resource Locators (URI)) et 8615 (Well Known URI). HTTP-SCT devrait également être pris en charge via :
    - Transfert d'état représentatif (REST) pour prendre en charge l'accès (GET, POST, PUT, PATCH et DELETE) aux liens de sites Web prédéfinis et aux ressources et/ou données associées (c'est-à-dire pour faciliter l'échange de services de système à système et d'utilisateur à système via HTTP-SCT). Au minimum, les systèmes de santé numériques des États membres de l'UA doivent prendre en charge cette approche architecturale pour l'accès aux bases de données du registre. Pour 2022, le protocole GTII actuellement applicable pour REST est RFC 6690 [voir aussi https://tools.GTII.org/id/draft-keranen-t2trg-rest-iot-05.html].
    - Simple Object Access Protocol (PAOS) pour prendre en charge l'échange d'informations via HTTP-SCT ou SMTP-SCT. Les systèmes de santé numériques des États membres de l'UA doivent prendre en charge cette norme (c'est-à-dire faciliter l'échange de services de système à système à l'aide de HTTP-SCT). Pour 2022, le protocole W3C actuellement applicable est le framework de messagerie PAOS version 1.2 (https://www.w3.org/TR/PAOS12-part1/).
    - Langage de balisage hypertexte (HTML) pour la présentation et le développement de pages Web. Les systèmes de santé numériques des États membres de l'UA doivent prendre en charge cette norme (c'est-à-dire faciliter le développement de pages Web accessibles aux utilisateurs ainsi qu'aux systèmes via HTTP-SCT). Pour 2022, le protocole GTTAHW et W3C actuellement applicable est la version HTML 5 [voir https://html.spec.whatwg.org].

Rubrique C : Cadre de mise en œuvre du EIS de l'Union africaine : Un cas de surveillance électronique des maladies

7. À titre d'illustration, cette section explique comment la politique et les normes EIS ont été mises en pratique grâce à l'utilisation de la surveillance électronique des maladies. Cloud computing et services partagés ; la création de nouvelles infrastructures ; le renforcement des capacités existantes ; suivi, évaluation et recherche; De plus, cette section met l'accent sur les effets positifs que le EIS des États membres de l'UA peut avoir sur les systèmes de santé numériques.

EIS pour les avantages de la surveillance électronique

La mise en œuvre initiale du EIS des États membres de l'UA pour la surveillance en ligne offrira les avantages suivants :

a) Temps de réponse
- Transmission rapide et opportune des données des sources de données inférieures (établissements et laboratoires) aux niveaux supérieurs (sous-national et national), permettant des actions de santé publique appropriées.
- Traitement, analyse et reporting automatisés plus rapides des données.
- Amélioration de la vitesse de détection des épidémies grâce à une alerte plus précoce.
- Amélioration de la capacité à déterminer le moment, les personnes et les facteurs de lieu d'une épidémie permettant des mesures de prévention et de contrôle plus efficaces.

b) L'échange de données
- Structure et format de données communs améliorant l'accessibilité, l'utilisation et l'interprétation des données.
- Collecte de données plus cohérente grâce à des outils automatisés standardisés.
- Facilité d'échange de données et de comparaison entre les établissements de santé grâce à la normalisation des données.
- Capacité à exploiter des ensembles de données communs et riches dans plusieurs entités de santé publique via l'interopérabilité et le partage des données.

c) Qualité des données
   - Les normes et flux de travail partagés assurent l'interopérabilité avec d'autres systèmes d'information.
   - Amélioration de la qualité des données grâce à la validation automatisée.

d) Contrôle et évaluation
   - Prise de décision basée sur les données grâce à des processus d'exploration de données.
   - Meilleur suivi et évaluation des interventions de santé publique grâce à une meilleure disponibilité des données et à des outils d'analyse automatisés.

e) La gestion des coûts
   - Réduction des coûts de gestion des épidémies.
   - Réduction des coûts de santé publique grâce à la détection plus précoce des épidémies.

La mise en œuvre et le maintien du EIS des États membres de l'UA pour la surveillance électronique nécessitent l'engagement et la participation de multiples parties prenantes. Le tableau 2 ci-dessous décrit les responsabilités de mise en œuvre de haut niveau par domaine de rôle et fournit le cadre de mise en œuvre associé.

Tableau 2. États membres de l'UA EIS pour les domaines de rôle et les responsabilités de la surveillance électronique

DOMAINE DE RÔLE	RESPONSABILITÉS DE MISE EN ŒUVRE	[voir Légende]
La mise en œuvre de la politique		
Cadre de gouvernance	Adopter les principes du EIS des États membres de l'UA pour la gouvernance de la surveillance électronique	[3]
	Surveiller l'adoption des principes de gouvernance	[1, 2]
	Surveiller et évaluer la mise en œuvre du EIS du système de surveillance électronique	[1, 2]
	Superviser la planification, la mise en œuvre, le suivi et l'évaluation, et l'amélioration du système de surveillance électronique	[1]
Cadre juridique	Mettre en œuvre les mesures réglementaires recommandées si nécessaire	[2]
	Surveiller les progrès de la mise en œuvre des actions réglementaires légales	[1, 2]
Politique de partage des données	Mettre en œuvre les politiques de partage des données EIS des Étatsmembres de l'UA pour la surveillance électronique et contribuer à leur évolution et à leur perfectionnement continus	[1, 3, 4]
	Surveiller la mise en œuvre de la politique de partage des données	[1, 2]
Accord de partage de données	Examiner et signer l'accord de partage de données	[3]
	Assurer la résolution en temps opportun des dérogations temporaires à l'accord de partage de données de l'UA	[1, 3]
Politique de confidentialité et de sécurité des données	Mettre en œuvre et se conformer aux EIS des États membres de l'UA pour les politiques de confidentialité et de sécurité des données de surveillance électronique	[1, 3]
	Surveiller la mise en œuvre des politiques de confidentialité et de sécurité des données	[1, 3]
Mise en œuvre des normes		

DOMAINE DE RÔLE	RESPONSABILITÉS DE MISE EN ŒUVRE	[voir Légende]
Normes techniques	Tenir à jour et fournir des commentaires au besoin pour l'évolution des normes de sécurité de la couche de transport et de la couche de transport de l'GTII	[1, 3, 5]
	Maintenir la connaissance et fournir des commentaires au besoin pour le INNT et les normes de hachage connexes	[1, 3, 5]
	Maintenir la connaissance et fournir des commentaires au besoin pour les normes W3C XML et GTTAHW HTML	[1, 3, 5]
Normes de messagerie	Assurer la représentation de l'UA au sein des organismes de normalisation de la messagerie : • HL7 RIRS • HL7 V2.5.1 • HL7 V3 ADC	[1, 3]
	Fournir une représentation de l'UA sur l'évolution de la norme EDA	[1, 3]
Normes de profil d'intégration	Assurer la représentation de l'UA au sein de l'organisme de normalisation IHE	[1, 3, 4]
	Fournir une représentation de l'UA au sein de l'organisme de normalisation Open EIS	[1, 3, 4]
Normes de sécurité	Mener des examens et des évaluations annuels des risques de sécurité	[1, 3]
	Surveiller et évaluer la conformité à la politique de sécurité des fournisseurs de services cloud	[1]
	Mener des audits annuels indépendants de la qualité des services et de la conformité à la politique de sécurité	[5]
Normes de vocabulaire	Assurer la représentation de l'UA dans les organismes de normalisation du vocabulaire : • CIM-11 • NCIOL • Norme Rx • SNOMED-CT	[1, 3]
	Sélectionner les termes préférés pour la surveillance et la riposte aux maladies de santé publique	[1, 3]
Mise en œuvre opérationnelle		
Infrastructure en nuage (C.12)	Sélectionnez le(s) fournisseur(s) de services cloud	[1]
	Migrer la surveillance électronique vers le cloud	[1, 3]
	Fournir une puissance de calcul, un hôte physique (stockage de base de données), la diffusion de contenu et d'autres ressources liées au réseau de manière évolutive et durable	[5]
Gestion de données	Gérer les données, les appareils et les identifiants de compte	[1, 3]
	Fournir une sauvegarde des données	[5]
Ressources de financement	Élaborer un plan d'action quinquennal avec des estimations de coûts associées pour les premiers États membres de l'UA EIS pour le financement de la surveillance électronique	[1]
	Investir dans le développement des infrastructures	[1, 2, 3, 4]
Services partagés	Spécifier et développer l'ensemble initial de services partagés	[1, 3]
	Contribuer au développement et à la mise en œuvre continus des services partagés	[1, 3]
Sécurité	Collaborer pour mettre en œuvre des modèles de sécurité conformément aux normes recommandées à la section 5.3	[1, 3]
	Appliquer des normes de sécurité cloud compatibles avec les normes de sécurité CDC Afrique	[5]
Développement de la main-d'œuvre	Offrir une formation technique en informatique de santé publique	[1, 4]
	Offrir une formation sur la surveillance et la riposte en santé publique	[1, 4]
	Fournir une formation sur l'utilisation des EIS des États membres de l'UA pour la surveillance électronique	[1, 3]

Légende: [1] CDC Afrique; [2] États membres de l'UA ; [3] INSP des États membres de l'UA ou équivalent ou ministère de la Santé ; [4] Partenaire(s) ; [5] Prestataire(s) de services

7. États membres illustratifs de l'UA EIS pour les cas d'utilisation de la mise en œuvre de la surveillance électronique

La section suivante fournit des cas d'utilisation décrivant comment la politique et les normes fournies dans la section B peuvent être appliquées à des domaines pathologiques spécifiques.

7.1. Surveillance basée sur les cas de COVID-19

But

Ce cas d'utilisation de la surveillance électronique offre un moyen standard d'envoyer par voie électronique des données de cas et de laboratoire COVID-19 au CDC africain, sur la base des politiques et des normes énoncées dans les recommandations du groupe de travail EIS du CDC africain.

Mise en œuvre

La figure 2 met en évidence les détails de mise en œuvre nécessaires pour réaliser ce cas d'utilisation.

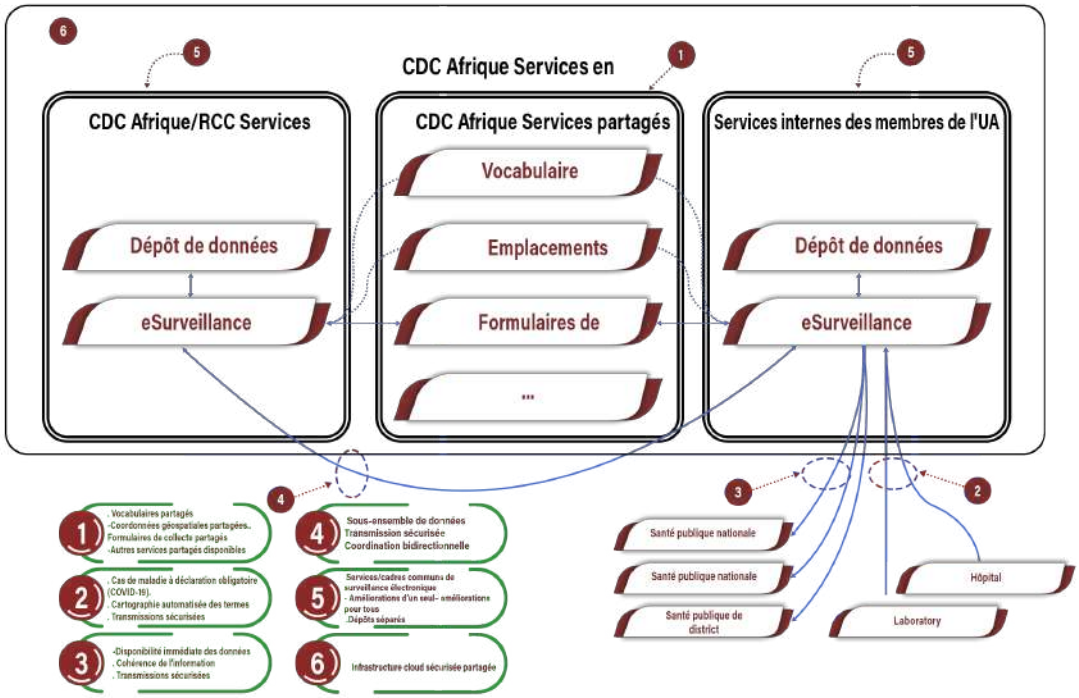

Figure 2. Mise en œuvre pour le cas d'utilisation COVID-19

Le graphique ci-dessus comprend les éléments suivants (tels qu'identifiés par chaque numéro encerclé) :

1. Services utilisés par toutes les instances de e-Surveillance et hébergés par CDC Afrique. Les services comprennent des normes définies par le CDC africain comme les termes et codes préférés, un registre des emplacements pour prendre en charge la cartographie EIS géospatiale et l'affichage des données de santé publique, des formulaires de collecte de données de santé publique précédemment développés avec un vocabulaire intégré qui peut être rapidement réutilisé par plusieurs États membres de l'UA, comme ainsi que d'autres services partagés et métadonnées pertinentes selon les besoins. Pour ce cas d'utilisation, tous les services de surveillance électronique des membres de l'UA peuvent facilement réutiliser un seul formulaire de collecte de données COVID-19 qui est mappé sur des terminologies standard. Le service de vocabulaire serait établi sur la base de ce que le groupe de travail CDC Afrique EIS for e-Surveillance dit qu'il devrait être fait.

2. Notification des maladies à déclaration obligatoire directement dans le système de surveillance électronique de l'État membre de l'UA à partir de sources hospitalières et de laboratoire conformément à leurs directives nationales respectives en matière de notification de surveillance. La saisie des données source peut se faire via une application Web utilisant des appareils mobiles et des ordinateurs. La terminologie source serait automatiquement mappée et transformée aux messages HL7 RIRS avec les documents de cas associés. Toutes les transmissions de données se feraient via un canal de réseau sécurisé pour assurer la sécurité et la confidentialité des données.

3. Le ministère de la Santé (MoH) de l'État membre ou le système national d'information sur la santé publique (INSP) ou équivalent, ainsi que les bureaux de santé publique régionaux et de district concernés, peuvent voir immédiatement les données déclarées. Tous les niveaux partagent les mêmes informations, ils ont donc tous la même image de l'évolution de la pandémie de COVID-19.

4. Un sous-ensemble de données déclarées est également immédiatement disponible pour le CDC Afrique (sur la base de l'accord de partage de données avec les États membres de l'UA). Les données seraient transmises au service de surveillance électronique CDC Afrique/CCR via des messages HL7 RIRS avec les données de cas et les documents associés. Toutes les transmissions de données se feraient via un canal de réseau sécurisé. Un sous-ensemble distinct de données déclarées peut également être immédiatement mis à la disposition de l'OMS (sur la base des directives de l'OMS et des accords d'utilisation des données). Les données seraient transmises à l'OMS via un format approprié fondé sur des normes. Toutes les transmissions de données se feraient via un canal de réseau sécurisé.

5. Solutions de santé numérique de surveillance électronique basées sur des normes communes résidant sur différents serveurs pour soutenir à la fois le CDC africain et chaque État membre de l'UA. Travailler en tant que communauté de pratique contribuera et

partagera des ressources, des experts, des efforts et des artefacts technologiques au profit de chaque participant de l'UA utilisant la solution de surveillance électronique. Des référentiels de données de santé publique distincts pour le CDC africain et chaque État membre de l'UA protègent les données nationales, mais avec des éléments de données définis communs, des définitions d'éléments et des structures permettraient un partage et un échange faciles des ensembles de données autorisés (à la fois entre l'État membre de l'UA et le CDC africain , mais aussi potentiellement entre d'autres membres de l'UA (par exemple, alertes à un État membre voisin d'une incidence accrue de cas de COVID-19 le long d'une frontière commune)).

La plate-forme pour CDC Afrique, les États membres de l'UA et les parties partagées de cette mise en œuvre peuvent être soit un environnement de services cloud (fourni par CDC Afrique, l'UA ou un fournisseur de services cloud tiers disposant d'installations sur le continent ; voir également Section 9) ou des centres de données détenus et gérés séparément par le CDC Afrique et chaque État membre. Le premier scénario réduit les coûts (pour l'équipement et les ressources), facilite le partage des données et facilite le partage des services et des mises à jour logicielles/système. Ces deux plans assurent la sécurité des données nationales.

Pour la réponse à la COVID-19, les rapports des États membres incluraient les éléments de données indiqués dans les annexes 6 et 7.

Évaluation

Le tableau 3 ci-dessous fournit une évaluation comparative entre les fonctionnalités actuelles de surveillance et de notification intégrées des maladies et la solution de surveillance électronique COVID-19 proposée.

Tableau 3. Évaluation de la solution de surveillance électronique pour la réponse au COVID-19

ZONE	FONCTIONNALITÉ ACTUELLE	FONCTIONNALITÉ DE SURVEILLANCE ÉLECTRONIQUE
Sécurité et confidentialité	• Pratiques mixtes	• Pratiques communes et uniformes basées sur les politiques et normes partagées des États membres de l'UA
Conformité aux normes	• Pratiques mixtes • Pas de norme uniforme	• Système uniforme commun, échange de données et normes de vocabulaire basés sur les recommandations de l'CDC Afrique EIS TF et convenus par consensus par les États membres
Évolutivité	• Non évolutif • Fonctionnalité cloisonnée	• Hautement évolutif dans un environnement cloud - le stockage de données et les ressources de calcul peuvent être ajoutés ou supprimés en quelques heures • La solution de services de surveillance électronique partagés soutient l'avancement pour tous les États membres de l'UA • Les services partagés garantissent la disponibilité rapide de nouveaux termes de vocabulaire, de nouveaux formulaires de collecte de données et de nouvelles données de localisation pour tous les participants à la surveillance électronique
Durabilité	• Pas viable à long terme • Ressources et temps importants nécessaires pour mettre en œuvre les changements	• Hautement durable • Le partage des connaissances et la formation pour une plate-forme commune soutiennent le mouvement rapide des ressources de santé publique entre les États membres et permettent au CDC africain de coordonner plus efficacement la surveillance continentale et la réponse à une pandémie • La solution commune de services de surveillance électronique permet une base de référence centralisée qui peut évoluer simultanément pour tous les membres de l'UA
Fluidité et facilité d'utilisation	• Ne peut pas être facilement traduit en un événement régional ou continental • Nécessite un développement de formation distinct pour chaque système distinct • Le personnel ne peut pas être facilement déplacé vers d'autres endroits dans le cadre de la réponse à la pandémie	• L'environnement cloud offre des avantages supplémentaires pour l'adoption rapide de la solution de surveillance électronique des États membres de l'UA (c'est-à-dire la nécessité de mettre en place et de maintenir un centre de données) • Développement de formation plus rentable • Amélioration de la facilité d'utilisation et de la capacité de réaffecter les ressources de santé publique à d'autres régions/emplacements à l'appui de la réponse à la pandémie
Rentabilité	• Pas rentable	• Coût inférieur pour le développement centralisé spécifique à l'UA par rapport à l'investissement redondant des États membres de l'UA • Réduction des coûts de déploiement dans un environnement cloud • Réduction des coûts à long terme en utilisant un environnement cloud pour augmenter ou réduire les ressources (c'est-à-dire ne payer que ce qui est nécessaire pour une période donnée)
Impact sur la décision	• Le manque de données opportunes et précises a une incidence sur la précision des prévisions de propagation de la maladie et le processus de prise de décision associé	• Des données cohérentes permettent une comparaison immédiate de l'état de la pandémie sur le continent, membre par membre • Permet des recommandations de santé publique et des contributions aux décideurs sur la base de la dernière image de la situation

ZONE	FONCTIONNALITÉ ACTUELLE	FONCTIONNALITÉ DE SURVEILLANCE ÉLECTRONIQUE
Probabilité de succès	• Mélange diversifié de processus papier et électroniques • Pas d'alignement cohérent avec les principes du développement numérique	• Application uniforme des principes du développement numérique via une plateforme commune • Plus grandes possibilités de réutilisation et rapidité de déploiement
Technologie	• Combinaison de systèmes et de technologies basés sur des normes et non basés sur des normes	• Ensemble de normes communes et convenues • Construit sur des normes reconnues de l'industrie

7.2. Surveillance basée sur les cas de VIH

But

Ce cas d'utilisation de la surveillance électronique fournit une méthode standard pour envoyer par voie électronique des données de cas de VIH et de laboratoire à CDC Afrique sur la base des politiques et des normes habilitantes spécifiées dans les recommandations du groupe de travail EIS de CDC Afrique.

Flux de données déclarables

CDC Afrique utiliserait la solution EIS for e-Surveillance pour soutenir la notification directe des données basées sur les cas de VIH des États membres aux CCR CDC Afrique ou directement à CDC Afrique pour les opérations futures sur le continent. Chaque nouveau cas de VIH serait signalé immédiatement si le test de laboratoire d'un patient se révélait positif. Au fur et à mesure que les médicaments de thérapie antirétrovirale (TRA) sont distribués, la conformité aux plans de traitement du VIH serait également signalée. La solution EIS for e-Surveillance permettrait aux États membres et aux entités déclarantes (telles que les hôpitaux et les laboratoires) de la région de collecter plus facilement des données détaillées (c'est-à-dire via un appareil mobile ou un ordinateur via des canaux de transmission de messages sécurisés), ainsi que de collecter plus types de données. Avec la solution EIS for e-Surveillance, le CDC Afrique serait en mesure de collecter de manière automatisée des données agrégées et prédéfinies basées sur des indicateurs auprès des États membres de l'UA. Au fur et à mesure que la riposte continentale au VIH évolue et se dirige vers la suppression du VIH dans la population africaine, le sous-ensemble d'indicateurs basés sur les cas changera également pour mieux soutenir la riposte continentale au VIH (par exemple, plus de détails sur la démographie des cas, les perdus de vue, décès dont le VIH/SIDA est la cause principale ou une comorbidité contributive, etc.). La solution peut également se connecter directement aux appareils de test de laboratoire et aux systèmes de dossiers médicaux électroniques des hôpitaux qui peuvent partager des données. Cela accélère la notification au sein des États membres.

Mise en œuvre

La mise en œuvre de ce cas d'utilisation sera similaire à la mise en œuvre prévue pour le cas d'utilisation COVID-19. Pour les États membres, leur instance de surveillance électronique suivra les données basées sur les cas de VIH, fournissant un ensemble de données plus riche pour la requête et l'analyse, et pour l'extraction d'ensembles de données agrégées selon les besoins du CDC Afrique. Les principales différences seront :

a) Différences dans les éléments de données rapportés (par exemple, initiation du TAR ; retrait des médicaments du TAR ; traitements de prévention de la transmission mère-enfant) (voir également l'annexe 2).
b) Différences dans les termes de vocabulaire (par exemple, pour la récence du VIH et les résultats des tests CD4 ; pour l'inclusion des données sur la tuberculose et les maladies sexuellement transmissibles)
c) Utilisation de la norme EDA pour l'échange de données agrégées entre les systèmes de surveillance électronique des États membres et l'instance de surveillance électronique du CDC africain.
d) Possibilités de consolidation des rapports aux partenaires externes.

Évaluation

Pour le cas d'utilisation de la surveillance basée sur les cas de VIH, l'évaluation de la fonctionnalité actuelle vs. La fonctionnalité EIS pour e-Surveillance est similaire à ce qui a été fait pour le cas d'utilisation COVID-19 dans la section précédente. Le EIS pour e-Surveillance peut également être utilisé pour des activités liées à la gestion des maladies chroniques.

7.3. Cloud et services partagés

Modèles recommandés

Les avantages du cloud et des services partagés pour EIS pour la mise en œuvre et le déploiement de la surveillance électronique sont décrits dans les tableaux 4 et 5 ci-dessous.

Tableau 4. Avantages de l'infrastructure cloud pour les États membres de l'UA EIS pour la surveillance électronique.

ZONE	AVANTAGES DE L'INFRASTRUCTURE CLOUD
Économies d'échelle	• Tirer parti des ressources informatiques, de la capacité de stockage de données, de la disponibilité continue de l'alimentation, des ressources de centre de données formées, des outils de gestion de centre de données et des options de connectivité Internet des centres de données tiers existants basés sur le cloud réduit le temps de développement et les coûts d'investissement initiaux, réduit les dépendances à long terme liés aux coûts d'infrastructure irrécupérables, fournit une évolutivité de l'infrastructure à la demande (vers le haut ou vers le bas selon les besoins) et maintient l'accent sur la principale mission de surveillance et d'intervention en ligne du CDC africain. • L'utilisation de fournisseurs de services cloud sur le continent pour les opérations quotidiennes d'CDC Afrique EIS pour les opérations de surveillance électronique réduit les coûts de communication longue distance (les centres de données hors continent0, cependant, peuvent toujours être utilisés à des fins de repli à court terme.
Flexibilité/modularité	• La prévision et la gestion des capacités de calcul, de stockage et de charge de pointe nécessaires sont informées par les projections de planification et d'analyse du centre de données, ce qui n'entraîne que des coûts pour la capacité utilisée au lieu de la capacité excédentaire inutilisée, comme ce serait le cas dans un scénario de centre de données autonome. • L'ajout et la suppression de serveurs, de stockage et de capacités de communication peuvent être gérés par le CDC africain et provisionnés ou dé provisionnés immédiatement, ce qui permet une plus grande flexibilité pour répondre aux pics d'événements de maladie et aux accalmies d'événements de maladie.
Externalisation des infrastructures	• Éviter la propriété d'actifs informatiques qui se déprécient rapidement • Fournir des coûts d'infrastructure prévisibles d'une année sur l'autre
Actualisation de la technologie	• Étant donné que toutes les technologies d'infrastructure ont une éventuelle fin de vie, l'utilisation d'un fournisseur de services cloud tiers garantit la disponibilité de la technologie la plus récente en constante évolution et surmonte les problèmes liés à l'obsolescence technologique et au non-support.
Disponibilité/fiabilité	• La spécification de niveaux de disponibilité et de fiabilité garantis via des accords de niveau de service permet de réduire les coûts mensuels lorsque les niveaux de service garantis ne sont pas atteints. • Un audit tiers indépendant des performances des fournisseurs de cloud offre une visibilité sur les problèmes potentiels des fournisseurs et identifie des étapes mesurables pour l'amélioration des processus et des services afin de respecter les niveaux de meilleures pratiques internationales.
Sécurité	• L'examen des politiques, des procédures et des artefacts de processus du fournisseur de services cloud fournit une indication directe de la manière dont le fournisseur gère la sécurité, la capacité de survie et l'intégrité des données et de la plate-forme. • Le contrôle de la sécurité du centre de données garantit que seul le personnel autorisé a accès aux ressources cloud prenant en charge les opérations d'CDC Afrique.

Tableau 5. Avantages des services partagés pour EIS pour la surveillance électronique.

ZONE	AVANTAGES DES SERVICES PARTAGÉS
Économies d'échelle	• Le développement d'un service une seule fois, puis le partage de ce service avec tous les États membres évite la duplication des temps de développement et des investissements. • La centralisation de certains services partagés permet aux États membres de disposer d'un retour d'information sur les performances des services et de mettre l'accent sur l'amélioration continue des processus du service. • La contribution d'un État membre à un service partagé rend les améliorations du service immédiatement disponibles pour tous les autres États membres.
Standardisation des processus	• L'utilisation d'outils, de services et de référentiels communs partagés expose chacun à un examen plus large, à des cas d'utilisation potentiels élargis et à une réutilisation facile des meilleures pratiques dans les États membres.
Plate-forme technologique commune de logiciels et de services	• Permettre une transformation coordonnée des front, middle et back-offices. • Fournir de nouveaux services qui répondent aux besoins du plus grand nombre de participants au CDC Afrique.
Culture	• L'optimisation de l'utilisation des ressources de formation garantit un large éventail de personnel doté des compétences et de l'état d'esprit nécessaires pour optimiser un modèle de services partagés particulier au-delà du back-office.
Membre INSP ou équivalent libre de se concentrer sur ses opérations et ses clients externes	• S'appuyer sur des services partagés pour le soutien réduit les dépenses individuelles des États membres pour ces services, au lieu de répartir le coût de chaque service selon une répartition prédéterminée entre tous les États membres.
Membre INSP ou équivalent libre de se concentrer sur la stratégie	• S'appuyer sur des services partagés pour la conformité, les contrôles et les informations statutaires permet de se concentrer davantage sur la prise de décision sur les stratégies de prévention et de réponse aux maladies.
Aide à la décision	• Veiller à ce que les données soient analysées et fournies sous forme d'informations fiables et exploitables
La flexibilité	• Fournir des services partagés à plusieurs canaux de distribution et/ou emplacements géographiques, ainsi que de nouvelles opportunités d'utilisation/réutilisation d'investissements irrécupérables.
Évolutivité	• La mise à l'échelle du modèle de prestation de services partagés permet une expansion rapide de la portée avec des coûts supplémentaires relativement faibles.

Pour réaliser la connectivité de surveillance continentale, CDC Afrique fournira une plate-forme de surveillance électronique sécurisée et interopérable basée sur le cloud, un logiciel en tant que service (SaaS) et un backend mobile en tant que service (MBaaS) qui centralise et partage les services informatiques communs nécessaires à la surveillance des maladies. En outre, le CDC Afrique et l'Union africaine aideront à créer des services cloud et partagés similaires entre les États membres pour un accès facile aux données.

Dans le cadre de l'CDC Afrique EIS for e-Surveillance, la mise en œuvre du modèle de cloud computing prendra l'une des formes suivantes :

a) **Infrastructure cloud CDC Afrique** - détenue, gérée et exploitée par CDC Afrique, et mise à disposition pour une utilisation exclusive par CDC Afrique et les États membres

de l'UA pour EIS pour la surveillance électronique afin d'atteindre des politiques et des exigences partagées. Cela est conforme au *Statut des Centres africains de contrôle et de prévention des maladies (CDC Afrique)* qui stipule que CDC Afrique est une institution appartenant à l'Afrique, les États membres conservant simultanément la propriété nationale de l'CDC Afrique, à la fois en tant que conseillers et par le biais direct. engagement programmatique. Cela représente le modèle de mise en œuvre le plus rapide car il serait entièrement sous le contrôle du CDC africain.

b) **Infrastructure cloud de l'UA** - détenue, gérée et exploitée par l'UA, et fournie pour répondre à une gamme de besoins informatiques, de réseautage et de services sur le continent africain pour elle-même et ses États membres, y compris EIS pour la surveillance électronique pour l'CDC Afrique et État membre INSP ou équivalent. Ce modèle n'est peut-être pas aussi rapide qu'une approche de cloud privé car il nécessite l'adhésion des États membres de l'UA. Cependant, l'adoption de ce modèle peut encourager les membres de l'UA à accélérer leur utilisation des services et outils partagés, ainsi que l'intégration d'autres services de santé numérique et de m-santé exclusivement à l'usage des membres.

c) **Infrastructure cloud hybride** - une combinaison des infrastructures cloud ci-dessus liées par une technologie standardisée pour permettre la portabilité des données et des applications (par exemple, l'équilibrage de charge entre les clouds). L'utilisation de (au moins) deux nuages offre la possibilité de répartir stratégiquement les considérations opérationnelles entre deux fournisseurs distincts (par exemple, le nuage CDC Afrique pour fournir des EIS opérationnels au jour le jour pour les services de surveillance électronique et le nuage AU pour sauvegarder les EIS pour les services de surveillance électronique). Données de surveillance) fournissant une réduction des risques dans le cas où un fournisseur deviendrait non viable à un moment donné dans le futur.

Parmi ces trois, le CDC africain recommande l'adoption du modèle d'infrastructure cloud du CDC africain dans l'immédiat et que l'UA fournisse son propre modèle d'infrastructure cloud continental de l'UA pour soutenir le modèle d'infrastructure cloud hybride ci-dessus à long terme. Les conditions préalables à une mise en œuvre réussie de l'infrastructure et des services basés sur le cloud sont présentées à l'annexe 9.

Services partagés requis

Les EIS des États membres de l'UA pour la surveillance électronique doivent fournir au minimum les services de référentiel partagé suivants :

a) **Service unique de gestion et d'appariement des identifiants d'entité -** fournissez un identifiant numérique unique de patient pour chaque patient dans toutes les applications du continent. Ce service facilite l'accès à des données démographiques et médicales essentielles précises et à jour sur les patients à partir de bases de données dans les États membres de l'UA. Les normes d'intégration et de mappage de profil recommandées à la section 4.5 seront mises en œuvre ici. Cela fournira des données et des outils pour associer rapidement de nouvelles données aux données précédemment déclarées afin d'éviter la duplication des décomptes de maladies à déclaration obligatoire (par exemple, nombre de tests, nombre d'infectés, nombre de personnes traitées, nombre de personnes récupérées, nombre de décès, nombre de personnes perdues de vue, etc.) , et assurer des rapports cohérents pour la planification, la prise de décision et l'efficacité de la riposte aux maladies. CDC Afrique ne recevra pas les identifiants réels des États membres mais utilisera ce service interne.

b) **Service de données géospatiales de localisation** - fournit des données et des outils pour associer un nom de lieu (par exemple, province, ville, hôpital, clinique) à ses coordonnées géospatiales associées ou à une entité géospatiale (par exemple, un fichier de forme) pour prendre en charge l'utilisation d'outils de cartograpEIS pour la surveillance, le suivi et la notification de l'état de la réponse en fonction de la localisation des maladies.

c) **Service de vocabulaire** - fournit des données et des outils pour identifier l'ensemble préféré de termes de vocabulaire et de concepts associés à la déclaration de maladies spécifiques afin d'assurer la cohérence des rapports des INSP des États membres ou équivalent et d'accélérer l'analyse de la progression de la maladie par CDC Afrique. Cela peut également inclure le mappage entre ces termes préférés et des termes équivalents pour faciliter le traitement automatisé des messages et la transformation dans la nomenclature préférée pour l'analyse des données. Cela favorisera l'interopérabilité de la surveillance des maladies entre les plateformes hétérogènes. Une terminologie et une nomenclature communes de surveillance des maladies seront utilisées, comme mentionné à la section 4.4, sur tout le continent pour partager en toute sécurité les informations de surveillance des maladies à l'aide de l'infrastructure basée sur le cloud.

d) **Service de partage de formulaires de collecte de données** - fournit des données et des outils pour définir les formulaires de collecte de données, les éléments de données et les vocabulaires associés pour la notification de maladies spécifiques à réutiliser par les États membres pour faciliter l'échange de données de santé publique et accélérer la diffusion des orientations de collecte de données à tous les États membres INSP de l'État ou équivalent.

Le EIS des États membres de l'UA pour la surveillance électronique doit fournir au minimum les services d'application suivants :

a) **E-Surveillance [saisie de données]** - fournit des outils pour gérer la saisie de données déclarables provenant des laboratoires et des hôpitaux des États membres.

b) **E-Surveillance [récupération et affichage des données]** - fournit des outils pour alerter les autorités de santé publique nationales, régionales et de district de la disponibilité de nouvelles données et pour accéder et afficher les données disponibles avec des contrôles appropriés sur la visibilité des données à chaque niveau. De même, fournir des outils pour alerter le CDC Afrique et le CCR associé de la disponibilité de nouvelles données publiées par une autorité nationale de santé publique d'un État membre et pour accéder et afficher les données disponibles avec des contrôles appropriés sur la visibilité des données.

c) **E-Surveillance [diffusion de données]** - fournit des outils pour affecter la publication et le transfert de nouvelles données au CDC Afrique et au CCR associé pour traitement. De même, fournir des outils pour affecter la publication et le transfert des données du CDC Afrique à l'OMS.

d) **E-Surveillance [coordination]** - fournit des outils permettant au CDC africain et aux autorités nationales de santé publique des États membres de collaborer sur des données partagées et des plans d'intervention.

e) **E-Surveillance [service de prise de décision et de visualisation des données]** - fournit les outils d'aide à la décision pour l'analyse des données, la visualisation des données, la diffusion de l'information, la prévision des maladies, la détection en temps réel des épidémies, les services d'alerte de santé publique et les composants réutilisables du tableau de bord des maladies pour faciliter l'évaluation de la surveillance actuelle des maladies et de l'état de la riposte.

Les EIS des États membres de l'UA pour la surveillance électronique doivent fournir au minimum les services de référentiel de données suivants :

a) **Référentiel de données** - fournir aux CDC/CCR africains et à chaque État membre un référentiel de données distinct pour toutes les données sous leur contrôle.

Chacun des ensembles de services ci-dessus sera créé par CDC Afrique soit seul, soit avec l'aide d'un tiers. Le EIS pour la surveillance électronique obtiendra plus de services partagés au fil du temps, en fonction de ce que disent le CDC Afrique et les États membres et de la manière dont ils prévoient d'améliorer le processus.

8. Le développement des infrastructures

L'infrastructure comprend le matériel, les logiciels, les personnes et les processus. Cette section définit les ressources nécessaires pour réaliser le modèle initial basé sur le cloud/services partagés pour l'CDC Afrique EIS pour la e-Surveillance.

Tableau 6. Étapes de développement de l'infrastructure

Étapes de développement de l'infrastructure
Étape 1: Identifier les capacités nécessaires du centre de données
1.1 Définir les capacités minimales du centre de données requises pour le EIS d'un État membre de l'UA pour le fournisseur de services cloud de surveillance électronique.
1.2 Mener une activité de recherche de source pour identifier les fournisseurs de services cloud intéressés et capables de fournir des services cloud à l'appui du EIS pour la surveillance électronique.
Étape 2: Identifier les capacités de services partagés nécessaires
2.1 Définir le service partagé pour la gestion et la correspondance de l'identifiant d'entité unique
2.2 Définir le service partagé pour les données géospatiales de localisation
2.3 Définir le service partagé pour le vocabulaire
2.4 Définir le service partagé pour le partage de formulaire de collecte de données
2.5 Définir le service partagé pour la prise de décision et la visualisation des données
2.6 Définir l'application partagée pour la e-Surveillance
2.7 Définir le modèle de données partagé pour les référentiels de données
Étape 3: Évaluer s'il convient d'internaliser ou d'externaliser pour chaque capacité
3.1 Examinez les réponses aux sources recherchées (à partir de 1.2) et déterminez s'il existe des fournisseurs disposant des capacités requises pour fournir des services cloud pour le EIS pour la surveillance électronique.
3.2 Examiner les services partagés nécessaires pour déterminer ceux qui doivent être développés en interne et ceux qui doivent être externalisés,

Étape 4.a : Pour les capacités externalisées, mener un processus de sollicitation concurrentiel	
4.a.1	Préparer des sollicitations distinctes pour les services
4.a.2	Distribuer chaque sollicitation et effectuer une analyse concurrentielle des réponses
4.a.3	Sélectionnez les réponses gagnantes pour chaque catégorie de services
Étape 4.b : Pour les capacités internes, développer un plan de mise en œuvre	
4.b.1	Affecter des ressources pour chaque service
4.b.2	Élaboration de plans pour chaque service
4.b.3	Spécifiez et passez en revue chaque architecture de service
4.b.4	Mettre en œuvre et revoir chaque service
Étape 5 : Gérer et améliorer/renforcer les capacités au fil du temps	
5.1	Préparer un plan pour la mise en œuvre et les opérations Suivi et évaluation (S&E)
5.2	Développer des ressources de formation et former le personnel de EIS pour les opérations de surveillance électronique
5.3	Effectuer un S&E pour chaque activité de mise en œuvre de service
5.4	Effectuer le suivi et l'évaluation des activités opérationnelles
5.5	Gérer le EIS au jour le jour pour les opérations de surveillance électronique

9. Renforcement des capacités

CDC Afrique et les États membres de l'UA fourniront les ressources nécessaires pour soutenir le EIS des États membres de l'UA pour le système de santé numérique, notamment :

a) Acquisition et approvisionnement de l'infrastructure du système.
b) Acquisition et fourniture de plate-forme(s) de cloud système.
c) Développement de cas d'utilisation basés sur la maladie pour la santé publique afin d'inclure les formats d'échange de messagerie, le contenu des messages et les vocabulaires associés.
d) Conception et développement de registres partagés.
e) Architecture, développement et intégration d'outils communs au système numérique de santé.
f) Audit continu de EIS pour la confidentialité et la sécurité des informations du système de santé numérique.
g) Examen et audit continus du EIS pour l'infrastructure du système de santé numérique et la ou les plateformes infonuagiques.
h) Participation et coordination avec les normes et les organisations partenaires.
i) Offrir des stages à court et à long terme aux étudiants en informatique et en sciences de la santé de niveau licence, master et doctorat du continent.

j) Élaborer un programme de bourses d'études en informatique de la santé et en épidémiologie pour former un cadre d'experts compétents en informatique de la santé et en science des données pouvant être déployés dans les États membres de l'UA.

k) Élaborer un cadre/plan pour favoriser l'engagement du secteur privé pour la durabilité à long terme du système de santé numérique.

10. Investissement

Développer un système de santé et investir dans la santé numérique deviennent une priorité dans les États membres de l'UA. Au cours de la dernière décennie, les États membres de l'UA ont investi de manière significative dans les interventions de santé numérique ; cependant, les décisions d'investissement éclairées envers EIS pour les systèmes de santé numériques manquent. Pour disposer d'un EIS pour les systèmes de santé numériques parmi les États membres de l'UA, un profil d'investissement comprenant un DSE national prenant en charge les EIS nationaux, régionaux et continentaux, un SIS national et un entrepôt de données, un portail patient et des registres (populations) est requis. Les principes suivants peuvent être suivis pour investir dans EIS pour les systèmes de santé numériques parmi les États membres de l'UA :

- **Approche pangouvernementale :** l'investissement pour EIS des systèmes de santé numériques parmi les États membres de l'UA doit suivre une approche pangouvernementale pour développer et mettre en œuvre une plate-forme EIS durable. Cette approche peut fournir des services numériques réutilisables à grande échelle avec un meilleur retour sur investissement [52].
- **Approche d'investissement coopératif** : cette approche invite les clients, les États membres de l'UA, les prestataires de soins de santé et les professionnels de la santé, les partenaires, le secteur privé, les fournisseurs de logiciels, de matériel et de services de santé numérique à se réunir pour investir dans EIS parmi les systèmes de santé numériques [53].
- **Cadre de dossier d'investissement :** pour investir dans le EIS pour les systèmes de santé numériques, il est nécessaire de comprendre les intrants, les processus, les extrants et les avantages. Le Mécanisme de financement mondial [54] a suggéré une approche pour développer un cadre de dossier d'investissement qui soutiendra l'investissement requis. Ce cadre, comme le montre la figure 3, doit être adopté par les États membres de l'UA pour une mise en œuvre réussie des EIS pour les systèmes de santé numériques.

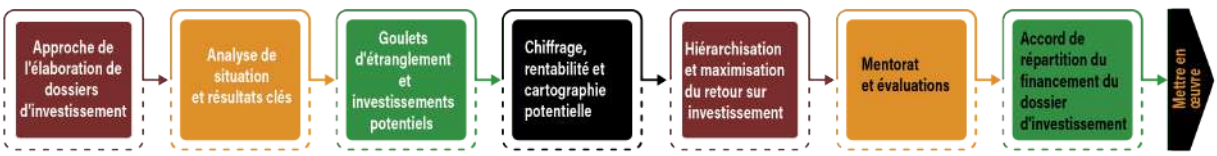

Figure 3: Cadre d'investissement du EIS pour les systèmes de santé numériques des États membres de l'UA. Source: Mécanisme de financement mondial [54].

- **Outil d'examen des investissements dans le cadre numérique :** les États membres de l'UA doivent utiliser l'outil d'examen des investissements dans le cadre numérique développé par Measure Evaluation [55]. L'outil fournit des conseils de haut niveau basés sur les meilleures pratiques largement acceptées telles que le principe du développement numérique et les principes d'investissement des donateurs qui peuvent être utilisés pour soutenir l'investissement stratégique dans l'utilisation des technologies numériques pour soutenir la santé publique et mondiale.

11. Suivi, évaluation et recherche

Les objectifs du suivi, de l'évaluation et de la recherche comprennent :

- Suivre les progrès vers la mise en œuvre de la politique et des normes de l'UA EIS,
- Identifier les différences critiques entre la mise en œuvre prévue et la mise en œuvre réelle,
- Identifier les obstacles et les facilitateurs de la mise en œuvre,
- Identifier et transmettre les priorités futures en entreprenant des recherches scientifiques

La surveillance doit inclure une évaluation manuelle et automatisée continue du EIS pour la mise en œuvre, le déploiement, l'adoption et l'utilisation du système de santé numérique. L'évaluation comprendra un examen du EIS pour la pertinence, l'efficacité, l'efficience et l'impact du système de santé numérique en termes d'évolution des buts et objectifs d'CDC Afrique. Les actions de suivi et d'évaluation spécifiques pour l'infrastructure du système de santé numérique EIS doivent inclure :

a) Sondage annuel de EIS pour les utilisateurs du système de santé numérique et le personnel de soutien afin de déterminer les niveaux de satisfaction, les services qui fonctionnent comme prévu, les services qui ne fonctionnent pas comme prévu et les domaines potentiels d'amélioration.
b) Visite initiale sur site des fournisseurs de services cloud pour examiner les politiques, les procédures et les artefacts de procédure existants ; évaluer l'état de sécurité du centre de données ; observer les opérations du centre de données ; et établir une évaluation de base et toute recommandation de changement de fournisseur.

c) Examen annuel du ou des rapports d'audit indépendants pour les fournisseurs de services cloud. Ces audits indépendants doivent être menés conformément aux normes d'audit internationales acceptées (par exemple, IISA 3402, SAEC 16, etc.).
d) Évaluation annuelle des performances du fournisseur de services cloud et élaboration de recommandations pour l'amélioration des services et/ou d'autres options de services cloud.
e) Test annuel des processus de basculement et de récupération des données du fournisseur de services cloud et examen des temps de réponse, du potentiel d'interruption des services et des recommandations d'amélioration.
f) Suivi de toutes les mesures prises pour mettre en œuvre chaque recommandation de S&E.

Les actions de suivi et d'évaluation spécifiques pour le EIS pour l'adoption et l'utilisation du système de santé numérique doivent inclure :

a) Mesurer et suivre la participation des États membres et l'adoption des meilleures pratiques promulguées par l'ANPHI.
b) Utilisation par les États membres du EIS pour les systèmes de santé numériques.
c) Progrès des États membres vers l'alignement et la maturité dans la réalisation des politiques, réglementations et normes détaillées dans les sections A et B.
d) Suivi de l'adhésion et de la participation aux organismes de normalisation de la messagerie et du vocabulaire.

Les actions spécifiques de S&E pour le EIS pour les opérations des systèmes de santé numériques doivent inclure :

a) Évaluation continue de l'amélioration de la qualité des données de chaque État membre.
b) Achèvement et utilisation efficace du EIS pour les ressources de formation du personnel de santé numérique.
c) Évaluation continue des charges de travail relatives, des temps de réponse et de la qualité de la prise de décision basée sur l'adoption du EIS pour la santé numérique au fil du temps.
d) Évaluation des mises en œuvre pilotes du EIS pour la santé numérique et recommandations d'amélioration avant le déploiement complet.
e) Utilisation d'outils de gestion et de surveillance du cloud pour évaluer l'utilisation, les performances et la santé des services, des applications, de l'infrastructure et des charges de travail du cloud.

Pour une mise en œuvre réussie de la politique et des normes EIS pour les systèmes de santé numériques, les États membres doivent travailler avec les universités nationales, les instituts de recherche et les partenaires pour :

a) Mener une enquête initiale sur la capacité des États membres en termes de ressources humaines, d'infrastructures et de finances à mettre en œuvre avec succès la politique et les normes EIS pour les systèmes de santé numériques.

b) Procéder à une évaluation périodique de la mise en œuvre de la politique et des normes EIS pour les systèmes de santé numériques.
c) Entreprendre une recherche scientifique pour identifier les facilitateurs et les obstacles à la mise en œuvre de la politique et des normes EIS pour les systèmes de santé numériques.
d) Mener des examens et des recherches scientifiques pour identifier et faire avancer les priorités futures.
e) Mener des recherches de haute qualité pour déterminer l'impact de la mise en œuvre de la politique et des normes EIS sur l'amélioration de la prestation des services de santé.

Pour les évaluations initiales et périodiques de la mise en œuvre du EIS pour les systèmes de santé numériques, le « Système d'information sur la santés Interoperability Maturity Toolkit » peut être utilisé [56]. La boîte à outils prend en compte les facteurs critiques pour une mise en œuvre réussie du EIS. Le kit comprend trois parties principales : un modèle de maturité, un outil d'évaluation et un guide de l'utilisateur. Le guide de l'utilisateur a une version française qui facilite l'utilisation de la boîte à outils entre les États membres francophones. Le modèle de maturité EIS repose sur trois domaines : leadership et gouvernance ; ressources humaines; et la technologie. Chaque domaine a des sous-domaines, pour un total de 18 sous-domaines.

L'outil d'évaluation peut être utilisé pour déterminer le niveau de maturité des États membres en ce qui concerne l'échange de données sur la santé à partir du niveau des établissements vers le CDC africain, l'OMS, les organismes régionaux africains (CCR et REC), les partenaires et les autres États membres, comme décrit dans le architecture continentale EIS. L'évaluation peut être effectuée avant et après la mise en œuvre de la politique et des normes AU EIS pour les systèmes de santé numériques.

Les références

1. CDC Afrique, *CDC Afrique Strategic Plan*. 2017: Addis Ababa. p. 57.
2. Union africaine, Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, A. Union, Editor. 2014, Union africaine. p. 37.
3. Lovells, H., Aperçu des lois sur la protection des données en Afrique, lexologie, éditeur. 2019, Lexologie.
4. Régulateur de l'information d'Afrique du Sud, Protection of Personal Information Act, 2013, in 4, I.R.S. Africa, Editeur. 2013, Régulateur de l'information d'Afrique du Sud, : Afrique du Sud. p. 156.
5. Otto, M., Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données - RGPD), dans Droit du travail international et européen : Commentaire article par article, E. Ales, et al, Editors. 2018, Nomos Verlagsgesellschaft mbH & Co. KG : Baden-Baden. p. 958-981.
6. Kish, L.J. et E.J. Topol, Les malades ne devraient pas être propriétaires de leurs données médicales. Littérature Biotechnologie 2015. 33(2015) : p. 921-924.
7. Ballantyne, A., Comment devrions-nous envisager la propriété des données cliniques ? 2020. 46(5) : p. 289-294.
8. Kostkova, P., et al, Qui possède les données ? Des données ouvertes pour les soins de santé. 2016. 4(7).
9. Université de Pittsburgh. Accords d'utilisation des données. 2020 [cité le 17/05/2020] ; Disponible sur : https://www.osp.pitt.edu/ccc-data-use-agreements
10. Université de Stanford. FAQ sur l'accord d'utilisation des données (DUA). 2020 [cité 2020 17/05/2020] ; Disponible sur : https://privacy.stanford.edu/other-resources/data-use-agreement-dua-faqs.
11. Dixon, B.E., et al, Une vision pour le contrôle et l'amélioration systématiques de la qualité des données de santé électroniques. Étude sur les technologies de la santé et l'information, 2013. 192 : p. 884-8.
12. Dixon, B.E., et al, Étendre un outil open-source pour mesurer la qualité des données : rapport de cas sur les données de santé observationnelles, la science et l'informatique (OHDSI). BMJ Santé Inform, 2020. 27(1).
13. La Fondation pour la Connaissance Ouverte. Qu'est-ce que l'Open Data ? 2020 [cité 2020 17/05/2020] ; disponible à l'adresse : https://opendatahandbook.org/guide/en/what-is-open-data/#menu.
14. Demski, H., S. Garde, et C. Hildebrand, Des modèles de données ouverts pour des applications interconnectées de santé intelligente : l'exemple de l'openEHR. BMC Méd Inform Decis Mak, 2016. 16(1) : p. 137.
15. Wilkinson, M.D., et al, Les principes directeurs FAIR pour la gestion et l'intendance des données scientifiques. Scientific Data, 2016. 3(1) : p. 160018.
16. Mons, B., et al, Nuageux, de plus en plus FAIR ; revisiter les principes directeurs de FAIR données pour la science ouverte européenne (European Open Science Cloud). Renseignements et utilisation, 2017. 37 : p. 49-56.
17. Waithira, N., B. Mutinda, et P.Y. Cheah, La gestion des données et la politique de partage : la première étape vers la promotion du partage des données. BMC Med, 2019. 17(1) : p. 80.
18. La Fondation Sunlight, Directives pour les politiques de données ouvertes. 3 ed. 2014, Washington, États-Unis : La Fondation Sunlight. 13.
19. Bureau du commissaire à l'information du Queensland. Politique en matière de données ouvertes. 2013 [cité 2020 17/05/2020] ; Disponible sur : https://www.oic.qld.gov.au/publications/policies/open-data-policy.
20. Le Centre sur la sécurité sanitaire mondiale, A Guide to Sharing the Data and Benefits of Public Health Surveillance (Guide pour le partage des données et des avantages de la surveillance de la santé publique). 2017, Londres, Royaume-Uni : The Royal Institute of International Affairs Chatham House 40..
21. Emerson, C., et al, Système mondial de données (WDS) Principes de partage des données. 2015, Zenodo : Genève, Suisse. p. 1.

22. Recherche de données Alliance, Principes de partage des données dans les pays en développement, dans RDA at Atelier international du CDSS sur les données ouvertes. 2014, Research Data Alliance : à Nairobi, au Kénya.
23. Université de Chicago. Accords de partage de données. 2011 [cité 2020 17/05/2020] ; Disponible sur : https://ura.uchicago.edu/page/data-sharing-agreements.
24. Labuschaigne, M., et al, Protéger les participants à la recherche en santé : L'accord sud-africain de transfert de matériel. 2019. Vol. 109. 2019.
25. Ayatollahi, H. et G. Shagerdi, " Évaluation des risques liés à la sécurité de l'information dans les hôpitaux ". Ouvert Méd Informatique J, 2017. 11 : p. 37-43.
26. Thieme, E., Vie privée, sécurité et confidentialité : Vers Trus, E.D. Brian, Editor. 2016, Presses académiques.
27. Zagar, T.R., et al, Evaluation de l'environnement pour le développement des normes CDC Afrique pour la surveillance électronique des maladies de santé publique. 2020.
28. Lauren Wu, P.B.T.C., Recommmandations pour un cadre mondial de soutien à l'échange d'informations sur la santé dans les pays à revenus faibles et moyens. 2016.
29. Kabaso, B. et M. Korpela. Archivage pour l'interopérabilité des systèmes d'information de santé en Afrique. in 8thHealth Informatics in Africa Conference (HELINA 2013). 2013. Eldoret, Kenya : Koegni eHealth, innovation pour le développement e.V. Allemagne.
30. Département national de la santé d'Afrique du Sud, Normes nationales de santé pour l'interopérabilité dans le domaine de la santé en ligne en Afrique du Sud, in 240075. 2014, CSIR et NDoH : Pretoria, Afrique du Sud. p. 381.
31. Organisation mondiale de la santé, Cinquante-huitième Assemblée mondiale de la santé : Résolutions et décisions. 2005, OMS : Genève, Suisse. p. 159.
32. Organisation mondiale de la santé, Soixante-sixième Assemblée mondiale de la santé : Rapport du Conseil exécutif sur ses 131e et 132e sessions 2013, OMS : Genève, Suisse. p. 6.
33. Organisation mondiale de la santé, soixante et onzième Assemblée mondiale de la santé : Utilisation de technologies numériques appropriées pour la santé publique (mHealth). 2018, OMS : Genève, Suisse. p. 5.
34. Organisation mondiale de la santé, soixante et onzième Assemblée mondiale de la santé : Troisième rapport du Comité A. 2018, OMS : Genève, Suisse. p. 8.
35. Ministère de la santé du Ghana, Ghana e-Health Strategy. 2010 : Accra, Ghana. p. 80.
36. Ministère de la santé et de la protection sociale, Stratégie nationale de santé numérique 2019 - 2024. 2019 : Dakar, Tanzanie. p. 62.
37. Ministère de la santé du Kenya, La politique nationale d'e-santé du Kenya 2016 - 2030. 2016 : A Nairobi, Kénya. p. 64.
38. Ministère de la santé du Rwanda, Plan stratégique national de santé numérique 2018-2023. 2018 : Kigali, Rwanda. p. 67
39. Ministère de la santé d'Éthiopie, Éthiopie Architecture eSanté 2017 : Addis-Abeba, Éthiopie. p. 29.
40. Oluwaseyi, A., et al, Modèle d'échange d'informations sur la santé pour le système d'information sanitaire nigérian. Manuel international d'informatique et de sécurité de l'information, 2019. 17(2) : p. 181-203.
41. Comité de l'Institut de médecine sur les normes de données pour la sécurité des patients, S., Patient Safety : La sécurité des patients : une nouvelle norme pour les soins dans La sécurité des patients : une nouvelle norme pour les soins, P. Aspden, et al : La sécurité des patients : une nouvelle norme pour les soins, P. Aspden, et al, éditeurs. 2004, National Academies Press (US) : Washington (DC). p. 550.
42. Les normes d'interopérabilité dans le domaine de la santé numérique : Selection and Implementation in an eHealth Project, in Requirements Engineering for Digital Health, S.A. Fricker, C. Thümmler, and A. Gavras, Editors. 2015, Springer International Publishing : Cham. p. 95-115.
43. Schulz, S., R. Stegwee, et C. Chronaki, Normes dans les données de santé, dans Fundamentals de la science des données cliniques, P. Kubben, M. Dumontier, et A. Dekker, éditeurs. 2019, springer publication internationale : Cham. p. 19-36.

44. Stroetmann, K., Écosystème de santé numérique pour les pays africains : Un guide pour les acteurs publics et privés pour l'établissement d'écosystèmes holistiques de santé numérique en Afrique. 2018, Bonn, Allemagne : Druckriegel GmbH, Frankfurt am Main.
45. Organisation mondiale de la santé, La diffusion mondiale de la santé en ligne : Rendre la couverture sanitaire universelle réalisable. Rapport de la troisième enquête mondiale sur la santé en ligne. 2016, Genève, Suisse : OMS.
46. Adebesin, F., et al, Examen des normes d'interopérabilité dans le domaine de la santé en ligne et impératifs pour leur adoption en Afrique : article de recherche. 2013. 50(1) : p. 55-72.
47. Broyles, D., et al, Chapitre 7 - Évolution de l'infrastructure d'information sur la santé, dans Santé échange d'informations, B.E. Dixon, éditeur. 2016, Académique Press. p. 107-122.
48. Alyea, J.M., et al, Chapitre 9 - Standardisation des données de santé à travers une entreprise, in Health Information Exchange, B.E. Dixon, Editor. 2016, Académique Press. p. 137-148.
49. Lee, M., et al, Développement d'une plateforme commune d'échange d'informations sur la santé pour mettre en œuvre un réseau national d'informations sur la santé en Corée du Sud. Santé Inform Res, 2015. 21(1) : p. 21-29.
50. Appari, A. et M.E. Johnson, Sécurité de l'information et protection de la vie privée dans les soins de santé : État actuel de la recherche. Journal international de la gestion des entreprises Internet, 2010. 6(4) : p. 279-314.
51. Organisation mondiale de la santé. Renforcer la sécurité sanitaire en appliquant le Règlement sanitaire international (2005). 2005 [cité 2020 20/05/2020] ; Disponible sur : https://www.who.int/ihr/about/en/.
52. Union internationale des télécommunications, Schéma d'investissement numérique pour les ODD : Une approche pangouvernementale de l'investissement dans les technologies numériques pour atteindre les ODD. 2019 : Genève, Suisse. p. 136.
53. Stroetmann, K., Écosystème de santé numérique pour les pays africains : Un guide pour les acteurs publics et privés pour l'établissement d'écosystèmes holistiques de santé numérique en Afrique. 2018 : Frankfurt, Allemagne. p. 48.
54. Facilité de financement mondiale et Banque mondiale, Guidance Notice : dossiers d'investissement. 2016 : Washington DC. p. 17.
55. Évaluation des mesures. Ressources mondiales en matière de santé numérique et modèles de maturité : A Summary. 2018 30/1/2021] ; Disponible sur : https://www.measureevaluation.org/resources/publications/fs-18-305#:~:text=Global%20Digital%20Health%20Resources%20and%20Maturity%20Models%3A%20A%20Summary,-Download%20Document%3A&text=Abstract%3A&text=A%20multidimensional%20maturity%20model%20focuses,of%20existing%20digital%20health%20capabilities.
56. Évaluation des mesures. Boîte à outils pour la maturité de l'interopérabilité des systèmes d'information de santé. 2019 30/06/2021] ; Disponible sur : https://www.measureevaluation.org/tools/health-information-systems-interoperability-toolkit.html.
57. Simbini, T., et al, Surveillance des maladies à travers les frontières : systèmes d'information intégratifs régionaux africains. MEDINFO, 2010 : p. 401-405.

Annexes

Annexe 1 : Définitions

La cybersanté est l'utilisation rentable et sécurisée des TIC à l'appui de la santé et des domaines liés à la santé, y compris les services de soins de santé, la surveillance de la santé, la documentation sur la santé et l'éducation, les connaissances et la recherche en matière de santé.

Un écosystème de santé numérique est l'application holistique des technologies de l'information et de la communication pour soutenir et améliorer la prestation des soins de santé ainsi que sa coordination et son intégration entre les prestataires aux niveaux local, de district, national et régional.

Les normes de données englobent les méthodes, les protocoles, les terminologies et les spécifications pour la collecte, l'échange, le stockage, l'analyse et la récupération des informations associées aux applications de soins de santé, y compris les dossiers médicaux, les médicaments, les images radiologiques, le paiement et le remboursement, les dispositifs médicaux et les systèmes de surveillance, et les informations administratives. processus.

La santé numérique implique le développement de systèmes de santé interconnectés utilisant des technologies informatiques, des appareils intelligents et des moyens de communication pour aider les professionnels de la santé et les patients à gérer les maladies et les risques pour la santé, ainsi qu'à promouvoir la santé et le bien-être.

L'interopérabilité implique la capacité de différents systèmes informatiques et applications logicielles à communiquer, à échanger des données et à utiliser les informations qui ont été échangées.

La confidentialité est la liberté de choisir quelles informations sont partagées ou non avec d'autres parties.

La confidentialité est l'obligation de garder secrètes les informations qui vous sont confiées.

La sécurité est la combinaison de mesures de protection administratives, techniques et physiques qui garantissent la confidentialité et favorisent la vie privée.

L'échange d'informations sur la santé est défini comme le transfert électronique d'informations cliniques et/ou administratives entre les organisations, les personnes et la technologie qui hébergent les écosystèmes définis.

Une norme est une manière convenue et reproductible de faire quelque chose.

La santé publique comprend toutes les activités dont le but principal est de promouvoir, restaurer et/ou maintenir la santé à travers le continent, les États membres ou les régions. Cela fait également référence aux personnes, aux institutions, aux ressources et aux politiques que les gouvernements mettent en place pour améliorer la santé publique.

La couverture sanitaire universelle signifie que toutes les personnes et communautés peuvent utiliser les services de santé promotionnels, préventifs, curatifs, de réadaptation et palliatifs dont elles ont besoin, d'une qualité suffisante pour être efficaces, tout en garantissant que l'utilisation de ces services n'expose pas l'utilisateur à des difficultés financières. .

La surveillance électronique est l'utilisation d'appareils numériques pour améliorer la collecte, le partage et la détection des épidémies de données de santé à tous les niveaux du système de santé.

Annexe 2 : Rapports

2.1. Rapports à CDC Afrique des États membres

Cette section traite des normes de messagerie, des normes de vocabulaire et des référentiels de données associés pour chacune de ces limites de système. Le CDC Afrique recommande aux États membres de l'UA d'utiliser les normes décrites ci-dessous non seulement pour la collecte de données de surveillance électronique pour le CDC Afrique, mais également pour leur collecte de données de surveillance électronique interne entre la SIMR nationale et les unités sous-nationales déclarantes, les établissements de santé. et laboratoires d'essais. Idéalement, la surveillance électronique au niveau national, régional/provincial et du district sera une mise en œuvre sécurisée, transparente et interopérable.

Tableau 7. Normes et référentiels associés

STANDARD	RÉFÉRENTIEL DE DONNÉES ASSOCIÉ
Registres de l'état civil (mortalité fœtale, mortalité infantile, décès) - données agrégées et cas par cas	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] Architecture de documents cliniques HL7 v3r2 [document de décès basé sur des cas] HL7 RIRS [messagerie basée sur des cas, échange de documents et de données agrégées] Profil EDA [données agrégées]
Normes de vocabulaire	SNOMED-CT [conditions autorisées à déterminer par CDC Afrique]
Référentiels de support	Conditions autorisées par le CDC africain pour la messagerie des enregistrements d'état civil
Surveillance des maladies à déclaration obligatoire - données agrégées et basées sur les cas	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] Architecture de documents cliniques HL7 v3r2 [document(s) de cas] HL7 RIRS [messagerie basée sur des cas, échange de documents et de données agrégées] Profil EDA [données agrégées]
Normes de vocabulaire	CIM-11, DSM, Rx-Norme [conditions autorisées à déterminer par CDC Afrique]
Référentiels de support	Conditions autorisées par le CDC africain pour les messages sur les maladies à déclaration obligatoire
Maladie à déclaration obligatoire en laboratoire - données agrégées et basées sur les cas	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] HL7 RIRS [messagerie basée sur des cas et échange de données agrégées] Profil EDA [données agrégées]
Normes de vocabulaire	NCIOL SNOMED-CT HL7 Lab Reporting [conditions autorisées à déterminer par CDC Afrique]
Référentiels de support	Conditions autorisées par CDC Afrique pour la messagerie de laboratoire
Surveillance syndromique continentale - globale et cas par cas	

STANDARD	RÉFÉRENTIEL DE DONNÉES ASSOCIÉ
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] Architecture de documents cliniques HL7 v3r2 [document(s) de cas] HL7 RIRS [messagerie basée sur des cas et échange de données de documents]
Normes de vocabulaire	CIM-11, DSM, RxNorm [conditions autorisées à déterminer par CDC Afrique]
Référentiels de support	Termes autorisés par le CDC africain pour les messages sur les maladies syndromiques
Surveillance basée sur les événements – alertes	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] HL7 RIRS [messagerie basée sur des cas, échange de documents et de données agrégées]
Normes de vocabulaire	(être déterminé)
Référentiels de support	Conditions autorisées par CDC Afrique pour la messagerie d'alerte

2.2. Faire rapport à l'autorité nationale (MOH, INSP ou équivalent) de la région/province

CDC Afrique recommande que chaque État membre suive un modèle similaire pour les normes de messagerie et de vocabulaire. CDC Afrique recommande que l'identification des référentiels nationaux spécifiques de surveillance électronique soit laissée à chaque État membre, à l'exception des référentiels recommandés ci-dessous.

Tableau 8. Normes et référentiels associés – de la région/province au national

STANDARD	RÉFÉRENTIEL DE DONNÉES ASSOCIÉ
Registres de l'état civil (mortalité fœtale, mortalité infantile, décès) - données agrégées et cas par cas	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] Architecture de documents cliniques HL7 v3r2 [document de décès basé sur des cas] HL7 RIRS [messagerie basée sur des cas, échange de documents et de données agrégées] Profil EDA [données agrégées]
Normes de vocabulaire	SNOMED-CT [conditions autorisées à déterminer par CDC Afrique]
Référentiels de support	Dépôt de données géospatiales (identification et limites nationales, provinciales/régionales et de district). Répertoire des établissements de santé (identification des ressources susceptibles de soutenir les activités de planification et d'intervention en santé publique). Référentiel de laboratoire (identification des ressources susceptibles de soutenir les activités de planification et d'intervention en santé publique).

Surveillance des maladies à déclaration obligatoire - données agrégées et basées sur les cas	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] Architecture de documents cliniques HL7 v3r2 [document(s) de cas] HL7 RIRS [messagerie basée sur des cas, échange de documents et de données agrégées] Profil EDA [données agrégées]
Normes de vocabulaire	CIM-11, DSM, norme Rx [conditions autorisées à déterminer par CDC Afrique]
Référentiels de support	Dépôt de données géospatiales (identification et limites nationales, provinciales/régionales et de district), Répertoire des établissements de santé (identification des ressources susceptibles de soutenir les activités de planification et d'intervention en santé publique). Référentiel de laboratoire (identification des ressources susceptibles de soutenir les activités de planification et d'intervention en santé publique).
Maladie à déclaration obligatoire en laboratoire - données agrégées et basées sur les cas	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] HL7 RIRS [messagerie basée sur des cas et échange de données agrégées] Profil EDA [données agrégées]
Normes de vocabulaire	NCIOL SNOMED-CT HL7 Lab Reporting [conditions autorisées à déterminer par CDC Afrique]
Référentiels de support	Dépôt de données géospatiales (identification et limites nationales, provinciales/régionales et de district). Répertoire des établissements de santé (identification des ressources susceptibles de soutenir les activités de planification et d'intervention en santé publique). Référentiel de laboratoire (identification des ressources susceptibles de soutenir les activités de planification et d'intervention en santé publique).
Surveillance syndromique continentale - globale et cas par cas	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] Architecture de documents cliniques HL7 v3r2 [document(s) de cas] HL7 RIRS [messagerie basée sur des cas et échange de données de documents]
Normes de vocabulaire	CIM-11, DSM, norme Rx [conditions autorisées à déterminer par CDC Afrique]
Référentiels de support	Dépôt de données géospatiales (identification et limites nationales, provinciales/régionales et de district). Répertoire des établissements de santé (identification des ressources susceptibles de soutenir les activités de planification et d'intervention en santé publique). Référentiel de laboratoire (identification des ressources susceptibles de soutenir les activités de planification et d'intervention en santé publique).

Surveillance basée sur les événements – alertes	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] HL7 RIRS [messagerie basée sur des cas, données documentaires et échange de données agrégées]
Normes de vocabulaire	(être déterminé)
Référentiels de support	Dépôt de données géospatiales (identification et limites nationales, provinciales/régionales et de district). Répertoire des établissements de santé (identification des ressources susceptibles de soutenir les activités de planification et d'intervention en santé publique). Référentiel de laboratoire (identification des ressources susceptibles de soutenir les activités de planification et d'intervention en santé publique).

2.3. Faire rapport à la région/province du district

CDC Afrique recommande que chaque État membre suive un modèle similaire pour les normes de messagerie et de vocabulaire entre la région/province et le district comme dans la section 2.2 ci-dessus. Des dépôts supplémentaires devraient être identifiés au niveau intermédiaire selon les besoins.

2.4. Notification au district par l'établissement de santé

CDC Afrique recommande que chaque État membre suive un modèle similaire pour les normes de messagerie et de vocabulaire entre le district et l'établissement de santé, comme indiqué ci-dessous. Des référentiels supplémentaires doivent être identifiés à ce niveau inférieur si nécessaire. À des fins de réutilisation et de rentabilité, il peut être avantageux pour les membres de l'UA de tirer parti d'une plate-forme commune pour la communication des données de santé publique afin que les petites cliniques ne supportent pas une charge disproportionnée.

Tableau 9 Normes et référentiels associés - de l'établissement de santé au district

STANDARD	RÉFÉRENTIEL DE DONNÉES ASSOCIÉ
Registres de l'état civil (mortalité fœtale, mortalité infantile, décès) - données agrégées et cas par cas	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] Architecture de documents cliniques HL7 v3r2 [document de décès basé sur des cas] HL7 RIRS [messagerie basée sur des cas, échange de documents et de données agrégées] Profil EDA [données agrégées]
Normes de vocabulaire	SNOMED-CT [conditions autorisées à déterminer par CDC Afrique]
Surveillance des maladies à déclaration obligatoire - données agrégées et basées sur les cas	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] Architecture de documents cliniques HL7 v3r2 [document(s) de cas] HL7 RIRS [messagerie basée sur des cas, échange de documents et de données agrégées] Profil EDA [données agrégées]
Normes de vocabulaire	CIM-11, DSM, norme Rx [conditions autorisées à déterminer par CDC Afrique]
Surveillance syndromique continentale - globale et cas par cas	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] Architecture de documents cliniques HL7 v3r2 [document(s) de cas] HL7 RIRS [messagerie basée sur des cas et échange de données de documents]
Normes de vocabulaire	CIM-11, DSM, norme Rx [conditions autorisées à déterminer par CDC Afrique]
Surveillance basée sur les événements – alertes	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] HL7 RIRS [messagerie basée sur des cas, données documentaires et échange de données agrégées]
Normes de vocabulaire	(être déterminé)

2.5. Rapports du LIMS national

Dans le cas où les données de laboratoire ne sont pas intégrées à l'e-Surveillance nationale, CDC Afrique recommande que chaque État membre suive le modèle ci-dessous pour les normes de messagerie et de vocabulaire entre CDC Afrique e-Surveillance et un LIMS national.

Tableau 10. Normes et référentiels associés - du LIMS national

STANDARD	RÉFÉRENTIEL DE DONNÉES ASSOCIÉ
Maladie à déclaration obligatoire en laboratoire - données agrégées et basées sur les cas	
Normes de messagerie	HL7 v2.5.1 [messagerie basée sur les cas] HL7 RIRS [messagerie basée sur des cas et échange de données agrégées] Profil EDA [données agrégées]
Normes de vocabulaire	NCIOL SNOMED-CT HL7 Lab Reporting [conditions autorisées à déterminer par CDC Afrique]
Référentiels de support	Termes autorisés par le CDC africain pour les messages sur les maladies syndromiques

2.6. Rapports du système d'information de laboratoire régional (SIL)

Dans le cas où les données de laboratoire ne sont pas intégrées à l'e-Surveillance nationale ou au LIMS, CDC Afrique recommande que chaque État membre suive le modèle de la section 2.5 ci-dessus pour les normes de messagerie et de vocabulaire entre l'e-Surveillance d'CDC Afrique et un SIL régional. Au besoin, des référentiels supplémentaires doivent être identifiés à ce niveau inférieur. Il peut être avantageux pour les membres de l'UA de tirer parti d'une plate-forme commune pour la communication des données de santé publique à des fins de réutilisation et de rentabilité, afin que les petits laboratoires ne soient pas surchargés de manière disproportionnée.

Annexe 3 : Principes de développement EIS et meilleures pratiques

Principes de développement EIS (tels que décrits sur https://digitalprinciples.org)

- ***Concevoir avec l'utilisateur*** - s'associer aux organisations membres de l'UA tout au long du cycle de développement et de mise en œuvre, co-créer des solutions, et recueillir et intégrer en permanence les commentaires des utilisateurs.
- ***Comprendre l'écosystème existant*** - tenir compte des structures et des besoins particuliers qui existent dans chaque État membre, région et communauté de l'UA.
- ***Conception pour l'échelle et l'adoption continentale*** - pensez au-delà de toute mise en œuvre initiale du pilote CDC Afrique avec des membres individuels de l'UA et faites plutôt des choix pour permettre une adoption généralisée par tous les membres de l'UA, et déterminez ce qui sera abordable et utilisable par un membre ou une région plutôt que par quelques-uns États pilotes de l'UA avec l'objectif à long terme d'échange d'informations continentales [57]. En outre, un programme coordonné de test et de développement de différents aspects des normes et des politiques dirigé par CDC Afrique afin que des «cas d'utilisation» nationaux appropriés puissent être développés, dans un cadre «d'apprentissage par l'action» destiné à trouver des solutions aux problèmes urgents. problèmes susceptibles d'entraver l'échange d'informations à l'intérieur et entre les pays.
- ***Construire pour la durabilité*** - créer des programmes, des plateformes et des outils numériques durables pour maintenir le soutien des utilisateurs et des parties prenantes et pour maximiser l'impact à long terme.
- ***Soyez axé sur les données*** - assurez-vous que des informations de qualité sont disponibles pour les bonnes personnes quand elles en ont besoin, et qu'elles utilisent ces données pour prendre des mesures et des réponses appropriées pour les maladies à déclaration obligatoire.
- ***Utiliser des normes ouvertes, des sources ouvertes, des données ouvertes et l'innovation ouverte*** - accroître la collaboration avec les communautés de développement numérique de l'UA (et d'autres) pour éviter la duplication du travail.
- ***Réutiliser et améliorer*** - rechercher des moyens d'adapter et d'améliorer les outils, ressources et approches existants.
- ***Abordez la confidentialité et la sécurité*** - examinez attentivement quelles données sont collectées et comment ces données sont acquises, utilisées, stockées et partagées.
- ***Soyez collaboratif*** - partagez des informations, des idées, des stratégies et des ressources avec les membres de l'UA pour accroître l'efficacité et l'impact de la surveillance électronique.

Bonnes pratiques de la plateforme de support

- La ou les plates-formes de surveillance électronique doivent être hébergées dans des installations sécurisées avec un accès contrôlé uniquement pour le personnel autorisé.
- La plate-forme de surveillance électronique doit être protégée contre tout accès non autorisé et fournir un accès basé sur les rôles aux données à des fins de sécurité et de protection.
- Un site sécurisé de récupération/sauvegarde à distance doit être disponible en cas de dommage ou de perte de la plate-forme et/ou de l'installation de surveillance électronique principale.
- Le système de surveillance électronique et les sauvegardes de données doivent être stockés sur un site de stockage sécurisé et distant.
- Les installations de soutien à la surveillance électronique doivent utiliser des sources d'alimentation durables et fournir des sources d'alimentation de secours et une capacité de production d'électricité en cas de perte et/ou de panne de courant.
- Le système de surveillance électronique doit prendre en charge une disponibilité d'au moins 99,9 % (c'est-à-dire que le temps d'arrêt total par an ne doit pas dépasser 526 minutes). En cas d'indisponibilité imprévue du système de surveillance électronique, la récupération sur le site distant doit avoir lieu dans un délai de 2 heures.
- Dans la mesure du possible, le système de surveillance électronique doit être relié à plusieurs fournisseurs de services Internet (par exemple, au moins deux fournisseurs distincts) pour assurer la continuité des opérations en cas de panne du fournisseur de services Internet.
- Le système de surveillance électronique doit utiliser un pare-feu matériel et/ou logiciel.
- L'e-Surveillance doit utiliser des logiciels libres et ouverts éprouvés dans la mesure du possible, et collaborer avec des organisations de logiciels ouverts pour étendre les produits existants afin de répondre aux besoins d'e-Surveillance.
- L'équipe de surveillance électronique doit tester et vérifier toutes les mises à jour logicielles et système sur un système de mise en scène distinct (mais potentiellement réduit) avant le déploiement et l'utilisation.

Fonctions minimales de traitement des messages

- Attribuer un identifiant anonyme unique aux enregistrements basés sur des cas traversant le système ; cela empêchera la collision potentielle des identifiants de cas uniques des États membres de l'UA.
- Extraire les IPI selon les besoins lors du partage et de la retransmission des données d'un État de l'UA à un autre.
- Reformatez les messages dans le format approprié requis par le destinataire (par exemple, e-mail, fichier sécurisé ou message de page Web).
- Faites respecter la qualité de la structure et du contenu des messages.

Annexe 4 : Mappage des normes de messagerie aux catégories de rapport du CDC africain

Le tableau ci-dessous établit une correspondance entre les normes de messagerie et les différentes catégories de rapports du CDC africain. Notez que le contenu et les champs réels des messages seront déterminés séparément par le CDC Afrique en coordination avec les États membres de l'UA.

Tableau 11. Cartographes des normes de messagerie

CATÉGORIE DE DÉCLARATION	FROM	TO	NORME DE MESSAGERIE
Mortalité et décès fœtaux et infantiles	État membre de l'UA	CDC Afrique / CCR	HL7 v2.5.1 [messagerie] HL7 ADC [documents] HL7 RIRS [messagerie/documents]
Surveillance des maladies à déclaration obligatoire	Systèmes de surveillance des États membres de l'UA	CDC Afrique / CCR	HL7 v2.5.1 [messagerie] HL7 ADC [documents] HL7 RIRS [messagerie/documents]
Maladie à déclaration obligatoire en laboratoire	Laboratoires des États membres de l'UA	CDC Afrique / CCR	HL7 v2.5.1 [messagerie] HL7 ADC [documents] HL7 RIRS [messagerie/documents]
Surveillance syndromique continentale	Hôpitaux des États membres de l'UA	CDC Afrique / CCR	HL7 v2.5.1 [messagerie] HL7 ADC [documents] HL7 RIRS [messagerie/documents]
Données agrégées / indicateurs	CDC Afrique / CCR	État membre de l'UA	Échange de données agrégées (EDA)

Annexe 5 : Cartographier les normes de vocabulaire avec les catégories de rapport du CDC africain

Le tableau ci-dessous établit une correspondance entre les normes de vocabulaire et les différentes catégories de rapport du CDC africain. Notez que le sous-ensemble de termes et de codes autorisés à partir des normes de vocabulaire sera déterminé séparément par le CDC Afrique en coordination avec les États membres de l'UA.

Tableau 12. Cartographier les normes de vocabulaire

CATÉGORIE DE DÉCLARATION	FROM	TO	NORME DE VOCABULAIRE
Mortalité et décès fœtaux et infantiles	État membre de l'UA	CDC Afrique CCR	SNOMED-CT [conditions autorisées à déterminer par CDC Afrique]
Surveillance des maladies à déclaration obligatoire	Systèmes de surveillance des États membres de l'UA	CDC Afrique CCR	CIM-11, DSM, Rx Norm [conditions autorisées à déterminer par CDC Afrique]
Maladie à déclaration obligatoire en laboratoire	Laboratoires des États membres de l'UA (nationaux et régionaux)	CDC Afrique CCR	LONC, NSDMED-TC, HL7 Lab Reporting [conditions autorisées à déterminer par CDC Afrique]
Surveillance syndromique continentale	Hôpitaux des États membres de l'UA (centres nationaux, régionaux et grands centres urbains)	CDC Afrique CCR	CIM-11, DSM, Rx Norm [conditions autorisées à déterminer par CDC Afrique]

Annexe 6 : Transaction minimale de surveillance et de déclaration de la COVID-19 définie par catégorie de déclaration

Tableau 13. Transactions minimales de surveillance et de déclaration de la COVID-19 par catégorie

ÉLÉMENT DE DONNÉES	VALEURS	CODE(S) DE TERMINOLOGIE
Numéro d'identification unique du patient	Code de l'État membre de l'UA + identifiant unique du patient	LIGNE : 94659-0 (ID de cas)
Date de naissance et/ou âge		SNOMED-CT : 413945008 (DATE DE NAISSANCE) LIGNE : 21612-7 (âge-temps rapporté par le patient) SNOMED-CT : 423493009 (age)
Sexe	Homme Femme	SNOMED-CT : 184100006
Adresse		SNOMED-CT : 184097001
Définition de cas	Syndromes grippaux (SG) et infections respiratoires aiguës sévères (IRAS)	SNOMED-CT : 6142004 (ILI) SNOMED-CT : 840539006 (COVID-19)
Symptômes à la présentation		SNOMÉ : 3006004 (trouble de la conscience) SNOMÉ : 36955009 (perte de goût) SNOMÉ : 84387000 (asymptomatique) SNOMÉ : 103001002 (sensation de fièvre) SNOMÉ : 193894004 (hyperémie conjonctivale) SNOMÉ : 288848001 (capable de respirer) SNOMÉ : 288849009 (incapable de respirer) SNOMÉ : 373895009 (détresse respiratoire aiguë)
Co-morbidités	Maladie cardiovasculaire, inc./hypertension Immunodéficience, y compris le VIH Diabète Maladie rénale Maladie du foie Maladie pulmonaire chronique Maladie neurologique/neuromusculaire chronique Malignité Autre(s), veuillez préciser : texte libre	SNOMÉ : 49601007 (trouble cardiovasculaire) SNOMÉ : 234532001 (Immunodéficience) SNOMÉ : 73211009 (diabète) SNOMÉ : 46177005 (maladie rénale) SNOMÉ : 235856003 (maladie du foie) SNOMÉ : 413839001 (maladie pulmonaire chronique) tbp SNOMÉ : 285645000 (malignité) tbp
Immunodéprimé	Oui Non inconnu	SNOMÉ : 373066001 (oui) SNOMÉ : 373067005 (non) SNOMÉ : 261665006 (inconnu)
Grossesse (trimestre...)	O/N	SNOMÉ : 118185001 (constat de grossesse): SNOMÉ : 57630001 (premier trimestre) SNOMÉ : 59466002 (deuxième trimestre) SNOMÉ : 41587001 (troisième trimestre)

ÉLÉMENT DE DONNÉES	VALEURS	CODE(S) DE TERMINOLOGIE
Date d'apparition des symptômes	jj/MM/aaaa	n / A
Date d'hospitalisation (le cas échéant)	jj/MM/aaaa	n / A
Date de prélèvement du spécimen	jj/MM/aaaa	LIGNE : 33882-2 (date de collecte)
Type d'échantillon	Texte libre	LIGNE : 66746-9 (type d'échantillon) : LIGNE : LA30056-8 (liquide amniotique) LIGNE : LA17759-4 (Sang) LIGNE : LA18005-1 (nasopharyngeal) LIGNE : LA16975-7 (respiratoire) LIGNE : LA4332-8 (peau) SNOMÉ : 122610009 (biopsie pulmonaire) SNOMÉ : 258411007 (aspiration nasopharyngée) SNOMÉ : 258412000 (aspiration oropharyngée) SNOMÉ : 258606004 (respiratoire inférieur) SNOMÉ : 309164002 (respiration supérieure) SNOMÉ : 418564007 (liquide pleural) SNOMÉ : 445447003 (trachée par aspiration) SNOMÉ : 472901003 (écouvillon sinus nasal) SNOMÉ : 697989009 (écouvillon des narines antérieures) SNOMÉ : 788707000 (plasma, sérum ou sang total)
Résultat du test de la grippe	positif négatif inconnu	SNOMÉ : 10828004 (positif) SNOMÉ : 260385009 (négatif) SNOMÉ : 261665006 (inconnu)
Date de confirmation du résultat du test de grippe	jj/MM/aaaa	n / A
Résultat du test VRS	positif négatif inconnu	SNOMÉ : 10828004 (positif) SNOMÉ : 260385009 (négatif) SNOMÉ : 261665006 (inconnu)
Date de confirmation du résultat du test VRS	jj/MM/aaaa	n / A
Date du test SARS-CoV2	jj/MM/aaaa	n / A
Date du résultat	jj/MM/aaaa	n / A
Résultat (nég, pos, indéterminé)	positif négatif inconnu	LIGNE : 31208-2 (COVID-19) : SNOMÉ : 10828004 (positif) SNOMÉ : 260385009 (négatif) SNOMÉ : 261665006 (inconnu)
Valeur du seuil de cycle (CT)		LIGNE : 94642-6
Résultat (récupéré, décédé, non disponible)	récupéré/en bonne santé pas récupéré référé mort inconnu autre	HL7 ATS : tbp HL7 ATS : tbp SNOMÉ : 419099009 (mort) SNOMÉ : 261665006 (inconnu) HL7 ATS : tbp

Annexe 7 : Éléments de données communs pour la déclaration de données agrégées sur la COVID-19

Au niveau continental, les données suivantes sur les cas de COVID-19 sont importantes pour la surveillance et la coordination des efforts de réponse à la pandémie :

- Nombre de cas de COVID-19 confirmés en laboratoire
    - Les cas confirmés peuvent recevoir le code CIM-10 U07.1 (Source - https://www.who.int/classifications/CIM/covid19/en/)
    - Les cas confirmés peuvent recevoir le code CIM-11 RA01.0
- Nombre de tests de laboratoire COVID-19 avec résultats
    - Cela permet de calculer la positivité
- Nombre de personnes sous enquête (PUI) pour COVID-19
    - Les cas non confirmés, ou les cas où les tests de laboratoire ne sont pas disponibles, peuvent recevoir le code U07.2 de la CIM-10 (https://www.who.int/classifications/icd/covid19/en/)
    - Les cas non confirmés, ou les cas où les tests de laboratoire ne sont pas disponibles, peuvent recevoir le code CIM-11 RA01.1
- Nombre de décès causés par le COVID-19
    - Les deux codes de la CIM-10, U07.1 et U07.2, peuvent être utilisés pour le codage de la mortalité comme cause de décès
- Nombre de personnes, confirmées en laboratoire ou PUI, qui sont à l'hôpital avec COVID
- Nombre de personnes, confirmées en laboratoire ou PUI, qui sont dans une unité de soins intensifs
- Nombre de personnes (non COVID) qui se trouvent dans une unité de soins intensifs
- Nombre de lits de soins intensifs disponibles pour les nouveaux patients, COVID ou non COVID
- Nombre de personnes, confirmées en laboratoire ou PUI, qui sont actuellement sous ventilateur
- Nombre de personnes (non COVID) qui sont actuellement sous ventilateur
- Nombre de ventilateurs disponibles pour les nouveaux patients (COVID ou non COVID)
- Pourcentage de travailleurs de la santé (TS) infectés ou mis en quarantaine à domicile

Les données sur les cas de COVID-19 sont essentielles à signaler dans les 24 heures étant donné la nécessité d'identifier rapidement les cas et de suivre les progrès vers la « flexion de la courbe » d'une maladie pandémique. La recherche des contacts et la gestion des ressources au sein d'un pays seront effectuées par le ministère de la Santé de chaque pays. CDC Afrique doit suivre la maladie au niveau continental et soutenir les nations dans leurs efforts locaux en consultation avec les ministères.

Annexe 8 : Éléments de données communs pour la notification des données agrégées sur le VIH

Au niveau continental, les données suivantes sur les cas de VIH sont importantes pour la surveillance et la coordination des efforts de riposte au VIH :

(source : https://www.who.int/hiv/data/UA2011_indicator_guide_en.pdf)

- Dépistage et conseil
    - Nombre d'établissements de santé qui fournissent des services de conseil et de dépistage du VIH
    - Nombre de femmes et d'hommes âgés de 15 ans et plus qui ont reçu un test de dépistage du VIH et des conseils (T&C) au cours des 12 derniers mois et connaissent leurs résultats
    - Pourcentage de femmes et d'hommes âgés de 15 à 49 ans qui ont subi un test de dépistage du VIH au cours des 12 derniers mois et qui connaissent leurs résultats
    - Pourcentage des populations les plus à risque qui ont subi un test de dépistage du VIH au cours des 12 derniers mois et qui connaissent leurs résultats
    - Nombre de tests de récence administrés
    - Pourcentage d'infections récentes positives
- La prévention en milieu de soins
    - Pourcentage d'établissements de santé où toutes les injections thérapeutiques sont administrées avec du nouveau matériel d'injection jetable et à usage unique
    - Nombre d'établissements de santé disposant de services de prophylaxie post-exposition disponibles sur place
- Prévention de la transmission sexuelle du VIH et prévention de la transmission par la consommation de drogues injectables
    - Estimation du nombre d'utilisateurs de drogues injectables (UDI)
    - Nombre de sites du programme d'échange d'aiguilles et de seringues (PSN)
    - Nombre de personnes sous traitement de substitution aux opiacés
    - Nombre de seringues/aiguilles distribuées par le NSP
    - Pourcentage d'UDI déclarant avoir utilisé du matériel d'injection stérile la dernière fois qu'ils se sont injectés

    - Pourcentage d'UDI déclarant avoir utilisé un préservatif lors de leur dernier rapport sexuel
    - Pourcentage de professionnel(le)s du sexe (PS) déclarant avoir utilisé un préservatif avec leur client le plus récent
    - Pourcentage d'hommes déclarant avoir utilisé un préservatif lors de leur dernier rapport sexuel anal avec un partenaire masculin
    - Pourcentage des populations les plus à risque (UDI-C6a, SWs-C6b, HSH-C6c) qui sont infectées par le VIH
- Se soucier
    - Pourcentage d'adultes et d'enfants inscrits dans les soins du VIH et éligibles à la prophylaxie au cotrimoxazole (CTX) (selon les directives nationales) recevant actuellement une prophylaxie au CTX
- VIH/TB
    - Nombre d'établissements de santé fournissant des services de TAR aux personnes vivant avec le VIH avec des pratiques démontrables de lutte contre l'infection qui incluent la lutte contre la tuberculose
    - Pourcentage de cas de tuberculose incidents séropositifs estimés qui ont reçu un traitement contre la tuberculose et le VIH
    - Pourcentage d'adultes et d'enfants nouvellement inscrits dans les soins du VIH qui commencent un traitement préventif à l'isoniazide (TPI)
    - Pourcentage d'adultes et d'enfants inscrits aux soins du VIH dont le statut tuberculinique a été évalué et enregistré lors de leur dernière visite
- Les infections sexuellement transmissibles
    - Pourcentage de femmes accédant aux services de soins prénatals (CPN) qui ont été testées pour la syphilis lors de la première visite de CPN
    - Pourcentage de participants aux soins prénatals positifs pour la syphilis
    - Pourcentage de participants aux soins prénatals positifs pour la syphilis qui ont reçu un traitement
    - Pourcentage de PS avec syphilis active
    - Pourcentage d'hommes ayant des rapports sexuels avec des hommes atteints de syphilis active

- Traitement antirétroviral
    - Nombre d'établissements de santé qui proposent des TAR
    - Pourcentage d'adultes et d'enfants éligibles recevant actuellement un TAR
    - Nombre d'adultes et d'enfants éligibles qui ont récemment commencé un TAR au cours de la période de référence (2010)
    - Pourcentage d'adultes et d'enfants séropositifs encore en vie et sous TAR :
        - 12 mois après le début du traitement chez les patients commençant un TAR en 2009
        - 24 mois après le début du traitement parmi les patients ayant commencé un TAR en 2008
        - 60 mois après le début du traitement parmi les patients ayant commencé un TAR en 2005
- Systèmes de santé
    - Pourcentage d'établissements de santé dispensant des ARV qui ont connu une rupture de stock d'au moins un ARV requis au cours des 12 derniers mois
    - Pourcentage d'établissements fournissant des TAR utilisant la surveillance des CD4 conformément aux directives/politiques nationales, sur place ou par référence
- Femmes et enfants
    - Nombre de femmes enceintes ayant assisté à la CPN au moins une fois au cours de la déclaration
    - Nombre d'établissements de santé fournissant des services de soins prénatals
    - Nombre d'établissements de santé offrant des services de soins prénatals qui proposent également des tests de dépistage du VIH et des conseils aux femmes enceintes
    - Nombre d'établissements de santé offrant des services de soins prénatals qui offrent à la fois le dépistage du VIH et des antirétroviraux pour la prévention de la transmission mère-enfant sur place
    - Nombre d'établissements de santé fournissant des services de soins prénatals qui fournissent également des tests de CD4 sur place, ou disposent d'un système de collecte et de transport d'échantillons de sang pour le test de CD4 pour les femmes enceintes infectées par le VIH
    - Nombre d'établissements de santé qui proposent des TAR pédiatriques
    - Pourcentage d'établissements de santé qui fournissent des services de dépistage virologique (par exemple PCR) pour le diagnostic du VIH chez les nourrissons sur place ou à partir de gouttes de sang séché (DBS)
    - Pourcentage de femmes enceintes qui ont été testées pour le VIH et ont reçu leurs résultats - pendant la grossesse, pendant le travail et l'accouchement, et

pendant la période post-partum (<72 heures), y compris celles dont le statut VIH était déjà connu

- Pourcentage de femmes enceintes fréquentant les soins prénatals dont le partenaire masculin a subi un test de dépistage du VIH
- Pourcentage de femmes enceintes infectées par le VIH évaluées pour l'éligibilité au TAR via la stadification clinique ou le test des CD4 69 #I8a
- Pourcentage de femmes enceintes infectées par le VIH qui ont reçu des médicaments antirétroviraux pour réduire le risque de transmission mère-enfant (TME)
- Pourcentage de nourrissons nés de femmes infectées par le VIH recevant des ARV pour la prophylaxie de la prévention de la transmission mère-enfant (PTME)
- Pourcentage de nourrissons nés de femmes infectées par le VIH qui ont commencé une prophylaxie au CTX dans les deux mois suivant la naissance
- Pourcentage de nourrissons nés de femmes infectées par le VIH ayant subi un test virologique pour le VIH dans les 2 mois suivant la naissance
- Répartition des pratiques d'alimentation (allaitement maternel exclusif, alimentation de remplacement, alimentation mixte/autre) pour les nourrissons nés de femmes infectées par le VIH lors de la visite DPT3
- Pourcentage d'enfants infectés par le VIH âgés de 0 à 14 ans qui reçoivent actuellement un TAR

Les données sur les cas de VIH doivent être communiquées à CDC Afrique sur une base mensuelle.

Annexe 9 : Conditions préalables à une mise en œuvre réussie d'une infrastructure et de services basés sur le cloud

a) ***Comprendre l'impact mondial du cloud computing*** - Il est possible de posséder et de contrôler EIS pour les données, les services et les outils de surveillance électronique à l'aide du modèle de cloud computing tout en tirant parti de l'infrastructure et des services existants d'un ou de plusieurs fournisseurs tiers. La Zambie a intégré des données provenant de plusieurs sources (par exemple, Smart Health DME, DHIS2, etc.) dans un environnement cloud au cours des trois dernières années pour améliorer la qualité, la visibilité et la réactivité des données. Avec un grand succès, le CDC américain a adopté un modèle cloud pour ses applications de messagerie interne, de voix sur IP et de productivité d'entreprise (Microsoft Office 365). (notamment à la lumière des perturbations dues à la pandémie de COVID-19). Il utilise également un modèle cloud pour permettre le déploiement rapide d'applications de santé publique dans des États et des juridictions individuels. Le UK Cloud est utilisé par le Royaume-Uni (UK) pour ses National Health Services (NHS).

b) ***Cadre juridique pour le cloud computing*** - Le transfert de données vers le cloud nécessite un cadre juridique pour protéger de manière adéquate les données nationales stockées dans le cloud tout en garantissant la confidentialité des données individuelles à des fins de santé publique. La Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles (2014-juin-27) exige le partage ouvert des données de santé publique entre CDC Afrique et les États membres, et lorsqu'elle est combinée avec l'accord de partage de données établi dans la section A de ce document, fournit des protections et des contrôles pour les données nationales stockées dans le cloud ainsi que la confidentialité des données individuelles, tout en permettant une utilisation appropriée de ces données à des fins de santé publique continentale. Dans l'Union européenne (UE), la directive UE 95/46/CE de 1995 exige la protection des libertés et droits fondamentaux des personnes physiques, notamment leur droit au respect de la vie privée à l'égard du traitement des données à caractère personnel. Les récents États-Unis La loi CLOUD (Clarifying Lawful Overseas Use of Data Act) de 2018 permet aux forces de l'ordre américaines d'obliger les entreprises technologiques basées aux États-Unis à fournir les données demandées stockées sur des serveurs, que les données soient stockées aux États-Unis ou dans un pays étranger via un mandat légal ou une citation à comparaître ; la loi comprend des mécanismes permettant aux entreprises ou aux tribunaux de rejeter ou de contester un mandat ou une assignation à comparaître s'il est estimé que la demande viole la confidentialité. maladie) peuvent être soumis aux demandes du CLOUD Act et à l'exigence que les données sur tout citoyen américain soient protégées de manière appropriée (comme c'est le cas ici sur la base des politiques de la section B et des normes de confidentialité et de sécurité de la section C) ; cependant, cela ne devrait pas avoir d'impact sur les droits à la vie privée des citoyens de l'UA.

c) ***Normalisation et réglementation transfrontalières*** - L'architecture du concept EIS for e-Surveillance envisage le partage transfrontalier des données de santé publique au niveau continental, ainsi que l'utilisation de ces données pour soutenir une réponse rapide aux maladies qui peuvent affecter plusieurs États membres. Les statuts et conventions existants de l'UA établissent les bases du partage transfrontalier des données, des infrastructures et des services, en particulier :

d) **Tableau 14. Statuts et conventions de l'UA existants sur le partage des données, des infrastructures et des services**

STATUTS ET CONVENTIONS EXISTANTS DE L'UA SUR LE PARTAGE DES DONNÉES, DES INFRASTRUCTURES ET DES SERVICES
Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles (2014-juin-27)
• Les données à caractère personnel ne peuvent être transférées vers un État non membre de l'UA que si cette entité assure un niveau adéquat de protection de la vie privée, des libertés et des droits fondamentaux des personnes dont les données font ou sont susceptibles de faire l'objet d'un traitement (Section III, article 14, paragraphe 6.a). • Bien que les données de santé publique ne soient pas soumises à cette interdiction spécifique, recommander des protections fortes pour les données personnelles relatives à l'origine raciale, ethnique et régionale, la filiation parentale, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle et les informations génétiques ou, plus généralement, des données sur l'état de santé d'une personne concernée (section III, article 14, paragraphe 1).
Statut des Centres africains de contrôle et de prévention des maladies (CDC Afrique) (2016-janvier-31)
• CDC Afrique aidera les États membres dans la réponse aux urgences sanitaires, la promotion et la prévention des maladies, le renforcement des systèmes de santé et la lutte contre les maladies transmissibles et non transmissibles, la santé environnementale et les maladies tropicales négligées (section un, article 3, paragraphe e). • Il s'agira d'une interaction transparente et ouverte et d'un échange d'informations sans entrave entre le CDC Afrique et les États membres (section un, article 4, paragraphe 6). • CDC Afrique facilitera l'accès facile aux informations critiques grâce à une diffusion rapide aux États membres (Section Un, Article 5, paragraphe 3.d). • Le secrétariat du CDC africain fournira un soutien technique pour le renforcement rapide des capacités des États membres en matière de contrôle et de prévention des maladies (section deux, article 20, paragraphe b). • Le secrétariat du CDC Afrique doit établir des centres d'information qui guident les États membres et les autres parties prenantes et servent de principale source d'information sur le contrôle et la prévention des maladies sur le continent (Section Deux, Article 20, paragraphe f).
Convention de l'Union africaine sur la coopération transfrontalière (Convention de Niamey) (2014-juin-27)
• Les États membres encouragent la coopération transfrontalière dans les domaines de la cartographie et de l'information géographique, de la santé, de la sécurité et d'autres domaines comme convenu (article 3, paragraphes 1, 2, 4 et 7). • Les États membres résolvent tout obstacle juridique, administratif, de sécurité, culturel ou technique susceptible d'entraver le renforcement et le bon fonctionnement de la coopération transfrontalière (article 4, paragraphe 1). • Chaque État membre prend les mesures nécessaires pour encourager, promouvoir et faciliter le partage d'informations et de renseignements, qui peut être demandé par un autre membre sur des questions relatives à la protection et à la sécurité des zones frontalières (article 5, paragraphe 2). • Les États membres sont encouragés à harmoniser leur législation nationale avec la présente convention (article 7).

e) ***Centres de données*** - Comme mentionné à la section 9.1, plusieurs fournisseurs d'infrastructure cloud étendent leur présence en Afrique en établissant des centres de données sur le continent. Les plus grands fournisseurs, en particulier Amazon, Google et Microsoft, investissent sur le continent africain pour prendre en charge le cloud computing et les services partagés basés sur le cloud, qui sont nécessaires pour CDC Afrique EIS pour la surveillance électronique. CDC Afrique recommande de solliciter des informations auprès de ces fournisseurs de services cloud afin de déterminer s'ils

peuvent répondre aux besoins de la plate-forme EIS pour la surveillance électronique et, dans l'affirmative, de solliciter des offres formelles pour les services de ceux qui sont jugés les plus qualifiés (c'est-à-dire un Tier 3 ou Tier 4). centre de données garantissant une disponibilité d'au moins 99,9 % avec des opérations auditées en externe selon SAS 70 (Statement on Auditing Standards No. 70), SAEC 16 (Statements on Standards for Auditing and Assessment.

f) ***Confiance dans les fournisseurs*** - Le EIS pour e-Surveillance nécessite un audit bien défini, transparent et continu des processus des fournisseurs (meilleures pratiques) pour assurer la conformité continue avec les normes minimales définies pour les centres de données basés sur le cloud ; le modèle et les processus de sécurité du fournisseur ; le modèle et les processus de sauvegarde et de récupération du fournisseur ; l'accessibilité de la plate-forme du fournisseur et la facilité de transfert des données et des outils d'CDC Afrique en cas de défaillance du fournisseur (par exemple, fournisseur principal pour le service avec un autre fournisseur).

Annexe 10 : Références de surveillance basée sur les cas de COVID-19

- Centres africains de contrôle et de prévention des maladies (CDC Afrique), Protocol for Enhanced Severe Acute Respiratory Illness and Influenza-Like Illness Surveillance for COVID-19 in Africa, mars 2020 ; [https://africacdc.org/download/protocol-for-enhanced-severe-acute-respiratory-illness-and-influenza-like-illness-surveillance-for-covid-19-in-africa/] identifie le COVID-19 définitions de cas, ensembles de données minimaux pour les rapports.
- Centres africains de contrôle et de prévention des maladies (CDC Afrique), COVID-19 [https://africacdc.org/covid-19/] ; fournit un tableau de bord, des documents de politique et d'autres ressources liées à COVID-19.
- Organisation mondiale de la santé (OMS), Orientations techniques sur la maladie à coronavirus (COVID-19) : Surveillance et définitions de cas, [https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/surveillance-and-case-definitions] ; fournit un formulaire de rapport recommandé basé sur les cas, un dictionnaire de données de rapport basé sur les cas et un formulaire de rapport hebdomadaire agrégé.
- Association des laboratoires de santé publique (APHL), Répondre à la pandémie de la maladie à coronavirus (COVID-19) [https://www.aphl.org/programs/preparedness/Crisis-Management/COVID-19-Response/Pages/default.aspx] ; fournit (membre APHL) un accès aux ressources de laboratoire et de test COVID-19, y compris des exemples de messages HL7.
- Association internationale des instituts nationaux de santé publique (IANPHI), COVID-19 Resources for Members and Global Public Health Professionals [https://ianphi.org/news/2020/covid-resources.html] ; fournit un résumé des conseils COVID-19 des instituts nationaux de santé publique du monde entier.
- NOUS Centers for Disease Control and Prevention (US CDC), COVID-19 Information Management Resources (VADS) [https://phinvads.cdc.gov/vads/SearchVocab.action] ; fournit des informations sur le COVID-19 pour inclure les rapports de santé publique, les rapports de laboratoire, le suivi/la surveillance des cas et les ressources d'échange de données géospatiales.

Annexe 11 : Références Cloud et services partagés

- NOUS National Institutes for Science and Technology (NIST), *SP 800-145, The NIST Definition of Cloud Computing*, Peter Mell & Tim Grance, septembre 2011 [https://csrc.nist.gov/publications/detail/sp/800-145 /final]
- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3500, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet et réseaux de nouvelle génération* / Technologies de l'information - Cloud computing - Vue d'ensemble et vocabulaire, août 2014 [https://www.itu.int/rec/T-REC-Y.3500/en]
- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3501, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes / Cloud computing - Cadre et exigences de haut niveau, juin 2016 [https://www.itu.int/rec/T-REC-Y. 3501/fr]*
- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3502, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes* / Technologies de l'information - Cloud computing - Architecture de référence, août 2016 [https://www.itu.int/rec/T-REC-Y. 3502/fr]
- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3505, *série Y : Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Aperçu et exigences fonctionnelles pour la fédération du stockage de données, mai 2018 [https://www.itu.int/rec/T-REC -Y.3505/fr]
- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3506, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes* / Cloud computing - Exigences fonctionnelles pour le courtage de services cloud, mai 2018 [https://www.itu.int/rec/T-REC-Y .3506/fr]
- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3507, *série Y : Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Functional requirements of physical machine, décembre 2018 [https://www.itu.int/rec/T-REC-Y. 3507/fr]
- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3508, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes* / Cloud computing - Aperçu et exigences de haut niveau du cloud distribué, août 2019 [https://www.itu.int/rec/T- REC-Y.3508/fr]

- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3509, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes / Cloud computing - Architecture fonctionnelle pour la fédération du stockage des données, décembre 2019 [https://www.itu.int/rec/T-REC-Y .3509/fr]*

- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3510, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes* / Exigences en matière d'infrastructure informatique en nuage, février 2016 [https://www.itu.int/rec/T-REC-Y.3510/en]

- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3512, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes* / Cloud computing - Exigences fonctionnelles du réseau en tant que service, août 2014 [https://www.itu.int/rec/T-REC- Y.3512/fr]

- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3513, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes* / Cloud computing - Exigences fonctionnelles de l'infrastructure en tant que service, août 2014 [https://www.itu.int/rec/T-REC- Y.3513/fr]

- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3515, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes* / Cloud computing - Architecture fonctionnelle du réseau en tant que service, juillet 2017 [https://www.itu.int/rec/T-REC- Y.3515/fr]

- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3517, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes / Cloud computing - Overview of inter-cloud trust management, décembre 2018 [https://www.itu.int/rec/T-REC- Y.3517/fr]*

- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3519, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes* /

Cloud computing - Architecture fonctionnelle des mégadonnées en tant que service, décembre 2018 [https://www.itu.int/rec/T-REC -Y.3519/fr]

- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3522, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes / Exigences de gestion du cycle de vie des services cloud de bout en bout, décembre 2018 [https://www.itu.int/rec/T-REC- Y.3522/fr]*

- UIT-Secteur de la normalisation des télécommunications de l'UIT, Recommandation UIT-T Y.3524, *série Y : Infrastructure mondiale de l'information, aspects du protocole Internet, réseaux de nouvelle génération, Internet des objets et villes intelligentes* / Exigences et cadre de maturité de l'informatique en nuage, décembre 2019 [https://www.itu.int/rec/T-REC-Y.3524/ fr]

- UIT-Secteur du développement des télécommunications, *Cloud Computing in Africa Situation and Perspectives*, avril 2012 [http://www.itu.int/ITU-D/treg/publications/Cloud_Computing_Afrique-e.pdf]

- Union européenne, Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel L 281, 23/ 11/1995 P. 0031 - 0050 [https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A31995L0046]

- NOUS HR4943 - Cloud Act, 115e Congrès (2017-2018) [https://www.congress.gov/bill/115th-congress/house-bill/4943]

Annexe 12 : Références de renforcement des capacités

- CDC Afrique, *Cadre pour le développement des personnels de santé publique, 2020-2025*, 10 mars 2020 [https://africacdc.org/download/framework-for-public-health-workforce-development-2020-2025/]

Annexe 13 : Valeurs et principes fondamentaux guidant le développement de la politique et des normes EIS

Le cadre de politique et de normes EIS des États membres de l'UA a les principes directeurs suivants :

I) Solidarité et coopération

Solidarité entre les États membres de l'Union africaine ; Coopération entre la Commission de l'Union africaine (CUA), les Communautés économiques régionales (CER), les institutions africaines et les organisations internationales ; l'engagement de tous les États membres de l'UA envers la réalisation du Règlement sanitaire international (RSI), de l'Agenda 2063, de l'accord sur la zone de libre-échange continentale africaine (AFCFTA) et des objectifs de développement durable (ODD) où le partage des données est un élément essentiel à leur réalisation.

II) Complet

Adopter une approche écosystémique globale dans la définition et l'application des éléments et des fondements nécessaires pour transformer le secteur de la santé et mieux préparer le continent aux pandémies.

III) Transformatif

Exploitez, exploitez et accélérez pleinement l'impact sur la société en accélérant le partage numérique et de données grâce au développement de cette politique d'échange d'informations sur la santé.

IV) Compris

Une transformation numérique pour les États membres de l'UA qui soit abordable et omniprésente, créant un accès égal aux opportunités et atténuant les risques d'exclusion.

V) Du terroir

VI) Il sera dirigé et détenu par les institutions africaines, ancré dans les réalités africaines, et libérera l'esprit africain de créativité et d'innovation pour générer l'adoption de technologies locales et le développement de solutions, tout en adoptant ce qui est bon et pertinent sans réinventer la roue. Des experts africains ont dirigé l'élaboration de ce document de politique et de normes à l'usage de l'Afrique.

VII) Nouvel état d'esprit

Bénéficier de la transformation numérique nécessite un changement d'état d'esprit ainsi que de nouvelles formes de collaboration entre les parties prenantes et entre les secteurs, ainsi qu'une facilitation et un réoutillage. Avec l'évolution rapide de la technologie et des infrastructures, le partage de données au niveau continental nécessitera un esprit ouvert et une volonté d'essayer quelque chose de nouveau.

VIII) Safe

IX) Tout en équilibrant les exigences de partage des données, la confidentialité et la sécurité des données de santé sont des priorités élevées. Ce document établit un équilibre entre les exigences de confidentialité, de sécurité et de partage de données.

X) Innovative

Ce cadre de politique et de normes EIS tente de tirer parti des dernières innovations en matière d'échange d'informations sur la santé en apportant les expériences mondiales en Afrique tout en laissant de la place pour plus de développement et de croissance.

Annexe 14 : Modèle d'accord de partage et d'utilisation des données

ACCORD DE PARTAGE ET D'UTILISATION DES DONNÉES

ENTRE

[CDC POUR L'AFRIQUE]

ET

[NOM DE L'ORGANISATION REQUÉRANTE]

Le présent accord de partage de données (ci-après dénommé « accord ») est conclu par et entre l'Union africaine (ci-après dénommée « UA »), agissant par l'intermédiaire des Centres africains pour le contrôle et la prévention des maladies (ci-après dénommés les « CDC africains ») dont l'adresse principale est au siège de l'Union africaine, P.O. Box 3243, rue Roosevelt W21K19, Addis-Abeba, Éthiopie d'une part ; et ABCD (ci-après dénommé « ABCD ») dont l'adresse principale est... d'autre part ;

CI-APRÈS, collectivement, les « Parties » et individuellement la « Partie » au présent Accord de partage de données.

CONSIDÉRANT que le CDC pour l'Afrique est une institution technique spécialisée de l'Union africaine chargée de promouvoir la prévention et le contrôle des maladies en Afrique, notamment par le biais de sa stratégie de nouvel ordre de santé publique qui prévoit : (i) une production accrue de vaccins, de diagnostics et de produits thérapeutiques, (ii) un personnel de santé publique renforcé, (iii) des partenariats respectueux orientés vers l'action, (iv) un financement national et (v) des institutions de santé publique renforcées.

ATTENDU QU'ABCD a pour mandat de... . ;

CONSIDÉRANT que l'article 5 (3) (a-d) du statut des CDC africains souligne que les CDC africains doivent faciliter l'accès aux informations critiques qui préparent et aident les pays à répondre aux événements de santé publique ;

ATTENDU QUE « ABCD » a approuvé le partage de données avec CDC Afrique, et « ABCD » a autorisé CDC Afrique à utiliser les données partagées pour éclairer ses actions en faveur d' « ABCD » et du continent dans le cadre de sa fonction mandatée et pour permettre à CDC Afrique de s'acquitter pleinement de ses responsabilités, qui sont énoncées à l'Annexe C.
ATTENDU QUE CDC Afrique et « ABCD » conviennent mutuellement de conclure le présent accord afin de se conformer aux exigences des politiques et procédures de l'agence nationale de santé publique, du comité d'éthique de la recherche et de l'Autorité nationale de la recherche en santé concernant le transfert, la manipulation, le stockage et la gestion des données fournies à CDC Afrique par « ABCD » dans la mesure où ces politiques et procédures s'appliquent, et pour se conformer à la... . ;
CONSIDÉRANT que les données (ci-après « Données ») doivent être collectées auprès de...

PAR CONSÉQUENT, compte tenu de ce qui précède et de toute autre considération bonne et précieuse, dont la réception et la suffisance sont reconnues par les présentes, les parties conviennent de ce qui suit :

1. *Durée*

Sauf résiliation contraire conformément aux présentes, le présent accord de partage de données entrera en vigueur à la dernière date de signature par les parties, comme indiqué par la signature du représentant dûment autorisé des parties.

2. *But*

Le but de cet accord est que « ABCD » partage toutes les informations relatives à la santé publique afin de permettre aux CDC africains de s'acquitter pleinement de leur mission consistant à utiliser des données précises et opportunes pour éclairer les actions des États membres de l'Union africaine.

3. *Définitions*

Le « droit applicable » fait référence au droit international auquel l'UA est soumise et aux lois, réglementations et exigences applicables ayant force de loi, dans les juridictions d'où proviennent les données et où le projet est réalisé dans la mesure où elles sont applicables à la question et aux activités envisagées dans le présent accord, et à condition que ce dernier ne soit pas contraire au droit international.

Les « données » désignent toutes les maladies transmissibles et non transmissibles, endémiques, épidémiques, émergentes et réémergentes émanant des institutions nationales de santé publique ou d'autres services concernés (par exemple, laboratoires, services de surveillance de la santé publique, divisions de préparation et d'intervention en cas d'urgence, divisions de prévention et de contrôle des maladies).

La « qualité des données » fait référence aux données et aux informations qui répondent à des critères spécifiques pour être adaptées à l'usage auquel elles sont destinées. Dans le domaine de la santé publique, les caractéristiques les plus recherchées en matière de qualité des données sont l'exhaustivité, l'actualité et l'exactitude.

« Les informations relatives à la santé publique font référence aux données et aux produits de recherche en santé publique, aux politiques de santé publique, aux stratégies, aux directives, aux procédures opérationnelles standard, aux informations relatives à l'administration de la santé et aux ressources humaines.

4. Transfert de données

4.1 « ABCD » partagera des données dépersonnalisées avec les CDC africains et pourra partager des données identifiables lorsque ces informations sont indispensables pour orienter les efforts de réponse des CDC africains à l' « ABCD » ou au continent. CDC Afrique suivra un protocole de transfert de fichiers sécurisé ou un service d'échange similaire qui sera convenu par les deux parties.

4.2 Les parties conviennent que des technologies telles que le protocole de transfert de fichiers sécurisé (sFTP) ou un service similaire seront utilisées. « ABCD » travaillera avec CDC Afrique avant le transfert de données afin de déterminer les protocoles, les informations d'identification et les exigences/alternatives de transmission spécifiques conformément aux lois de l'Union africaine et d' « ABCD »

4.3 Les parties conviennent que « ABCD » assume la responsabilité de la sécurité des informations jusqu'à ce qu'elles soient reçues par CDC Afrique conformément à la méthode convenue.

4.4 Les parties conviennent que CDC Afrique dispose de serveurs sécurisés pour héberger les données et a développé un système de gestion des données qui hébergera les données et servira de plate-forme analytique pour les données partagées, respectivement.

4.5 CDC Afrique consultera « ABCD » avant le transfert de données afin de déterminer les protocoles spécifiques, les informations d'identification et les exigences/alternatives de transmission conformément à la loi régissant l'Union africaine ou/et « ABCD ».

4.6 Les CDC pour l'Afrique n'utiliseront les données « ABCD » que dans le but de protéger la santé de la SEP et du continent, notamment pour la production de rapports et de publications conjointes dans des revues scientifiques. CDC Afrique ne partagera pas les données en dehors de la Commission de l'Union africaine.

4.7 CDC Afrique n'est pas autorisée à utiliser ou à divulguer les données d'une manière qui violerait toute clause énoncée dans cet accord, y compris la confidentialité et la confidentialité de toute donnée identifiable.

5. Qualité des données, architecture d'échange et fréquence

5.1 « ABCD » doit prendre des mesures responsables pour s'assurer que les données communiquées sont de haute qualité.

5.2 Les parties conviennent que toutes les données seront échangées au niveau national avec la ou les institutions autorisées de « ABCD ». Les données des référentiels des CDC en Afrique doivent être partitionnées afin de permettre aux Parties de contrôler leurs propres données de santé numériques et le calendrier de toute publication ultérieure de ces données.

5.3 Les parties conviennent que les données seront envoyées à CDC Afrique et qu'une fois reçues, les données seront consultées par CDC Afrique et l' « ABCD » conformément au présent accord.

5.4 « ABCD » partagera toutes les informations et données sur les maladies et événements à déclaration obligatoire en vertu du Règlement sanitaire international pour un signalement immédiat avec les CDC africains. Ces données doivent être partagées dans les 24 heures suivant la détection.

5.5 Toutes les informations relatives aux épidémies, y compris, mais sans s'y limiter, les types de données suivants : laboratoire, gestion des cas, surveillance, communication des risques et réponse Les données doivent être partagées quotidiennement. L'ABCD partagera des informations sur toutes les autres maladies et événements chaque semaine avec les CDC pour l'Afrique. Toutes les autres informations relatives à la santé publique doivent être partagées dès qu'elles sont disponibles ou qu'une mise à jour est apportée à une version existante.

6. Protections des informations.

6.1 Dans le cadre de l'exécution des obligations en vertu du présent accord, chaque partie adoptera et utilisera des mesures de protection administratives, physiques et techniques appropriées pour préserver l'intégrité et la confidentialité des données et pour empêcher leur utilisation ou leur divulgation, sauf dans les cas autorisés par le présent accord ou conformément aux lois sur la protection des données et de la vie privée.

6.2 Toutefois, il n'y aura aucune obligation de confidentialité ni aucune restriction quant à l'utilisation des données lorsque :

i. Les données sont accessibles au public ou deviennent accessibles au public autrement que par une action de la partie destinataire ; ou
ii. Les données étaient déjà connues de la partie destinataire (comme en témoignent ses dossiers écrits) avant leur réception.
iii. Les données ont été reçues d'un tiers ne violant aucune obligation de confidentialité

6.3 Sauf dans la mesure requise par la loi, aucune des parties n'aura la responsabilité de s'assurer que l'autre partie prend les mesures nécessaires pour se conformer aux lois applicables. CDC Afrique peut demander à « ABCD » une copie de sa politique de confidentialité et d'accès aux données afin de déterminer les contrôles en place et les mesures visant à garantir le respect des lois applicables relatives à la protection et à la confidentialité des données.

7. Publications

7.1 Le CDC pour l'Afrique doit attribuer de manière appropriée la fourniture des données dans toutes les publications ou présentations orales des données qui en résulteront, conformément aux remerciements énoncés ci-dessous. Les auteurs nommés doivent être déterminés conformément aux normes de publication généralement acceptées et aux politiques MS.

7.2 Avant qu'une partie ne soumette un article ou un résumé pour publication ou ne divulgue autrement publiquement des informations concernant les données, la partie qui souhaite publier doit s'assurer que l'autre partie dispose d'au moins trente (30) jours pour examiner la publication ou la divulgation proposée et que les commentaires fournis seront traités de bonne foi. En l'absence de toute objection de la part de la Partie destinataire dans un délai de trente (30) jours concernant l'atteinte à ses droits de propriété, la Partie qui souhaite publier doit procéder à la publication.

8. Propriété intellectuelle

8.1 Il est expressément convenu que ni « ABCD » ni CDC Afrique ne transfèrent en vertu du présent Contrat à l'autre Partie aucun droit ou licence sur des brevets, des droits d'auteur ou tout autre droit de propriété détenus à la date de début du Contrat ou découlant de recherches menées dans le cadre du présent Accord. Toutes les autres informations, travaux, droits d'auteur, brevets, secrets commerciaux ou autres droits de propriété intellectuelle associés à des procédures, des flux de travail, des méthodes, des rapports, des manuels, des aides visuelles, de la documentation, des idées, des concepts, des techniques, des visuels, des processus, des articles, des articles ou autres œuvres d'auteur développés, à condition qu'ils aient été créés par CDC Afrique, au cours du présent accord, seront la propriété de CDC Afrique. Les deux parties reconnaissent que « ABCD » reste propriétaire des données.

8.2 Les termes de cette section et de ses sous-parties survivront à la résiliation, à l'expiration, au non-renouvellement ou à l'annulation du présent Contrat.

9. *Conformité*

« ABCD » et CDC Afrique acceptent d'utiliser les données et d'exécuter le présent accord conformément à toutes les lois, réglementations, politiques et politiques applicables de leurs institutions respectives, y compris, sans s'y limiter, celles relatives aux sujets humains. Le cas échéant, « ABCD » et CDC Afrique se conformeront aux lois et réglementations applicables, telles que modifiées de temps à autre, en ce qui concerne la collecte, l'utilisation, le stockage et la divulgation de toutes données, y compris mais sans s'y limiter.

10. *Remarque*

10.1 Toute notification requise en vertu du présent Contrat doit être faite par écrit et doit être remise personnellement ou envoyée par courrier recommandé ou certifié, par télécopie aux adresses indiquées ci-dessous ou à toute autre adresse que l'une des parties aura notifiée à l'autre partie.

À l'Union africaine :

Le réalisateur

CDC Afrique

Union africaine

P.O. Boîte 3243

Addis-Abeba

Ethiopie

À « ABCD » :

10.2 Chaque partie peut, par notification écrite adressée à l'autre partie, désigner des représentants supplémentaires ou substituer d'autres points focaux aux personnes désignées dans le présent article.

11. Résiliation

11.1 Résiliation motivée. Dans le cas où CDC Afrique a enfreint une disposition importante du présent accord et ne parvient pas à remédier à cette violation dans les trente (30) jours suivant la réception d'une notification écrite d' « ABCD ». « ABCD » aura le droit de résilier le Contrat moyennant un préavis écrit de trente (30) jours à la Partie en infraction et demandera à CDC Afrique de renvoyer toutes les données.

11.2 Résiliation pour des raisons de commodité. Le présent accord peut être résilié par « ABCD » ou CDC Afrique en donnant à l'autre partie un préavis écrit d'au moins trente (30) jours, sous réserve de la conclusion ordonnée de toutes les activités en cours et du règlement des obligations en suspens.

11.3. Obligations continues en matière de confidentialité. L'obligation de chaque partie de protéger la vie privée des participants dont les données font l'objet du présent accord est continue et survit à toute résiliation, annulation, expiration ou autre conclusion du présent accord ou de tout autre accord entre les parties.

12. Destruction et retour des données.

12.1. CDC Afrique archivera toutes les données reçues d' « ABCD » et détruira toutes les données reçues à la demande d' « ABCD ». CDC Afrique préservera la confidentialité des ensembles de données avec des identifiants personnels afin de préserver l'intégrité du processus de partage des données.

13. Obligations continues en matière de confidentialité.

L'obligation d'CDC Afrique de protéger la confidentialité des données est continue et survit à toute résiliation, annulation, expiration ou autre conclusion du présent accord concernant toute partie des données, maintenue par CDC Afrique après une telle résiliation, annulation, expiration ou autre conclusion du présent accord.

14. Utilisation du nom

Aucune des parties n'utilisera les noms ou marques de commerce de l'autre partie ou de l'une des entités affiliées de l'autre partie à des fins de publicité, d'approbation ou de promotion, à moins que l'autre partie n'ait donné son consentement écrit préalable pour l'utilisation particulière envisagée. Les termes de cette section survivront à la résiliation, à l'expiration, au non-renouvellement ou à l'annulation du présent Contrat.

15. Statut des parties

Aucune disposition du présent Contrat ne doit être considérée ou interprétée comme créant une relation d'emploi, de coentreprise ou d'agence entre « ABCD » et CDC Afrique. Ni « ABCD » ni CDC Afrique ne sont habilités à faire des déclarations, des représentations ou des engagements de quelque nature que ce soit, ou à prendre des mesures contraignantes pour une autre partie, sans l'autorisation écrite préalable de l'autre partie.

16. Exclusion de garantie et limitation de responsabilité

16.1 AUCUNE DES PARTIES NE FAIT DE DÉCLARATION NI NE DONNE DE GARANTIE, EXPRESSE OU IMPLICITE, CONCERNANT SON EXÉCUTION DANS LE CADRE DU PRÉSENT CONTRAT, Y COMPRIS, MAIS SANS S'Y LIMITER, LA COMMERCIALISATION, L'UTILISATION OU L'ADÉQUATION À UN USAGE PARTICULIER DES DONNÉES DÉVELOPPÉES ET FOURNIES DANS LE CADRE DE CE TRAVAIL, OU LE FAIT QUE CES DONNÉES N'ENFREIGNENT AUCUN DROIT DE PROPRIÉTÉ DE TIERS. EN AUCUN CAS, L'UNE OU L'AUTRE DES PARTIES NE SERA RESPONSABLE ENVERS L'AUTRE EN VERTU DES PRÉSENTES POUR DES PERTES SPÉCIALES, DES DOMMAGES CONSÉCUTIFS, ACCESSOIRES OU AUTRES DOMMAGES INDIRECTS RÉSULTANT DE OU EN RELATION AVEC CET ACCORD.

16.2 « ABCD » et CDC Afrique acceptent d'être responsables de leurs actes répréhensibles, de leur négligence et/ou de leurs actes ou omissions imprudents dans l'exercice de leurs fonctions en vertu des présentes et sont financièrement et légalement responsables de toutes leurs dépenses, responsabilités et honoraires d'avocat résultant ou attribuables à de tels actes ou omissions. Aucune des parties n'a l'obligation d'indemniser l'autre en vertu des présentes. Les termes de ce paragraphe survivront à l'expiration du présent accord.

17. Aucune assignation

Aucune des parties ne peut céder ses droits en vertu des présentes à une tierce partie sans le consentement écrit préalable de l'autre partie ; étant entendu qu'une partie peut céder ses droits sans le consentement écrit préalable de l'autre partie à une filiale ou à une autre entité qui contrôle, est contrôlée par ou est sous contrôle commun avec cette partie. Toute prétendue cession en violation de cette clause est nulle. Ce consentement écrit, s'il est donné, ne dégage en aucune manière le cédant de sa responsabilité quant à l'exécution du présent Contrat par son cessionnaire.

18. Effet contraignant

Le présent accord lie les deux parties et s'applique au bénéfice des parties, des représentants légaux, des successeurs et des ayants droit.

19. Résolution des litiges

Les parties mettent tout en œuvre pour résoudre tout litige à l'amiable et par la voie diplomatique.

20. La loi applicable

Cet accord est régi par le droit international.

21. Privilèges, immunités et facilités des deux parties

Aucune disposition du présent accord ne doit être interprétée comme une renonciation ou une modification des privilèges, immunités et facilités dont bénéficie l'Union africaine en vertu des accords internationaux et des lois applicables aux parties.

22. Divisibilité

Si une disposition du présent Contrat est jugée invalide ou inapplicable, cette disposition sera supprimée et les autres dispositions resteront pleinement en vigueur et en vigueur comme si le présent Contrat avait été exécuté avec la disposition invalide éliminée. Si une disposition du présent Contrat est ainsi jugée invalide ou inapplicable mais serait valide ou exécutoire si une partie de la disposition était supprimée, la disposition en question s'appliquera avec les modifications nécessaires pour la rendre valide.

23. Intégralité de l'accord, renonciation, modification

Les parties au présent accord ne peuvent pas amender, altérer ou modifier sauf par un accord écrit ou un échange de lettres signé par les deux parties. Aucune disposition du présent accord ne peut faire l'objet d'une dérogation, sauf par un accord écrit signé par les parties renonciantes. La renonciation à un terme ou à une disposition ne doit pas être interprétée comme une renonciation à toute autre condition ou disposition. Le présent accord constitue l'accord final, complet et exclusif entre les parties en ce qui concerne son objet particulier uniquement (le partage de données anonymisées) et remplace tous les accords, promesses et accords passés et contemporains, oraux ou écrits, entre les parties.

24. Homologues

Le présent Contrat peut être signé en plusieurs exemplaires, dont chacun, une fois signé et livré (qui peut être envoyé par courrier électronique), constitue un original, et les photocopies, fac-similés, copies électroniques ou autres ont le même effet à toutes fins utiles qu'un original signé à l'encre. Chaque partie aux présentes consent à être liée par photocopie ou télécopie des signatures du représentant de cette partie aux présentes.

EN FOI DE QUOI, les soussignés, dûment autorisés à cette fin par les parties respectives, ont signé le présent accord de partage de données.

Fait à [...], [...] en ce... jour de...

LES SIGNATURES APPARAISSENT SUR LA PAGE SUIVANTE

« ABCD »

Par : _____

Nom : _____

Titre : _____

Date:_____

Union africaine

Par : _____

Nom : _____

Titre : _____

Date:_____

Annexe 15 : Liste des membres et des contributeurs du groupe de travail

Tableau 15 Membres et contributeurs du groupe de travail

SN	MEMBRES DU GROUPE DE TRAVAIL	AFFILIATION	RÔLE
1	Justin Maeda	CDC Afrique	Coordinateur principal de l'Équipe spéciale
15	Kyeng Mercy Teth	CDC Afrique	Coordinateur du groupe de travail
2	Ahmed Abdulwahab	HISP-SA	Chef de projet et membre du TF
3	Binyam Tilahun	Université de Gondar	Responsable technique de l'ensemble des travaux HIE
4	Adane Letta Mamuye	Université de Gondar	Responsable technique des normes
5	Tesfahun Melese Yilma	Université de Gondar	Responsable technique pour les directives
6	Tadesse Wuhib	CDC DES ÉTATS-UNIS	Chef du co-groupe
7	Tom O. Oluoch	HELINA	Chef de groupe
8	Steven Wanyee Macharia	DHSRI	Chef de groupe
9	Manish Kumar	Évaluation de MEASURE	Chef du co-groupe
10	Chris Murrill	CDC DES ÉTATS-UNIS	Chef de groupe
11	Brian Dixon	OpenHIE	Chef de groupe
12	Ahmed Zaghloul	CDC Afrique	Coordinateur principal de l'Équipe spéciale
13	Jay Varma	CDC Afrique	Coordinateur principal de l'Équipe spéciale
14	Chris Seebregts	Jembi	Chef du co-groupe
16	Pierre Dane	VitalWave	Chef du co-groupe
17	Atinkut Alamira	Université de Gondar	Chef du co-groupe
18	Simisola Atkintola	Université d'Ibadan	Chef de groupe
19	Karl Schenkel	QUI SIÈGE	Membre
20	Benido Impouma	QUI AFRO	Membre
21	Pierre Nabeth	QUI EMRO	Membre
22	Henri Mwanyika	Trajectoire	Membre
23	Al Shiferaw	JSI	Membre
24	Rimameyati Usman Yashe	Afrique de l'Ouest	Membre
25	Mazyanga Mazaba	Afrique du Sud	Membre
26	Yasser Shehata	Afrique du Nord	Membre
27	David Soti	Afrique de l'Est	Membre
28	Marguerite Loembe	CDC Afrique	Membre
29	Classe Pooben	HISP-SA	Membre
30	Luc Duncan	IntraHealth	Membre
31	Marc Wien	PocketpatientMD	Membre
32	M. Moctar Yedaly	Union africaine	Membre

Union Africaine

AFRICA CDC
Le Centre africain de prévention et de lutte contre les maladies
Protection de la santé de l'Afrique

Les Centres Africains de Contrôle et de Prévention des Maladies (Afrique CDC),
Commission de l'Union africaine
Roosevelt Street W21 K19, Addis Abeba, Éthiopie

+251 11 551 7700 www.africacdc.org africacdc@africa-union.org africacdc @AfricaCDC