

NATIONAL GUIDE FOR THE MANAGEMENT OF EPIDEMIOLOGICAL SURVEILLANCE DATA

— MINSANTE CAMEROON —

JUNE 2024



Elizabeth Glaser
Pediatric AIDS
Foundation

*Until no
child has
AIDS.*



Table des matières.

Preface	vii
Appreciation.	viii
Technical drafting committee	ix
Glossary	xi
Sigles et abréviations.	xiii

I Overview of data management

1 General introduction	1
1.1 Background and justification	1
1.2 Aims and objectives	2
1.2.1 Aims	2
1.2.2 Objectives	3
1.3 Scope	3
1.4 Target audience	3
2 The components of data management	4
2.1 General information on data management.	4
2.2 Data management stages	5
2.2.1 Data collection and entry	6
2.2.2 Data quality assurance	6
2.2.3 Data transmission	9
2.2.4 Data analysis	10
2.2.5 Exploitation and dissemination of results/information	10
2.2.6 Data processing and feedback	10
2.2.7 Information dissemination tools	10
2.2.8 Means of distribution	11
2.2.9 Data storage and archiving	11
2.3 Data governance	11
2.3.1 Guiding principles of data governance	12
2.3.2 Roles and responsibilities of governance actors	12
2.3.3 Data security and hosting	14
2.3.4 A few data security principles	14

2.3.5	Some hosting principles	15
2.3.6	Interoperability	17

3 Implementation of the Different Components of Data Management

20

3.1	EPD data management	20
3.1.1	Data collection and entry	20
3.1.2	Data analysis and interpretation.	21
3.1.3	Data exploitation	21
3.1.4	Data security and hosting.	21
3.2	Management of maternal and perinatal deaths and response surveillance data.	22
3.2.1	Data collection and entry	22
3.2.2	Data transmission	23
3.2.3	Quality assurance	23
3.2.4	Data analysis	23
3.2.5	Exploitation and dissemination of results	24
3.3	Management of EPD and PD data across the laboratory	24
3.3.1	Data collection	24
3.3.2	Transmission of information from the laboratory	25
3.3.3	Data quality assurance	25
3.3.4	Data analysis	25
3.3.5	Exploitation and dissemination of results/information	26
3.3.6	Data storage	26
3.4	Data Management Guidelines for Care	27
3.4.1	Data Collection	28
3.4.2	Data Transmission	28
3.4.3	Data Quality Assurance	28
3.4.4	Data Analysis	28
3.4.5	Utilization and Dissemination of Results/Information	29
3.4.6	Data Storage	29
3.5	Data Management at Border Health Posts	29
3.5.1	Data Collection and Entry	29
3.5.2	Data Transmission	29
3.5.3	Data Processing	30
3.5.4	Storage	30
3.5.5	Data Analysis	30
3.6	Management of Mortality Data	31
3.6.1	Data Collection and Entry	31
3.6.2	Quality Assurance	32
3.6.3	Data Transmission	32
3.6.4	Data Analysis	32
3.6.5	Utilization and Dissemination of Results	32

3.7	Management of MEV Data	32
3.7.1	Sources of Surveillance Data for MEV	32
3.7.2	Data Collection for MEV Surveillance	32
3.7.3	Data Collection for MEV and MAPI Surveillance	32
3.7.4	Reporting and Data Transmission Tools	33
3.7.5	Quality Assurance	33
3.7.6	Data Processing and Analysis	33
3.7.7	Utilization and Dissemination	33
3.7.8	Storage and Archiving	33
3.8	Data Management Guidelines for Case Management	33
3.8.1	Data Collection	34
3.8.2	Data Transmission	34
3.8.3	Data Quality Assurance	34
3.8.4	Data Analysis	34
3.8.5	Utilization and Dissemination of Results/Information	35
3.8.6	Data Storage	35

II

Standard Operating Procedures

Data Collection and Notification of Surveillance Data	37
Data Quality Assurance	42
Data Storage and Archiving for Epidemiological Surveillance .	48
Data Security and Access for Epidemiological Surveillance ...	53
Management of Community Signals and Cases	58
Analysis of Epidemiological Surveillance Data	64
Management of Epidemiological Surveillance Data in the Laboratory	71
Sharing (dissemination) of Information	77
Transmission of Epidemiological Surveillance Data and Feedback	82
Bibliography	86

Liste des tableaux.

2.1	Some tools for assessing data quality	7
2.3	Some data quality assessment tools	8
2.5	Roles and responsibilities of the actors in the epidemiological data management system	13
3.1	Reference Laboratory Network by Disease and Platform	26

Liste des figures.

2.1	Data life cycle	4
2.2	RDQA conceptual framework	8
2.3	IDSR data transmission circuit, IDSR 3 rd edition	9
2.4	Interoperability Architecture	17
2.5	Cameroon's Digital Health Architecture	18
3.1	Laboratory information transmission circuit	26
3.2	Screenshot of a data entry form in DHIS2	29
3.3	Information circulation and feedback circuits	31

Preface

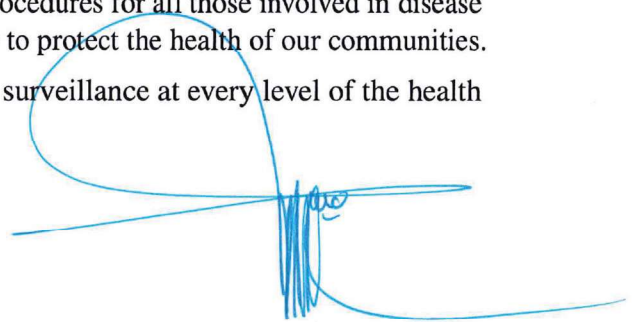
Recent public health events around the world, and in particular the COVID-19 pandemic, have placed greater emphasis on the need to strengthen health surveillance. Countries' ability to effectively prevent, detect and respond to potential health threats depend on a robust epidemiological surveillance system, which enables informed decision-making and the development of appropriate health policy. Such a system must be fed by exhaustive, reliable data in real time.

Since 2017, our country has had a decentralised electronic system for collecting, centralising and disseminating epidemiological data. However, this system, which includes data from just over 6,000 public and private health facilities in all the health districts, and satisfactory completeness of activity reports (over 90%), has a number of identified shortcomings. These shortcomings relate in particular to the low capacity for systematic collection of community data, the need to revise certain variables and facilitate their disaggregation, the review of data quality, and the low capacity for analysis and effective use of said data for decision-making at all levels. A number of actions are being implemented to correct the gaps identified.

With this view of improving the management of epidemiological surveillance data, this guide has been designed to provide an additional resource for those involved in epidemiological surveillance at all levels of the health pyramid, in both routine and emergency health situations. It is intended to guide stakeholders and harmonize practices at all levels of the health pyramid with regard to the implementation of data collection, quality assurance, analysis and use activities related to epidemiological surveillance in Cameroon.

The National Guide to Epidemiological Surveillance Data Management is intended as a pocket book, with a narrative section and standard operating procedures for all those involved in disease surveillance, helping to strengthen our collective ability to protect the health of our communities.

I therefore urge all those involved in epidemiological surveillance at every level of the health pyramid to make good use of it.



Dr. MANAOUA MALACHIE
Minister of Public Health



Appreciation.

The development of the National Epidemiological Surveillance Data Management Guide has been an assiduous and participatory process in which all the stakeholders involved have made rich and relevant contributions.

The process involved all those involved in epidemiological surveillance, foremost among them representatives of the technical departments of the Ministry of Public Health, who received technical and financial assistance from the Elizabeth Glaser Pediatric AIHD Foundation and contributions from other development partners.

The Ministry of Public Health would also like to thank all those who contributed to the finalisation and production of this guide. Their commitment and expertise have been essential in making this guide a valuable resource designed to enhance the quality and efficiency of data management in the field of epidemiological surveillance.

Technical drafting committee.

Coordination

- Dr. MANAOUA Malachie, Minister of Public Health.

Supervision

- Pr. NJOCK Louis Richard, Secretary General/MINSANTE ;
- Dr ETOUNDI MBALLA Georges Alain, Director of Disease Control, Epidemics and Pandemics, MINSANTE ;

Secretariat

Editorial and proofreading team

- Dr FEZEU Maurice, Head of the Health Information Unit, MINSANTE ;
- Mr BATOUM Emmanuel, Head of the IT Unit, MINSANTE ;
- Mr YOPNDI Charles, Head of the Monitoring Unit, MINSANTE ;
- Dr. ESSO ENDALLE Linda, Deputy Director of Epidemic and Pandemic Control, MINSANTE ;
- Dr. BILOUNGA NDONGO Chanceline, Head of Surveillance Unit, MINSANTE ;
- Dr. NGOMBA Armelle, Head of the Epidemic and Pandemic Response Unit, MINSANTE ;
- Ms TOUNA Claudine, Head of Studies Assistant No. 2, MINSANTE ;
- Mr EKANI Guy, Head of Studies Assistant No. 2, MINSANTE ;

Other members

- Mr MOUANGUE Christian, Staff/DLMPEP ;
- Mr KOMPGUEP Boris, Staff/DLMPEP ;
- Dr YOPA Sandra, Staff/DLMPEP ;
- Ms EFFEMBA Manuella, Staff/DLMPEP ;
- Mr BAKEBEG Luc, Staff/DLMPEP ;
- Dr ATANGANA Nestor, Staff/DLMPEP ;
- Mr NTAMACK Théodore, Staff/DLMPEP ;
- Ms NJEMTA Adeline, Staff/DLMPEP ;
- Mrs ATONGAPAI Diana, Staff/DLMPEP ;
- Mrs Belle AJONG FONTEM, Staff/DLMPEP ;
- Mr KONGNE Loïc, Staff/DLMPEP ;
- Mr JUGNIA Bertin, Staff/HDF ;
- Mr BONYOHE Martial, Staff/DROS ;
- Ms MAGON Sandrine, Staff/CIS ;
- Dr GANDAR Joël, Head of Surveillance Section, ONSP ;
- Ms TIOLA Denise, Staff/ONSP ;

-
-
- Mr TCHUALEU Bertrand, Staff/NPHL ;
 - Mr OTTHOU Jean-Noël, CBIS/RDPH CENTRE ;
 - Mr MAPOUO Clovis, CBIS/RDPH WEST ;
 - Mr MALOUA Marius, CBIS/RDPH LITTORAL.

Technical and Financial Partners

- Dr ADAMA N'dir, CDC Cameroon ;
 - Dr SIMO Leonie, EGPAF ;
 - Mr BICHARA Lawane, EGPAF ;
 - Mr MAIDEY Hamadama, EGPAF ;
 - Mr WANDJI Hans Ferry, EGPAF ;
 - Mr NGUEMKAM Gildas, EGPAF ;
 - Mr MOMA Elvis, EGPAF ;
 - Mr NGWAYU Claude, CHAI.
-

Glossary

Archiving : a set of actions designed to guarantee the long-term accessibility of information (files, documents, data) that must or wishes to be kept for legal, historical or cultural reasons.

Data confidentiality : protection of communications or stored data against interception and reading by unauthorised persons.

Cyber crime : all offences committed through cyberspace by means other than those usually used, and complementary to traditional crime.

Cyber Security : a set of prevention, protection and deterrence measures of a technical, organisational, legal, financial, human and procedural nature, as well as other actions that make it possible to achieve the security objectives set for electronic communications networks, information systems and the protection of personal privacy.

Data lifecycle : phases of the process by which data is created, recorded, processed, reviewed, analysed and reported, transferred, stored, retrieved and monitored until it is retired and destroyed.

Data : raw, uninterpreted basic elements that provide objective representations of facts or observations but have no meaning of their own.

Health data : data "relating to health conditions, reproductive outcomes, demographics, causes of death and quality of life" of an individual or population.

Information : the result of processing data using algorithms, data analysis and interpretation, making the raw data comprehensible and intelligible.

Interoperability : The ability of several computer systems and software applications to communicate with each other, exchange data and use the information exchanged.

Digital Health : the use of information and communication technologies (ICTs) in health and related field, including health services, health monitoring, health literature and education, health knowledge and research.

Backup : a copy of one or more electronic files created as a backup.

Data security : all the measures taken to prevent data corruption. **Data management** : the practice of collecting, storing and using data securely, efficiently and cost-effectively.

Data manager : a person skilled in collecting, storing and using data securely, efficiently and cost-effectively.

Data governance : arrangements made to ensure that data, regardless of the format in which it is generated, recorded, processed, stored and used to ensure a complete, consistent and accurate record throughout the data lifecycle.

Public health surveillance : the systematic and continuous collection, analysis and interpretation of data on the occurrence of disease and/or public health events, and their timely dissemination for decision-making purposes.

Data authentication system : controls access to systems by checking whether a user's credentials match the credentials contained in a database of authorised users or a data authentication server.

Sigles et abréviations.

- **ADX** : Average Directional Index
- **AEFI** : Adverse Events Following Immunisation
- **AMR** : Antimicrobial Resistance
- **CBIS** : Head of Information System Office
- **CERPLE** : Regional Centre for the Prevention and Control of Epidemics and Pandemics (Centre Régional de Prévention et de Lutte contre les Epidémies et les Pandémies)
- **CIS** : Health Information Unit (Cellule d'Information Sanitaire)
- **CMMS** : Computer-aided Maintenance Management
- **CNLS** : National AIHD Control Committee (Centre National de Lutte contre le Sida)
- **CTG/EPI** : Central Technical Group/Expanded Programme on Immunisation
- **DAMA** : Data Management
- **DHIS2** : District Health Information Software 2
- **DQA** : Data Quality Assessment
- **EGPAF** : Elizabeth Glaser Pediatric AIHD Foundation
- **EMR** : Electronic Medical Record
- **EPD** : Epidemic-Prone Diseases
- **EWARS** : Early Warning and Response System
- **HAI** : Healthcare-Associated Infections
- **HD** : Health District
- **HF** : Health Facility
- **HIV** : Human Immunodeficiency Virus
- **HL7** : Health Level 7
- **ICT** : Information Communication Technology
- **IDSR** : Integrated Disease Surveillance and Response
- **IT** : Information Technology
- **LMIS** : Laboratory Management Information System
- **MAR** : Monthly Activity Report
- **MINSANTE** : Ministry of Public Health
- **mpCHW** : Multi-purpose Community Health Worker
- **MPHDR** : Maternal and Perinatal Deaths Surveillance and Response
- **NHIS** : National Health Information System
- **PC** : Personal Computer
- **PD** : Priority Diseases
- **PHEOCC** : Public Health Emergency Operations Coordination Centre
- **PNLP** : National Malaria Control Programme
- **PNLT** : National Tuberculosis Control Programme
- **PRISM** : Performance of Routine Information System Management
- **PSSN** : Digital security awareness platform
- **RDPH** : Regional Delegation for Public Health
- **RMNCAH** : Reproductive Maternal, Newborn, Child And Adolescent Health
- **SCORE** : Survey, Count, Optimize, Review, Enable

-
- **SDG** : Sustainable Development Goals
 - **SFP** : Surveillance Focal Point
 - **SOP** : Standard Operating Procedures
 - **SQL** : Structured Query Language
 - **SVA** : Supplementary Vaccination Activities
 - **SWOT** : Strength Weakness Opportunity and Threat
 - **UHC** : Universal Health Coverage
 - **USAID** : U.S. Agency for International Development
 - **VPN** : Virtual Private Network
 - **WHO** : World Health Organisation



Overview of data management

1	General introduction	1
1.1	Background and justification	
1.2	Aims and objectives	
1.3	Scope	
1.4	Target audience	
2	The components of data management	4
2.1	General information on data management.	
2.2	Data management stages	
2.3	Data governance	
3	Implementation of the Different Components of Data Management	20
3.1	EPD data management	
3.2	Management of maternal and perinatal deaths and response surveillance data.	
3.3	Management of EPD and PD data across the laboratory	
3.4	Data Management Guidelines for Care	
3.5	Data Management at Border Health Posts	
3.6	Management of Mortality Data	
3.7	Management of MEV Data	
3.8	Data Management Guidelines for Case Management	

Chapitre 1: General introduction

1.1 Background and justification

The performance of a health system depends on the regular use of reliable data from a well-designed routine health information system. Since 2018, WHO ¹ has introduced the SCORE package to support Member States in strengthening national data systems and capacity to monitor progress towards the health-related SDGs and other national and sub-national health priorities. To this end, a range of tools at the global level have been developed and made available to countries to guide the surveillance of public health threats and other areas relevant to improving the health of populations.

In Africa, Health Information Systems (HIS) are evolving with the gradual integration of digitalisation. To facilitate this transformation, several countries, notably Tanzania, Kenya, Ivory Coast, Burundi and Madagascar ², with the support of MEASURE EVALUATION and USAID, have assessed their routine health information systems and drawn up strategic plans to strengthen them. Resources and tools have been developed to support the actors, including manuals of procedures for managing health data, the "Performance of Routine Information System Management (PRISM)", "Standards and Best Practices for Data Sources", "Guidelines for Data Management Standards in Routine Health Information Systems", etc.

Cameroon has made progress in strengthening its epidemiological surveillance system with the adoption of the third edition of the Technical Guide to Integrated Disease Surveillance and Response (IHDR) and the introduction of electronic surveillance data management platforms, including District Health Information Software 2 (DHIS 2), Data Management (DAMA), Electronic Medical Record (EMR), Laboratory Management Information System (LMIS), etc. These platforms facilitate the integration and management of data from several sources, in particular those relating to the performance of health service provision, the monitoring of medical products, human and financial resources and epidemiological surveillance. These platforms facilitate the integration and management of data from several sources, including data on the performance of health service provision, the monitoring of medical products, human and financial resources and epidemiological surveillance. To strengthen the monitoring of data management activities, several documents have been drawn up, such as the "National Digital Health Strategic Plan 2020 - 2024", the "DHIS2 Operational Plan 2022-2024", the "National Guide to Data Quality Review", and the "Guide to reviewing data to assess the performance of health programmes". There are also more specific resources produced at the level of programmes and other health structures, such as the "Manual of HIV Data Management Procedures" and the "Operational Guide to Case-based HIV Surveillance".

Despite efforts by the Ministry of Public Health to harmonize, coordinate and integrate the various strategies developed, the system is still encountering difficulties in producing the quality data needed for decision-making (epidemiological surveillance, planning, emergency management and response, etc.).

1. WHO SCORE PACKAGE
2. Evaluation reports

The advent of COVID-19 has challenged healthcare systems, including data management. To improve the performance of the data management system, two evaluations were carried out. In 2023, the Ministry of Public Health, with the support of its development partners, in particular the World Health Organisation (WHO) and the Elisabeth Glaser Pediatric AIHD Foundation (EGPAF), evaluated the Health Information System. These assessments revealed several weaknesses in the system, including :

a) **At peripheral level :**

- 55% of the data managers evaluated have not received any formal training in data management in the last 03 years ;
- 50% of the health facilities evaluated do not have an analysis tool for verifying data, and 87.5% of them do not use the data they produce ;
- The district completeness and timeliness rates for the first quarter of 2023 are 66% and 27% respectively ;
- 33% of the health districts evaluated have good data accuracy³ and 38% of them use the data ;

b) **At regional level :**

- The data completeness rate was 33.45% for the 1st quarter of 2023 ;
- 44% of data managers know the most important activities for improving data quality ;

c) **At the central level :**

- There is insufficient coordination between the stakeholders, the requirements for ensuring interoperability between the various electronic platforms have not yet been met, although some intermediate software components have been developed, and there is no procedures manual for managing health data in the context of routine and emergency health care.
- We also note that some tools are not interoperable, a multiplicity of data collection tools, there is a deviation from the conventional data reporting circuit and dispersal of resources.

Several initiatives have been launched to address these problems, including the development of a roadmap for improving the management of epidemiological surveillance data, and the creation of technical groups working on strengthening the data management system.

This guide will serve as a reference document for stakeholders at all levels for optimal management of epidemiological surveillance data in routine and emergencies. The second chapter covers the general aspects of data management, i.e. data governance and the components of data management, in particular data collection, data transmission circuit, analysis, archiving, quality and use. The third chapter addresses these components according to certain scopes, as presented later in the document. This guide also includes Standard Operating Procedures for the optimal implementation of data management activities (see Appendices).

1.2 Aims and objectives

1.2.1 Aims

This guide will enable epidemiological surveillance data to be used effectively for evidence-based decision-making.

3. Based on 03 selected indicators

1.2.2 Objectives

1.2.2.1 General objective

To define national guidelines for the management of epidemiological surveillance data in routine and emergency health situations.

1.2.2.2 Specific objectives

Specifically, this will involve :

- Promoting the governance and compliance of epidemiological surveillance data ;
- Describing the implementation of data management components ;
- Defining standard operating procedures for data management at all levels of the health pyramid ;

1.3 Scope

This document deals with data management in both routine and emergencies. It covers the following topics :

- Surveillance of EPD, PD and other public health emergencies (indicator-based, event-based)
- Vaccination (Routine, AEFI, SVA, surveys, studies, evaluations, reports)
- Logistics (Management of laboratory and case management inputs)
- Care (treatment centre, care units)
- Laboratory (EPD, sentinel surveillance, genomic surveillance, HAI surveillance, AMR surveillance)
- Border surveillance
- Mortality surveillance
- Maternal and Perinatal Deaths Surveillance and Response (MPHDR)
- Surveillance of Chronic Non-Communicable Diseases
- Surveillance of Neglected Tropical Diseases

1.4 Target audience

This guide is intended for those involved in epidemiological surveillance at all levels of the healthcare pyramid, in particular :

- Health service providers
- Health facility managers
- Heads of Health Offices
- Heads of Health Districts
- Surveillance Focal Points
- Data managers
- Heads of Health Information Offices
- The CERPLE Coordinators
- Those involved in surveillance within the technical directorates and priority programmes
- Development partners

Chapitre 2: The components of data management

2.1 General information on data management.

According to the World Health Organisation (WHO), data is quantitative or qualitative information, usually numerical, that is collected, recorded, stored, processed, analysed and interpreted for surveillance, research, planning, implementation and evaluation of health activities. They are also known or assumed facts that can be used to calculate, reason or plan.

Health data is any data "related to health conditions, reproductive outcomes, demographics, causes of death and quality of life" of an individual or population. Health data includes clinical measures as well as environmental, socio-economic and behavioural information relevant to health and well-being. Routine data are data collected by healthcare providers in the course of their work, by supervisors and through routine surveys in healthcare institutions. The sources of this data are generally individual medical records, records of services provided and records of health resources. Data is generated at regular intervals (no more than one year) and is collected in public and private health facilities, as well as in Border Health Posts (BHPs) and at the community level. All these interactions require management that takes into account several stages, this is data management.

Data management is the practice of collecting, storing and using data securely, efficiently and cost-effectively. Given the central role that data plays today, a sound data management strategy and a modern data management system are essential to every organisation. The data management process comprises tasks and procedures, such as collecting, processing, validating, exploiting and storing data using tools. These may be from primary, secondary and/or physical and electronic sources.

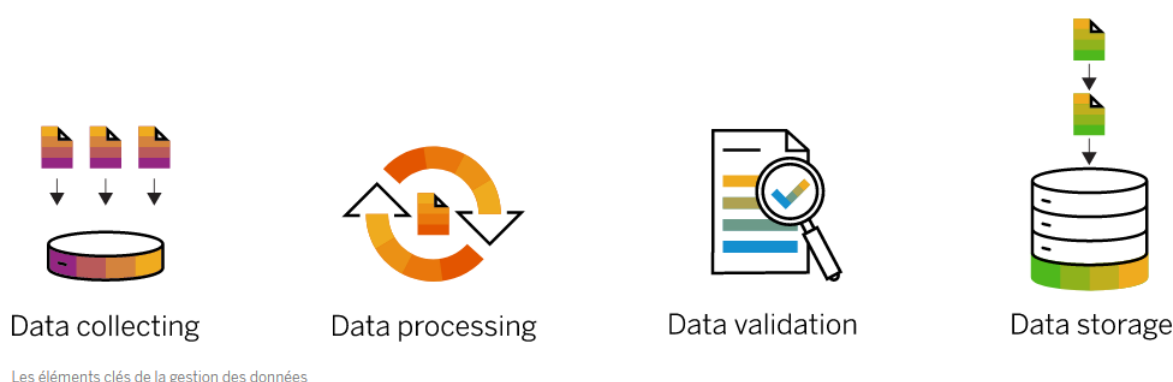


FIGURE 2.1 – Data life cycle

In addition to the above tasks, the data management process may also include the following points :

- Integration of different types of data from disparate sources, including structured and unstructured data ;

-
- Guaranteed high availability and disaster recovery ;
 - Managing the use of and access to data by individuals and applications ;
 - Protecting and securing data and guaranteeing data confidentiality.

In Cameroon, health data management is governed by several regulatory instruments which set out how the National Health Information System (NHIS) is to operate and be strengthened at all levels of the health pyramid, including the community level. The regulatory framework for this management describes the roles and responsibilities of each player at the central, intermediate and peripheral levels. It also defines the data to be collected, the collection tools, the information circuit and the practical aspects of the information system. There are several national texts and laws on data management. These include :

- Law No. 2010/012 of 21 December 2010 on cyber security and cyber crime in Cameroon ;
- Law No. 2010/013 of 21 December 2010 governing electronic communications in Cameroon ;
- Law No. 2020/010 of 20 November 2020 governing statistical activity in Cameroon and its implementing decree ;
- Order N°1899/MINSANTE of 21/08/2020 on the creation, organisation and operation of the Interministerial Committee responsible for monitoring the implementation of Cameroon's National Digital Health Strategic Plan 2020-2024 ;
- Health Sector Strategy 2020-2030 ;
- The National Strategic Plan for Digital Health 2020-2024 ;
- The DHIS2 2022-2024 Operational Plan ;
- Circular Letter No. D36-59/L/MINSANTE/SG/CIS, on the Ministry of Public Health's new health information management requirements ;
- The manual of guidelines for the production of statistics from administrative sources.

The normative framework is made up of four components : the operation of the NHIS, the information circuit, the list of indicators and the responsibilities of those in charge of data management.

- The operation of the NHIS consists of defining its functions, determining the staff profile, defining the neeHD in terms of human resources, materials and equipment at all levels of the health pyramid, indicating the minimum procedures for compliance and monitoring data quality.
- The health information circuit specifies the rules for transmitting data between health units, District Public Health Services, Regional Delegations of Public Health and the central level, as well as feedback (see information circuit figure).
- A list of the main variables to be reported is contained in a template for the monthly activity report (MAR), the weekly notification forms for Epidemic-Prone Diseases (EPD) and the Community MAR.
- Those in charge of health data management are responsible for the various processes involved in collecting, transmitting, processing, analysing, storing and disseminating data at the required health level.

2.2 Data management stages

Health data management involves the following stages : collection, processing, analysis, dissemination, storage and archiving.

2.2.1 Data collection and entry

Data collection is the process of gathering and recording data using appropriate tools to obtain information that meets a specific need. It is carried out as part of the routine or emergency system, or as part of specific surveys and studies. It is an important stage in the information generation process. Data can be collected from existing sources, through the introduction of new data collection media and using physical or electronic tools. Data should be collected from sources such as key informants, CHWs and within health facilities. These data are entered into primary data collection tools such as forms and registers, and then into standard software such as DHIS2 and other platforms adopted by MINSANTE for data reporting.

2.2.2 Data quality assurance

Quality data is essential for monitoring progress toward the Sustainable Development Goals (SDGs) and national health priorities. It is also essential for strengthening countries' capacity to prevent, prepare for and respond to health emergencies. Reliable and timely data is essential for successful interventions to improve the health of populations.

Several criteria or dimensions have been defined to describe data quality. These are mainly :

- Accuracy or validity : Accurate data contains minimal errors and bias,
- Reliability : Data is reliable when it is measured and collected systematically over time,
- Completeness or exhaustiveness : Complete data captures all the individuals, services, sites or other eligible units it is intended to measure,
- Accuracy : Accuracy means that the data is sufficiently detailed to measure the indicators following their definition,
- Timeliness : Data is timely when it meets the deadlines for submitting reports to the next level,
- Integrity and confidentiality : refers to all the measures taken to prevent any modification of the data, unauthorised use of the data, and modification of the system put in place to collect the data.

Data Quality Assurance (or Data Quality Control DQA) is an approach or concept based on a methodology for the rapid assessment of the quality and adequacy of health data used for the planning and development of public health policies.

It uses a set of guidelines for data verification, paper and electronic tools to facilitate data collection and analysis, and draws on several assessment methods or tools, including :

- **DQA (Data Quality Assessment) :** which focuses exclusively on verifying the quality of reported data, assessing the management of basic data and systems reporting standard programme indicators, carried out by an entity external to the delivery site ;
- **RDQA (Routine Data Quality Assessment) :** is a simplified version of the DQA and consists of a self-assessment of the service site (to prepare the DQA). It focuses on a specific theme and is carried out routinely as part of monitoring and evaluation activities ;
- **DQR (Data Quality Review) :** is a global approach to harmonizing data quality assurance in health programmes. It uses a set of tools and methods for cross-cutting assessment of data quality and provides guidelines for implementation in developing countries ;
- **DQA (Data Quality Audit) :** aims to assess the impact of data quality on the performance of health programmes. It uses 16 quantitative evaluation models specific to HIV/AIDS, malaria and tuberculosis indicators to assess data quality, and a generic qualitative "System Evaluation" module to assess gaps and weaknesses in the reporting system.

The table below gives a more detailed description of the various data quality assessment tools :

TABLEAU 2.1 – Some tools for assessing data quality

Items	ASSESSMENT TOOLS		
	DQR	DQAudit	RDQA
Description	A global approach to harmonizing data quality assurance in health-care programmes	aims to assess the impact of data quality on the performance of health-care programmes	A form of self-assessment and capacity building, a simplified version of Data Quality Assessment
Methodology	Uses the Master Facility List to select the sample of health facilities to be evaluated and collects information on a maximum of 05 priority health programmes.	16 quantitative evaluation models to assess data quality, and a generic qualitative "System Evaluation" module to assess gaps and weaknesses in the notification system	Focuses on one area/theme for monitoring/evaluation purposes
Implementation period	between 3 and 6 months	At least 3 months	One week
Frequency of use	annual	Si besoin est (plurianuelle)	regularly (as part of routine supervision)
Level of implementation	Strategic (national)	External evaluation (partner, landlord, etc.)	Health facilities and intermediate levels (district and region)

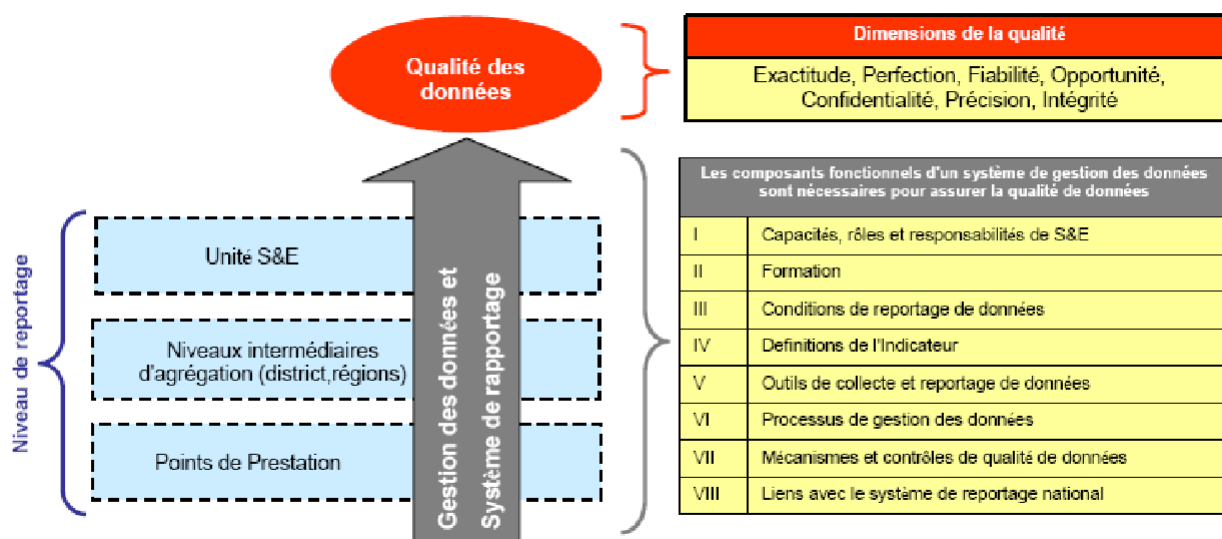


FIGURE 2.2 – RDQA conceptual framework

In the specific case of the RDQA recommended for the peripheral and intermediate levels, the activities to be carried out to improve data quality are presented in the table below :

TABLEAU 2.3 – Some data quality assessment tools

Level	Actors	Activities to be carried out
Community	Community Health Worker	<ul style="list-style-type: none"> • Check that tools are filled correctly and completely (see SOP) • Transmission of full reports
Peripheral	Data manager/health facilities and districts SFP	<ul style="list-style-type: none"> • Checking that physical and electronic tools are correctly and filled (see SOP) • Complete reports delivered on time
	Head of health facilities and health districts	<ul style="list-style-type: none"> • Ensure the training of staff responsible for data collection and entry ; • Ensuring that the SOPs for the various tools used on the site are available, • Organize data validation meetings at the sites ;
		<ul style="list-style-type: none"> • Coordinate on-site data quality monitoring • Take part in data review meetings at the regional level

Intermediate	Head of Health Information Office	<ul style="list-style-type: none"> • Coaching HD in quality assurance • Monitor tool availability at the peripheral level • Leading regional data review meetings
	Regional Delegate of Public Health	Chair regional data review meetings
Central	Data Managers/statisticians and demographs of the central directorates and Programs; Head of the Epidemiological Surveillance Service	<ul style="list-style-type: none"> • Planning and carrying out DQA • Organise national data review meetings • Monitor the availability of tools at the operational level • Make up for missing data

2.2.3 Data transmission

Data transmission refers to the sharing of any type of information by physical or digital means. It takes place at all levels, bilaterally and at a defined frequency. Feedback must be given from the higher level to the lower level so that action can be taken or for feedback. For better data quality, transmission must be both physical and electronic at the peripheral and intermediate levels. Similarly, in emergencies, a rapid data exchange system should be set up following the deadlines recommended by the IHR (2005).

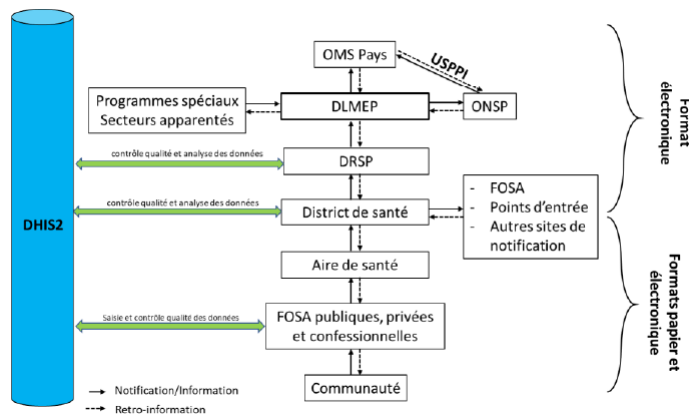


FIGURE 2.3 – IDSR data transmission circuit, IDSR 3rd edition

2.2.4 Data analysis

Surveillance data analysis is a process in which data is examined, processed and interpreted so that it can be used to understand the health status of a population. It aims to identify patterns, trends, correlations and associations between risk factors, exposures and diseases. The main objective of data analysis is to provide essential information for understanding the distribution of disease, assessing risk factors, guiding public health interventions and making evidence-based decisions for disease prevention and control. This analysis is generally carried out on a weekly, monthly, quarterly, annual (routine) and/or daily (emergency) basis. The data analysis process includes :

- **Data mining** : The first step is to ensure that the expected reports and variables are complete.
- **Descriptive analysis**
 - **Analysis by time, place and person** : enables you to see how the various diseases under surveillance are progressing.
 - **In-depth analysis** : consists of calculating descriptive statistics to understand the distribution of cases, and deaths and to monitor performance. This can be done using tools such as Excel, R, Python, etc.
- **Spatial analysis** involves using mapping tools and GIS techniques to highlight the geographical distribution of cases and deaths and identify high-risk areas.
- **Explanatory analysis** : enables aggravating factors to be examined using a risk assessment matrix. Using models, this method also highlights the cause-effect relationships, underlying processes and mechanisms involved in a given phenomenon. In short, explanatory analysis seeks to answer the "how" and "why" of a situation or event.

2.2.5 Exploitation and dissemination of results/information

Data exploitation, or data enhancement, consists of using data to extract useful information and identify trends to optimise decision-making. Dissemination involves making the results obtained available to users by various means. The exploitation process can include data analysis, statistical modelling and data visualisation.

2.2.6 Data processing and feedback

Data is used at all levels of the health pyramid. To do this, the analyses carried out beforehand at each level will make it possible to visualise the trends in the key indicators, which will facilitate better decision-making. Changes over time in the same type of data should raise the alarm if there are significant differences from what is generally observed.

2.2.7 Information dissemination tools

Information is disseminated and promoted through several channels, including :

- **Reports** : format generally used by public authorities, organisations, consultants, etc.
- **Posters** : format generally used to disseminate results in certain structures
- **Images/Videos (visuals)** : generally used to raise awareness, spread information about the situation of a health event or encourage community engagement.
- **Dashboard** : these are drawn up for both routine and emergencies. In a routine context, they are used to assess the status and development of diseases to detect potential epidemics. In an emergency, they present the status of ongoing epidemics.

2.2.8 Means of distribution

The results and information produced are made available to users in a variety of ways :

- Websites and other digital communication platforms are used to disseminate these tools on a routine or emergency basis. These include :
 - Minsante website : www.minsante.cm
 - PHEOCC website : www.ccousp.cm
 - NPHO website : www.onsp.minsante.cm
 - Minsante Digital Library : www.cdnss.minsante.cm
 - Health map : www.dhis-minsante-cm.org
- Emails : used to share reports and various databases with the concerned parties ;
- Correspondences : generally carried out through physical persons, involving the delivery of documents to the concerned structures after drafting the accompanying official notes.

2.2.9 Data storage and archiving

Data storage refers to the preservation of information on a physical and/or digital medium that is generally used frequently. Data archiving is the secure, long-term storage of information that is no longer frequently used but must be kept for legal, historical or regulatory reasons. It is a long-term preservation method designed to guarantee the integrity and availability of data over an extended period. For good data archiving, you need to choose the right storage medium.

2.2.9.1 Storage medium

It is important to choose the archiving method that best suits your need in terms of security, access and long-term preservation. Data can be stored :

- **On physical media** : Use of folders, boxes and shelves to store printed documents such as the various notification forms ;
- **In the cloud** : Data stored on remote servers via cloud services. E-mails, drives and online data collection platforms are all part of this ;
- **On removable media and immovable media (fixed hard disks)** : these are disks or storage devices that can be connected to and disconnected from a computer without switching it off, such as CHD, DVHD, USB sticks or external hard drives. Fixed hard drives are those built into electronic devices.

The components of the data life cycle range from collection to archiving, analysis, interpretation, transmission and dissemination. However, given the sensitive nature of health data, it is important to add regulation of its flow and coordination between the actors involved in its management : this is data governance supported by relevant criteria such as security and interoperability.

2.3 Data governance

Health data governance refers to the set of policies, procedures, standards and practices that guide the management, use and protection of health data. It aims to ensure that health data is collected, stored, processed, shared and used ethically, securely and in compliance with current standards and regulations. It encompasses various aspects : data quality, security, confidentiality, interoperability and data-driven decision-making. The importance of data governance in achieving the objectives set out in the aforementioned standard-setting documents. It involves all public and private sector actors who collect, manage or use data as part of their activities. It also covers the data inherent in community activities, for which the guiding principles and the roles and responsibilities of the actors form the basis.

2.3.1 Guiding principles of data governance

The National Strategic Plan for Digital Health (NSPDH) 2020-2024 refers to the relevant criteria in data governance, which are guiding principles that are factors enabling the effectiveness of the data management system, namely :

- **Transparency** : any action involving the collection, use, consultation or processing of data must be traceable and verifiable ;
- **Purpose limitation** : the data collected must only be used for known and pre-identified purposes and should never be used for any other purpose that is incompatible with the aim of the project ;
- **Interoperability** : Data exchange with existing systems (DHIS2, UHC, SIGLe, telemedicine, etc.) must be effective and secure ;
- **Data minimisation** : the data collected must be useful, relevant and appropriate to the project's objective ;
- **Data accuracy** : the personal data collected must be accurate and regularly updated ;
- **Limiting data retention** : the data collected must be retained for a period that is useful for the programme's objectives. In the event of death, the deceased patient's data should not be kept beyond a statutory period, unless expressly requested by the judicial authorities.
- **Security and integrity** : data is collected and processed in such a way as to guarantee its security through the implementation of technical and organisational mechanisms.
- **Informed consent** : patients must be informed and have consented to their data being processed and stored electronically ;
- **Respect for patients' rights** : patients have the right to respect the confidentiality of their data, as well as information about their illness. They also have the right to be informed about their illness and the indications for treatment. To this end, they have the right to consult their electronic medical record at any time and for any purpose. Patients may also request :
 - Rectification or deletion of data that is incomplete, erroneous, out of date or unnecessary for the project ;
 - The portability of information for any useful purpose ;
 - Restricting access to personal data.
- **Confidentiality and non-disclosure of data** : : This principle implies that those involved in the electronic data processing process must sign a confidentiality clause and undertake to implement every mechanism to protect the personal data collected (encryption, access restriction, security audit, etc.). Non-disclosure of data unless expressly requested by the judicial authorities as part of proceedings pending before the courts and involving the patient, the personal data collected may under no circumstances be disclosed without the patient's express and formal agreement.

The repressive framework relating to the violation of professional secrecy is set by Article 310 of the Cameroon Penal Code (2016), which punishes with imprisonment of 03 months to 3 years and a fine of 20,000 to 100,000 FCFA, anyone who reveals, without the authorisation of the person to whom he belongs, a confidential fact that he knew or that was only revealed to him because of his profession or position. Except where expressly requested by the judicial authorities or for legal expertise.

2.3.2 Roles and responsibilities of governance actors

The texts guiding data governance assign specific roles and responsibilities to those involved in the management of epidemiological surveillance data. These actors must take into account

all aspects relating to the confidentiality and security of routine and emergency health data. Each level is responsible for implementing the provisions of this guide in its activities, and for monitoring their application. Data governance is ensured at all levels of the health pyramid by the following actors :

TABLEAU 2.5 – Roles and responsibilities of the actors in the epidemiological data management system

Level	Actors	Roles and responsibilities
Community	Community Health Worker	<ul style="list-style-type: none"> • Collection and transmission of community signals • Notification of cases • Quality assurance and archiving of records
Peripheral	<ul style="list-style-type: none"> • Health facility Data Manager • Health facility Surveillance Focal Point • District Data Manager • HD Surveillance Focal Point 	<ul style="list-style-type: none"> • Implementation of overall site intervention activities • Entering data into systems • Liaison with the technical team for equipment maintenance and troubleshooting • Archiving of records • RDQA
	<ul style="list-style-type: none"> • Health facility Managers (categories 1 to 6) • Health District Heads 	<ul style="list-style-type: none"> • Validation of data entry by data managers • Monitoring and coordination of surveillance activities • Staff proposal and replacement plan in the event of potential unavailability
Intermediate	District Data Manager	<ul style="list-style-type: none"> • Site supervision • Monitoring and reporting activities • Archiving
	CBIS	<ul style="list-style-type: none"> • Capacity building of proposed staff • Formative supervision (RDQA) • Monitoring and evaluation of digital health interventions on sites
	Program Data Managers	Regional technical assistance (monitoring and evaluation tools, capacity building, reporting, etc.)

	<ul style="list-style-type: none"> • Program Managers • Regional Public Health Delegate 	Monitoring and coordination
Central	Data Managers/Statisticians and Demographers from the Directorates and Programs	<ul style="list-style-type: none"> • Management of epidemiological databases • Formative supervision • Monitoring-evaluation (RDQA) • Digital archiving
	IT Specialists	<ul style="list-style-type: none"> • Installation and maintenance of systems and equipment : computers, tablets, servers, databases, etc. (security and updates) • Digital archiving
	Heads of the Sub-Directorate for Epidemiological Surveillance	Facilitating the coordination platform for epidemiological surveillance data management activities

2.3.3 Data security and hosting

Data security is essential to health data governance. It encompasses multiple dimensions, including the recommendation of good practice in the collection, storage, use, dissemination, analysis and disposal of health data. Aspects of data security are found in all the health data governance principles, but it is also a fundamental principle in its own right. This section deals with the business processes for guaranteeing data security, because in the context of the implementation of digital health, the issue of data security is of a highly sensitive nature, requiring compliance with recommendations for hosting and securing applications and epidemiological surveillance data. Circular No. D36-80/LC/MINSANTE/SG/CI of 09 December 2021 from the Minister of Public Health on the hosting of applications and data at Minsante therefore recommends that the IT unit be contacted for the following processes :

1. Choice of accommodation
2. Choice of hosting provider (technical and commercial criteria)
3. Choosing a domain name
4. Choosing the type of accommodation
5. Application and data hosting
6. Repatriation of outsourced platforms and databases

The following requirements are prescribed to ensure safety, availability, maintainability and evidence-based decision-making.

2.3.4 A few data security principles

- User access to epidemiological surveillance data must be via a strong authentication system that incorporates certificates generated by the national PKI;
- The authentication system must be configurable and enable access profiles and privileges to be defined;

-
- Communications between the sites of the various entities called upon to interact must be transported via VPN links ;
 - Data must be highly available ; to this end, all equipment must be duplicated and configured.
 - All operations carried out on the data must be recorded in a centralised logging system ;
 - A data monitoring system (technological and security) with related procedures ;
 - The off-site backup system must be set up to back up and archive the data handled ;

Total security must be offered in terms of access and data management, with the following functionalities in particular :

- **Access security** : access to information must be strictly controlled. Only authorised users may access it ;
- **Authorisation** : a hierarchical, manageable authorisation system, with user profile management, must enable users to be granted or denied access to the various processing and consultation procedures. The functionalities expected at this level are as follows :
 - Access rights by option, by user with a high level of confidentiality, by password or other ;
 - Temporary standby/lock of the application by the user ;
 - Usage profiles by level of responsibility and by remit ;
 - All procedures carried out on the system must be traceable and must include the operation carried out, the identification of the user, the date of processing and the initial and final status of the data affected ;
 - Confidentiality : the system must also ensure the confidentiality of data exchanged on the network ;
 - Backup : in addition to the backup procedures that the system administrator may undertake according to his or her need, the system must have backup procedures that are systematically triggered according to events that have been pre-set. It must be possible to restore these backups using a clearly defined procedure.
 - Technical security procedures must comply with the legal requirements in force, in particular the laws on cybersecurity and electronic communications, and the law on the protection of personal data.

It must also be able to integrate with encryption tools or VPNs. It must also be able to integrate with strong authentication solutions on the market so that security mechanisms can be put in place to detect and prevent any attempt at access or violation by intruders in good time.

2.3.5 Some hosting principles

The platforms managing health data are hosted in data centres in France and abroad. They must comply with the following principles :

2.3.5.1 Availability and Reliability

Availability : Operate 24 hours a day, 7 days a week. The maximum acceptable rate of unavailability is :

- 15 minutes per day during the period from 7 AM to 11 PM,
- 30 minutes per day during the period from 11 PM to 7 AM,
- 3 hours per year for maintenance,
- The annual number of downtimes must not exceed 6 occurrences.

Reliability : No data loss is tolerated.

At least once every six months, a complete restoration of the application on the functional qualification environment followed by a data encryption procedure as described in the confidentiality

and traceability requirements below.

2.3.5.2 Maintainability, Maintenance, and Upgrading

Maintain the system based on an annual maintenance contract, renewable year by year and to be signed at the end of the warranty period. In addition, the design and configuration of the Computerised Maintenance Management System (CMMS) must take into account the following three aspects :

- Preventive maintenance ;
- Corrective maintenance ;
- Upgradable maintenance.

2.3.5.3 Sizing and Performance

Access to applications and data is via fixed and mobile workstations. The number of user workstations depend on the category and status of the health facility.

2.3.5.4 Confidentiality and traceability of data

The existence of a data anonymisation procedure will enable production data to be copied to other platforms (development, integration, qualification, etc.) while guaranteeing the anonymity of confidential data. Any malfunction of this procedure should be recorded as a serious anomaly.

2.3.5.5 Data backup and archiving

- Data backup procedures must be automatic, using the tools provided.
- Backups must be able to be launched "hot" (without stopping operations).
- Complete management of data archiving, with the possibility of consulting archives and retrieving archived data if necessary. This retrieval must comply with the data confidentiality policy.

2.3.5.6 Physical security

Physical data security refers to the measures taken to physically protect sensitive information and the infrastructures that store or process it. It aims to prevent unauthorised access, manipulation or destruction of data by malicious individuals or natural disasters. This form of security is essential to guarantee the integrity, confidentiality and availability of data. The following minimum data security requirements must be complied with :

- **Restricted Physical Access** : Control physical access to the premises where data is stored or processed using locking systems, access cards, keys, or biometric devices.
- **Surveillance and Video Monitoring** : Install surveillance cameras to monitor the premises where data is handled or stored to detect any suspicious or unauthorized activity.
- **Visitor Control** : Implement procedures to verify the identity of visitors and regulate their access to sensitive areas where data is processed or stored.
- **Physical Security of Servers and Equipment** : Install security systems such as safes, protective cages, or air conditioning systems to protect servers and equipment from theft, physical damage, or malfunctions.
- **Protection Against Natural Disasters** : Take measures to protect data against natural disasters like fires, floods, or earthquakes by using fire detection and suppression systems, off-site backups, or surge protection devices.
- **Waste Management** : Implement policies and procedures for the secure destruction of end-of-life physical data storage media, using destruction methods such as shredding, disintegration, or magnetic degaussing.

2.3.6 Interoperability

The interoperability of IT systems refers to the ability of different systems, applications, or software components to work together transparently and efficiently, without requiring significant effort on the part of the user. This enables the exchange of information and cooperation between different technologies, even if they come from different suppliers.

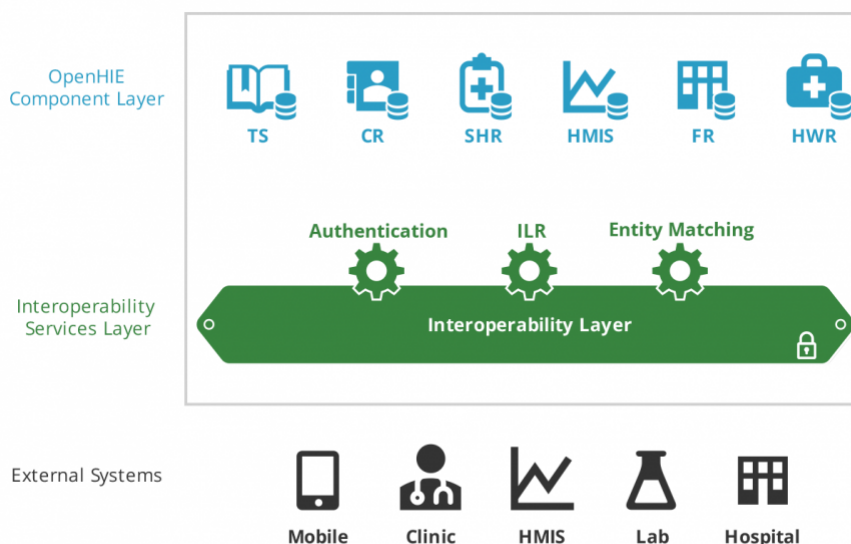


FIGURE 2.4 – Interoperability Architecture

2.3.6.1 Cameroon's Digital Health Architecture

Cameroon's Digital Health Enterprise Architecture is a conceptual model describing the information system, data sources and integrations that Cameroon's Ministry of Health intends to implement to achieve its strategic objectives. Its ambition is to create "a sustainable digital health architecture that is integrated, computerised, accessible by all stakeholders, efficient at all levels, enabling information to be shared and producing quality health information, to measurably improve health outcomes".

Its objectives are to :

- Optimize the use of ICT resources through the curation, publication, and dissemination of the digital health architecture diagram.
- Create and maintain the detailed roadmap of the Digital Health Architecture. Advise project teams and health software development providers on integration steps and the use of standards.
- Create and maintain an inventory of existing digital health applications (including mobile applications).
- Optimize digital health investments by creating reusable components, standards, and an integration plan.

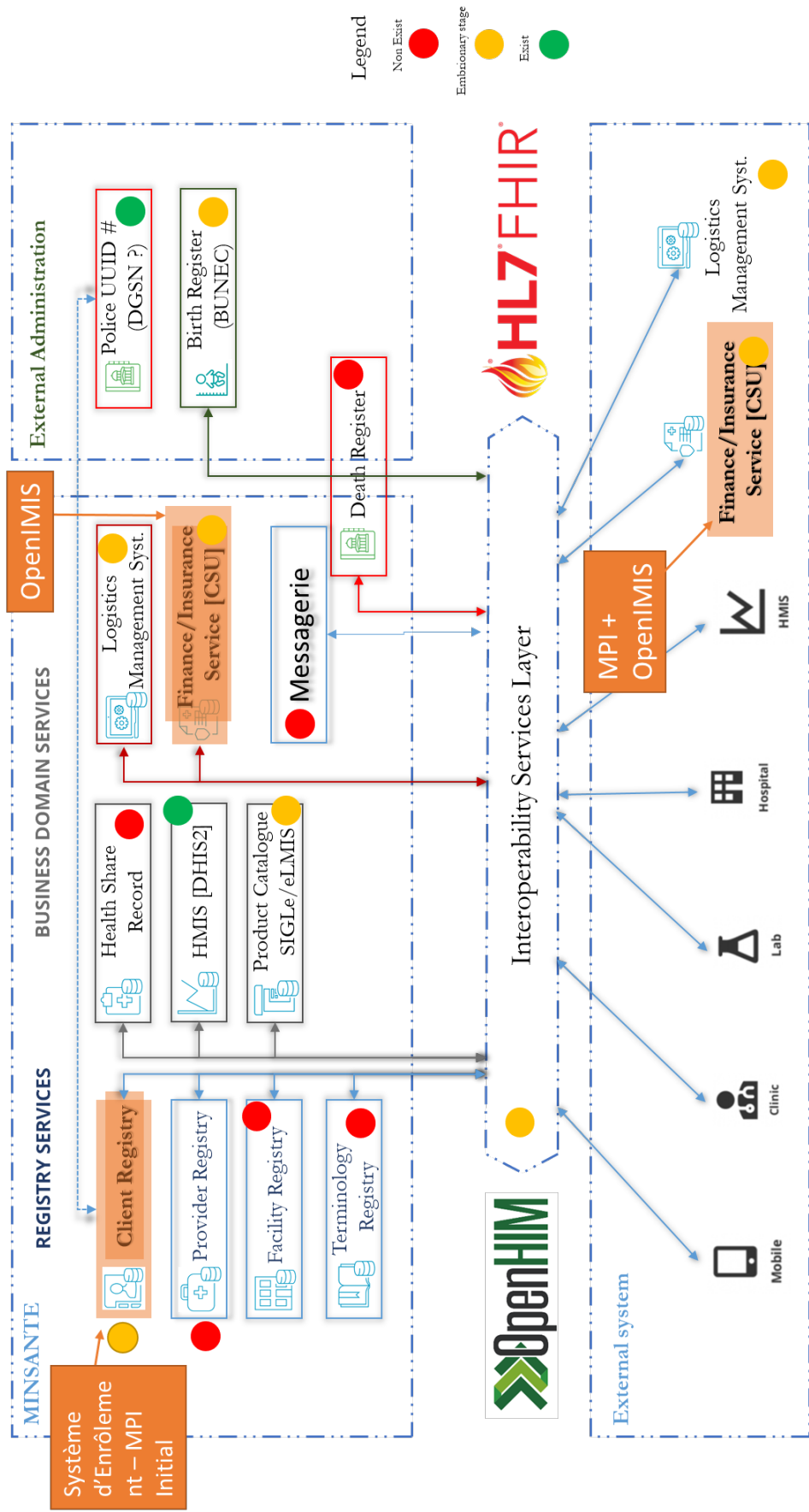


FIGURE 2.5 – Cameroon’s Digital Health Architecture

2.3.6.2 Interfaces between applications

To enable healthcare data to be exchanged, the software used must "speak the same language". Interoperability must be technical, by defining common formats to enable the different software used in the healthcare system to interconnect. Without interoperability, there can be no sharing or exchange of data, and therefore no value-added services based on this data. Interoperability enables dematerialised health data to be used increasingly in an organised environment. To guarantee the secure exchange of health data, interoperability relies on the identification and authentication of the parties accessing it. This foundation of tangible and intangible infrastructures now constitutes a "trusted space" aligned with public health objectives. It makes possible a new generation of patient-focused services based on the use of structured data.

2.3.6.3 Ease of Use and Human Factors

The system user interface must be :

- Graph ;
- Easy to use : assisted input, windowing and mouse use ;
- User-friendly : ergonomic, use of colours in screen grids, graphic interface, windowing system, use of buttons.

2.3.6.4 Accessibility Requirements

When it comes to workstations, data must be accessible :

- On desktop computers (PCs) ;
- On laptops ;
- On tablet PCs and smartphones.

Chapitre 3: Implementation of the Different Components of Data Management

Effective data management plays a crucial role in improving public health and making informed decisions to promote the well-being of populations. The previous chapter theoretically addressed the different components of data management. The aim of this chapter is to practically present how these components are implemented according to the different scopes in the country's context.

3.1 EPD data management

3.1.1 Data collection and entry

Epidemiological surveillance data is collected and entered in Cameroon through a variety of mechanisms, ranging from mandatory reporting systems to health information systems and specific surveillance initiatives. The aim is to ensure that reliable and timely information is available to inform public health decisions and the response to epidemics and other health emergencies. The process involves several actors and stages.

3.1.1.1 Data collection sources.

Health facilities receive patients every day, who provide them with detailed information on the signs and symptoms of their illnesses and the laboratory tests carried out. This information is recorded in consultation and laboratory registers. In the community, major events of interest are recorded by community health workers and described by them in logbooks. These various documents are sources of surveillance data.

3.1.1.2 Data collection tools.

We distinguish primary data collection tools, which include consultation registers and laboratory registers. We also distinguish secondary data collection tools, such as notification forms (immediate, weekly, monthly) and community health worker logbooks. Additionally, we identify electronic collection tools, namely DHIS2, Kobbocollect, and EWARS.

3.1.1.3 Data collection methodology.

A distinction is made between passive and active surveillance. Passive surveillance is carried out systematically by the surveillance focal points in the health facilities, which use the available registers. Active surveillance is carried out as part of investigations. Teams are deployed in the field to actively search for cases in the community and health facilities.

3.1.1.4 Data notification circuit.

Some diseases such as cholera, poliomyelitis and yellow fever are subject to mandatory and immediate reporting. The surveillance focal points (SFP) in the health facilities are required to report suspected or confirmed cases to the highest hierarchical level, i.e. the Health District. Cases are reported electronically via the DHIS2, but also by telephone, and a copy of the physical case report form is also sent. Other diseases that are reported weekly or monthly follow the same circuit as immediately notifiable diseases but do not need to be notified by telephone.

3.1.2 Data analysis and interpretation.

The analysis and interpretation of epidemiological surveillance data in Cameroon generally involve several stages :

3.1.2.1 Data cleansing.

Before analysis, data is often cleaned to identify and correct errors or inconsistencies. This may include checking for missing data, outliers or duplicates. With the introduction of regional coaching, data review meetings are organized at regional and national levels to facilitate this process.

3.1.2.2 Statistical analysis.

The data is then analysed using statistical methods to identify trends, seasonal variations, spatial or temporal clusters, and other relevant epidemiological indicators. Statistical analysis can include techniques such as trend testing, correlation analysis, regression models and time series analysis. DHIS 2 offers pre-defined dashboards for instant monitoring of certain key indicators.

3.1.2.3 Interpretation of results.

The results of the analysis are interpreted to provide useful information about the epidemiological situation, potential risk factors, public health needs and recommended control measures. This interpretation may involve comparing the data with predefined epidemiological thresholds, national or international standards and historical data.

3.1.3 Data exploitation

As for data exploitation, it includes :

3.1.3.1 Communication of results.

The results of the analysis are communicated to relevant stakeholders, including health authorities, health professionals, implementing partners and the public. This may be done at epidemiological surveillance coordination meetings or through regular epidemiological reports, presentations at meetings, epidemiological bulletins and situation reports.

3.1.3.2 Using the results

The results of epidemiological analysis are used to guide decisions on public health policy, programme planning, resource allocation and the implementation of interventions. They can also contribute to ongoing public health surveillance and to assessing the impact of health interventions.

3.1.4 Data security and hosting.

The security and hosting of surveillance data in Cameroon is generally ensured by various technical and organisational measures to guarantee the confidentiality, integrity and availability of the data and to protect it against potential threats and risks.

3.1.4.1 Secure infrastructure.

User access to epidemiological surveillance data in Cameroon is via a strong authentication system that integrates certificates generated by the national PKI. Access to information is strictly controlled. Only authorized users can access it. Surveillance data is stored on secure servers located in data centres or facilities managed by the country. These facilities are often equipped with physical security measures.

3.1.4.2 Data encryption.

Sensitive data is often encrypted when stored on servers to prevent interception or unauthorised access. Encryption ensures that even if data is compromised, it remains unreadable without the appropriate decryption key.

3.1.4.3 Access control.

Access control mechanisms are in place to restrict access to data to authorized persons only. Patient information entered is confidential and only authorised persons have access to it. Access permissions based on roles and responsibilities to reinforce the security of user accounts are assigned at the community level, from the health facility to the various directorates and programmes at the central level.

3.1.4.4 Data backup and recovery.

Regular backup strategies are put in place to ensure data availability in the event of disaster or data loss. Back-up copies are generally stored in secure locations separate from the primary data.

3.1.4.5 Regulatory compliance.

Data security practices often comply with national and international regulations on personal data protection and confidentiality, such as Cameroon's data protection law or the European Union's General Data Protection Regulation (GDPR), where applicable.

3.1.4.6 Hosting principles.

The platforms managing health data are hosted in data centres in France and abroad. They comply with the principles of availability and reliability. Maintainability is ensured based on an annual maintenance contract, renewable year by year and signed at the end of the guarantee period. Three aspects are taken into account : preventive maintenance, corrective maintenance and upgradable maintenance.

3.1.4.7 Data backup and archiving.

Data is backed up automatically using various tools. Backups are launched "immediately" (without stopping operations). Complete management of data archiving means that archives can be consulted and archived data recovered if necessary. This recovery respects the data confidentiality policy.

3.2 Management of maternal and perinatal deaths and response surveillance data.

The MPDRS is a continuous cycle of measurements designed to provide actionable, concrete data in real-time on levels of maternal mortality, stillbirths and neonatal deaths, and as the causes and contributing factors of deaths. The MPDRS aims to identify, report and review all maternal deaths, stillbirths and neonatal deaths in communities and health facilities, providing information to develop effective, evidence-based interventions to reduce maternal mortality, stillbirths and neonatal deaths, measure their impact and plan the response.

3.2.1 Data collection and entry

The data is collected by the MPDRS focal points. They must collect individual and aggregated data on cases of death. This data is collected using various physical and electronic tools, such as hospitalization registers, delivery room registers, notification forms, investigation forms, death review forms, the MPDRS line list, EPD forms, MAR forms and the DHIS2 platform.

Data collection begins mainly by identifying and recording cases of death. This involves recording the deaths of all women of childbearing age (15 to 49 years), all stillbirths and deaths of all newborns in health facilities (in all departments including the mortuary) and in the communities. In the community, suspected deaths are identified by a Community Health Worker (CHW), Traditional Birth Attendants (TBAs), a member of the Health Area Committee or another community representative. However, in the health facility, identification is based on the medical records of all women of childbearing age, regardless of the reason for consultation or hospitalisation. In the same way, information on the circumstances of death is recorded for all newborns, both dead and stillborn. Data collection then continues with the notification of cases. Cases of maternal death, stillbirths and neonatal deaths are reported to the next level up so that appropriate action can be taken. This notification must be made within 24 hours for institutional deaths by the MPDRS focal point for the health area/health facility manager. Deaths occurring in the community are reported to the relevant authorities by a community health worker or community representative within 48 hours. As part of this surveillance, data is also collected during the investigation and review of deaths. Investigation is the in-depth gathering of various types of information (medical and non-medical, as well as standard demographic data) from eyewitness accounts, photographs and written records about an institutional death, to gain a better understanding of the case. It is carried out by the District team, with possible support from the regional and district levels. It differs from the verbal autopsy, which is the study of maternal deaths at the community level. This study makes it possible to determine the medical causes of death and to check the personal, family or community factors that may have contributed to the death taking place outside a health facility. The review involves analysing the medical and non-medical factors that led to the death, assessing the measures taken to prevent it and formulating recommendations for an effective response. This action makes it possible to confirm the case of maternal death, stillbirth and neonatal death and to determine the exact cause of death. It is carried out in the health facility.

3.2.2 Data transmission

Data is transmitted immediately from all levels, following the notification circuit. In the event of a confirmed death, the health area MPDRS focal point notifies and informs the district MPDRS focal point within 24 to 48 hours using a telephone call, SMS or e-mail. The district MPDRS focal point will inform the regional and national MPDRS focal points. The district MPDRS focal point then fills in the notification section of the MPDRS line list (Excel) and forwards it to the regional level, which then forwards it to the central level. Similarly, after each death review, the district MPDRS focal point completes the review section of the MPDRS line list and the transmission circuit to the higher level remains the same.

3.2.3 Quality assurance

Several factors improve data quality, including (i) the correct and exhaustive completion of standardized data collection tools and reporting forms ; (ii) the completeness and timeliness of data or reports ; (iii) functional information systems ; and (iv) documented data review procedures.

3.2.4 Data analysis

3.2.4.1 Descriptive analysis of data

The data from the MPDRS are compiled, and analyzed (in time, place and person) to determine trends, compared with data from previous periods and interpreted so that they can be used for public health actions.

3.2.4.2 Analysis of medical causes and contributing factors in deaths

The medical causes of death (according to ICD-10) are analysed by classifying all deaths into direct or indirect causes. This analysis also makes it possible to identify the primary causes of death, which can serve as a basis for possible responses. In addition, this analysis aims to highlight the frequency of health services and non-medical factors contributing to maternal, perinatal and neonatal deaths. Examination of these factors gives an insight into the possibility of avoiding each death. Interviewing family members and healthcare staff and analyzing patients' medical records can provide a clear picture of the hospital's external and internal situation that contributed to the death.

3.2.5 Exploitation and dissemination of results

Information is disseminated and promoted through some channels, including :

- **Reports** : format generally used by public authorities, organisations and consultants. In the context of surveillance, a distinction is made between (i) weekly MPDRS reports, which
- **MPDRS Committee** : meets every six months to review policies and strategies to combat maternal and neonatal mortality and the response.

3.3 Management of EPD and PD data across the laboratory

The use of Laboratory Information Management Systems (LIMS) to streamline all phases of laboratory testing (pre-analytical, analytical and post-analytical) has become inevitable for the management of EPD and PD data flows.

3.3.1 Data collection

- Screening sites (community, health facility, SFP)
As soon as an alert is received, the laboratory's surveillance focal point proceeds as follows :
 - Notifies the SFP of the HA/HD/RDPH
 - Notifies the NPHL
 - Completes the sample notification and accompanying sheet
 - Collect the sample according to the SOP
 - Carryout the RDT according to the SOP if available
 - Registers in the approved register
 - Integrates the information from each case into the platforms (DHIS2, 3MS, MA-MALPRO, etc.)
 - Packs and sends the sample to the reference laboratory following the SOP, together with the form
- Reference laboratories at the Health District level (TB, HIV viral load, etc.) Le point focal surveillance du laboratoire procède ainsi qu'il suit :
 - Receives the form and sample following the SOP
 - Verifies the information on the form and sample is correct
 - Delivers the receipt
 - Analyze the sample following the SOP
 - Registers in the approved register
 - Enter results into platforms (DHIS2, 3MS, PLACARD, etc.)
 - Transmit results (screening site, NPHL, HD, RDPH, DLMEP)
 - Transmits summaries of samples received, analyzed and results to line management (NPHL, HD, RDPH, DLMEP)

-
- Regional reference laboratories (COVID-19, TB, cholera, AMR, HIV viral load, Mpox, etc.) The laboratory's surveillance focal point procedure is as follows :
 - Receives the form and sample following the SOP
 - Verify that the information on the form and sample is correct
 - Delivers the receipt
 - Analyze the sample following SOP
 - Registers in the approved register
 - Enter results into platforms (DHIS2, 3MS, PLACARD, etc.)
 - Transmit results (screening site, NPHL, HD, RDPH, DLMEP)
 - Transmits summaries of samples received, analysed and results to line management (NPHL, HD, RDPH, DLMEP)
 - Central-level reference laboratories (TB, AMR, HIV-HBV-HCV viral load, influenza, COVID-19, cholera, bacterial meningitis, FHV, Mpox, MEV, genomic sequencing, etc.) The laboratory's surveillance focal point proceed as follows :
 - Receives the form and sample following the SOP
 - Verify that the information on the form and sample is correct
 - Delivers the receipt
 - Analyzed the sample following SOP
 - Registers in the approved register
 - Enter results into platforms (DHIS2, 3MS, PLACARD, etc.)
 - Transmit results (screening site, NPHL, HD, RDPH, DLMEP)
 - Transmits summaries of samples received, analysed and results to line management (NPHL, HD, RDPH, DLMEP)

3.3.2 Transmission of information from the laboratory

The transmission of data on analysis results and the summary of samples received and analyzed is carried out immediately and every week by all levels, in compliance with the notification circuit.

3.3.3 Data quality assurance

The testing sites, reference laboratories, and DS/DRSP/DLMEP ensure the quality of data on all forms, namely :

- The completeness of the sociodemographic, clinical and paraclinical information and the results of the analyses of each case
- Data consistency
- Completeness and timeliness of data and feedback
- Retention of physical versions of data, in particular, laboratory registers and individual case notification forms
- SOP is available, legible, up to date and respected
- Validated software
- Ongoing staff training
- Adequate, good-quality equipment and back-up
- Monitoring and evaluation

3.3.4 Data analysis

All levels (screening sites, reference laboratories, HD, RDPH, DLMEP) must analyse the data to observe trends. A descriptive analysis will be carried out according to time, place and person :

- Time analysis will be carried out using an epidemiological curve at weekly intervals.

- The mapping should show the distribution of the epidemic according to the location
- A description of the individuals concerned will show the age groups affected, their gender and clinical characteristics.

3.3.5 Exploitation and dissemination of results/information

Situation reports must be produced and presented at coordination meetings at all levels, to ensure wide dissemination.

3.3.6 Data storage

All data must be entered in DHIS2 Hard disks and cloud space will be used to store the results and summary of the samples received and analysed.

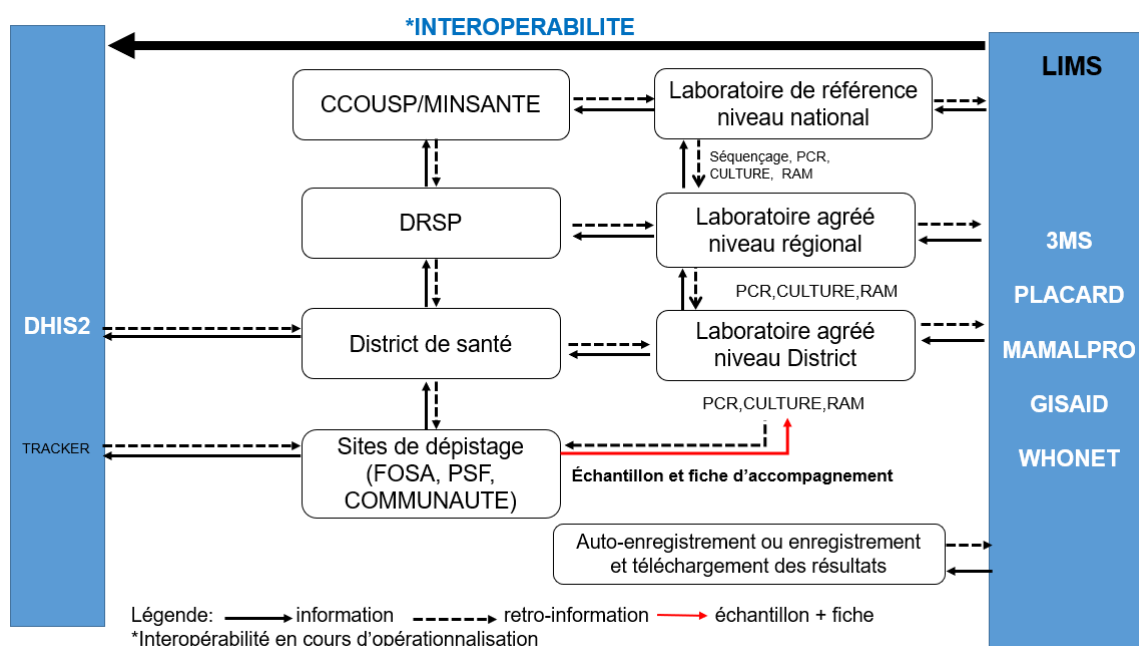


FIGURE 3.1 – Laboratory information transmission circuit

TABEAU 3.1 – Reference Laboratory Network by Disease and Platform

Reference Laboratory Network by Pathology	Level	Platform	Interoperability with DHIS2
Genomic Sequencing Laboratory	Central	GISAID	No
Accredited Laboratories for COVID-19	Central	3MS, MAMALPRO, PLACARD	No
Accredited Laboratories for COVID-19	Regional	3MS, MAMALPRO, PLACARD	No

Accredited Cholera Laboratories	Central	DHIS2 (non-operational)	NA
Accredited Cholera Laboratories	Regional	DHIS2 (non-operational)	NA
RAM Surveillance Laboratories	Central	WHONET	Yes
RAM Surveillance Laboratories	Regional	WHONET	Yes
TB Laboratories	District	None	None
TB Laboratories	Regional	None	None
TB Laboratories	Central	None	None
HIV Viral Load Laboratories	District	None	None
HIV Viral Load Laboratories	Regional	None	None
HIV Viral Load Laboratories	Central	None	None
Accredited Influenza Laboratory	Central	PLACARD	No
Accredited Mpox Laboratories	Central	None	None
Accredited Mpox Laboratories	Regional	None	None
Accredited Bacterial Meningitis Laboratories	Central	None	None
Accredited Bacterial Meningitis Laboratories	Regional	None	None
Accredited Hepatitis B and C Viral Load Laboratory	Central	None	None
Accredited MEV Laboratory	Central	None	None

3.4 Data Management Guidelines for Care

Care data are essential for managing an epidemic. They allow for observing the evolution of the epidemic, adjusting response mechanisms, and anticipating the progression of the epidemic based on trends. Data are produced by the community, care centers, and any health facility that may receive cases.

3.4.1 Data Collection

The collected data include sociodemographic, clinical, laboratory information, case prognosis, and outcomes (recovered, deceased, stable).

- **In the Community :** Community health workers (ASC) and key informants identify and report cases using the community case definition. These cases are immediately registered (in a logbook). The information will be sorted and verified by the area supervisor. If the case is confirmed, it will be recorded in the ASC's linear list.
- **In Health Facilities (FOSA) :** Health facilities use case definitions for identifying cases. They record information about the case using the data collection tools provided (linear list, CBS tracker, individual notification form, consultation and care register).
- **At the Health Area Level :** The health area supervisor compiles the linear lists from the FOSAs in their jurisdiction.
- **At the District Level :** The district data manager compiles data from all the health areas under their responsibility, as well as from specialized treatment centers in the district.
- **At the Regional Level :** The regional health department compiles all the linear lists from the districts in its jurisdiction.
- **At the Central Level :** The data manager compiles databases from all regions.

3.4.2 Data Transmission

- For diseases requiring immediate notification, data transmission occurs immediately at all levels, following the notification circuit according to the command chain principle. The data transmission format is an Excel database (linear lists). The CBS tracker must also be filled out with verification at all levels. This data is also transmitted weekly to DHIS2.
- For diseases that require weekly reporting, data is transmitted weekly to DHIS2.

3.4.3 Data Quality Assurance

- From health facilities (FOSA) to the Central Level, data quality must be verified. The health facility or care center must ensure the completeness of sociodemographic, clinical, paraclinical, and prognostic information on cases.
- Higher levels must ensure the completeness and timeliness of data from the units under their jurisdiction during coordination meetings and site visits.

Health facilities must retain physical versions of data, including care registers and individual case notification forms. These documents will help verify the accuracy of the data. The district, region, and central levels must ensure data consistency. In the case of inconsistent data, information must be verified using physical records. If necessary, site visits should be conducted to ensure the quality of the collected and recorded data.

3.4.4 Data Analysis

All levels must analyze the data to observe trends. Descriptive analysis will be performed based on time, location, and demographics. Temporal analysis will use an epidemic curve on a weekly basis. Mapping will represent the distribution of the epidemic by location. A description of demographics will highlight affected age groups, gender, and clinical characteristics (type of dehydration). Other indicators such as case fatality rate, attack rate, etc., should be calculated.

An analysis of associated factors will be conducted, particularly during outbreak investigations, to produce data useful for prevention.

3.4.5 Utilization and Dissemination of Results/Information

During epidemics, situation reports must be produced and presented at coordination meetings at all levels, along with Sitreps to ensure wide dissemination.

3.4.6 Data Storage

All data must be entered into DHIS2 for archiving purposes. Hard drives and cloud storage will be used to retain Excel databases.

3.5 Data Management at Border Health Posts

There are three types of entry points in Cameroon : air, sea, and land. Border health posts (PSF) are responsible for monitoring public health events.

3.5.1 Data Collection and Entry

Disease collection registers are not standardized and vary by each type of entry point. The collected data is reported on a summary form designed by the ONSP, named the daily health control report at entry points, Monthly Activity Report, and MAPE.

3.5.2 Data Transmission

3.5.2.1 Transmission

Data transmission occurs through DHIS2.

Saisie de données ?

Unité d'organisation: CM du Port Autonome de Douala (PSF)

Ensemble de données: PSF_RAPPORT QUOTIDIEN DU CONTRÔLE SANITAIRE aux PoEs

Période: 2024-03-12

RAPPORT QUOTIDIEN DU CONTRÔLE SANITAIRE AUX POINTS D'ENTREE (PoE)

Identification du PSF

Nom du gestionnaire de données : Numéro de Téléphone :

Données globales sur les moyens de transport et les passagers

Nombre (Nb) des moyens de transport :	<input type="text"/>	Nb de moyens de transport désinfectés/fumigés:	<input type="text"/>
Nb de passagers arrivés : Total :	Femme : <input type="text"/>	Homme : <input type="text"/>	<input type="text"/>
	Fièvre jaune	<input type="text"/>	
Nb de passagers ayant une carte	Covid-19 :	<input type="text"/>	Choléra: <input type="text"/> Rougeole : <input type="text"/>

FIGURE 3.2 – Screenshot of a data entry form in DHIS2

3.5.2.2 Transmission Deadlines

- Weekly (MAPE)
- Daily (daily health control report at entry points)
- Monthly (RMA)

Border Health Posts are health facilities classified from 4th to 6th category. As such, they are integrated into the normal data flow for epidemiological surveillance. However, in case of an emergency and in accordance with the IHR 2005, data may simultaneously be sent through the normal circuit and at the national level (National IHR Focal Point) to facilitate timely notification.

3.5.3 Data Processing

Surveillance data can be entered and stored manually or electronically. Regardless of the method used, the following steps should be taken :

- Update the weekly or monthly summary totals, ensuring they encompass events actually reported that week or month. Late notifications from previous weeks or months must be entered in the corresponding week or month, and totals recalculated ;
- Write "zero" when no cases have been reported. A "zero" allows higher levels to know that surveillance has not detected any cases of disease, priority conditions, or public health events ;
- Identify and correct duplicates ;
- Establish ongoing contact with notification sectors to resolve issues of missing information or errors, and discuss any inconsistencies detected in notifications ;

3.5.4 Storage

Electronic data storage is systematically performed after data registration in DHIS2.

Data aggregation forms must be systematically archived in folders or archive boxes based on the type of data collected (daily, weekly, and monthly).

3.5.5 Data Analysis

Collected data must be analyzed and interpreted at all levels (PoE, Health Districts, DRSP, Central). This analysis is conducted using indicators specific to the sectors operating at the PoE. (Include analysis indicators in the monitoring-evaluation section.) Here are examples of indicators that could be calculated and monitored :

- Number of events identified across all PoEs in the country by incoming and/or outgoing travelers during a given period.
- Number of events at the PoE level by incoming and/or outgoing traveler, by type of PoE (i.e., port, airport, land crossing) during a given period.
- Number of events by number of transport means following the same route during a given period.
- Etc...

A review of the analysis results should be conducted internally on a daily basis to ensure early detection of any potential public health events of international concern (USPPI).

Sectors producing data at the PoEs should meet monthly to make decisions aimed at improving public health actions.

After analyzing the data, it is important to generate relevant information for decision-making. To do this, it is necessary to :

- Present weekly graphs, maps, and tables of the results obtained ;

- Systematically review conclusions based on the analysis plan at the PoE, if it exists (see SIMR);
- Systematically study the results to :
 - Assess whether the situation is improving or not;
 - Find reasons for the observed situation.

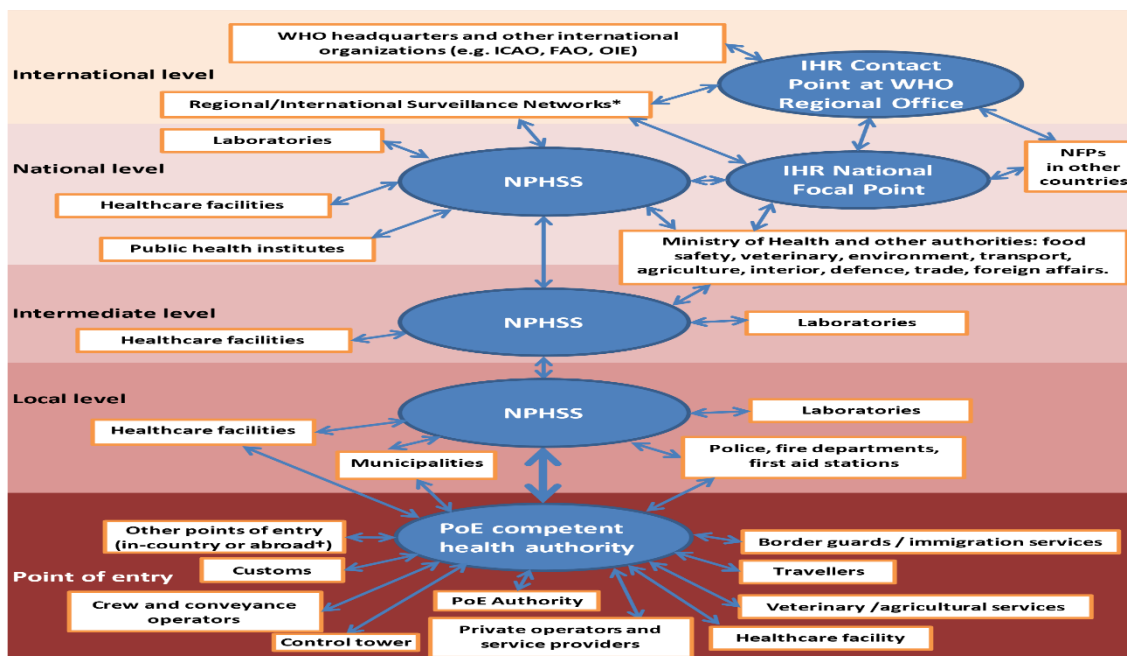


FIGURE 3.3 – Information circulation and feedback circuits

3.6 Management of Mortality Data

The management of mortality data is a process aimed at understanding mortality trends, identifying factors associated with deaths, evaluating the impact of public health interventions, and informing health policies. It is essential for understanding the dynamics of mortality within a given population and for guiding actions aimed at improving public health and preventing avoidable deaths.

3.6.1 Data Collection and Entry

Data on deaths are collected by health sectors (hospitals, communities), civil registration centers, and the National Security Sector. However, it should be noted that data from the community are still very limited. Collection is done using various physical tools, which are then integrated into electronic tools. The tools include :

- Death notification form
- Death certificate
- Civil registration death declaration register
- Cause of death certificate
- Data Entry Module of DHIS2
- ICD-11 Module of DHIS2

In the community, data on deaths are collected by Community Health Agents (ASC). In health facilities (FOSA), they are collected by the mortality surveillance focal point.

3.6.2 Quality Assurance

Data quality assurance is conducted at various levels of the health pyramid through :

- Verification of completeness and timeliness of data in DHIS2
- Conducting data harmonization meetings at all levels of the health pyramid
- Regular feedback to various stakeholders on reported data
- Data triangulation
- Conducting data reviews

3.6.3 Data Transmission

In the health sector, data is transmitted following the data transmission circuit within the framework of the SIMR (see figure). The tools used are the Data Entry and ICD-11 modules of DHIS2.

3.6.4 Data Analysis

Mortality surveillance data can be directly analyzed on the various collection platforms once their quality is assured. However, default dashboards are available in DHIS2, allowing for visualization of the distribution of recorded deaths over time and space, as well as the distribution of deaths by cause.

Using certain DHIS2 modules such as the Data Viewer, Event Viewer, and Mapping, it is possible to formulate custom queries to obtain specific tables, graphs, or maps.

3.6.5 Utilization and Dissemination of Results

Mortality data are generally presented monthly during surveillance meetings held every Friday.

3.7 Management of MEV Data

3.7.1 Sources of Surveillance Data for MEV

Information regarding the epidemiological surveillance of MEVs is recorded in consultation registers, hospitalization registers, MEV notification forms, MEV and MAPI investigation forms, MEV and MAPI registers, MEV and MAPI monitoring tables, MEV validation forms, and linear case lists for MEV.

3.7.2 Data Collection for MEV Surveillance

3.7.3 Data Collection for MEV and MAPI Surveillance

Data collection for MEV and MAPI surveillance occurs at each level of the health pyramid.

- At the community level, signals are collected through traditional healers' registers and from the SFE. Additionally, environmental samples are collected for the search for polioviruses at pre-selected sites.
- At the health facility level (FOSA), for each suspected case, the FOSA fills out the MAPI or MEV notification/investigation form.
- At the health district level, the surveillance focal point conducts site visits as part of the active surveillance of cases, collecting data through an electronic form (Integrated Supportive Supervision). The health district also conducts MEV investigations in support of the FOSA.
- At the regional level, data collection for surveillance is ensured by the Biological Sample Reception Posts (PREB). The PREB receive biological and environmental samples from FOSA/health districts and investigation forms for suspected MEV cases. This data is recorded in registers and in DHIS2 (new process).

-
- At the national level, after receiving the investigation forms, this data is entered into a database. However, with the new process in place, data will be entered into DHIS2, and each entity will ensure the completeness of each step.

3.7.4 Reporting and Data Transmission Tools

- At the FOSA level : investigation and notification forms are transmitted to the health district.
- At the health district level : investigation and notification forms are transmitted to the regional level. Data from active surveillance is transmitted through ODK.
- At the regional level : investigation forms are entered into the MEV tracker in DHIS2 and subsequently transmitted to the central level.
- At the central level : investigation forms are entered into the MEV database (a process currently being replaced by the MEV tracker) and transmitted to the reference laboratory.

3.7.5 Quality Assurance

To ensure the quality of data for MEV surveillance, a weekly triangulation exercise is conducted at each level between the number of samples received and the MEV data reported in the DHIS2 MAPE.

The completeness of variables on investigation forms is verified at the regional and central PREB levels.

3.7.6 Data Processing and Analysis

- **Health Facilities** : Data analysis is conducted using standard analysis tools (monitoring graphs for routine vaccination) or by directly checking in the collection tools and MEV monitoring tables.
- **At the Health District Level** : A MEV monitoring dashboard is created at the health district level. MAPI dashboards are also used to monitor the quality of MEV data.
- **At the Regional and Central Levels** : Automated data analysis tools have been developed for monitoring MEV indicators. A report on the indicators is generated weekly.

3.7.7 Utilization and Dissemination

A SITREP is prepared every epidemiological week for each MEV and shared at all levels and with supporting partners.

A monthly activity report is produced by the region, summarizing the activities conducted within the framework of MEV surveillance.

3.7.8 Storage and Archiving

MEV data are updated weekly, stored in Microsoft Access databases for each MEV, and backed up in the Microsoft Teams workspace of the PEV.

DHIS2 also serves as an archiving source. Periodic extraction of MEV data is performed and saved in the Teams space.

3.8 Data Management Guidelines for Case Management

Case management data are crucial for epidemic management. They allow for monitoring the evolution of the epidemic, adjusting response mechanisms, and anticipating the trajectory of the epidemic based on trends. The data are produced by the community, care centers, and any health facility that can receive cases.

3.8.1 Data Collection

The collected data include sociodemographic, clinical, laboratory information, case prognosis, and outcomes (recovered, deceased, stable).

- In the community : ASCs and key informants identify and notify cases using the community case definition. These cases are immediately recorded (in a logbook). The information is then triaged and verified by the area chief. If the case is confirmed, it will be entered into the ASC's linear list.
- In FOSA : health facilities have case definitions for identifying cases. They enter information about the case using the collection tools provided (linear list, CBS tracker, individual notification form, consultation and management register).
- At the health area level : the area chief compiles linear lists from the FOSA in their jurisdiction.
- At the district level : the data management officer compiles data from all health areas under their charge as well as from specialized treatment centers in the district.
- At the regional level : the DRSP compiles all linear lists from the districts in its jurisdiction.
- At the central level : data managers compile databases from all regions.

3.8.2 Data Transmission

- For immediately reportable diseases, data transmission occurs immediately at all levels, adhering to the notification circuit according to the chain of command principle. The data transmission format is an Excel database (linear lists). The CBS tracker must also be filled out with verification at all levels. This data is also transmitted weekly in DHIS2.
- For diseases requiring weekly reporting, data is transmitted weekly in DHIS2.

3.8.3 Data Quality Assurance

- From FOSA to the Central level, the quality of data must be verified. The health facility or care center must ensure the completeness of sociodemographic, clinical, paraclinical, and prognostic information on cases.
- Higher levels must ensure the completeness and timeliness of data from units under their jurisdiction during coordination meetings and site visits.

Health facilities must retain physical versions of data, including care registers and individual case notification forms. These records will allow verification of data accuracy. The district, regional, and central levels must ensure data consistency. In cases of inconsistent data, information should be verified using physical registers. If necessary, site visits should be conducted to ensure the quality of collected and recorded data.

3.8.4 Data Analysis

All levels must analyze the data to observe trends. A descriptive analysis will be conducted based on time, place, and people. Time-based analysis will be done using an epidemic curve on a weekly basis. Mapping will represent the distribution of the epidemic by location. A description of the affected population will highlight age groups, gender, and clinical characteristics (e.g., type of dehydration). Other indicators, such as the case fatality rate and attack rate, should also be calculated.

An analysis of associated factors will be conducted, particularly during outbreak investigations, to generate useful data for prevention.

3.8.5 Utilization and Dissemination of Results/Information

During epidemics, situation reports must be produced and presented at coordination meetings at all levels, as well as Sitreps to ensure widespread dissemination.

3.8.6 Data Storage


All data must be entered into DHIS2 to ensure archiving. Hard drives and cloud storage will be used to retain Excel databases.



Standard Operating Procedures

Data Collection and Notification of Surveillance Data	37
Data Quality Assurance	42
Data Storage and Archiving for Epidemiological Surveillance	48
Data Security and Access for Epidemiological Surveillance	53
Management of Community Signals and Cases	58
Analysis of Epidemiological Surveillance Data	64
Management of Epidemiological Surveillance Data in the Laboratory	71
Sharing (dissemination) of Information	77
Transmission of Epidemiological Surveillance Data and Feedback ..	82
Bibliography	86

Data Collection and Notification

	Data Collection and Notification of Epidemiological Surveillance
Code :	
I. Objective	
General Objective : Facilitate data collection and notification for surveillance at the operational level.	
Specific Objectives :	
<ul style="list-style-type: none">• Master data collection tools and their usage ;• Adhere to the data transmission circuit ;• Make available data from investigations, death reviews, surveys, vaccination, rapid response, and CATI ;	
II. Target Audience	
This document is aimed at actors in epidemiological surveillance at the operational level (District Health Services, FOSA)	
III. Prerequisites for Implementation	
<ul style="list-style-type: none">• Know the definitions of signals and community cases ;• Understand standard case definitions (in hospital settings) ;• Trained personnel in the use of data collection tools.	
IV. Expected Results	
<ul style="list-style-type: none">• All information on a suspected case of disease or public health event in the community is immediately (within 24 hours) collected in the logbook, electronic notification form for community signals and cases, and call center register ;• All information on a suspected case is collected within the allotted time : 24 hours for immediately reportable diseases (individual data) and by Monday before 6 PM for MAPE, AP, and other monitored diseases (aggregated data) ;• All data from investigations, death reviews, surveys, vaccination, rapid response, CATI, etc. are collected and available in physical and electronic formats (DHIS2, Excel, Kobocollect, Red Cap) ;• Laboratory data are collected and recorded in physical and electronic formats.	
V. Human Resources	
<ul style="list-style-type: none">• Community Members : ASCP	

-
- **Health Personnel** : Data manager and PFS of FOSA/laboratory/PSF, and the district management team ;
 - **Monitoring Unit** : Call center (telephone operators, medical regulators), media monitoring team.

Equipment/Tools

- Office kit (computer) ;
- Software (DHIS2, Excel, Kobocollect, ODK, EWARS, WHONET, etc.) ;
- Communication kit (tablet, phone, internet modem, etc.).

Documents


- Technical guide SIMR ;
- Approved or adapted consultation registers ;
- Laboratory register ;
- Call register ;
- ASCP logbook ;
- Individual notification forms for different diseases or events based on structures and programs ;
- Investigation forms ;
- Death review forms ;
- Validation forms ;
- MAPE and AP forms ;
- RMA ;
- User manuals for electronic platforms (DHIS2, WHONET, etc.).

VI. Procedures			
A. In the Community			
A community-based surveillance team under the responsibility of the area chief should be established, consisting of ASCP and other volunteers, with each ASCP assigned to one or more geographical areas (communities).			
Responsible	Activities	Tasks	Frequency
ASCP	Establish a network of key informants composed of community leaders	<ul style="list-style-type: none"> Assist in identifying key informants (traditional leaders, religious leaders, traditional healers, school teachers, etc.) in their area; Brief them; Set up a discussion platform (WhatsApp group or meeting days). 	Immediate
	Home visits in their action area	<ul style="list-style-type: none"> Conduct a courtesy interview with the head of the household or other responsible individuals to inquire about any illnesses in the household or neighborhood, dead animals from strange diseases, wild animals in the area, or other unusual situations. If there is a sick person in the household or neighborhood, record information on the suspected case (signal) in the logbook, which will be passed to the PFS/ FOSA manager at the end of the day, and in the electronic notification form in Kobocollect and EWARS. Similarly, gather information in large gathering areas : churches, markets, fields, schools. Immediately inform the PFS/FOSA manager via a call or any other quick means. 	Immediate
B. In the FOSA/PSF/LAB			

<p>PFS or data manager of the FOSA and PSF</p>	<p>Collect information with physical and electronic tools</p>	<ul style="list-style-type: none"> • Identify responsible individuals at collection points; • Create an exchange platform (WhatsApp, meetings); • Immediately report any immediately reportable diseases or events to the PFS of the DS by call/text or any other means upon their registration at the FOSA; • Fill out the individual notification form for the case and submit it to the PFS of the DS within 24 hours of registration; • Summarize weekly by counting the number of cases and deaths by age group, gender, diseases, and laboratory results from all services, including the laboratory of the FOSA (on Monday morning); • Directly enter the weekly MAPE notification form into DHIS2 no later than Monday before 6 PM. 	<p>Immediate, Weekly</p>
<p>PFS of the Laboratory</p>	<p>Collect information with physical and electronic tools</p>	<ul style="list-style-type: none"> • Provide a daily summary of the data on samples received, analyzed, and results for immediately reportable diseases in the laboratory register; • Fill out the individual notification form for immediately reportable diseases; • Provide a weekly summary of collected data by counting the number of samples received, analyzed, and results in the registers (by Monday morning) to be sent to the PFS of the FOSA; • Input data into electronic platforms. 	<p>Daily, Weekly</p>
<p>C. In the Health District</p>			

<ul style="list-style-type: none"> • CBS • PFS • Data manager at the DS level 	Collect information with physical and electronic tools	<ul style="list-style-type: none"> • Fill out individual case forms during investigations, vaccination campaigns, and surveys; • Compile these data into a linear list at the DS level; • Compile all results from laboratories into a harmonized linear list. 	Daily, Weekly, Monthly, Quarterly, and Annually as needed
D. In the Call Center			
<ul style="list-style-type: none"> • Telephone operators, • Medical regulators. 	Collect data using physical and electronic tools	Record data from community calls in the call register	Daily, Weekly.

Data Quality Assurance

 Assurance of Epidemiological Surveillance Data Quality
Code :
I. Objective
General Objective : Ensure the availability of quality data in epidemiological surveillance at all levels of the health pyramid.
Specific Objectives : <ul style="list-style-type: none">• Ensure that collected and transmitted data meet quality criteria.• Establish a continuous quality assurance system at all levels of the health pyramid.
II. Target Audience
This procedure is aimed at health facility staff and data managers at all levels, as well as any other actors involved in data management.
III. Prerequisites for Implementation
<ul style="list-style-type: none">• Good mastery of the SIMR.• Mastery of physical and electronic data collection tools (DHIS2, EWARS, notification forms).• Basic knowledge of quality assurance criteria.
IV. Expected Results
<ul style="list-style-type: none">• Collected and transmitted data undergo quality verification, with feedback provided at lower levels.• A permanent quality assurance system is established at all levels of the health pyramid.
V. Resources
Equipment/Tools
<ul style="list-style-type: none">• Computer.• Software (Excel, DHIS2).• Notification forms.• Phones/tablets, internet connection, etc.
Documents

-
- SIMR Guide (case definitions, etc.).
 - SBC Guide (definition of signals and community cases).
 - SFE Guidelines.
 - National Guide for Managing Epidemiological Surveillance Data.
 - DHIS2 Manual.


VI. Procedures			
A. Health Facility Level			
Responsible Parties	Activities	Tasks	Frequency
<ul style="list-style-type: none"> • FOSA PFS • FOSA Data Manager 	Verification of collected or entered data	<ul style="list-style-type: none"> • Ensure all primary tools are available and filled out correctly. • Properly complete notification forms, MAPE, and RMA forms. • Ensure accurate data entry in DHIS2 and other available electronic tools, and ensure data consistency with paper tools. 	Daily
FOSA PFS / FOSA Data Manager	Completeness Check	<ul style="list-style-type: none"> • Verify that all physical and electronic forms are completely filled out. • Involve data collection staff to complete missing information. • Ensure all reports are produced and transmitted. 	Weekly
FOSA PFS / FOSA Data Manager	Timeliness Check	<ul style="list-style-type: none"> • Ensure that data from the previous week are submitted every Monday before 6 PM. • Ensure all reports are submitted on time. • Take corrective actions in case of delays. 	Weekly NB : Correct aberrant data within 24 hours of notification by the health district.

FOSA Data Manager	Data Validation	<ul style="list-style-type: none"> • Ensure completeness, timeliness, accuracy, and consistency of data. • Eliminate duplicates : Identify and remove duplicate entries in databases. • Identify and correct entry errors and aberrant values. • Check the consistency of related variables (e.g., the number of deaths must be less than or equal to the number of cases). 	Weekly (during RDQA)
B. Health District / Regional Level			
Surveillance Focal Point/Data Manager	Completeness Check	<ul style="list-style-type: none"> • Verify that all physical and electronic forms are completely filled out. • Check the report transmission rate. • Conduct regular checks to identify gaps in records. • Involve data collection staff to complete missing information. 	Weekly
Surveillance Focal Point/Data Manager	Timeliness Check	<ul style="list-style-type: none"> • Ensure data and reports are submitted in a timely manner. 	Weekly NB : Correct aberrant data within 24 hours of notification to the FOSA if the correction has not been made by them.

Surveillance Focal Point/Data Manager	Data Cleaning	<ul style="list-style-type: none"> • Use analytical tools to spot inconsistencies. • Document changes made to the data. • Verify ambiguous data with the FOSA. • Coach the FOSA and/or district in correcting aberrant data within the prescribed timeframes. 	Weekly
Surveillance Focal Point/Data Manager	Data Validation	<ul style="list-style-type: none"> • Identify extreme/aberrant values by comparing the current indicator value against the past three periods. • Define thresholds for acceptable values. 	Weekly
Surveillance Focal Point/Data Manager	<ul style="list-style-type: none"> • Supervision of FOSAs and/or health districts. • Performance evaluation. 	<ul style="list-style-type: none"> • Review data received from an RDQA tool. • Calculate key performance indicators using predefined formulas for calculating rates and coverage, etc. • Interpret indicators clinically and epidemiologically. • Provide recommendations and feedback to improve data quality. 	Monthly
C. Central Level			
Central Data Manager / PFS	Evaluation of Data Quality Indicators	<ul style="list-style-type: none"> • Aggregate data from lower levels using DHIS2 and/or Excel databases. • Assess completeness, timeliness, accuracy, and internal consistency. • Calculate key performance indicators. • Interpret indicators clinically and epidemiologically. 	Weekly

Central Data Manager / PFS	Data Validation	<ul style="list-style-type: none"> • Review data and communicate anomalies observed in the national database (MAPE, etc.) to regions. • Coach regions in verifying and correcting deemed aberrant data. • Follow up on the integration of required corrections. • Implement regular audits of data collected by the operational level. 	Weekly and semi-annual (audits)
Central Data Manager / PFS	Development and Dissemination of a Quality Assurance Plan at All Levels	<ul style="list-style-type: none"> • Identify data quality issues encountered at each level. • Identify involved parties. • Define a timeframe for implementing quality assurance activities. 	Weekly and semi-annual (audits)

Data Storage and Archiving

	<h2>Data Storage and Archiving for Epidemiological Surveillance</h2>
Code :	
I. Objective	
General Objective : Ensure the storage and archiving of epidemiological surveillance data.	
Specific Objectives :	
<ul style="list-style-type: none"> • Store data in secure locations. • Manage access with controls for authorized personnel only. • Archive epidemiological surveillance data. • Securely destroy obsolete epidemiological surveillance data. 	
II. Target Audience	
This document is aimed at all stakeholders involved in epidemiological surveillance.	
III. Prerequisites for Implementation	
<ul style="list-style-type: none"> • Be a participant in the health system. • Be involved in data collection for surveillance. • Be responsible for compiling, analyzing, and producing surveillance data reports. • Be a recipient of surveillance data or reports. 	
IV. Expected Results	
<ul style="list-style-type: none"> • Health data is stored in secure systems and/or in registers with restricted access based on need. • Access management is limited to authorized personnel with controls (two-factor authentication : password and ID). • Epidemiological surveillance data is archived. • Obsolete or expired surveillance data is securely destroyed. 	
V. Resources	
Human Resources	
<ul style="list-style-type: none"> • Central Level : All technical departments and priority programs. • Intermediate Level : DRSP (Regional Delegate, Head of Health Information and Planning Service, Head of Health Information Office, Planning Office, CERPLE, Surveillance Focal Point) and Regional Technical Groups (Coordinator, Monitoring and Evaluation, Data, etc.). • Peripheral Level : DS (District Heads, Health Facility Managers, Data Managers, ASCP, etc.). 	
Equipment/Tools	

-
- Computer.
 - Software (DHIS2, Excel, Word, PowerPoint, etc.).
 - Notification forms.
 - Registers.
 - Servers.
 - External hard drives.
 - Communication kit (tablet, phone, internet modem, etc.).

Documents


Guide for Managing Epidemiological Surveillance Data.

VI. Procedures			
A. Community Level			
Responsible Parties	Activities	Tasks	Frequency
ASCP	Storage of forms/registers and/or RMAC	<ul style="list-style-type: none"> The ASCP stores completed forms/registers at the health area level. The ASCP stores data entered into the system. 	Daily (for immediate declaration events); Weekly (MAPE); Monthly (RMAc)
B. At the FOSEA (including Lab, PSF, etc.)/District			
FOSEA Personnel	Access Management	<ul style="list-style-type: none"> Access management is limited to authorized personnel based on the head of the structure's decision. Two-factor authentication (password and ID) controls access. 	Ongoing
	Document Storage	<ul style="list-style-type: none"> FOSEA staff identifies storage locations (cabinet, office/service). Staff properly organizes forms/registers/RMA/surveillance data reports in these locations. 	Daily (for immediate declaration events); Weekly (MAPE); Monthly (RMA)

	<p>Document Archiving</p> <ul style="list-style-type: none"> • FOSA staff identifies archiving locations. • Staff differentiates between physical and digital archiving. • For physical archiving, documents are organized in folders, boxes, cabinets, etc. • For digital archiving (computer, external hard drive, USB), folders are created by activity, period, event, and importance. 	
	<p>Archive Destruction</p> <ul style="list-style-type: none"> • Obsolete surveillance data is destroyed by shredding, deletion, burning, or cutting. • Surveillance data whose retention period has expired is destroyed similarly. 	
Area Chief	<p>Archiving Registers and/or RMAC</p> <p>In addition to FOSA staff tasks, the Area Chief archives forms/registers submitted by the ASCP.</p>	Daily (for immediate declaration events); Weekly (MAPE); Monthly (RMAc)
C. Regional/Central Level		
Staff	<p>Access Management</p> <ul style="list-style-type: none"> • Access management is limited to authorized personnel based on the head of the structure's decision. • Two-factor authentication (password and ID) controls access. 	Ongoing

<p>Document Storage</p>	<ul style="list-style-type: none"> • Staff identifies storage locations (cabinet, office/service). • Staff properly organizes forms/registers/RMA/surveillance data reports in these locations. 	<p>Daily (for immediate declaration events); Weekly; Monthly; Quarterly; Semi-annual; Annual</p>
<p>Document Archiving</p>	<ul style="list-style-type: none"> • FOSA staff identifies archiving locations. • Staff differentiates between physical and digital archiving. • For physical archiving, documents are organized in folders, boxes, cabinets, etc. • For digital archiving (computer, external hard drive, USB, cloud), folders are created by activity, period, event, and importance. 	
<p>Archive Destruction</p>	<ul style="list-style-type: none"> • Obsolete surveillance data is destroyed by shredding, deletion, burning, or cutting. • Surveillance data whose retention period has expired is destroyed similarly. 	

Data Security and Access

	Data Security and Access for Epidemiological Surveillance
Code :	
I. Objective	
General Objective : Ensure the security and access to surveillance system data.	
Specific Objectives :	
<ul style="list-style-type: none"> • Protect surveillance data • Ensure the confidentiality of surveillance data • Ensure accessibility of data to authorized personnel 	
II. Target Audience	
This document is intended for all stakeholders in the health pyramid responsible for the confidentiality, integrity, and availability of epidemiological surveillance data.	
III. Prerequisites for Implementation	
<ul style="list-style-type: none"> • Be a participant in the health system • Be involved in data collection for surveillance • Be responsible for compiling, analyzing, and producing surveillance reports • Have knowledge of data security 	
IV. Expected Results	
<ul style="list-style-type: none"> • Data protection techniques are known • Surveillance data is confidential • Access to data is restricted to authorized individuals 	
V. Resources	
Human Resources	
<ul style="list-style-type: none"> • Central Level : Information system managers of technical departments, priority programs • Intermediate Level : DRSP (Regional Delegate, Head of Health Information and Planning Service, Head of Health Information Office, Planning Office, CERPLE, Surveillance Focal Point) and Regional Technical Groups (Coordinator, Monitoring and Evaluation, Data Manager, etc.) • Peripheral Level : DS (District Heads, Health Facility Managers, Data Managers, ASCP, etc.) 	
Equipment/Tools	

-
- Computer
 - Software (DHIS2, Excel)
 - Internet modem
 - Servers
 - Removable storage devices (USB flash drives, external hard drives)

Documents


- SIMR Guide 3rd Edition
- Registers
- PSNSN
- National Guide for Managing Epidemiological Surveillance Data, 2024

VI. Procedures			
A. Community Level			
Responsible Parties	Activities	Tasks	Frequency
ASCP	<ul style="list-style-type: none"> Physical Security 	<ul style="list-style-type: none"> Raise staff awareness about the importance of physical security Implement physical access controls such as locked offices for areas where forms, medical records, RMA, etc. are stored 	<ul style="list-style-type: none"> Ongoing
B. At the FOSA/District Level			
IT Staff/Network Administrator	Physical Security	<ul style="list-style-type: none"> Raise staff awareness about the importance of physical security Implement physical access controls such as alarm systems, surveillance cameras, safes for areas where forms, medical records, RMA, etc. are stored Set up workstations with secure access and store staff computers in restricted-access offices Adequately protect all storage media (hard drives, USBs) using software tools such as BitLocker and protect printed documents against theft, loss, or destruction 	Ongoing
	Software Security	<ul style="list-style-type: none"> Raise staff awareness about software security practices Install antivirus software on workstations Update software as scheduled and enable operating system firewalls Regularly back up surveillance data on password-protected removable disks or authentication systems 	<ul style="list-style-type: none"> Ongoing

	Confidentiality	<ul style="list-style-type: none"> • Ensure data security practices comply with regulations on confidentiality and health data protection • Create user accounts (staff or third parties) requiring access to data • Define access privileges based on each user's responsibilities • Disable or delete inactive user accounts to prevent unauthorized access • Protect access to sensitive data with strong authentication mechanisms, such as unique identifiers, strong passwords, and multi-factor authentication methods 	Ongoing
C. Regional/Central Level			
IT Staff/Network Administrator	Physical Security	<ul style="list-style-type: none"> • Raise staff awareness about the importance of physical security • Implement physical access controls such as alarm systems, surveillance cameras, safes for areas where forms, medical records, RMA, etc. are stored • Set up workstations with secure access and store staff computers in restricted-access offices • Install servers in restricted-access areas known only to the server administration team • Adequately protect all storage media (hard drives, USBs) using software tools such as BitLocker and protect printed documents against theft, loss, or destruction 	Ongoing

Software Security	<ul style="list-style-type: none"> • Raise staff awareness about software security practices • Install antivirus software on workstations • Update software as scheduled and enable operating system fire-walls • Regularly back up surveillance data on password-protected removable disks or authentication systems 	Ongoing
Confidentiality	<ul style="list-style-type: none"> • Ensure data security practices comply with regulations on confidentiality and health data protection • Create user accounts (staff or third parties) requiring access to data • Define access privileges based on each user's responsibilities • Disable or delete inactive user accounts to prevent unauthorized access • Protect access to sensitive data with strong authentication mechanisms, such as unique identifiers, strong passwords, and multi-factor authentication methods 	Ongoing

Management of Community Signals and Cases

	Management of Community Signals and Cases
Code :	
I. Objective	
<p>General Objective : Define mechanisms for monitoring signals and rumors that may indicate the emergence of public health events of epidemiological interest.</p> <p>Specific Objectives :</p> <ul style="list-style-type: none"> • Acquire best practices in signal management • Master the management of community cases • Process data from media monitoring 	
II. Target Audience	
This operational procedure concerns stakeholders in surveillance (refer to Human Resources)	
III. Prerequisites for Implementation	
<ul style="list-style-type: none"> • Know hospital and community signals • Understand definitions of community cases • Be trained in Event-Based Surveillance • Have basic knowledge of software use (Excel, EWARS, Kobocollect, DHIS2) 	
IV. Expected Results	
<ul style="list-style-type: none"> • Best practices in signal management are acquired • Management of community cases is mastered • Processing of media monitoring data is completed 	
V. Resources	
Human Resources	
<ul style="list-style-type: none"> • Community Members : ASCP, community leaders, key informants, community members • Health Personnel : all health personnel from FOSA, epidemiological surveillance focal points at all levels, data (Districts, regions), CERPLE, central level actors, central coaches • Monitoring Unit : call center (teleoperator, supervisor, call center head, media monitoring team) 	
Equipment/Tools	

-
- Computer, tablet, phone
 - Internet modem
 - Software (Excel, KoboCollect, DHIS2, EWARS...)
 - List of community signals
 - List of hospital signals
 - Risk assessment matrix
 - Investigation form
 - List of definitions of community cases

Documents

- SIMR Guide (case definitions)
- SFE Guidelines
- Coaching Guide

VI. Procedures		
A. Community Level		
Responsible Parties	Activities	Tasks
ASCP; Key Informants; Community Leaders; Any Community Member	Informal information collection	<ul style="list-style-type: none"> • Monitor media • Detect signals • Notify signals • Record signals in the logbook • Participate in response tasks • Participate in field investigations • Participate in risk assessments
B. Call Center (Regional Level)		
Teleoperators	Ensure media monitoring and signal detection	<ul style="list-style-type: none"> • Receive calls from the community (1510) • Ensure media monitoring • Detect and notify signals from calls and media monitoring on the notification form • Record signals from calls and media monitoring in the signal register
Supervisor	Analyze received information	<ul style="list-style-type: none"> • Ensure media monitoring • Conduct triage • Verify information
Call Center Head	Relay information to hierarchy	<ul style="list-style-type: none"> • Ensure media monitoring • Contact the regional CERPLE • Contact the District Head

Frequency

Immediate
(24h)

Daily
(24h)

Immediate
(24h)


Immediate
(24h)

C. Call Center (Central Level)		
Teleoperators	Ensure media monitoring and signal detection	<ul style="list-style-type: none"> • Receive calls from the community (1510) • Ensure media monitoring • Detect and notify signals from calls and media monitoring on the notification form • Record signals from calls and media monitoring in the signal register
Supervisor	Analyze received information	<ul style="list-style-type: none"> • Ensure media monitoring • Conduct triage • Verify information • Redirect signals to regional call centers
Call Center Head	Relay information to hierarchy	<ul style="list-style-type: none"> • Ensure media monitoring • Contact the regional CERPLE • Contact the District Head
D. FOSA Level		
All Health Personnel	Collect unusual information	<ul style="list-style-type: none"> • Ensure media monitoring • Detect hospital signals • Inform the PFS of the FOSA

Surveillance Focal Points of FOSA	Review registers	<ul style="list-style-type: none"> • Ensure media monitoring • Detect hospital signals • Receive signals detected by any health personnel • Record signals on the signal notification form and the signal register • Notify signals to the AS surveillance focal point and/or AS Head • Participate in field investigations • Participate in risk assessments 	Immediate (24h)
E. Health Area Level			
Health Area Head or Health Area Surveillance Fo- cal Point	Signal recording and processing	<ul style="list-style-type: none"> • Ensure media monitoring • Receive signals from the community, FOSA, and call center • Conduct triage and verification of signals • Conduct preliminary investigation • Transform signals of interest into events • Conduct risk assessment • Notify the event to the District Health PFS and enter it into DHIS2 • Prepare and send the weekly SFE synthesis form to the DS • Provide feedback to ASCP 	Immediate (24h)
F. District Health Level			

District Health PFS	Signal recording and processing	<ul style="list-style-type: none"> • Receive events from the Health Area Head • Ensure media monitoring • Receive signals from the Call Center • Receive weekly SFE synthesis forms • Conduct risk assessments • Conduct investigations • Consolidate and transmit the weekly SFE database to the DRSP • Provide feedback to AS PFS 	48h
G. DRSP Level			
CERPLE	Report preparation	<ul style="list-style-type: none"> • Receive events from the Health Area Head • Ensure media monitoring • Disseminate response data • Support risk assessment • Prepare SPOTREP for confirmed alerts • Notify the central level (central coach...) 	Weekly
H. Central Level			
Central Level Surveillance Actors	Data compilation and analysis	<ul style="list-style-type: none"> • Ensure media monitoring • Prepare the epidemiological situation of the SFE • Provide feedback at all levels • Redirect signals that did not follow the protocol and ensure they are processed at the AS, DS, and regional levels 	Weekly

Analysis of Epidemiological Surveillance Data

	Analysis of Epidemiological Surveillance Data
Code :	
I. Objective	
<p>General Objective : Facilitate the analysis of epidemiological surveillance data at all levels of the health pyramid.</p> <p>Specific Objectives :</p> <ul style="list-style-type: none"> • Improve the description of cases by time, place, and person for diseases or events under surveillance; • Master the procedure for detecting alert thresholds and epidemics. 	
II. Target Audience	
<p>This document is intended for stakeholders in surveillance at the levels of : FOSA, Health Districts, Regional, Central, and reference laboratories.</p>	
III. Prerequisites for Implementation	
<ul style="list-style-type: none"> • Basic knowledge of Microsoft Excel ; • Basic knowledge of mapping, statistical analysis, and visualization software (QGIS, R) is an additional asset ; • Basic knowledge of health program indicators. 	
IV. Expected Results	
<ul style="list-style-type: none"> • Data on diseases or events under surveillance are analyzed by time, place, and person ; • Alert and epidemic thresholds are detected. 	
V. Resources	
Human Resources	
<ul style="list-style-type: none"> • Data managers at all levels ; • All healthcare providers trained in data analysis ; • Biostatisticians, computer scientists, statisticians, and demographers. 	
Equipment/Tools	
<ul style="list-style-type: none"> • Office kit (computer) ; • Software (DHIS2, Excel, QGIS, R, Python, Epi Info, SPSS, etc.) ; • Stable internet connection (internet modem, etc.). 	
Documents	

-
- SIMR Guide (case definitions);
 - SBC Guide (definition of signals and community cases);
 - Any normative document of a specific program enabling data analysis.

VI. Procedures			
A. At the FOSA Level (including PSF, LABO)			
Responsible Parties	Activities	Tasks	Frequency
Data Manager of the FOSA	Identification of indicators to monitor by service	<ul style="list-style-type: none"> Identify key variables for calculating indicators ; Define the analysis period. 	Daily, weekly, monthly, quarterly, and annually as needed.
	Data Analysis	<ul style="list-style-type: none"> Compile data collected at each service level and produce monitoring tables ; Develop and update monitoring tables describing priority diseases and conditions by time, place, and person ; Interpret results and identify any disease or condition exceeding expected case numbers, occurring in unusual places, or presenting unusual trends ; Produce an analysis report. 	Daily, weekly, monthly, quarterly, and annually as needed.
B. At the Health District Level			


<ul style="list-style-type: none"> • PFS • CBS 	<ul style="list-style-type: none"> • Identification of indicators to monitor • Data analysis 	<ul style="list-style-type: none"> • Identify key variables for calculating indicators; • Define an analysis period; • Extract data from data management platforms (DHIS2, etc.) in Excel or CSV format; • Verify data quality according to procedures; • Compile data from reports submitted by healthcare facilities for immediately reportable diseases; • Present data according to appropriate visualization types (graphs, tables, maps, etc.), respecting the three dimensions : time, place, and person; • Compare obtained data to those from previous periods; • Formulate conclusions on trends, thresholds, and analysis results; • Describe risk factors for priority diseases and conditions; • Produce an analysis report and share it for decision-making. 	<p>Daily, weekly, monthly, quarterly, and annually as needed.</p>
C. At the Regional Level (including Call Center, etc.)			
<p>Call Center Data Manager</p>	<p>Identification of indicators to monitor</p>	<ul style="list-style-type: none"> • Identify key variables for calculating indicators; • Define an analysis period. 	<p>Daily, weekly, monthly, quarterly, and annually as needed.</p>

<p>Data Analysis</p>	<ul style="list-style-type: none"> • Verify data quality according to procedures (see SOP for data quality assurance); • Present the number of calls received for a fixed period by type of interest (reporting a suspected case, need for information, etc.); • Present the number of calls received by location (create histograms); • Present the number of calls received by age group (age pyramids); • Compare obtained data to those from previous periods; • Formulate conclusions on trends and analysis results; • Produce a data analysis report and share it for decision-making. 	<p>Daily, weekly, monthly, quarterly, and annually as needed.</p>
<ul style="list-style-type: none"> • CBIS • PFS 	<p>Identification of indicators to monitor</p> <ul style="list-style-type: none"> • Identify key variables for calculating indicators; • Define an analysis period. 	<p>Daily, weekly, monthly, quarterly, and annually as needed.</p>

Data Analysis	<ul style="list-style-type: none"> • Extract data from data management platforms (DHIS2, etc.) in Excel or CSV format ; • Verify data quality according to procedures ; • Compile data from reports submitted by healthcare facilities for immediately reportable diseases ; • Present data according to appropriate visualization types (graphs, tables, maps, etc.), respecting the three dimensions : time, place, and person ; • Compare obtained data to those from previous periods ; • Formulate conclusions on trends, thresholds, and analysis results ; • Describe risk factors for priority diseases and conditions ; • Produce a surveillance data analysis report and share it for decision-making ; • Produce periodic information bulletins such as BEC, SITREP, and regional epidemiological situations. 	Daily, weekly, monthly, quarterly, and annually as needed.
D. At the Central Level		

<p>Central Call Center Data Manager</p>	<ul style="list-style-type: none"> • Identification of indicators to monitor; • Data analysis 	<ul style="list-style-type: none"> • Identify key variables for calculating indicators; • Define an analysis period; • Extract data from data management platforms (DHIS2, etc.) in Excel or CSV format; • Verify data quality according to procedures; • Compile data from reports submitted by healthcare facilities for immediately reportable diseases; • Present data according to appropriate visualization types (graphs, tables, maps, etc.), respecting the three dimensions : time, place, and person; • Compare obtained data to those from previous periods; • Formulate conclusions on trends, thresholds, and analysis results; • Describe risk factors for priority diseases and conditions; • Produce a surveillance data analysis report and share it for decision-making; • Produce periodic information bulletins such as BEC, SITREP, and regional epidemiological situations; • Develop a dashboard for monitoring indicators. 	<p>Daily, weekly, monthly, quarterly, and annually as needed.</p>
---	---	---	---

Management of Epidemiological Surveillance Data in the Laboratory

	Processing of Signals and Community Cases
Code :	
I. Objective	
General Objective : Facilitate the management of epidemiological surveillance data in the laboratory	
Specific Objectives : <ul style="list-style-type: none"> • Improve data collection of samples from any suspected case of disease or public health event at all levels of the health pyramid • Enhance information transmission to the laboratory • Improve quality assurance of laboratory data • Enhance data analysis and storage 	
II. Target Audience	
This document is intended for all stakeholders involved in laboratory epidemiological surveillance at all levels of the health pyramid	
III. Prerequisites for Implementation	
<ul style="list-style-type: none"> • Be an actor in laboratory epidemiological surveillance • Be trained in SIMR • Be trained on available and functional data management software (DHIS2, PLACARD, WHO-NET) • Knowledge of case collection and notification tools 	
IV. Expected Results	
<ul style="list-style-type: none"> • Data collection of samples from any suspected case of disease or public health event is improved at all levels of the health pyramid ; • Information transmission from the laboratory is improved following the notification circuit ; • Quality assurance of laboratory data is improved according to the procedure ; • Data analysis in the laboratory is conducted in a timely manner, and data storage is improved. 	
V. Resources	
Human Resources	
<ul style="list-style-type: none"> • Laboratory surveillance focal points at all levels • Laboratory managers 	
Equipment/Tools	

-
- Office equipment (computer, external hard drives. . .)
 - Software (DHIS2, WHONET, MAPE and AP databases, etc.)
 - Communication kit (Tablet, phone line, internet modem, etc.)
 - Teleconferencing equipment

Documents

- SIMR Technical Guide
- Notification and support form for samples from suspected cases to the reference laboratory
- User manuals for platforms (DHIS2, 3MS, MAMALPRO, WHONET. . .)
- Approved/standardized laboratory registers
- Daily/weekly summary sheets of MAPE and AP samples
- Investigation and notification forms
- RMA forms
- Non-conformity register
- Call register
- List of trained personnel
- List of reference laboratories
- List of laboratory subnetworks
- Validated and up-to-date standard operating procedures


VI. Procedures			
Central Level : National Reference Laboratory (Genomic sequencing, TB, COVID-19, Cholera, Influenza, Viral Load (HIV, HBV, HCV), Bacterial Meningitis, AMR, etc.)			
Responsibles	Activities	Tasks	Frequency
PFS of the Laboratory/NRL	Sample data collection from any suspected case of disease or public health event	<ul style="list-style-type: none"> • Ensure that the individual notification form accompanying the samples is correctly filled out • Record non-conformities, if any, in the specified register • Record case information in the approved register and platform (DHIS2, PLACARD, WHONET, etc.) • Enter the case analysis results in the approved register and platform • Summarize the samples sent to the international reference laboratory • Fill in the summary form for received, analyzed samples and results by disease or public health event • Compile data of all analysis results by laboratory sub-network 	Immediate Daily Weekly
	<ul style="list-style-type: none"> • Transmission of laboratory information 	<ul style="list-style-type: none"> • Acknowledge receipt of received samples • Provide feedback on non-conformities, if any • Transmit case analysis results (screening site, NPHIL, DS, DRSP, DLMEP) • Transmit summary of received, analyzed samples and analysis results by disease or public health event to NPHIL/PROGRAMS/DLMEP • Transmit summary of all analysis results by laboratory sub-network to NPHIL/PROGRAMS/DLMEP • Transmit summary of samples sent to the international reference laboratory to NPHIL/PROGRAMS/DLMEP 	Immediate Daily Weekly

Data quality assurance in the laboratory	<p>Ensure the data quality, namely :</p> <ul style="list-style-type: none"> • Completeness of sociodemographic, clinical, paraclinical, and analysis result information • Data coherence • Data completeness and timeliness • Data validity 	Immediate Daily weekly
Analysis and use of results	<ul style="list-style-type: none"> • Extract data from platforms (DHIS2, PLACARD, WHONET, etc.) in Excel format • Check data quality according to procedure • Present data in the appropriate visualization (graphs, tables, maps, etc.) respecting three dimensions : time, place, and person • Compare data obtained to those from previous periods • Draw conclusions on trends, thresholds, and analysis results • Produce a data analysis report and share for decision-making • Develop a dashboard for indicator monitoring • Develop epidemiological bulletins 	Immediate Daily weekly Monthly Quarterly
Data storage and archiving	<ul style="list-style-type: none"> • Store hard copies of collected data by disease type and period • Use external hard drives or cloud space to store electronic results and summaries of received and analyzed samples 	Immediate Daily weekly Monthly Quarterly
Regional Level : Reference Laboratory (TB, HIV Viral Load, COVID-19, Cholera, AMR, etc.)		

<p>PFS of the Laboratory/RL</p>	<p>Sample data collection from any suspected case of disease or public health event</p>	<ul style="list-style-type: none"> • Ensure that the individual notification form accompanying the samples is correctly filled out • Record non-conformities, if any, in the specified register • Record case information in the approved register and platform (DHIS2, PLACARD, WHONET, etc.) • Complete the case results in the approved register and platform after analysis • Summarize positive samples/isolates sent to the central-level laboratory (NPHIL/CPC/CIRCB) • Fill in the summary form for received, analyzed samples and results by disease or public health event • Compile data of all analysis results by laboratory sub-network 	<p>Immediate Daily Weekly</p>
	<p>Transmission of laboratory information</p>	<ul style="list-style-type: none"> • Acknowledge receipt of received samples • Provide feedback on non-conformities • Transmit case analysis results (screening site, NPHIL, DS, DRSP, DLMEP) • Transmit summary of received, analyzed samples and results by disease or public health event to the hierarchy (NPHIL/CPC/DLMEP/MINSANTE) • Transmit summary of positive samples/isolates sent to the central-level laboratory (NPHIL/CPC/CIRCB) • Transmit summary of all analysis results by laboratory sub-network to the hierarchy (DLMEP, MINSANTE) 	<p>Immediate Daily Weekly</p>

Data quality assurance in the laboratory	<p>Ensure the data quality, namely :</p> <ul style="list-style-type: none"> • Completeness of sociodemographic, clinical, paraclinical, and analysis result information • Data coherence • Data completeness and timeliness • Data validity 	Immediate Daily weekly
Analysis and use of results	<p>Ensure data quality, namely :</p> <ul style="list-style-type: none"> • Extract data from platforms (DHIS2, PLACARD, MAMALPRO, 3MS, WHONET, etc.) in Excel format • Check data quality according to procedure • Present data in the appropriate visualization (graphs, tables, maps, etc.) respecting three dimensions : time, place, and person • Compare data obtained to those from previous periods • Draw conclusions on trends, thresholds, and analysis results • Produce a data analysis report and share for decision-making • Develop a dashboard for indicator monitoring • Develop epidemiological bulletins 	Immediate Daily weekly Monthly Quarterly
Data storage and archiving	<ul style="list-style-type: none"> • Store hard copies of collected data by disease type and period • Use external hard drives or cloud space to store electronic results and summaries of received and analyzed samples 	Immediate Daily and weekly Monthly Quarterly

Sharing (dissemination) of Information

	Sharing (dissemination) of Information
Code :	
I. Objective	
<p>General objective : Establish secure and compliant procedures for sharing/disseminating epidemiological surveillance data between the MINSANTE, other sectors, civil society, and technical and financial partners (PTFs).</p>	
<p>Specific objectives :</p> <ul style="list-style-type: none"> • Identify authorized individuals to share epidemiological surveillance data externally • Obtain informed consent for the sharing of personal data • Notify in case of incidents, security breaches, or unauthorized use of data • Control the flow of information between the MINSANTE, other sectors, civil society, and PTFs • Document sharing activities 	
II. Target Audience	
<p>This document is intended for health system actors, related sectors, civil society, and PTFs</p>	
III. Prerequisites for Implementation	
<ul style="list-style-type: none"> • Be an actor in the health system • Be an actor responsible for collecting surveillance data • Be an actor who compiles, analyzes, and produces surveillance data reports • Be a collaborating actor in the health system • Be a data user • Be an actor involved in scientific research 	
IV. Expected Results	
<ul style="list-style-type: none"> • Authorized personnel for data sharing is clearly identified ; • Informed consent before sharing personal data is documented and archived according to privacy policies* ; • Notification procedures for incidents, security breaches, or unauthorized data use are implemented through corrective measures ; • The flow of information between MINSANTE, other sectors, civil society, and PTFs is controlled ; • Sharing activities are documented. 	
V. Resources	
Human Resources	

-
- **Central Level** : technical departments, priority programs, related sectors, Civil Society, and Technical and Financial Partners
 - **Intermediate Level** : DRSP (Delegate, Regional Health Information and Planning Service Head, Health Information Office Head, Planning Office Head, CERPLE, Surveillance PF) and Regional Technical Groups (Coordinator, Monitoring and Evaluation, data, etc.)
 - **Peripheral Level** : DS (District Heads, Health Facility Managers, Data Managers, ASCP...)

Equipment/Tools

- Computer
- Software (DHIS2, Excel, Word, PowerPoint...)
- Communication kit (Tablet, phone, internet modem, ...) Servers

Documents


- Notification forms
- Registers
- PSNSN

VI. Procedures			
A. At the Community Level			
Responsibles	Activities	Tasks	Frequency
ASCP	Written authorization for data sharing from a superior	<ul style="list-style-type: none"> The ASCP verifies the availability of a written authorization from their superior before sharing data with third parties The ASCP is only authorized to share data validated by the area chief Related sectors, Civil Society, and PTFs must approach the ASCP/DS/Region/central level with written authorization from the hierarchy 	Daily (other events requiring immediate reporting); Weekly (MAPE); Monthly (RMAc)
B. Within the Fosa (including Laboratory, PSF, etc./District/Region/Central Level)			
Data Manager/Centre Head	Written authorization for data sharing from a superior	<ul style="list-style-type: none"> The Data Manager/Centre Head verifies the availability of a written authorization from their superior before sharing data with third parties The Data Manager/Centre Head is only authorized to share data validated by the Centre Head or District Head 	Daily (other events requiring immediate reporting); Weekly; Monthly; Quarterly; Biannual; Annual
	Obtaining informed consent from patients	<ul style="list-style-type: none"> The Data Manager/Centre Head verifies that the patient has consented to their personal data being shared The Data Manager/Centre Head drafts an agreement protocol to document this consent The Data Manager/Centre Head archives the informed consent in the FOSA 	Weekly; Monthly; Quarterly; Biannual; Annual

Information flow control	<ul style="list-style-type: none"> • The Data Manager/Centre Head verifies that confidentiality policies are known to their collaborators • The Data Manager/Centre Head monitors the use and purposes of the information shared with third parties • The Data Manager/Centre Head limits and restricts access to the expressed needs of users 	Weekly; Monthly; Quarterly; Biannual; Annual
Notification in case of incident, breach, or unauthorized access	<ul style="list-style-type: none"> • The Data Manager/Centre Head notifies unauthorized persons of their access to the data in writing • The Data Manager/Centre Head informs their hierarchy of any breach of confidentiality • The Data Manager/Centre Head notifies the competent authorities in case of an incident 	Weekly; Monthly; Quarterly; Biannual; Annual
Sharing documentation	<ul style="list-style-type: none"> • The Data Manager/Centre Head records in a document the persons authorized to share the data • The Data Manager/Centre Head keeps the agreement protocols and letters sent to third parties • The Data Manager/Centre Head makes confidentiality policies available 	Weekly; Monthly; Quarterly; Biannual; Annual
Dissemination of information	Sharing epidemiological bulletins, semiannual/annual reports, knowledge products (policy briefs, information notes, blogs...)	Weekly; Monthly; Quarterly; Biannual; Annual

<p>Related sectors, CTD, Civil Society, PTFs</p>	<p>Use of data</p>	<ul style="list-style-type: none"> • Related sectors, Civil Society, and PTFs draft a request addressed to the superior (DS/Region/central level) • Justify the use of the data 	
--	--------------------	---	--

Data Transmission and Feedback

	Transmission of Epidemiological Surveillance Data and Feedback
Code :	
I. Objective	
General Objective : Ensure the transmission of epidemiological surveillance data and feedback.	
Specific Objectives :	
<ul style="list-style-type: none"> • Transmit epidemiological surveillance data on time • Provide feedback among different levels of the health pyramid 	
II. Target Audience	
This document is intended for all actors in the health pyramid.	
III. Prerequisites for Implementation	
<ul style="list-style-type: none"> • Be an actor in the health system • Be an actor responsible for collecting surveillance data • Be an actor who compiles, analyzes, and produces surveillance data reports • Be an actor who receives surveillance data or reports 	
IV. Expected Results	
<ul style="list-style-type: none"> • Epidemiological surveillance data is transmitted on time ; • Feedback is effectively provided among the different levels. 	
V. Resources	
Human Resources	
<ul style="list-style-type: none"> • Central Level : all technical departments, priority programs, and Technical and Financial Partners • Intermediate Level : DRSP (Delegate, Regional Health Information and Planning Head, Health Information Office Head, Planning Office Head, CERPLE, Surveillance PF) and Regional Technical Groups (Coordinator, Monitoring and Evaluation, Data, etc.) • Peripheral Level : DS (District Heads, Health Facility Managers, Data Managers, ASCP...) 	
Equipment/Tools	

-
- Computer
 - Software (DHIS2, Excel, Word, PowerPoint...)
 - Registers
 - Notification forms
 - Communication kit (Tablet, phone, internet modem, ...)

Documents

- SIMR Guide 3rd Edition (case definitions)
- Coaching Guide 2021
- SBC Guide 2023

VI. Procedures			
A. At the Community Level			
Responsible	Activities	Tasks	Frequency
ASCP	Data entry and transmission of surveillance data	<ul style="list-style-type: none"> The ASCP enters epidemiological surveillance data in the registers; The ASCP inputs epidemiological surveillance data into DHIS2; The ASCP transmits epidemiological surveillance data to the FOSA; 	Daily (other events requiring immediate reporting); Weekly (MAPE); Monthly (RMAc)
B. Within Health Facilities (including Lab, PSF, etc.)			
Care Provider/Surveillance PF	Data entry and transmission	<ul style="list-style-type: none"> The Surveillance PF fills out the registers The Surveillance PF compiles data into the RMA The care provider/Surveillance PF enters data into DHIS2 The care provider/Surveillance PF transmits data to the District 	Daily (other events requiring immediate reporting); Weekly (MAPE); Monthly (RMA); • No later than the fifth (5th) day of the following month
C. In the Health District/Region/Central Level			
Surveillance PF/Data Manager	Transmit surveillance data	<ul style="list-style-type: none"> Verify the quality of data transmitted to the upper level Validate the data Transmit surveillance data to the upper level Correct outlier data 	Daily (other events requiring immediate reporting); Weekly (MAPE); Monthly (RMA); Quarterly; Semiannual; Annual; 24 hours after report availability
	Transmit the feedback report	Officially transmit the feedback report to the lower level.	

	Follow up on the feedback from the report to the FOSA and ensure that the FOSA data in DHIS2 is corrected	
Follow up on feedback		

Bibliography

- (1) Data Quality Review (RQD); A Toolkit for Monitoring Health Facility Data Quality, Implementation Guidelines ; WHO.
- (2) Data Quality Assessment Tool, Instructions for data preparation. WHO.
- (3) Data Quality Review : A toolkit for facility data quality assessment, Module 1 : Framework and Metrics, WHO, November 2016.
- (4) Data Quality Review : A toolkit for facility data quality assessment, Module 2 : Desk Review of Data Quality, WHO, November 2016.
- (5) Guide National de Revue de la Qualité des Données,MINSANTE, Mars 2017.
- (6) Guide to the health facility Data quality report card.
- (7) Plan Stratégie National de la Santé Numérique 2020-2024,MINSANTE.

