DISEASE SURVEILLANCE REPORTING INFORMATION SYSTEM CASE STUDY AMURIA GENERAL HOSPITAL

PAUL OKURAJA

J23/MUC/BSIT 014

A PROJECT REPORT SUBMITTED TO THE FACULTY OF ENGINEERING, DESIGN AND TECHNOLOGY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY OF UGANDA CHRISTIAN UNIVERSITY

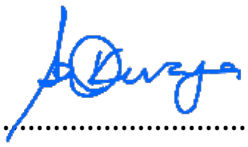
October,2024

UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa

DECLERATION

I Okuraja Paul declare that this is my original research report and it therefore not copied at any institution or collage within country for award of a Bachelor of Science information technology of Uganda Christian University, Mbale university collage.

Field work signature  .....

Name Okuraja Paul

Date 22/8/2024

Approval

I here to certify that Okuraja Paul with Registration number J23/MUC/BSIT/014 has completed the research report titled Disease Surveillance Reporting Information System conducted at Amuria General Hospital. It was conducted under my supervision and therefore, be submitted to Uganda Christian University, Mbale university collage.

Student Name Okuraja Paul

Signed..... Date 22/8/2024

supervisor's Name Dr Eilu Emmanuel

Singed..... Date 10/10/2024

DEDICATION

I dedicate this report to my family especially my beloved woman and children for the word of encouragement to study in this level, I also want applaud my brothers, sisters and lecturers for support offered to me towards my studies and not forgetting Obany Edith who contributed a lot in my educational progress. Lastly would like to thank the class colleagues for having encouraged and helped me academically

ACKNOWLEDGMENT

I praise to God for giving me knowledge, wisdom peace of mind to prosper academically. Besides that, am grateful to Medical Superintendent Amuria General Hospital for giving me room to conduct my internship attachment at the Hospital promises. Also do thank the Hospital staff of Amuria General Hospital especially Okello Pius for responding question on the Question on surveillance reporting information system, operation and knowledge of guidance offered to me in this struggle and not for getting the following lectures Mr. Watuwa Emmanuel, Mandu jackson, Mukalere Justine, Mutemere Joseph, Agatha, Dr Eilu Emmanuel others who gave me knowledge and advice

“May God reward you all according to his will”

Abstract

A Disease Surveillance Reporting Information System (DSRIS) is a comprehensive, technology-driven platform designed to support early detection, monitoring, and management of communicable and non-communicable diseases. This system streamlines the collection, analysis, and dissemination of health data from multiple sources—including healthcare facilities, laboratories, and community health workers in real time. By integrating automated reporting, standardized case definitions, and analytical tools, the DSRIS enhances the accuracy and timeliness of disease notifications. It enables rapid identification of outbreaks, supports evidence-based decision-making, and strengthens public health responses at local, national, and global levels. Through improved data quality, interoperability, and visualization capabilities, the system contributes to more efficient resource allocation, better coordination among health authorities, and ultimately the reduction of disease burden and prevention of public health emergencies.

Disease Surveillance reporting information system

Contents

Chapter one

Introduction

This chapter presents the background of the study, problem statement, objective, scope and significance to the study.

1.0 The background of the study.

Epidemiology surveillance is the ongoing systematic, collection, recording, analysis, interpretation and dissemination of health data reflecting the current health status of the community or population.

Surveillance reports provide essential information about a disease or health-related condition according to person, time and place. They often provide the basis to identify burden of illness and may include related information, such as trends in risk factor frequency or prescribing practices. Surveillance reports inform strategies to address targeted health conditions and may identify the need for additional clinical care or public health action

Disease surveillance at the health facility focuses on identification, management and reporting of prone diseases to the district and ministry, these common districts include; cholera, measles, dysentery, Covid 19, polio, Malaria, yellow fever, leprosy, guinea worm etc

1.1 Problem statement

The health workers play a major role in epidemiological surveillance and reporting, therefore there is a problem of disease identification and reporting as some health workers take it for granted to be done with specific officers.

The laboratory plays a major role in surveillance, including confirming the start and end of an outbreak.

Knowing the causative agent for an outbreak informs the development of response strategies and management plans for a public health event. However, issues and challenges may arise that limit the effectiveness or efficiency of laboratories in surveillance.

Among the challenge in surveillance is poor timeliness and frequency of feedback regarding test results from the central laboratory to health facility and surveillance units was a major constraint to surveillance and outbreak investigation that needed to be addressed.

There is also another problem of sample rejection by the central laboratory the is caused by poor handles of sample, poor packing either in different containers or less quantity of the spacemen needed

1.2 Main objective

The main objective was to develop online surveillance reporting information system that will enable health workers to report on prone diseases from the health facility to ministry of health.

1.2.1 Specific objective

- To study the current systems used to manage and report data surveillance data from health facilities to the ministry.
- To design an online surveillance reporting information system at health facility using identified requirement.
- To implement the designed online surveillance reporting information system using various programming languages like MySQL, PHP, Java scripts etc.
- To test and validate online surveillance reporting information system so as to evaluate whether the systems meets the requirement.

1.3 The scope of the study

The scope of the study will focus on the surveillance reporting, the design of the system and its implementation. It will focus on data management, reporting and its impact on system users among the hospital staff.

The researcher of system will assess the equipment and tools needed during implementation, also time frame needed for its implementation.

1.4 Significance of study

The study will benefit me to acquire practical skills and knowledge to do more tasks related to professional skills and more so will add a foundation for future researchers.

The study will also benefit in terms of Hospital in term of disease identification and reporting of prone disease and to control the outbreaks

Chapter Two

Literature review

2.0 introductions

This chapter presents the background of the information to the study, it highlighting the technology the system, how it works, benefits, strengthens and weakness of the system.

Surveillance reporting refers to the regular collection of health information in terms of health indicators, the routine analysis of indicators over time, place, and between population groups, the sharing of available scientific knowledge, and the regular dissemination of results.

In 2000 Uganda adopted the integrated disease surveillance and reposes strategy, the goal was to build the country to detect report promptly and effectively respond to public health emergencies and priorities. In 2000 - 2010 surveillance system in Uganda continued to rely on paper base forms that were used to collect data at the community and health facilities. The integrated surveillance and response strategy, recommended by office (WHO AFRO) in 1998, was successfully implemented in Uganda

The ministry introduced surveillance information system in order to achieve the number of performance indicators including, improved reporting at the district level (49% 2001 to 85% in 2007). increase timeliness reporting from the health facilities, district to central level. Also to have an increase in analysed data at the local level from 10% to 47% analysing at least one target disease.

In 2011 Uganda replaced the older system for transmitting weekly surveillance data via paper-based reports, paid phone calls and short message system were used via Mobile tracking system (MTrac). The mobile health (MHealth) system in Uganda is a routine data system that uses rapid short messages services (SMS) to accelerate the submission of community and health facility data from local to national levels, including disease surveillance, malaria treatment and drug stock indicators.

Still in 2011 the

Still in 2011the MoH introduced the district health management information software system version 2 (DHIS2) to further strengthen district-based health reporting to the ministry. This system was used for data entry, retrieval visualization and reporting, also 1985 to capture and analyze morbidity data and non-communicable diseases and other services like immunization and family planning, later 1987-1994 the ministry of health added other services to be monitored and these include improve access to health service, clinical prevention services, environmental quality, metal health, oral health, reproduction and sexual health, Maternal infant and child health. Since 1985 when the health information system was designed to capture and analyze morbidity data and non – communicable diseases in the health facilities of Uganda, this

system was still using paper-based technology for reporting data from health facilities to the district and to the ministry of health.

In 2010 the Health Management Information System (HMIS) was revised as an integrated reporting system used by the Ministry of Health, development Partners and Stakeholders to collect relevant and functional information on a routine basis to monitor the Health Sector Strategic Plan (HSSP) indicators, to enable planning, decision making and monitoring and evaluation of the health care delivery system

On 1st July 2012 the district started submitting reports to the ministry of health electronically using electronic health management information system (eHMIS) which reduced paper base system of reporting and improved quality of reports submitted.

2.1 Types of Disease surveillance reporting information systems

2.2.1 Integrated Disease Surveillance and Response (IDSR): IDSR is a widely adopted framework by countries, including Uganda, to enhance surveillance and response to priority diseases. It integrates multiple disease surveillance systems into a unified structure. For details on IDSR implementation in Uganda, you can refer to the World Health Organization (WHO)'s documentation on IDSR (WHO IDSR Technical Guidelines: WHO IDSR Guidelines)

2.2.2HIV/AIDS Reporting System: Uganda has a well-established HIV/AIDS reporting system managed by the Uganda AIDS Commission and supported by various stakeholders. For more information, you can explore reports and publications from the Uganda AIDS Commission. (Uganda AIDS Commission)

2.2.3 Malaria Surveillance and Reporting System: Malaria is a significant health concern in SUganda, and the country has a dedicated malaria surveillance system. The Uganda Malaria Surveillance Project and the National Malaria Control Program oversee this system. For detailed information, you can refer to resources from the Uganda Ministry of Health. (Ministry of Health Uganda: Ministry of Health Uganda)

2.2.3Tuberculosis (TB) Reporting System: Uganda's National Tuberculosis and Leprosy Program (NTLP) manage the TB reporting system. This system monitors TB cases, treatment outcomes, and drug resistance patterns. For more information, you can explore reports and publications from the NTLP. (Uganda NTLP: Uganda NTLP)

2.2.4Fortifiable Disease Reporting System: Uganda operates a fortifiable disease reporting system to track diseases mandated by law to be reported to public health authorities. For details, you can refer to official documents and reports from the Ministry of Health Uganda. (Ministry of Health Uganda: Ministry of Health Uganda)

2.2.4Health Management Information System (HMIS): Uganda's HMIS integrates health data, including surveillance data, from health facilities nationwide. This system supports reporting and analysis

of health indicators. For more information, you can explore resources from the Ministry of Health Uganda. (Ministry of Health Uganda: Ministry of Health Uganda)

2.2.7 Related surveillance systems

2.27.1 Physical surveillance

According (Lyon, 2007) Physical surveillance refers to the observation or monitoring of individuals, locations, or activities in person, typically by trained personnel, with the aim of gathering information covertly or overtly. Here's a breakdown of its advantages and disadvantages (This book by J. P. O'Neill provides comprehensive insights into the principles, techniques, and operational considerations of physical surveillance in law enforcement and security contexts

2.2.7.2 How Physical Surveillance Works:

¬ʎDeployment of Agents: Trained personnel are strategically placed in locations where the subject of surveillance is likely to be or where activities of interest are expected to occur.

¬ʎObservation Techniques: Agents use various techniques such as stakeouts, following subjects discreetly, using binoculars or cameras for documentation, and blending into the surroundings to avoid detection.

¬ʎReporting**:** Observations and findings are recorded in detailed reports which may include photographs, videos, or written notes

2.2.7.3 Advantages of Physical Surveillance

1.Direct Observation**:** Physical surveillance allows for direct observation of subjects or activities, providing real-time and accurate information.

2.Flexibility**:** It can adapt to changing situations or environments, allowing surveillance teams to follow subjects or events as they unfold.

3.Contextual Understanding: Observers can gather contextual information that may not be captured through other surveillance methods, such as body language, interactions, or environmental factors.

4.Evidence Collection: Physical surveillance can provide visual and behavioral evidence that can be crucial in legal proceedings or investigations.

5.Covert Operations**:** When conducted covertly, it can gather intelligence without alerting subjects, potentially revealing undisclosed activities or behaviors.

2.2.7.4 Disadvantages of Physical Surveillance

1.Resource Intensive: It requires significant resources, including personnel, time, and equipment, which can be costly.

2.Risk of Detection**:** There is a risk of detection by subjects under surveillance, which may compromise the operation or endanger the safety of personnel.

3.Legal and Ethical Concerns**:** There are ethical considerations regarding privacy invasion and legal implications related to the collection and use of surveillance data.

4.Limited Coverage: Physical surveillance is typically limited to specific locations or individuals being monitored, which may not provide comprehensive insights into larger networks or activities.

5.Subjective Interpretation: Observers' interpretations of events or behaviors may be subjective, leading to potential biases in reporting or analysis

Conclusion

In conclusion, while surveillance systems provide significant advantages such as improved public safety and crime prevention, they must be carefully managed to address concerns regarding privacy, misuse of data, and the potential impact on civil liberties. Striking a balance between security needs and individual rights remains crucial in the deployment and operation of surveillance systems.

2.2.7.5 Electronic Surveillance System:

According (Rule & Mangan, 2017) Electronic surveillance systems encompass a variety of technologies used for monitoring, data collection, and analysis. These systems are widely employed in law enforcement, security, intelligence gathering, and various other domains. They include. Closed-circuit television (CCTV), Wireless video/audio transmission systems, Electronic monitoring devices (e.g., ankle bracelets for parolees), Communications interception (e.g., phone tapping, email monitoring) reference:

2.2.7.6 How electronic surveillance work

Electronic surveillance involves the use of electronic devices to monitor and record activities or communications of individuals or groups. This typically includes data collection through devices like CCTV cameras, wiretaps, and internet monitoring tools. The collected data is transmitted, stored, and analyzed for various purposes such as law enforcement, national security, or commercial use. Legal frameworks

govern its implementation to balance security needs with privacy rights, sparking ongoing debates about ethical and legal implications.

2.2.7.7 Advantages of Electronic Surveillance Systems

1. Increased Coverage: Electronic surveillance systems can monitor large areas or multiple targets simultaneously, providing broader coverage compared to physical surveillance.
2. Enhanced Data Collection: They enable the collection of digital evidence, including video recordings, audio recordings, and electronic communications, which can be crucial for investigations and legal proceedings.
3. Real-time Monitoring: Many electronic surveillance systems provide real-time data and alerts, allowing for immediate response to incidents or suspicious activities.
4. Deterrence: The presence of visible surveillance cameras can deter criminal activity and misconduct, contributing to public safety and crime prevention.
5. Cost-effectiveness: Over time, electronic surveillance systems can be more cost-effective than physical surveillance, especially in terms of manpower and operational expenses.

2.2.7.8 Disadvantages of Electronic Surveillance Systems

- Cost: High setup, maintenance, storage expenses and requires regular troubleshooting
- Privacy Concerns: Electronic surveillance raises significant privacy issues, as it can intrude into individuals' private lives and activities without their consent or knowledge.
- Legal and Ethical Issues: There are legal and ethical concerns regarding the use of electronic surveillance, including compliance with laws, regulations, and human rights standards.
- Data Security Risks: The storage and transmission of surveillance data can be vulnerable to breaches, hacking, or unauthorized access, posing risks to the integrity and confidentiality of collected information.
- Potential for Misuse: Electronic surveillance systems can be misused or abused for unlawful purposes, such as unwarranted surveillance of individuals or groups.
- Limitations in Effectiveness: Despite their capabilities, electronic surveillance systems may have limitations in certain environments or situations, such as low-light conditions for CCTV cameras or encryption methods for electronic communications and Relies on power and connectivity.

Conclusion:

Electronic surveillance systems are powerful tools for enhancing security, gathering intelligence, and monitoring activities in various contexts. However, their deployment should be accompanied by robust legal frameworks, ethical guidelines, and oversight mechanisms to balance their benefits with privacy

protections and accountability. Effective implementation requires careful consideration of technological capabilities, operational requirements, and adherence to human rights principles to ensure responsible and effective use. Integrating electronic surveillance with other surveillance methods and employing

2.5.7.9 Computer and network surveillance

According to Smith, J. (2020), computer and network surveillance refers to the monitoring of computer activity and network traffic within an organization or across a network of computers. This surveillance can involve various methods and technologies aimed at observing and recording digital communications, user behaviors, and system activities.

2.5.8.0 How Computer and network surveillance

Computer and network surveillance is the monitoring of computer activity and data stored locally on a computer or data being transferred over computer networks such as the Internet. This monitoring is often carried out covertly and may be completed by governments, corporations, criminal organizations, or individual

2.5.8.1 Advantages of computer surveillance

1. Being able to access executive information on the status of our installations and checking up on our most critical technological assets.

2. Access to our computer system's status in real time.

3. Improve the efficiency and performance in maintenance tasks performed on the system.

4. Detecting instance origins of the crime.

5. Creating system inventories (maps, lists).

6. Planning growth based on the real use of your systems. Through usage reports, you can detect tendencies and know when you will need more storage space, a new server, or a memory upgrade.
7. Under the same premises we can detect systems that are underused.

8. Cost efficient and effectiveness, the costs of setting up

2.5.8.1 Disadvantages of Computer system

1. Lack of robustness

Computer networks rely on the main server called the central server. If the central server malfunctions or there is an issue in the central server, then the entire network will stop functioning. So, this is a major disadvantage due to dependency on a single server.

`

2. Spread of computer virus

As computers in a network are interconnected, there is a high probability that if one of the computers is affected by the virus, others too can get affected. This spread can actually damage the entire system. Also,

if the central server gets corrupted, then it's quite dangerous as the network depends on the central server.

3.Costly to set-up and maintain
While computer networks save costs in terms of resource sharing and data storage, they also incur considerable implementation costs. Moreover, maintaining computer networks is a costly and time-consuming affair.

4.Lack of productivity
Since a network has a lot of advantages and applications, it certainly results in the simultaneous use of many services that cause distraction. Thus, due to employees focusing on a myriad of tasks, productivity issues are quite common.

5. Lowers the ability to retain and analyze information
With computer networks storing vast amounts of data and processing basic requests in a fraction of the time, people are losing the ability to retain important information. Even processing basic information is a task, as individuals are becoming increasingly dependent on computer networks to do these tasks for them.

6. Unauthorized access
When multiple devices are connected to a network, there is a greater potential for unauthorized access and data breaches

Conclusion

Computer and network surveillance offers significant benefits in terms of security, accountability, and operational insights, these advantages must be balanced against potential drawbacks such as privacy infringement, reduced trust, and legal risks. Organizations implementing surveillance should prioritize ethical considerations, transparency, and compliance with relevant laws to mitigate these concerns. Striking a balance between security needs and respecting individuals' rights is crucial for fostering a positive organizational environment and maintaining public trust in surveillance practices.

2.5.8.2 Social surveillance

According Mann, S & Ferenbok J. (Eds.) (2013) Social surveillance refers to the monitoring and observation of individuals' social interactions, behaviors, and activities within social settings or online platforms, often using technological means.

2.5.8.3 How social surveillance work

Social surveillance operates through various technological and social mechanisms to monitor individuals' activities, interactions, and behaviors within social contexts. It often involves the use of digital platforms, social media, and other online tools to gather and analyze data about individuals' social interactions and behaviors

2.5.8.4 Advantages of Social Surveillance

1.Real-time Insights: Social surveillance provides real-time information about public opinion, trends, and events, enabling timely responses and interventions.

2.Broad Coverage**:** It can monitor a wide range of topics, including public health issues, political sentiment, consumer preferences, and crisis situations, across diverse demographics.

3.Cost-effective: Compared to traditional surveys or focus groups, social surveillance can be more cost-effective for gathering large-scale data and conducting sentiment analysis.

4.Targeted Marketing: Businesses can use social surveillance to understand consumer preferences and behaviors, allowing for targeted marketing strategies and product development.

5.Early Warning System: It can serve as an early warning system for potential crises or public health emergencies by detecting emerging trends and anomalies.

2.5.8.5 Disadvantages of Social Surveillance

1.Privacy Concerns: Social surveillance raises significant privacy issues, as it involves monitoring individuals' online activities without their explicit consent or awareness.

2.Ethical Issues: There are ethical considerations regarding the use of personal data for surveillance purposes, including the potential for exploitation or manipulation.

3.Accuracy and Bias: Social surveillance data may be subject to inaccuracies, biases, and misinterpretations due to the dynamic nature of social media content and algorithms.

4.Legal Considerations: There are legal challenges related to data protection laws, consent requirements, and the rights of individuals to control their personal information.

5.Over-reliance on Digital Data: Relying solely on social surveillance may overlook offline behaviors, opinions, and sentiments that are not reflected online.

Conclusion

Social surveillance offers powerful insights into public opinion, behaviors, and trends in real time, making it valuable for various applications such as public health monitoring, market research, and crisis management.

However, its implementation should adhere to ethical standards, respect privacy rights, and comply with legal regulations to mitigate risks and ensure responsible use of data. Integrating social surveillance with other sources of information and employing transparent practices can enhance its reliability and effectiveness while safeguarding individual rights and societal trust.

2.5.8.6 Financial Surveillance

According to Maurer, B Nelms T. C & Swartz, L. (Eds.) (2013) financial surveillance refers to the monitoring of financial transactions, activities, or behaviors, typically conducted by financial institutions, regulators, or governments to detect fraud, money laundering, or compliance issues

2.5.8.7 How Financial Surveillance Works

Financial surveillance systems utilize technologies such as data analytics, machine learning, and artificial intelligence to analyze large volumes of financial data. They monitor transactions, conduct risk assessments, identify anomalies, and generate alerts for further investigation by regulatory authorities or law enforcement agencies.

2.5.8.7 Advantages of financial systems

1. Transparency
Financial systems enable the smooth and secure transfer of funds between individuals, businesses, and institutions.

2. Payment systems
They provide payment systems, such as electronic funds transfer, credit cards, and digital wallets, which facilitate the settlement of transactions and support economic activities

3. Cost Savings from Automated Monitoring
With eyes that never sleep, IVS reduces the need for round-the-clock human monitoring, slashing labor costs while elevating surveillance efficacy.

4. Reduction in Security Personnel Expenditures

Automated surveillance trims the payroll. It allows for the redeployment of security personnel to tasks that necessitate human ingenuity and discernment.

5. Decrease in Theft and Fraud Incidents

Intelligent systems are formidable foes against theft and fraud, often preventing such events before they unfold, thus safeguarding as

2.5.8.8 Disadvantages of financial system

1. High Initial Costs: Setting up an information system can be expensive. This includes the cost of hardware, software, training, and maintenance. Small businesses, in particular, may find it challenging to afford the initial investment.

2. Maintenance Costs: Information systems require regular maintenance and updates to ensure they function effectively and remain secure. This ongoing cost can be significant, especially for complex systems.

3. Security Risks: Information systems are vulnerable to security breaches, including hacking, malware, and data theft. Protecting sensitive information from unauthorized access is a constant concern for organizations.

4. Complexity: Information systems can be complex, especially in large organizations with multiple software applications and databases. Managing and integrating these systems can be challenging and require specialized expertise.

5. Dependency: Organizations can become heavily dependent on their information systems. If a system fails or experiences downtime, it can disrupt operations and lead to significant losses in productivity and revenue.

6. Training Needs: Employees need to be trained to use information systems effectively. Training can be time-consuming and costly, especially when new systems are introduced or existing systems are updated.

7. Compatibility Issues: Integrating different systems and software applications can sometimes lead to compatibility issues. This can result in data inconsistencies, errors, and inefficiencies.

Conclusion

Financial surveillance plays a crucial role in maintaining financial integrity, preventing financial crimes, and ensuring regulatory compliance. However, its implementation should balance the need for security and transparency with respect for privacy rights and adherence to ethical standards. Effective financial surveillance requires collaboration among stakeholders, robust regulatory frameworks, and continuous innovation in technology and analytics to address emerging threats and challenges in global financial systems.

2.5.8.9 Biometric Surveillance

According to (Jones & Brown, 2020) Biometric surveillance relies on capturing and analyzing biometric identifiers such as fingerprints, facial patterns, iris scans, voiceprints, and gait patterns. These identifiers are used to verify or identify individuals for security, access control, and monitoring purposes.

2.5.9.0 How Biometric Surveillance Works

Biometric surveillance systems capture biometric data using sensors or scanners, which are then processed and compared against stored templates in a database. Algorithms analyze the data to verify or identify individuals based on predefined criteria (e.g., matching fingerprint patterns or facial features).

2.5.9.1 Advantages of Biometric Surveillance

1. Accuracy**:** Biometric identifiers are unique to individuals, providing a high level of accuracy in identification and authentication compared to traditional methods like passwords or ID cards.
2. Security: Biometric surveillance enhances security measures by preventing unauthorized access and reducing the risk of identity fraud or theft.
3. Convenience**:** It offers convenience to users who can access secure areas or devices quickly without the need for carrying physical tokens or remembering passwords.
4. Efficiency**:** Biometric systems can process large volumes of data rapidly, facilitating faster identification and response times in security-sensitive environments.
5. Non-transferable: Unlike passwords or tokens, biometric identifiers cannot be easily replicated or transferred, enhancing security against impersonation.

2.5.9.2 Disadvantages of Biometric Surveillance

1.Privacy Concerns: Biometric data is sensitive personal information, and its collection and use raise significant privacy concerns regarding surveillance, tracking, and potential misuse.

2. Accuracy and Reliability**:** Factors such as environmental conditions, aging, and changes in biometric characteristics can affect the accuracy and reliability of biometric systems.

3.Security Risks**:** Biometric data storage and transmission can be vulnerable to breaches, hacking, or unauthorized access, compromising individuals' privacy and security.

4.Legal and Ethical Issues**:** There are legal challenges related to the collection, use, and retention of biometric data, including compliance with data protection laws and regulations.

5.High Cost: Biometric authentication systems can be expensive to implement and maintain. The hardware and software required for biometric authentication can be costly, and the systems need to be regularly updated and maintained to ensure their effectiveness.

Conclusion

Biometric surveillance offers significant advantages in terms of accuracy, security, and convenience for identification and access control purposes. However, its implementation should prioritize privacy protections, transparency, and compliance with legal frameworks to address ethical concerns and mitigate potential risks. Balancing technological advancements with ethical considerations is crucial to ensure responsible use of biometric surveillance technologies in safeguarding security while respecting individual rights and freedoms

2.6.0 Benefits of the system

1. Surveillance helps a country to monitor and evaluate emerging patterns and trends of disease.

2. Surveillance is crucial because it contributes to better prevention and management of no communicable diseases.

3. Surveillance system helps to detecting disease outbreaks quickly before they spread.

4. Effective surveillance can improve disease outbreak detection in emergency settings, such as in countries in conflict or following a natural disaster

5. Surveillance helps in reduction in communicable disease reporting time

6. Increase in the number of laboratory reports received by public health

7. Ability to push data entry back to the source to reduce reporting time and data transcription errors while improving data quality.

8. It has reduced paper-based reporting.

2.6.0 Challenges of surveillance system

1. Poor data Management
2. .Early Detection of Emerging Diseases
3. Inadequate Computing Resources
4. Shortage of Skilled Staff
5. Emerging Data Useful for Surveillance
6. Real-Time Data
7. Electronic Health Records
8. Health Information Exchanges

2.6.1 Comparison of the related system

S/N	System	Strengthen	weaknesses	Technology
1	Physical Surveillance	Flexibility: Allows for adaptive monitoring strategies in various environments. Targeted Observation: Provides focused monitoring on specific individuals or areas. Covert Operations: Can be conducted discreetly to minimize detection.	Resource Intensive: Requires significant manpower, time, and financial resources. Risk of Exposure: Subjects may detect surveillance, compromising operations. Legal and Ethical Concerns: Raises privacy issues and requires adherence to strict guidelines. Limited Coverage: Challenging to maintain continuous surveillance over large or remote areas	Web - based
2	Electronic surveillance	Enhanced Security: Provides real-time monitoring to prevent crime and enhance public safety. Efficiency: Enables continuous monitoring without constant human presence, making it cost-effective. Evidence Collection: Provides clear and irrefutable evidence for legal proceedings. Public Safety: Monitors public	Privacy Concerns: Raises ethical and legal questions about invasion of privacy. Misuse and Abuse: Risk of unauthorized surveillance, profiling, or discrimination. Technical Limitations: Vulnerable to technical failures, hacking, or manipulation. Social Impact: Can create distrust and anxiety among the	**Web-based**

		spaces for emergencies and suspicious activities.	public, affecting freedoms.			
3	Computer and network surveillance	Efficiency: Enable rapid data processing and communication across vast distances. Connectivity: Facilitate seamless collaboration and information sharing globally. Scalability: Can expand to accommodate growing needs and users. Automation: Support automated tasks and processes, increasing productivity.	Vulnerabilities: Prone to cyber threats such as hacking, malware, and data breaches. Dependency: Over-reliance on technology can lead to disruptions if systems fail. Complexity: Managing large networks and diverse systems can be challenging. Privacy Concerns: Risks of unauthorized access and data misuse raise privacy issues.			

4	Social surveillance	Crime Prevention: Can deter criminal activity and improve public safety. Behavioural Insight: Provides data for understanding social patterns and trends. Emergency Response: Facilitates quicker responses to emergencies and crises. Community Engagement: Enhances community involvement in safety and security.	Privacy Concerns: Raises ethical issues regarding invasion of privacy. Bias and Discrimination: Risk of profiling and discrimination based on surveillance data. Legal and Ethical Issues: Requires clear guidelines and safeguards to protect civil liberties. Public Trust: Potential erosion of trust and societal impact on personal freedoms.	Web-based	
5	Financial surveillance	Fraud Detection: Helps in detecting and preventing financial crimes such as fraud and money laundering. Compliance: Ensures adherence to regulatory requirements and financial laws. Market Stability: Contributes to maintaining stability in financial markets by monitoring transactions. Risk Management: Assists in assessing and mitigating financial risks for institutions and investors.	Privacy Concerns: Raises concerns about the invasion of financial privacy and confidentiality. Cost: Implementing and maintaining effective surveillance systems can be expensive. Complexity: Financial transactions can be complex, requiring sophisticated tools and expertise for monitoring. False Positives: May generate false alerts or overlook suspicious activities due to the volume and diversity of transactions.	Web-based	

6	Biometric Surveillance	Enhanced security through unique biological identifiers like fingerprints which improve identity verification and reduce fraud. They also streamline access control and can aid in tracking individuals in various contexts.	Privacy infringement and the potential misuse of personal as biometric information is inherently sensitive data. Difficulties in accommodating changes to biometric features over time.		

Web- based

.6.3. Conclusion.

Despite surveillance is the ongoing systematic, collection, recording, analysis, interpretation and dissemination of health data reflecting the current health status of the community or population, however surveillance activities require much to investigate cases and implement the out breaks.

Chapter three

Methodology

3.0 Introduction

The methodology focuses on the research approaches of data collection, techniques for analysis and tools to be used for designing and implementing surveillance reporting system. The methodology is in line with the specific objective of the proposed online surveillance reporting information system.

3.1 System study and analysis

The study focuses on the research methodology used in a study, including how data is collected, analyzed, and interpreted. It also involves the techniques used in to determine system and the user requirement as well as system inputs and outputs. These determine what the system is expected to do.

3.2 Data collection techniques

3.2.1 Interviews

This involves conducting structured or semi-structured conversations with individuals or groups to gather qualitative data. Interviews can provide deep insights into participants' perspectives, experiences, and opinions. Also to certain the challenges faced while using the system and suggestions for improvement, perceptions of data accuracy and usefulness.

3.2.2 Observation

The use of observation method was most instrumental in that it involves physical seeing on how the data was being collected and entered in to the system from different departments using different tools such as forms or treatment sheets, log books as well as in to an intergraded health facility management system and sometime registers are used for emergency when there is a technical problem with the system.

3.2.3 Reviewing Existing Documents:

Document review would involve analyzing existing reports, protocols, guidelines, and documentation related to the surveillance reporting information system. This could include studying system manuals, data quality reports, previous research studies, and relevant policies or regulations.

3.3 Data analysis methods

The research use data analysis application software which includes Microsoft Excel that was used to captured data from their observation like taking history at the time when clinicians was interacting with the client, the level of congestion and long waiting time in the queue was further explained in the bar graph.

3.4 System analysis and design

System analysis and design involves the process of examining current surveillance practices and designing a structured system to collect, store, analyze, and report surveillance data effectively. It includes identifying user requirements, defining system objectives, designing data collection methods, creating databases for storage, developing algorithms for data analysis, and designing user interfaces for reporting purposes. The goal is to ensure the system efficiently supports surveillance activities, enhances data accuracy, and facilitates timely reporting for informed decision-making.

3.4.1 System Analysis

System analysis involves studying and understanding a system's components, processes, and interactions to identify its goals, requirements, and constraints. It aims to improve system efficiency, effectiveness, and functionality through detailed examination and evaluation.

3.5 functional attributes of a surveillance reporting information system include:

1. Data Collection: Gather data from diverse surveillance sources such as cameras, sensors, and databases.
2. Data Storage: Securely store collected data to ensure integrity and availability.
3. Data Processing: Process data through filtering, cleaning, and normalization for analysis.
4. Data Analysis: Use algorithms to identify patterns, trends, anomalies, and correlations in surveillance data.
5. Reporting: Generate reports and visualizations to summarize analyzed data for decision-making.
6. Alerting: Provide notifications for critical events or deviations in surveillance data.
7. User Interface: Offer an intuitive interface for easy data access, analysis, and reporting.
8. Integration: Interact with other systems to exchange data and enhance functionality.
9. Security: Implement measures to protect data confidentiality, integrity, and availability.
10. Compliance: Adhere to regulatory requirements and standards for data handling and reporting.

3.5 non-functional attributes of a surveillance reporting information system include:

1. Performance: Ensuring the system responds quickly to user interactions and processes data efficiently, even under high load conditions.
2. Reliability: The system should be dependable, with minimal downtime and the ability to recover quickly from failures.
3. Scalability: Capability to handle increasing amounts of data and users without significant degradation in performance.
4. Security: Implementation of robust security measures to protect sensitive surveillance data from unauthorized access, breaches, and cyber-attacks.
5. Usability: Providing an intuitive and user-friendly interface that requires minimal training for users to operate effectively.
6. Availability: Ensuring the system is accessible and operational whenever needed, with measures in place for planned maintenance and unexpected outages.
7. Maintainability: Ease of maintaining and updating the system, including software updates, bug fixes, and system enhancements.
8. Compatibility: Ability to integrate and work seamlessly with other systems, hardware, and software components in the surveillance ecosystem.
9. Compliance: Adherence to legal and regulatory requirements related to data privacy, security, and reporting.
10. Performance Efficiency: Optimizing resource usage such as CPU, memory, and storage to maximize system performance and minimize operational costs.

3.6 System design

System design is the process of defining the architecture, components, interfaces, and data for a system to meet specified requirements effectively and efficiently. It involves breaking down the system into manageable modules, designing interfaces between components, specifying data structures, algorithms, and user interfaces. System design aims to create a detailed plan or blueprint that guides developers in implementing the system. It encompasses considerations such as scalability, performance, security, and usability to ensure the system meets both functional and non-functional requirements. Overall, system design transforms user requirements into a structured solution that forms the basis for the development and implementation phases of a project.

3.7 System implementation

System implementation is the phase in the system development life cycle (SDLC) where a newly developed or upgraded information system is put into operation. It involves installing and configuring hardware and software components, migrating data from existing systems, conducting thorough testing to ensure functionality and performance, providing training to users, and creating documentation for ongoing support and maintenance. Implementation aims to transition from development to operational use, ensuring the system meets specified requirements and supports business processes effectively. Successful implementation requires careful planning, coordination, and testing to minimize disruptions and ensure a smooth deployment of the system.

Implementation Tools

3.7.1 Database (MySQL, MariaDB, PostgreSQL): The choice of database depends on the specific requirements of your SRIS. MySQL and its fork MariaDB are popular choices due to their reliability, performance, and ease of use. PostgreSQL is another powerful option known for its advanced features and scalability, suitable for large-scale applications.

3.7.2 Programming Language (PHP, Python, etc.): PHP is commonly used in WampServer setups due to its integration with Apache and MySQL/MariaDB. It's well-suited for web development and offers extensive libraries and frameworks (like Laravel or Symfony) for building robust applications. Python with frameworks like Django or Flask is also a viable option for backend development.

3.7.3 HTTPSusing SSL/TLS certificates is crucial for securing data transmission between clients and the server. Additionally, using secure coding practices, input validation, and access control mechanisms (such as authentication and authorization) are essential for protecting sensitive surveillance data.

3.7.4 HTML, or Hypertext Markup Language, is the standard markup language used to create and structure content on web pages and web applications. It defines the structure of web content by using various elements and tags to describe how the content should be displayed in a web browser.

3.8 System testing and validation

3.8.1 System Testing

System testing is the process of evaluating the entire integrated system to verify that it meets specified requirements and functions correctly as a whole. It involves testing the system's behaviour against its expected outcomes and validating its functionalities under different conditions

3.8.2 System validation

System validation is the systematic process of verifying that a system or its components meet specified requirements and fulfill their intended purpose. It involves rigorous testing, evaluation, and documentation to ensure that the system operates correctly under various conditions and meets user expectations.

Validation also includes incorporating user feedback, ensuring regulatory compliance (where applicable), and mitigating risks associated with system failures or performance issues. Overall, system validation ensures that the right system is built correctly and meets the needs of its users and stakeholders effectively.

Conclusion

Chapter three of the research report on a surveillance reporting system outlines the methodology employed to investigate the effectiveness, usability, or impact of the system. It describes the research design chosen, which could be qualitative, quantitative, or mixed-methods, depending on the research questions and objectives. The chapter details the data collection methods used, such as surveys, interviews, observations, or analysis of system logs, to gather information about how the surveillance reporting system functions in practice.

References

Electronic Frontier Foundation (EFF):

- The EFF focuses on defending civil liberties in the digital world, including issues related to surveillance. EFF Surveillance Resources

Surveillance Studies Network (SSN):

- An international network of surveillance scholars and researchers. Surveillance Studies Network

ACLU - American Civil Liberties Union:

- The ACLU works to defend and preserve individual rights and liberties, including privacy rights in the context of surveillance. ACLU Surveillance Issues

Chapter four

4.0 System study, analysis and design

This chapter concerns the study of the existing system analysis of requirement for the system, process and data modeling

4.1 The study of the existing system

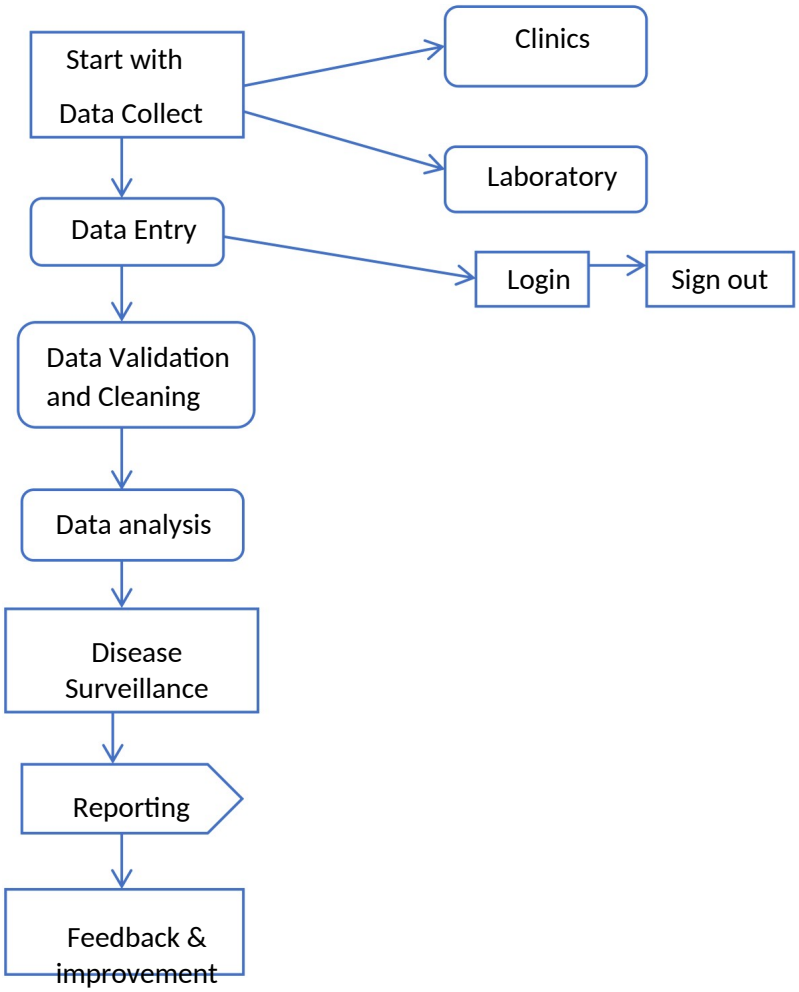
From the data collected above the existing Disease surveillance reporting information system through interviews, Observation and review of the existing documents the researcher found the patients patient had to seek for medical service from the health facility starting from the OPD department on daily basics, documentation in done on electronic system on data capture or on patient history taking and later transfer to patient treatment book, it's from these background that users of the system collates data on routine basic for reporting on prone diseases.

Further analysis of the existing disease surveillance reporting information system yield flow chart that shows the disease surveillance reporting processes right from patient registration at OPD to data collection and reporting

Disease Surveillance Workflow

1. Data Collection
2. Data Entry & Integration
3. Data Validation & Cleaning
4. Data Analysis
5. Disease Surveillance
6. Reporting

Feedback & Improvement



4.1.2 Strength of the existing system

1.It is able to generate data form the system for data analysis.

2. It stores and retrieves data or information on surveillance diseases.

3.Surveillance reporting information system helpsto gather data from multiple sources, integrating it into a centralized platform

4.It provides real-time data collection and analysis, enabling timely responses to emerging issues 5.Improved Communication and Coordination**:** The system facilitates better communication and coordination among various stakeholders by providing a shared platform for information access and reporting.

6.Security and Privacy**:** Robust SRIS include security measures to protect sensitive data from unauthorized access or breaches, ensuring that information remain confidential and secure.

4.1.3 Weakness of existing System

1. High Costs: Implementing and maintaining Surveillance reporting system can be expensive for instance it requires internet for bundles

2. Data Quality**:** Inaccurate or incomplete data inputs can lead to unreliable outputs, affecting the overall effectiveness of the system.

3. Data Overload: The sheer volume of data collected can be overwhelming, making it difficult to discern meaningful

4. User Resistance: Users may resist adopting new systems due to a lack of familiarity or perceived complexity, which can affect the system's effectiveness and utilization.

5. The existing system lacks instant verification and validation of

4.2 Data analysis results

Different data collection techniques were used by the researchers to collect data that was analyzed in order to obtain accurate information and generate reports. The researchers were able to find out the different challenges that are associated with the current surveillance reporting information system.

The major challenges faced with the current system during the reporting period is traffic congestion, server down time and making it difficult to report on time. The analyzed data was represented in tables and graphs to give more meaning and easy interpretation. Here is an example of an analyzed data for the four weeks of current system is as shown below in Table

Challenges Associated with delayed reporting

Date of report	Name of the report	No of reports	No of reports Submitted on Time	% of reports on
	Weekly surveillance report	1	0	O%
	Weekly surveillance report	1	1	100%
	Weekly surveillance report	1	1	100%
	Weekly surveillance report	1	0	0%

4.2.2 The Graphical Representation of the Challenges faced by surveillance reporting system

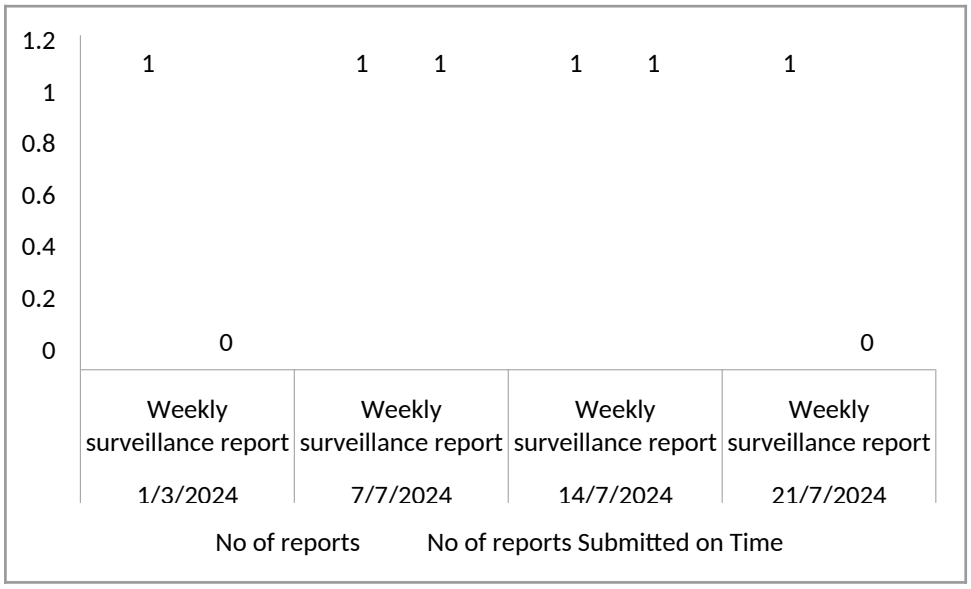


Figure 4. 1: A graphical presentation of the challenges faced by health surveillance reporting information system.

4.2.1 User Requirements

These are the statements, in a natural language, of what services is expected to provide and the constraints under which it must operate. Below are the user requirements of the system

1.The system is expected to generate or retrieve reports on diseases.

2.The users of system should able to submit reports on weekly basics

3.The system is expected to report cases of suspected outbreak.

4. The system is expected to be user friendly.

4.2.2 Functional requirements

A Functional requirement is a description of activities and services that the Disease surveillance reporting information system provides in terms of proceeding and data handling. So according to the tools used to collect data from the users, the following functional requirements were met;

1.The system should generate reports on disease surveillance

2.The system should store and retrieve information about disease surveillance

3.The system should enable to view data on surveillance

4.The system should update the data entry form after every entry.

5.The system should enable users to submit report.

6.The system should enable users enter data of diseases

4.2.3 Non-functional requirements

A non-functional requirement is description of other features, characteristics and constraints that define the satisfactory of the system therefore it describes how the Online Disease surveillance reporting Information System was to perform. Some of these requirements which were considered during the design of the system include;

1. The user should be able to access the system at any time of the day.

2. The system should authenticate users through username and password.

3. The system should provide fast processing to all user requests.

4. The system should be flexible, and easy to update.

5. The system should process user's tasks as fast as possible.

6. The online Surveillance reporting information System should be reliable.

4.2.4 System requirement

The system requirement includes requirements that are needed to include certain functionality in the system. It involved describing the system and the properties in that system. They include the hardware and software requirements as follows.

4.2.4.1 Hardware Requirements

Table 1: Hardware requirements

Hardware Components	**System requirements**	**Justifications**
Processor	Intel Pentium IV or abovePentium IV has the new technology (Hyper Threading) and the number of pins as well as cache memory has	

		been increased.
Processor Speed	800MHZ or above	This has enough speed, or clock rate to run the online Disease Surveillance information System.
Disk Space	80 GB or above	This is enough disk space or storage size for the data stored in the database of the online disease Surveillance information

4.2.4.2 Software Requirements

Table 2: Software requirements

Software Components	System requirements	Justifications
Operating System for the server	Windows NT or above	Windows NT adopts a new layered device-driver architecture that provides many advantages in terms of flexibility, maintainability, and portability
Operating system for the client PC	Windows XP	Windows XP can be used on personal computers, including home and business desktops, laptops and media canters.
Web Server	Apache Web Server Version 1.3	This is a web server software notable for playing a key role in the initial growth of the World Wide Web.
Database Management System	MySQL server version 3:23.48	MySQL is an open source relational database management system (RDBMS) that runs as a server providing multi-user access to a number of databases.

4.3 System Design

In the system design phase, process modeling involved use of Data Flow Diagrams (DFD), and Data modeling involved use of Entity Relationship Diagrams (ERD).

4.3.1 Architectural Design for the System

The architectural design shows how the DSRIS is comprised of the different subsystems namely Data collection, Data Processing, Data Storage and Data Display. The figure below shows an architectural diagram of the online disease surveillance reporting information system.

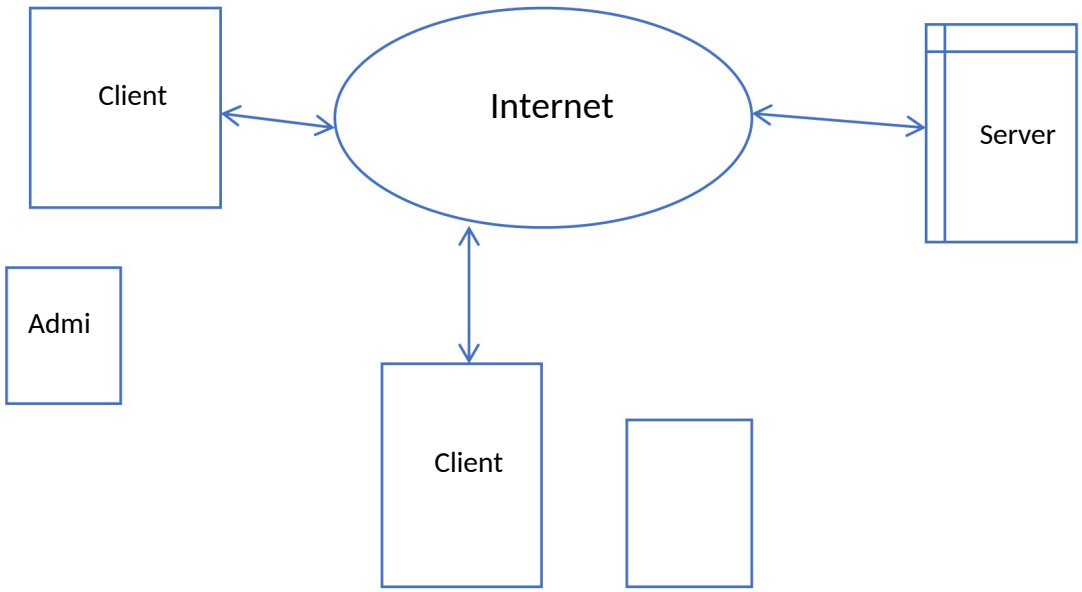
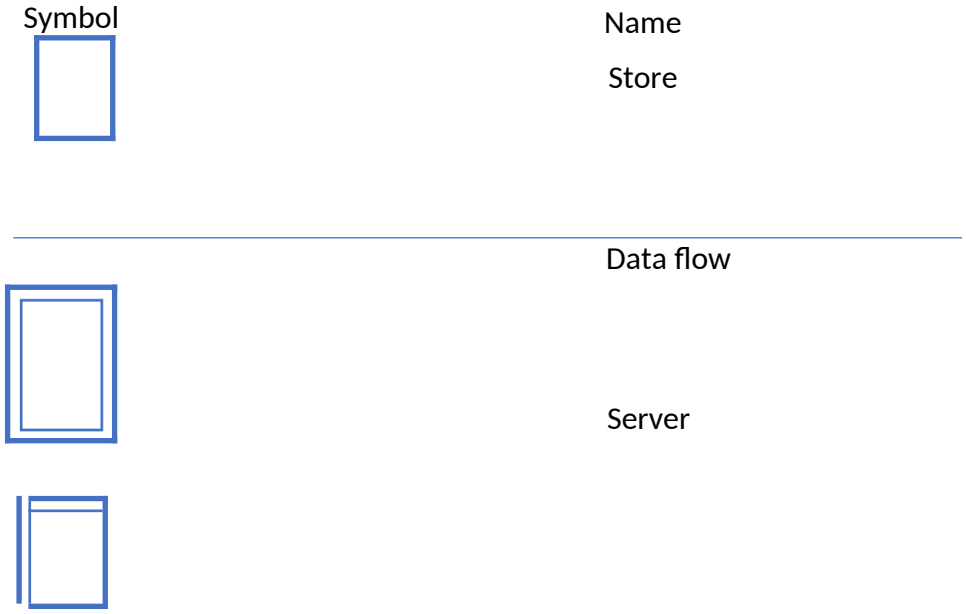


Figure 4.3: The Architectural Design for an online disease surveillance reporting information system.

4.3.2 Process Modeling

These show how information or data will be moving around the financial Management Systemfrom the entry to various repositories or data stores.

4.3.2.1 Key Symbols



Client

1.Data store shows where data is stored after being processed. This can be a database or a file.

2.Data flow shows the movement of data within the system and also connects processes, data stores and external entities.

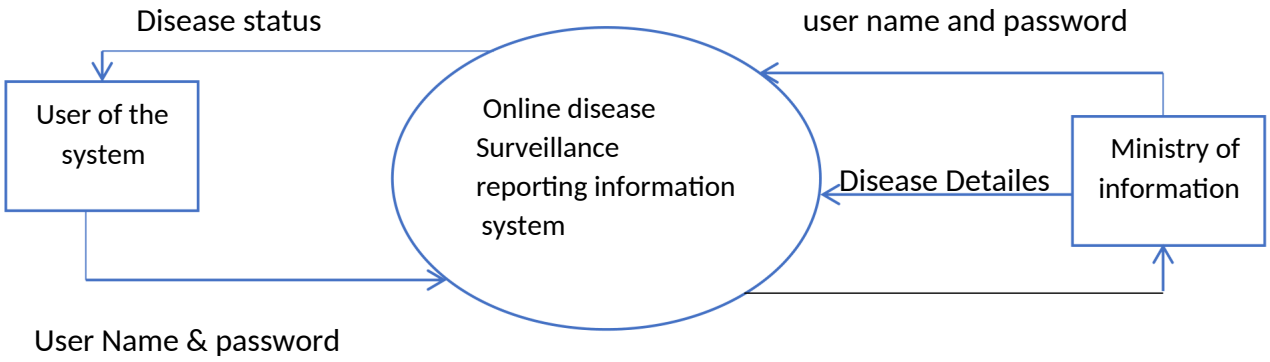
3.A Process is a series of activities or actions to accomplish a desired task.

4.Computer for input and output of data.

4.3.3 Data Flow Diagrams (DFD).

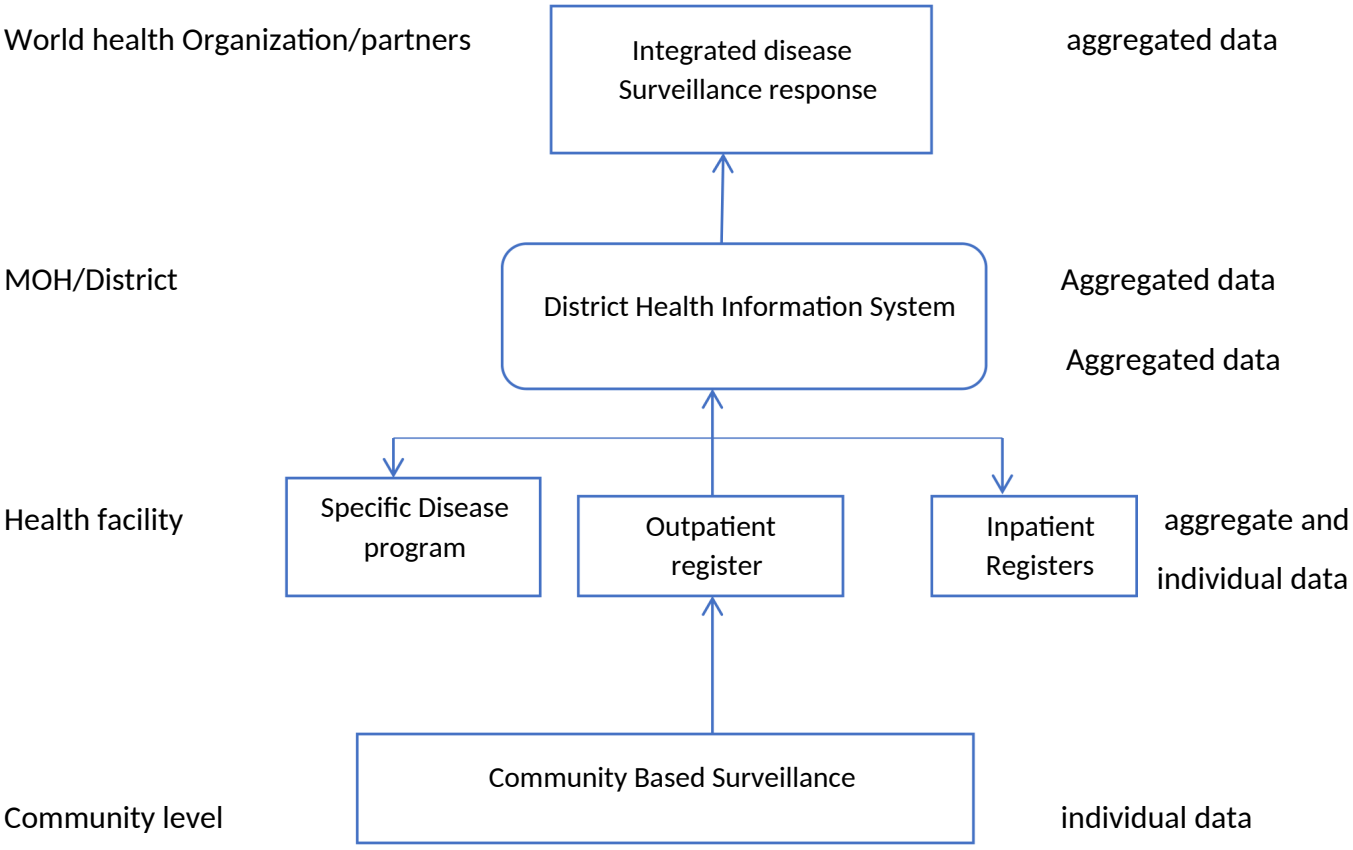
It is one of the most important moldings tools used by system analysts. It is used to illustrate used dataflow in the system. Data flow diagrams use a number of symbols to represent systems. There are four kinds of symbols. These are used to represent four kinds of system symbol components, data entry and process, data store, data flow and external entities

4.3.3.1 The Context Level DFD



Disease reports submitted

4.3.2 The level 1 of data flow diagram of Surveillance information system



4.4.3. Description for Processes

Table 3: Description of Processes

Process	Description
Data collection	Data is collected fromlaboratories submit disease data, such as case reports, test results, and epidemiological information.
Data entry	Enter data to all cells or Input the collected data into the EHR
Data Management and Storage	Databases are centralized repository for storing large volumes of data securely and efficiently.
Data Analysis and Reporting	Perform statistical analysis, trend detection, and outbreak investigation. Presentations of data such as graphs, charts, and maps to aid in quick decision-making
Security and Privacy	Data Encryption: Protection of data during transmission and storage

4.3.4 Description of Data Stores

Table 4: Description for Data stores

Data store	Description
Data collection	Stores all relevant collected data
User data entry	Stores disease details
User data storage	Store all large volumes of data
Data analysis	Store data for analysis.
Data security	Protect all stored data.

4.3.4 Description for External Entities

Table 5: Description of External Entities

Entity	Description
Healthcare Providers	Hospitals, clinics, doctors, and other healthcare professionals who report cases of diseases, symptoms, or outbreaks.
Laboratories department	Diagnostic labs that conduct tests and report results of diseases and infections to the surveillance system.
Patients	Individuals who receive medical care and services from the hospital
Researchers and Academics	Individuals or institutions that use data from the system for research and analysis purposes.
Governmental and Regulatory Bodies	Entities that set regulations or provide guidelines on disease reporting and data management.
Non-Governmental Organizations	Organizations involved in public health, or disease prevention that might use the data for advocacy and intervention strategies.

4.3.4 Identification of Entities and their Attributes

Table 6: Identification for Entities and their Attributes

Entity	Description	Attributes
A user	A user is a person who use the system	user_id Username other_name Telephone E-mail location sex nationality Age

Hospital	A place where patients receive medical care services	hospital_id name Address Location
Department	Place where test diagnostics are investigated	department_id name Telephone
Patients	Individual who receive service from the hospitals	Patient_id Name: Age sex Address Telephone disease_id
Diseases	Disease is chronic illness	Disease_id Disease- name Code Category
Health care provider	Health care provider	Professional_id fname lname Title telephone email address

4.3.5 Modeling Relationships between Entities

Figure 4. 2: Relationship between system and user

System can contain one or more accounts is contained while a user able to contain one and only one account.

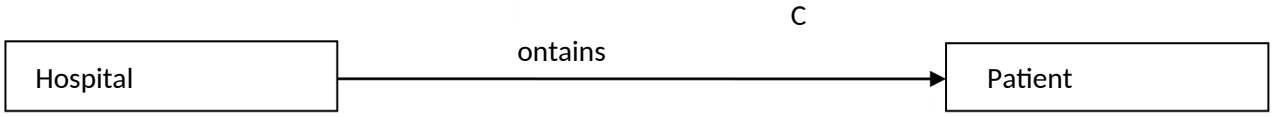


Figure 4. 3: Relationship between Hospital and Patient

A hospital can have one or more patients and patient can belong to one Hospital

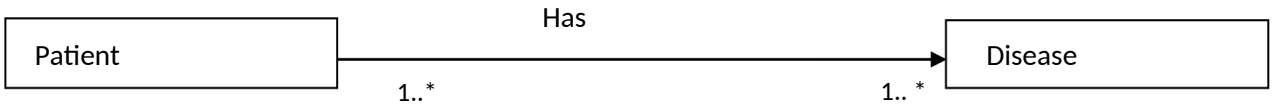


Figure 4. 4: Relationship between Patient and Diseases

A patient can have one or more diseases and a disease can only attack one patient

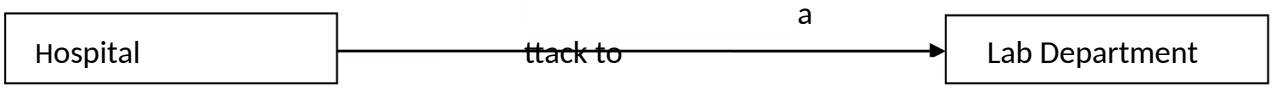


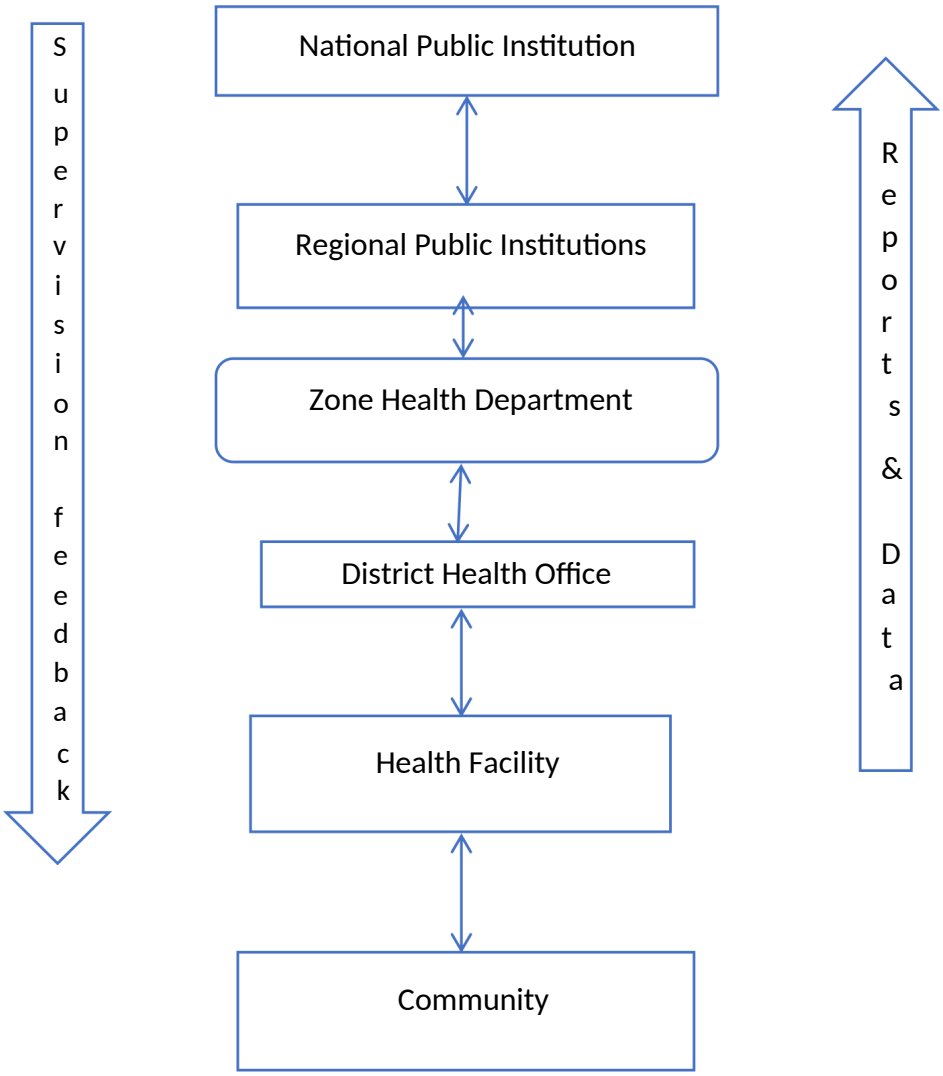
Figure 4. 5: Relationship between Lab Department and Hospital

A Hospital may have one or more departments and departments may belong to one and only one Hospital

Figure 4. 6: Relationship Hospital Bank and Employee

A hospital consists of one or more employees while an employee is paid under of the only one Hospital.

4.3.6 The entity Relationship Diagram



4.3.7 Mapping of ERD to Relational Schema

4.3.7.1 User

Table 7: The User table

Field Name	Data Type	Constraint
CuserID	int(12)	Primary Key, Not null
Fname	varchar(20)	Not null
Lname	varchar(20)	Not null
Telephone	int(12)	Not null
Email	varchar(30)	Not null
Address	varchar(30)	Not null
Sex	varchar(6)	Null
Nationality	varchar(20)	Not null
Age	int(100)	Null
location	Varchar(16)	Not null
accountID	Int(16)	Foreign Key, Not null

4.3.7.2 Hospital

Table 8: The Hospital table

Field Name	Data Type	Constraint
HospitalID	int(16)	Primary Key, Not null
Name	varchar(20)	Not null
Telephone	Int(12)	Not null
Address	varchar(20)	Not null

4.3.7.3 Department

Table 9: The Department table

Field Name	Data Type	Constraint
DepartmentID	int(16)	Primary Key, Not null
Name	varchar(20)	Not null
Type	varchar(20)	Not null
Telephone	Int(16)	Not null

4.3.7.4 Patient

Table 10: The Patient table

Field Name	Data Type	Constraint
PatientNO	int(16)	Primary Key, Not null
Name	varchar(20)	Not null
sex	Varcher(8)	Not null
Age	Int(6)	Not null
Telephone	Int(12)	Not null
Address	Varcher(15)	Not null
diseaseID	Int(10)	Primary Key, Not null

4.3.7.5 Disease

Table 11: The Disease table

Field Name	Data Type	Constraint
DiseaseID	int(16)	Primary Key, Not null
Name	varchar(20)	Not null
Category	Varcher(12)	Not null

4.3.7.6 Employee

Table 12: The Employee table

Field Name	Data Type	Constraint
employeeID	int(16)	Primary Key, Not null
Fname	varchar(20)	Not null
Lname	varchar(20)	Not null
Telephone	int(12)	Not null
Email	varchar(30)	Not null
HospitalID	Int(16)	Foreign Key, Not null

4.4 Conclusion

In summary, this chapter was mainly based on the study of the existing system, analysis of the requirements for the system, processes and data modeling.

Chapter Five

System Implementation, Testing and Validation

This section describes the implementation of the design models in of the system and also shows the different results generated by the system. Therefore screen shots of the system will be displayed to show how the system displays results given a command.

5.1 System Functions

The Disease Surveillance Reporting Information System provides the administrator with a role of Managing system functionality, user access, and ensure data security and integrity is provided in the system.

System administrator ensures accurate data entry and system functionality to maintain the quality and reliability of the information. Performs data analysis, data validation and generate reports for presentation and dissemination.

The users are able to collect data, enter, submit, and view reports patient data from surveillance reporting information system.

Also users to analyze data, generate reports, and coordinate responses to disease threats and data analysis, identify trends

5.1.1 Functions provided to all users.

In a Disease Surveillance Reporting Information System, all users can submit disease data, access relevant information based on their permissions, receive alerts and notifications about trends or urgent issues, search for specific data, and view visual dashboards summarizing key surveillance metrics.

5.1.2 Functions provided to a patient

The patient's functions are typically limited to submitting personal health data related to symptoms or diagnoses, viewing their own health reports if the system allows, and receiving notifications or alerts related to their condition or necessary actions. They generally do not have access to broader data or system management features.

Bottom of Form

5.1.3 Functions provided health care provider

Healthcare providers can submit and update patient health data, including diagnoses and test results, access detailed patient records and disease trends, receive alerts on outbreaks or critical health issues, and

generate reports to support clinical decision-making and public health responses. Their role is crucial for accurate data entry, monitoring patient conditions, and contributing to overall disease surveillance efforts.

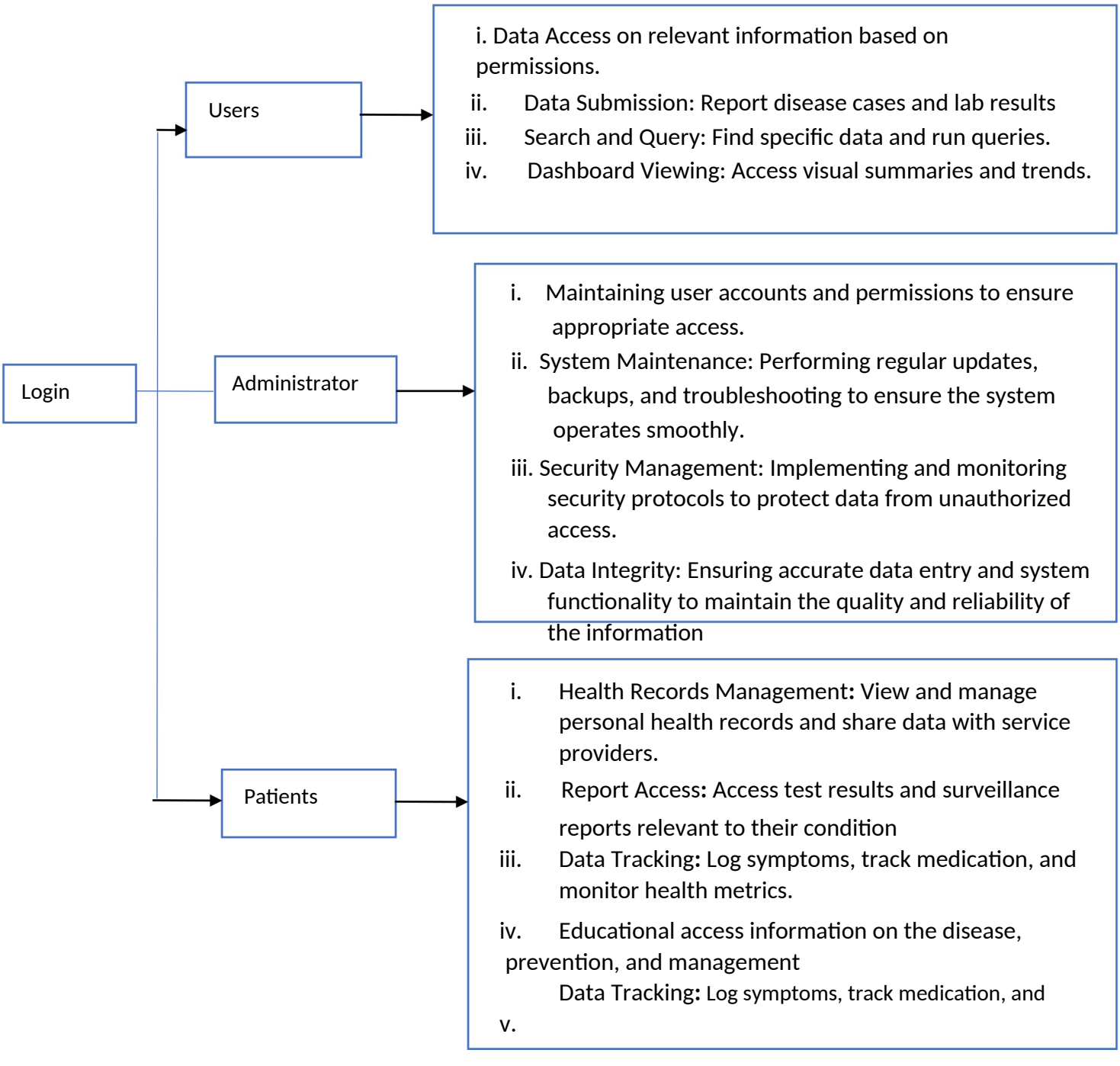
5.1.4 Functions provided system administrator on disease Surveillance.

Facility in charge of a Disease Surveillance Reporting Information System is responsible for overseeing system operations, ensuring that data is accurately collected and reported, coordinating with healthcare providers for seamless data integration, managing user training and support, and ensuring compliance with relevant regulations. They play a key role in maintaining system functionality and ensuring effective disease monitoring and response.

Top of Form Bottom of Form

5.2 System map

Figure 5.1: System Map showing functions provided by the system to each user

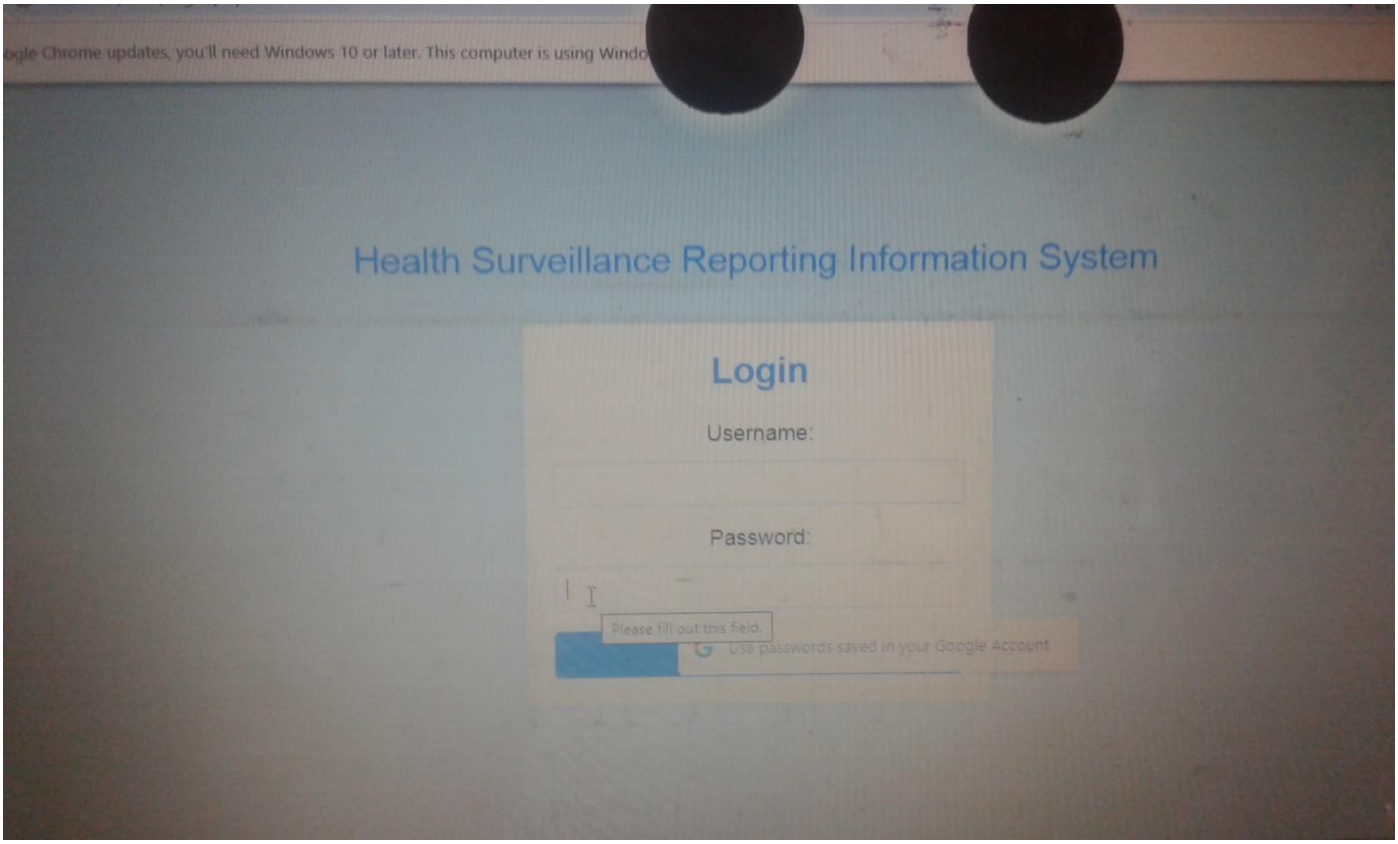


monitor health metrics

5.3 Sample Screen-shots

5.3.1 System login page

Figure 5.2 Shows the homepage that allows users of the system to login into the system in order to access health surveillance dashboard. Below is the login page.



Disease surveillance dashboard

These is the home page where the health users are expected to perform numerous activities such as data entry and report submission to system after collecting data from different service points like Laboratory department, Outpatient department and others.

The users are able to view and generate reports on prone diseases to enable them to analyze the data and more so to validate for the specific period, also the data can be generate data for performance review and feedback.

The dashboard can be used to display weekly trends of that in the dash board as shown below.

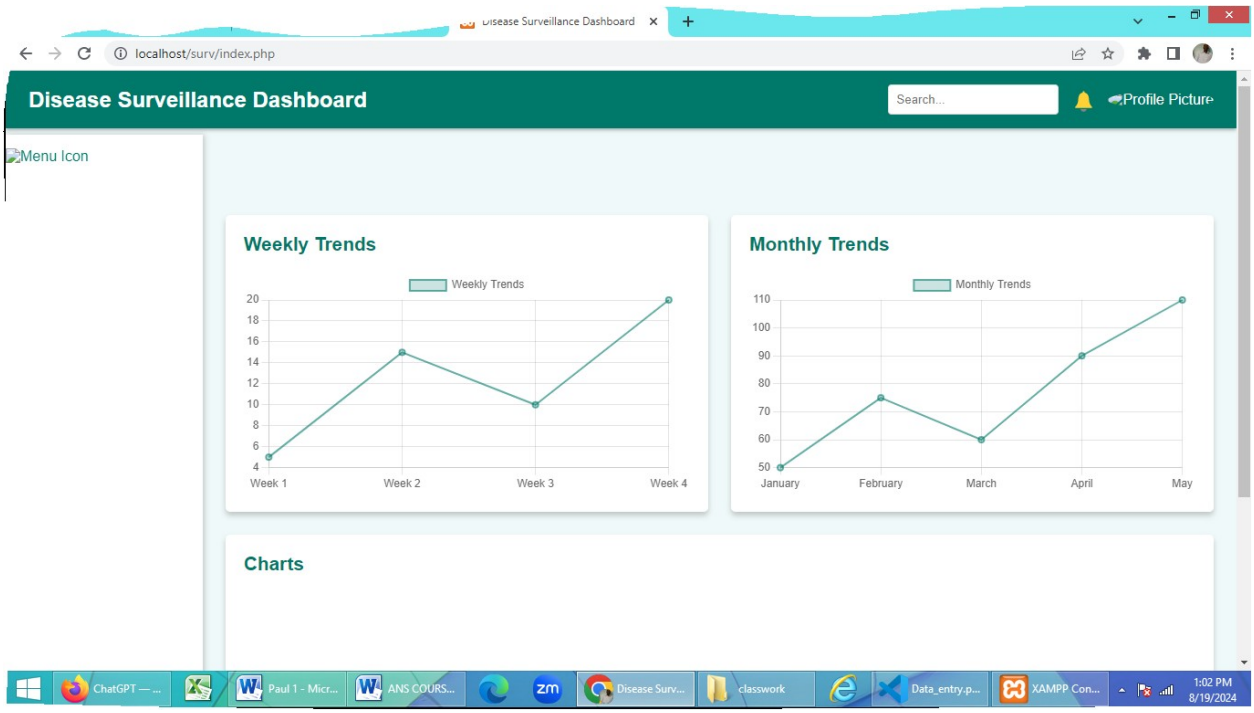
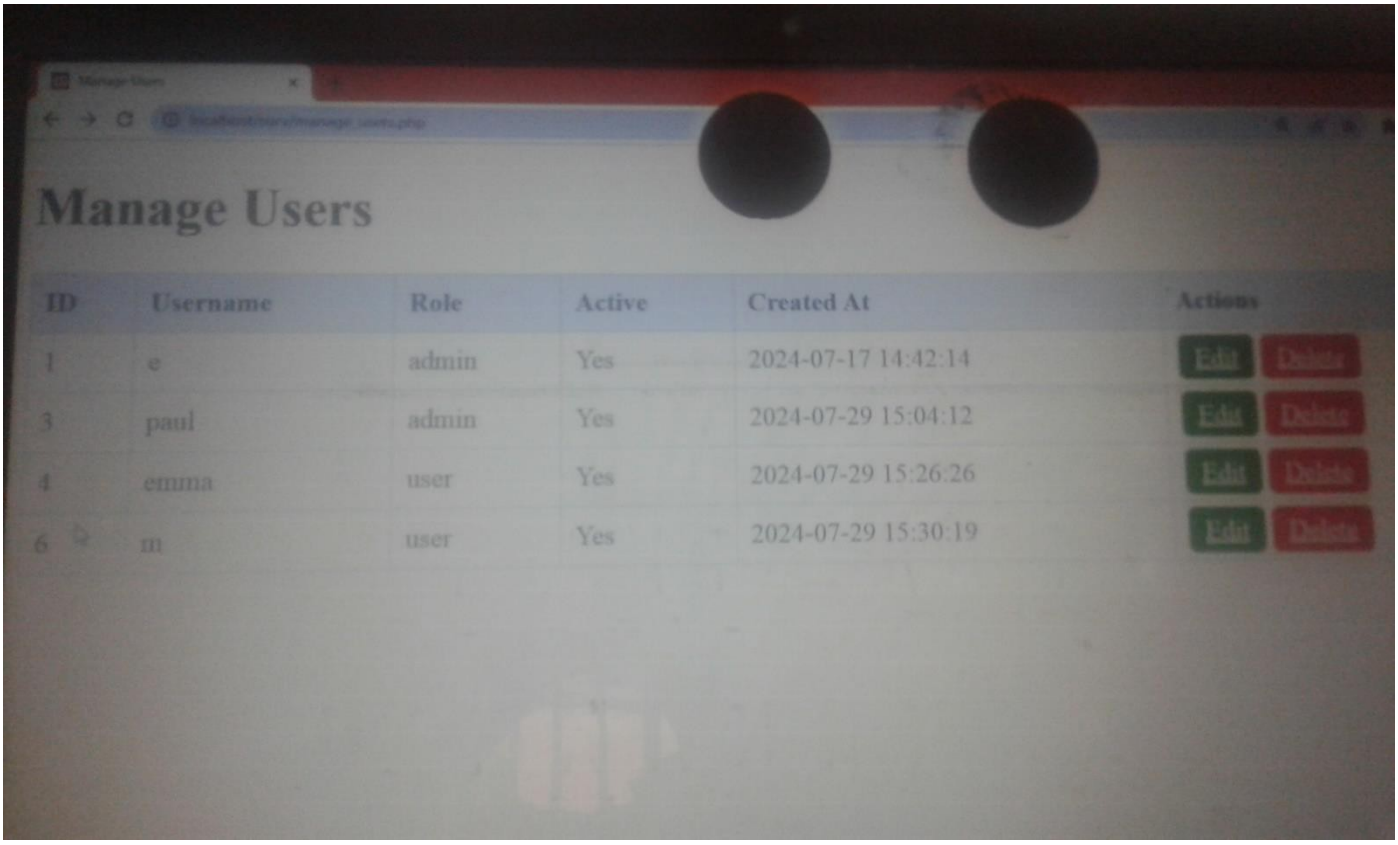


Figure 5. 1: Administrator user Management page

5.3.3 Administrative user management

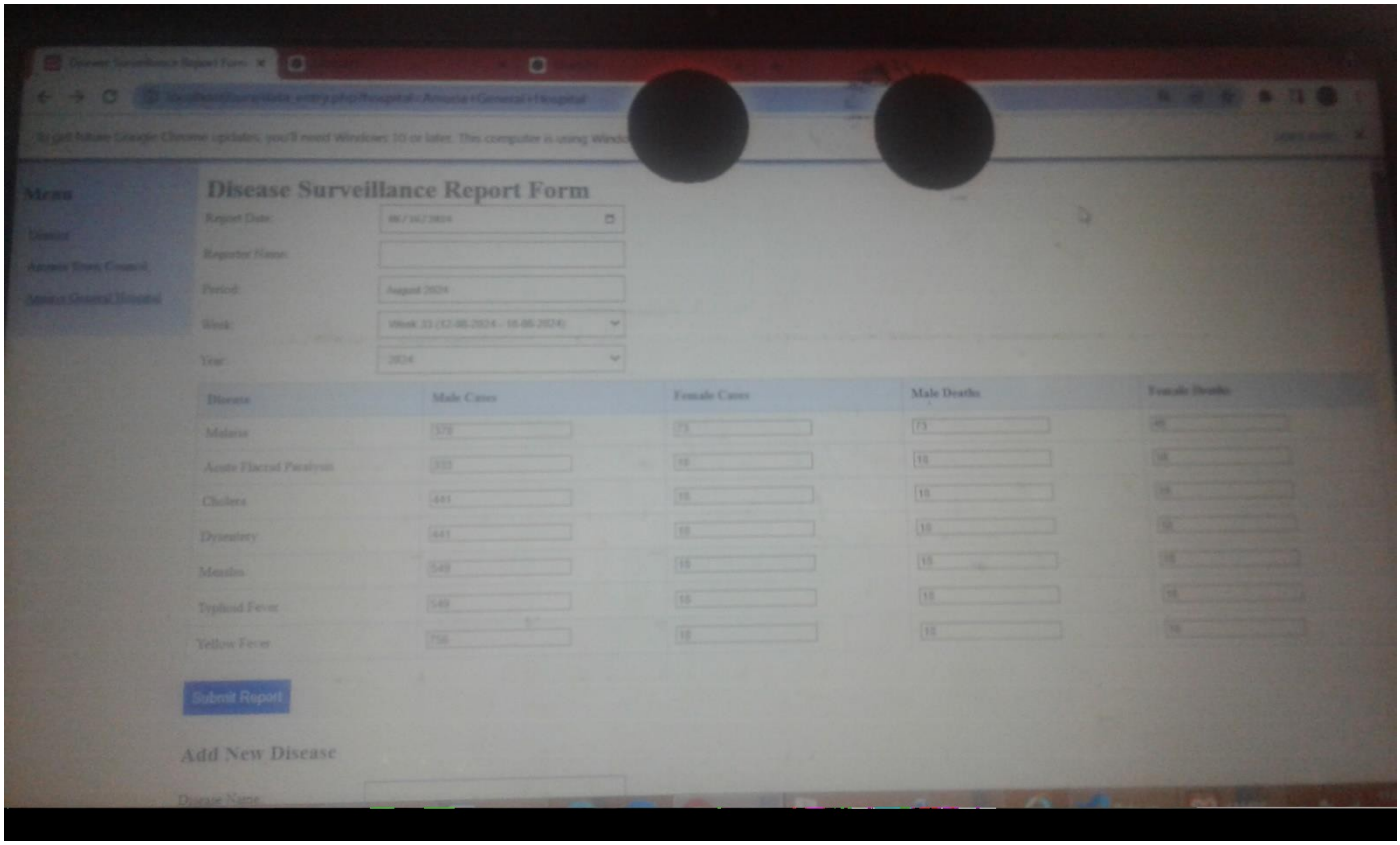
Figure 5.4: Shows the administrator fully user management dashboard where he can perform the function of deleting, edit and add the users to the system. The page is shown as below.



Data entry form

The data entry dashboard is the page were reports of surveillance prone disease data are entered in to the system and submitted to the next level and also data will be kept in the database

The illustration to the form is as below



Generate reports

This page designeted for generting data from the system, the users are empowered to generate reports the purpose to enable the facility to plan for the curse of action. The users are able to view reports on prone diseases to enable them to analyze the data and more so to validate, organized it for top management meeting and performance review and feedback.

Chapter Six

Summary, Recommendations and Conclusion

6.1 Summary

All the stated objectives of the of disease surveillance reporting information system have been successfully achieved. The system has been designed to enter prone disease data on gender affiliation to easy data to enable to detect on the sex is more prone to attack.

For security reasons, each user is given a user name and password and this will be the only way they will be able to log into the system but using a similar interface. The administrator has the overall privileges.

6.2 Recommendations

There is need for more research in this field so that the weaknesses of the system can be addressed privet organization and report suspected out break to the district of their jurisdiction

Similar the systems should be developed for the other NGO in the Uganda which are still using manual systems for keeping records in the boxes files of records management

6.4 Conclusions

The surveillance reporting information System objectives were achieved. The major strength of this system was detect and report on prone or outbreak of disease site.

References

Dr. Anne Schuchat: Former CDC Principal Deputy Director, influential in developing public health surveillance systems in the U.S.

- **CDC Contact:**CDC

Dr. Michael Ryan: Executive Director of WHO Health Emergencies Programme, overseeing global disease surveillance efforts.

- **WHO Contact:**WHO

Dr. Amesh Adalja: Senior Scholar at Johns Hopkins Center for Health Security, provides insights into disease surveillance and public health responses.

- **Johns Hopkins Center Contact:**Center for Health Security

Dr. Marc Lipsitch: Professor at Harvard T.H. Chan School of Public Health, specializes in epidemiology and disease surveillance.

- **Harvard T.H. Chan Contact:**Harvard

Areas where disease surveillance reporting systems are implemented include:

United States: CDC's National Notifiable Diseases Surveillance System (NNDSS).

United Kingdom: NHS Digital's Public Health Surveillance Systems.

European Union: European Centre for Disease Prevention and Control (ECDC) systems.

- **Global**: WHO's Global Influenza Surveillance and Response System (GISRS).

Sure! Below is a questionnaire designed to gather data on a Surveillance Reporting Information System. It includes both open-ended and closed-ended questions to get a comprehensive view of users' experiences and opinions.

Surveillance Reporting Information System Questionnaire

Section 1: General Information

Name of Respondent (Optional):

……

Position/Role:

…….

Organization/Department:

…….

How long have you been using the Surveillance Reporting Information System?

Less than 6 months

6 months to 1 year

1 to 2 years

More than 2 years

How frequently do you use the system?

Daily

Weekly

Monthly

Occasionally

Section 2: System Usability

On a scale of 1 to 5, how would you rate the overall ease of use of the system?

1 (Very Difficult)

2 (Difficult)

3 (Neutral)

4 (Easy)

5 (Very Easy)

How would you rate the following aspects of the system? (Rate each on a scale of 1 to 5)

User Interface Design

1 (Very Poor)

2 (Poor)

3 (Average)

4 (Good)

5 (Excellent)

Navigation and Accessibility

1 (Very Poor)

2 (Poor)

3 (Average)

4 (Good)

5 (Excellent)

Speed and Performance

1 (Very Poor)

2 (Poor)

3 (Average)

4 (Good)

5 (Excellent)

Reliability and Downtime

1 (Very Poor)

2 (Poor)

3 (Average)

4 (Good)

5 (Excellent)

Have you encountered any technical issues with the system?

Yes

No

If yes, please describe the issues:

……

Section 3: Functionality and Features

Which features of the system do you use most frequently? (Select all that apply)

Data Entry

Data Retrieval

Reporting

Data Analysis

Alerts/Notifications

User Management

Other (Please specify): [Text Field]

Are there any features or functionalities you find particularly useful?

[Text Field]

Are there any features or functionalities that you feel are missing or could be improved?

[Text Field]

Section 4: Data Reporting and Analysis

How effective is the system in generating accurate and timely reports?

Very Ineffective

Ineffective

Neutral

Effective

Very Effective

How satisfied are you with the data analysis capabilities of the system?

Very Unsatisfied

Unsatisfied

Neutral

Satisfied

Very Satisfied

Do you encounter any challenges when generating or interpreting reports?

Yes

No

If yes, please explain:

……

Section 5: Training and Support

How would you rate the quality of training you received on using the system?

Very Poor

Poor

Average

Good

Excellent

How accessible and helpful is the technical support for the system?

Very Unhelpful

Unhelpful

Neutral

Helpful

Very Helpful

Have you had any training on the system?

Yes

No

If yes, was it adequate for your needs?

Yes

No

If no, what additional training would you have found useful?

……..

Section 6: Overall Experience

Overall, how satisfied are you with the Surveillance Reporting Information System?

Very Unsatisfied

Unsatisfied

Neutral

Satisfied

Very Satisfied

Would you recommend this system to others in your field?

Yes

No

If no, please explain:

……..

Do you have any additional comments or suggestions for improving the system?

……