Ghana Health Service Enterprise Architecture

(The eHealth Architecture)

Copyright © 2009

Table of Contents

 Copyright © 2009

1. Introduction

The European Commission defines e-Health as:

“The use of modern information and communication technologies to meet needs of citizens, patients, healthcare professionals, healthcare providers, as well as policy makers.

e-Health is today‘s tool for substantial productivity gains, while providing tomorrow‘s instrument for restructured, citizen-centered health care systems and, at the same time, respecting the diversity of Europe‘s multi-cultural, multi-lingual health care traditions. There are many examples of successful e-Health developments including health information networks, electronic health records, telemedicine services, wearable and portable monitoring systems, and health Portals”.

This report is the Enterprise Architecture (EA) for the Ghana Health Service (GHS), which is a deliverable from the eGhana Enterprise Architecture project. The GHS Enterprise Architecture (EA) provides the framework for developing e-Health in Ghana. The GHS EA is more than just technology architecture. It involves primarily four architecture perspectives (Business Architecture, Applications Architecture, Data Architecture and Technical Architecture). The process of defining the Enterprise Architecture included defining relationships that depict how these architectures interrelate and will change as new events occur.

The future of healthcare services in Ghana is based on improving communication between Government and the GHS, National Health Insurance Authority (NHIA) and other insurance companies; employers; hospitals, clinics and doctors, clinicians and allied healthcare professionals; and patients. The population in general and various communities within the population are also deeply involved. The GHS is currently organised through a variety of separate healthcare facilities and their departments, which have very little regular or formal connection with each other in the way their services are delivered. Each department tends to implement its own processes and delivery channels. Patients, who are effectively the end consumers of the Healthcare services, must often deal with several departments that have no apparent commonality in the way that they work, or even in the way that they appear to the patient. With the technology of the Internet, mobile communications, and powerful yet affordable computers becoming commonplace, there is an opportunity to redesign the way many of these services are delivered.

The overall aim of the GHS EA is to move Healthcare towards a series of easily available, interconnected, reliable and efficient services. The EA is a model on which such solutions can be built.

The EA describes the underlying infrastructure and provides the groundwork for aligning business and Information and Communication Technology (ICT) strategy of the Service. The GHS EA is based on the Ghana Government Enterprise Architecture (GGEA) framework, which defines the architecture principles and standards to be adopted by Ministries, Departments and Agencies (MDAs).

This report presents a detailed analysis of the current state of the GHS' business and ICT environments with the aim to improve services provided by the Service. It also provides a roadmap to move away from current applications and supporting technologies to an environment that better meets the current and future needs of the Service.

The remainder of the document is structured as follows:

- Chapter 2 presents the results of current state assessments of the sites
- Chapter 3 presents strategic and the SWOT analysis;
- Chapter 4 provides the recommendations for the future state architecture
- Chapter 5 defines a security architecture to support the EA;
- Chapter 6 defines an Enterprise ICT Management approach;
- Chapter 7 presents recommendations on governance;
- Chapter 8 presents the strategic plans for implementing the recommendations;
- Appendices.

2. Current State Analysis

The Ministry of Health (MoH) implements its services to the public via various departments and agencies that deliver on its behalf. It is responsible for implementing government directives and commitment towards providing health to the people of Ghana using the public sector apparatus for service provision.

The GHS is a service provision agency for the Ministry of Health (MoH). It is an autonomous Public Service Executive Agency (PSEA) responsible for the implementation of national policies under the MoH, through its governing Council - the Ghana Health Service Council. The GHS reports quarterly and annually to the MoH on services delivered by almost forty-thousand (40,000) employees managing over one thousand (1,000) health facilities ranging from two-hundred (200) beds in regional hospitals to one-man units or stations. The GHS is part of the public sector but its employees are no longer part of the civil service.

Hence, GHS managers are not required to follow all civil service rules and procedures. The independence of the GHS is designed primarily to ensure that staffs have a greater degree of managerial flexibility to carry out their responsibilities, than would be possible if they remained wholly within the civil service. Ghana Health Service does not include Teaching Hospitals, Private and Mission Hospitals.

The GHS is mandated to draw on the policies and priorities agreed by the health sector to provide universal access to a basic package of health services, and improve the quality and efficiency of health services through facilities or contracted agents'. In other words, it has a mandate to provide and prudently manage comprehensive and accessible health service with special emphasis on primary health care at regional, district and sub-district levels in accordance with approved national policies. As part of government efforts to reform the health sector to become more equitable, efficient, accessible and responsive under the Medium Term Health Strategy (MTHS), led to the establishment of the GHS. It is an essential part of the key strategies identified in the Health Sector Reform process.

The MoH consists of four main sections i.e. the Medical & Dental Council (MDC), the Ghana Health Services Council (GHS), the Public Health Council (PHC) and the Nursing & Midwifery Council (NMC).

The GHS consists of nine (9) sub functions/departments controlled by its Director General i.e. Institutional Care Directorate (ICD), Human Resource Development Department (HRDD), Public Health (PH), Policy Planning Monitoring & Evaluation (PPME), Family Health (FH), Stores Supplies and Drugs Management (SDDM), Health Administration & Support Services (HASS), Finance Department (FD) and Internal Audit Department (IAD). The main objectives of the GHS are:

- Implement approved national policies for health delivery in the country;

- Increase access to good quality health services;
- Manage prudently resources available for the provision of the health services.

For the purposes of achieving its objectives the GHS will perform the following functions amongst others provide comprehensive health services at all levels directly and by contracting out to other agencies. As part of this function, the GHS will:

- Develop appropriate strategies and set technical guidelines to achieve national policy goals/objectives;
- Undertake management and administration of the overall health resources within the service;
- Promote healthy mode of living and good health habits by people;
- Establish effective mechanism for disease surveillance, prevention and control;
- Determine charges for health services with the approval of the Minister of Health;
- Provide in-service training and continuing education;
- Perform any other functions relevant to the promotion, protection and restoration of health.

The GHS (one of the four sections under the Ministry of Health) is a service provision Agency organised at Five (5) functional levels i.e.

- National Level;
- Regional Level;
- District Level;
- Sub-district Level;
- Community Level.

GHS has a Director General who controls ten (10) regional districts within which there are district hospitals that provide direct health services to citizens.

From a services point of view, the GHS delivers Healthcare services to citizens.

The Regional/District/Sub-District centres/hospitals are modes of health service delivery. They provide a platform or presence for consultation with patients/citizens, knowledge development and dissemination (3500), health regulations and compliance (3900) as well as financial assistance (3400), health credit and insurance (3300) and marketing (3600).

Support for the delivery of services is in the controls and oversight actions (4100) taken by the GHS at all the functional levels. Risk management (4300), public affairs (4600) and regulatory development (4700) are all support providers for the delivery of health services.

All the components of resource management on the Business Reference Model are applicable to the GHS.

Administratively, the GHS is organised at three levels: national, regional and district levels. National Level:

- Ghana Health Service Council;
- Office of the Director General and Deputy Director General;
- Eight National Divisional Directors;

Regional Level:

- Regions are headed by 10 Regional Directors of Health Services;
- Supported by Regional Health Management Teams;
- Regional Health Committees.

Districts Level

- All 110 districts are headed by District Directors of Health Services;
- Supported by the District Health Management Teams;
- District Health Committees;

The above administrative levels are organised as Budget Management Centres or Cost centres for purposes of administering Government of Ghana and Developmental Partner Funds. There are a total of 223 functional BMC's and 110 Sub-Districts BMC's of Record. Breaks down of the BMC's are as follows: Currently, the headquarters of the GHS is managed as one BMC; 10 Regional Health Administration, 8 Regional Hospitals, 110 District Health Administrations and 95 District Hospitals.

2.1 CURRENT STATE BUSINESS ANALYSIS

The key functions of GHS are to develop appropriate strategies and set technical guidelines to achieve national policy goals or objectives for the health sector. GHS undertakes management and administration of the overall health resources within the service and promote healthy mode of living and good health habits by people. GHS must also establish effective mechanism for disease surveillance, prevention and control as well as determine charges for health services with the approval of the Minister of Health. Provisions of in-service training, continuing education are added functions as well.

Functionally, GHS administrative functions are divided into Divisions, Departments and Sections:

- **Division** - is the administrative name of a functional directorate at the headquarters and is headed by a Divisional Director. All Divisional Directors exercise authority as derived from and consistent with one's responsibilities as well as authority delegated by the immediate superior (Director General or in his absence, the Deputy Director General) consistent with the superior's responsibilities. In effect, the Divisional Director is directed, guided and accountable to the Director General and his/her authority in turn mediates interdepartmental issues.

- **Department** - is the next level to the Division and a coalition point of a number of Sections with authority for the execution of specific functions consistent with the Division's responsibilities and is headed by a Deputy Director.
- **Section** - comprises of the operatives of the Division who perform functions assigned to them based on their professional expertise and competence. In this sense, they are technical officers with the relevant qualifications. Each Section may have a head as the coordinator of the professionals under the Unit and is accountable to the Divisional Deputy Director.

The Management Class of the Service ends at the Deputy Director Level. All other functionaries shall retain their professional classifications for purposes of promotion and salaries. The Director General is the head of the GHS.

GHS is made up of 10 divisions (directorates) namely:

- Policy, Planning, Monitoring and Evaluation Division (PPME);
- Institutional Care Division (ICD);
- Public Health Division(PHD);
- Human Resource Development Division (HRDD);
- Health Administration and Support Services Division (HASS);
- Supplies, Stores and Drugs Management Division (SSDM);
- Finance Division(FD);
- Internal Audit Division(IAD);
- Family Health Division (FHD);
- Operational Research Division (ORD).

2.1.1 Policy, Planning, Monitoring and Evaluation Division (PPMED)

This division is responsible for the analysis of national, bilateral and international policies and its use in the development of strategic plans and implementation guidelines for the GHS. The division executes this function in collaboration with other Divisions and implementation partners. It's also responsible for the Coordination, guidance and development of short, medium and long-term plans and budgets for the GHS's development, including the preparation of projects and programmes for local and international financing which are consistent with the Sector-Wide/Multi-Donor Budget Approach.

Also the division develops level specific performance indicators and contracts consistent with national, bilateral and international expectations as well as a comprehensive system of research, monitoring and evaluation of programmes and projects in collaboration with other Divisions and implementing agencies with a view to determining programme effectiveness and efficiency. PPME also reviews health financing and resource (human and infrastructure) allocation strategies and its impact on access, quality and efficiency to consumers alongside the production

and management of health information as a management decision support system, made accessible to all functionaries of the service for effective decision-making.

2.1.2 Institutional Care Division (ICD)

This division coordinates, guide and develop short, medium and long-term plans and budgets for the GHS's clinical care development, including the preparation of projects and Programmes for local and international financing consistent with the Sector-Wide/Multi-Sector Approach. It's also responsible for the development of clinical governance and infection control systems. The division supports, monitors and evaluate Programme and projects in collaboration with the Regions, Districts and other health Programme implementing agencies with a view to promote clinical care effectiveness and efficiency.

The HASS reviews clinical care intervention financing and resource (human and infrastructure) allocation strategies and its impact on access, quality and efficiency to consumers and produce and manage clinical care information as a decision support system, and make it accessible to all divisions and stakeholders for effective decision-making. The division also monitors the implementation of all clinical care field Programmes and projects initiated by the service in collaboration with the Public Health Division to ensure Programmes effectiveness and sustainability. They also supervise and provide technical support for the Regional Public Health Reference Laboratories.

2.1.3 Public Health Division (PHD)

The division coordinates, guide and develop short, medium and long-term plans and budgets for the GHS's public health programme development, including the preparation of projects and programmes for local and international financing consistent with the Sector-Wide/Multi-Sector Approach. It also develops surveillance and disease control systems for both communicable and non-communicable diseases consistent with national, bilateral and international expectations. The division also provides support, monitoring and evaluation of EPI programmes and projects in collaboration with the regions, districts and other health programme implementing agencies with a view to promoting Programme effectiveness and efficiency. The Public Health division reviews public health intervention financing and resource (human and infrastructure) allocation strategies and its impact on access, quality and efficiency to consumers. It also produces and manages health information for general public consumption as a decision support system, made accessible to health consumers, individuals and households for effective decision-making. The Provision of Maternal, Adolescent, Child and Reproductive health and nutrition services through the development of collaborative strategies with other service providers is a main responsibility of the division. Also the Public Health Department monitors the implementation of all public health field Programmes and projects initiated by the service and ensure the prudent utilization of budget provisions as well as the Provision of technical support for the Regional Public Health Reference Laboratories and the development of early warning systems for the management of epidemics.

2.1.4 Health Administration and Support Services Division (HASS)

This division initiates and implements administrative improvement schemes and cost-reduction programmes in the GHS. They determine appropriate levels, specification, procurement and replacement of equipment and transport consistent with national policy and GHS requirements. The division is also responsible for

Monitoring and supervising all building and construction projects meant for the GHS to ensure value for money. Also they prepare and periodically update infrastructure and equipment situations and specifications for the GHS in collaboration with the PPME Division. The HASS pursues the development and implementation of adequate proficiency programmes to improve the recruitment and competence of staff in secretarial and security support, estates and equipment maintenance in the GHS in collaboration with the HRD Division. Also, they ensures the proper acquisition and take custody of the documentation of all estates and chattels of the GHS once these have been acquired and develop procedures for undertaking planned and routine maintenance by all levels.

2.1.5 Human Resource Development Division (HRDD)

The HR Development division is responsible for carrying out the conventional HR responsibilities which include:

- Establishes and maintains systems and procedures for planning, training and manpower development for the Service;
- Institutes measures for the periodic review of the organisation structure, including job classifications, descriptions, schemes of service and job descriptions;
- Provides guidance in determining training needs of all categories of workers in the service and ensures that appropriate training programmes are developed and implemented;
- Establishes and maintains systems and procedures for the promotion, retirement, co-operation and advancement in all personnel affairs to ensure fairness and consistency in the treatment of staff of the Service;
- Oversees the recruitment, selection and placement of new staff and monitors the progress of newly-engaged staff – local and expatriate - to ensure that they become efficient and committed to their work within the Service;
- Establishes and maintains an efficient personnel records-keeping system to promote easy accessibility to and retrieval of files;
- Serves as the liaison Division for industrial relations;
- Determines appropriate manpower levels consistent with organizational requirements and pursues the development and implementation of adequate proficiency programmes to improve the competence of staff in the Service;

- Co-ordinates and collates training and manpower development budget and when approved, institutes measures to back up its implementation;
- Keeps and updates records on the training history of all staff.

2.1.6 Supplies, Stores and Drugs Management Division (SSDM)

Undertake periodic review of drug and chemical situation of the Service and that of its Programme implementation partners with a view to improving on efficiency and quality. The functions include:

- Developing in collaboration with the PPME/PH/ICD Divisions, a national procurement management plan for the short, medium and long term consistent with the Services Programme of work;
- Procuring drugs and equipments based on set national policies and existing legislature;
- Coordinating and manage the supply and distribution of all drugs and non-drug logistics (local and international;
- Carrying out the inspection and provide support to all levels and partners of the Service in drugs and chemicals handling and management;
- Collaborating with the HRD Division to constantly appraise and develop appropriate capacity for drugs and logistics management personnel for all the relevant/appropriate units of the health service;
- Maintaining a national information base on the national drugs and supply situation of GHS;
- Undertaking periodic drug education campaigns in collaboration with the PH and ICD Divisions.

2.1.7 Finance Division (FD)

The finance division ensures that financial records and reports are prepared accurately and timely. They work in conjunction with PPMED for preparation of budget estimates as well as develop and promote mechanisms to Support and Monitor the Financial performance of all Health Divisions Levels and Institutions. The division collates and prepare Periodic Financial reports for the GHS and also ensures the timely transfer of GOG and external Donor Funds to all levels of the GHS. Additionally, they provide financial management information to officers of the GHS, the donor community, MOH and external agencies. The finance division develops and promote efficient and effective accounting systems within the GHS and provides effective cost management systems and ensure the proper control and valuation of stocks held by the GHS. They also institute financial management policies, systems and controls to safeguard assets of the Service, assure accountability and promote efficiency as well as assure the integrity, completeness and timeliness of financial data from all divisions and units and undertake physical verification of stocks and accounts in any unit of GHS at any time.

2.1.8 Internal Audit Division (IAD)

The internal audit department is responsible for overseeing the finances and compliance issues as well as reviewing performance levels. Their functions include:

- To verify and ensure that financial statements are the true reflection of underlying books and records;
- To verify that Financial Reports and records preparation tasks are performed only by officers acting within the scope of their Authority;
- To verify compliance to Policies of the GHS;
- To verify that official documents are kept in secured places and are easily retrievable.
- To verify documents and stores;
- To verify whether expenditures conform to stated objectives and activities for which funds are released;
- To prepare periodic audit reports.

2.1.9 Family Health Division (FHD)

The Family Health division is responsible for the development of strategies and plans for the provision of maternal, adolescent, child and reproductive health and nutrition services through innovative and effective means. It also monitors the implementation of Programmes and projects that have been initiated by GHS and other collaborating partners to ensure consistency and effectiveness.

2.1.10Operational Research Division (ORD)

The operational research division is responsible for the coordination and conduct of all operations research to serve the GHS and the Health Sector as a whole. It's also responsible for setting up the agenda for research and assisting in the training and capacity building in area of Health Research. It will also coordinate the operations of the satellite research sections (including Regional and District Operational Research Units).

2.1.11GHS Interfaces

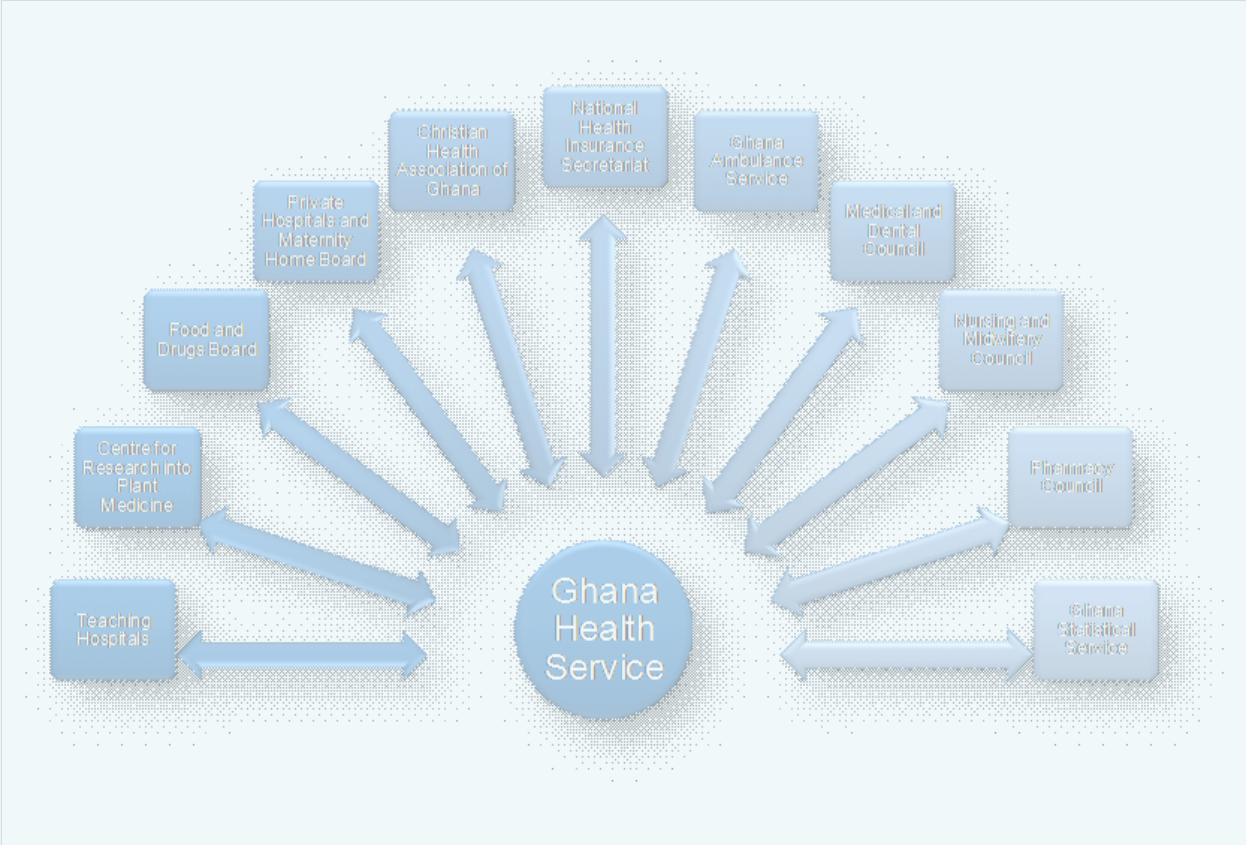


Figure 1: GHS Interfaces

Currently, the GHS implements the government's national Healthcare policies by providing services, the coordination of which comes under the control of the Director General. The GHS interfaces the following agencies in providing its mandated services:

- **The Medical and Dental Council**: ensures the highest level of training of Medical and Dental Practitioners and prescribes and enforces the highest standards of professional conduct. The council also determines the adequacy and quality of service facilities, promotes Continuing Medical Education and protects the rights of the patients and clients. Among the key activities of the council is the registration of Medical and Dental Practitioners both locally and foreign trained, and those on short programmes in the country and the inspection and accreditation of Medical and Dental Schools and Institutions for Housemanship Training.
- **The Ghana Ambulance Service**: aims at providing accessible 24-hour ambulance service nationwide through its own ambulance service and by collaborating with other service providers such as the Fire Service and other hospital-based ambulances. The service also provides improved pre-hospital care in accidents, emergencies and disasters. To facilitate such activities, the service generates timely, complete and accurate information for the efficient operations of the service and ensures the provision of rapid

response for persons involved in accidents, emergencies and disasters. As part of its mandate, the Ghana Ambulance Service promotes first aid training to the public and collaborates with other emergency services in national disaster planning.

- **The Nurses and Midwives Council**: focuses on the training of nursing and midwifery personnel for health care delivery. Their key objective is to ensure that there are enough competent nursing and midwifery human resources at every level of the healthcare delivery system, delivering safe and efficient care. The Council also ensures that these nurses practice in appropriate environment. To meet these requirements, the council has oversight responsibility for the training of nurses and midwives and prescribes conditions of registration of nurses and midwives. Other responsibilities include verification of registration/licensure, orientation of foreign-trained nurses and midwives, and supervising nurses and midwives at both public and private health facilities.
- **The Pharmacy Council**: is primarily responsibility for ensuring the highest standards in the practice of pharmacy in Ghana. This is done by assuring competence of service providers through licensing of personnel and prescribing standards of Practice for them. The council also ensures a reliable medicine supply and distribution system and promotes rational use of drugs. Such responsibilities are also executed through licensing of premises, inspections and enforcement of standards through monitoring.
- **The Food and Drugs Board**: control the manufacture, importation, exportation, distribution, use and advertisement of all food, drugs, cosmetics, medical devices and household chemical substances in the country. Among its specific duties are the registration of products and manufacturing facilities and the control of importation and exportation of such commodities. The Board also undertakes safety monitoring, post market surveillance and product promotion including allocations of narcotics and psychotropic substances ensuring their safety, quality and efficacy.
- **Teaching Hospitals**: provide tertiary and specialist services and act as the main referral centers in the country. Apart from the teaching responsibilities, each of the Teaching Hospitals has a number of centers of excellence that provide services to patients from Ghana and other countries.
- **The Christian Health Association of Ghana**: coordinates activities and services provided at mission hospitals in the country. Among its responsibility is to ensure that services delivered meet standards approved by the Health Sector Laws.
- **The Private Hospitals & Maternity Homes Board**: deals with issues of registration and monitors service delivery within the private health facilities. These include hospitals, health centres, clinics and maternity homes. While other agencies deal with the human resource, the board ensures that these facilities are manned and function according to standards. The board thus registers and renews the registration of these facilities.
- **The Centre for Research into Plant Medicine**: is a WHO Collaborating Centre for Research and Development of Traditional Medicine. Its main business is to conduct and promote scientific research in herbal medicine through its own research activities and by

providing technical support to institutions and individual herbalists. Among the key responsibilities of the centre is the collation of information on indigenous knowledge on herbal remedies and the establishment of arboreta across the country.

- **The Ghana Statistical Service**: conduct surveys to obtain statistical figures such as Census, Demographic and Health Surveys. They also make sure statistic information are up to date and reflects the prevailing situation.
- **National Health Insurance Secretariat**: administer the National Health Insurance Scheme respectively but is not Departments or Agencies under the Ministry of Health.

All of these service-providing/inspection/monitoring agencies operate in collaboration with the GHS.

2.2 CURRENT STATE TECHNOLOGY ANALYSIS

Currently the most widely used application software by the GHS to execute its processes is the Microsoft Office Productivity tools (Word, Powerpoint, Excel and Access) deployed on local Personal Computers (PC) and a few servers scattered around the offices. There are no central Data Centre facilities to host business applications for the GHS. There is a Microsoft Access database which holds sector performance indicators and data used for Monitoring and Evaluation processes. The Service is therefore considered to be a "Greenfield" site from business applications standpoint. The Service has PCs and laptops running Microsoft Office 2000 and 2007 with windows XP and Vista. There was information on the number of desktops, laptops and servers and their models at the time of writing. It is understood that contracts have been awarded to technology providers to implement the necessary infrastructure and business applications at some of the main Regional hospitals but there was no detailed information on technologies deployed at the time of writing.

The GHS has deployed a limited Wide Area Network infrastructure to provide connectivity for the stores and there are plans to expand this infrastructure to the districts to connect all sites and offices.

3. SWOT Analysis

Table 1 below is a SWOT analysis of the GHS captured during the analysis of the current state.

Table 1: SWOT Analysis

	Helpful to Achieving Objectives	Harmful to Achieving Objectives

Internal Origin (Attributes of GHS)	**Strengths:** 1. Good collaboration with statutory agencies 2. Good leadership 3. Current state business processes defined	**Weaknesses:** 1. No solid ICT organization in place 2. WAN/LAN infrastructure network and support inadequate 3. Lack ICT expertise and skills 4. No business applications and SQL compliant databases in place 5. Lack of consistent strategic ICT strategy for improvement 6. Electronic Health Records not in place 7. Skills gaps: e.g. Management Information Reporting/Analytics 8. Automatic data exchange with statutory agencies 9. Low ICT headcount
External Origin (Attributes of the Environment)	**Opportunities:** 1. Adoption of EA to improve ICT 2. Introduction of new technologies to automate business processes 3. eGhana transformation philosophy to improve business functions of the GHS 4. Consolidation and leveraging national ICT Shared Services 5. The introduction of ICT Governance model for increased accountability	**Threats:** 1. Weak national infrastructure backbone 2. Competition for national ICT resources 3. Lack of funds for major ICT deployments 4. Financial constraints 5. Regulatory and legislative developments 6. Lack of accountability in technology selection/evaluation process

RECOMMENDATIONS SUMMARY

To transform GHS through technology enablement a gap analysis was conducted in conjunction with the SWOT analysis and a summary of the recommendations that will drive the GHS EA are provided below:

- Improving health information exchange. Data exchange between the GHS and other agencies such as NHIA is not effective and causes delays in processing transactions and managing Healthcare. There is a need for robust Health Information Exchange (HIE) and Clinical Data Exchange (CDE) mechanisms that will ensure timely and secure transfer of information between the GHS and the other agencies, within the GHS and with international bodies such the WHO.
- The GHS currently lacks industrial strength applications to automate core business processes. There is a need for the introduction of best in class applications to automate business processes such as Logistics, Policy Management, Research and Development, Human Capital Management, Finance, etc.

- The lack of a robust network infrastructure limits the GHSs ability to collaborate effectively internally and externally with other agencies. There is a need for a Government wide Wide Area Network infrastructure to enable collaboration across Government.
- In terms of security, the challenge is to help keep data safe. This means not only ―locked away‖ but also guarded against misuse, unauthorized access, malicious amendment and the consequences of computer failure and malfunction. A key factor is establishing and verifying the identity of users and their authority to access specific systems and patient data.
- In terms of interoperability, the challenge is to draw together accurate, relevant data from many diverse sources and systems and to present that data in a coherent, fit for purpose, format. Further the capability of carrying out a single business process across many systems and ensuring complete and accurate execution is required.
- In terms of privacy, the challenge is to help make patient-related data available at point of need to those, and only those, with a need to know. The patient has the right to restrict his or her information to the healthcare professionals of his or her choosing and further to help control the availability of sensitive information. When used outside a legitimate patient–professional care relationship, health data must be made anonymous to help prevent identification of the patient.
- In terms of legacy, the challenge is to use the capabilities and data managed by the many thousands of exiting healthcare systems. This use must be ―seamless to the user and extends the challenge of interoperability, mentioned above, to existing applications.
- In terms of trust, the challenge is to help ensure that all data recorded, stored, retrieved and presented is in context, accurate, timely and relevant; and may be relied upon in making decisions that are literally matters of life or death. Similarly, requests for action must happen, quickly, accurately and completely with appropriate confirmations. Only by establishing trust, will systems be used and the necessary critical mass of data formed that will provide the desired foundation for electronic healthcare services.

4. Future State Enterprise Architecture

This section describes the recommended future-state EA that will enable the GHS to improve its services to the people of Ghana. As dictated by the Ghana Government Enterprise Architecture

framework, it is recommended that the GHS defines a future-state EA based on Service Oriented Architecture (SOA) to facilitate the orchestration of multiple systems elements (e.g., applications, services, interfaces) across the various departments.

SOA is a strategic architectural framework that will support and enable true business agility, enabling GHS to develop and deploy applications quickly and reduce applications development and maintenance costs.

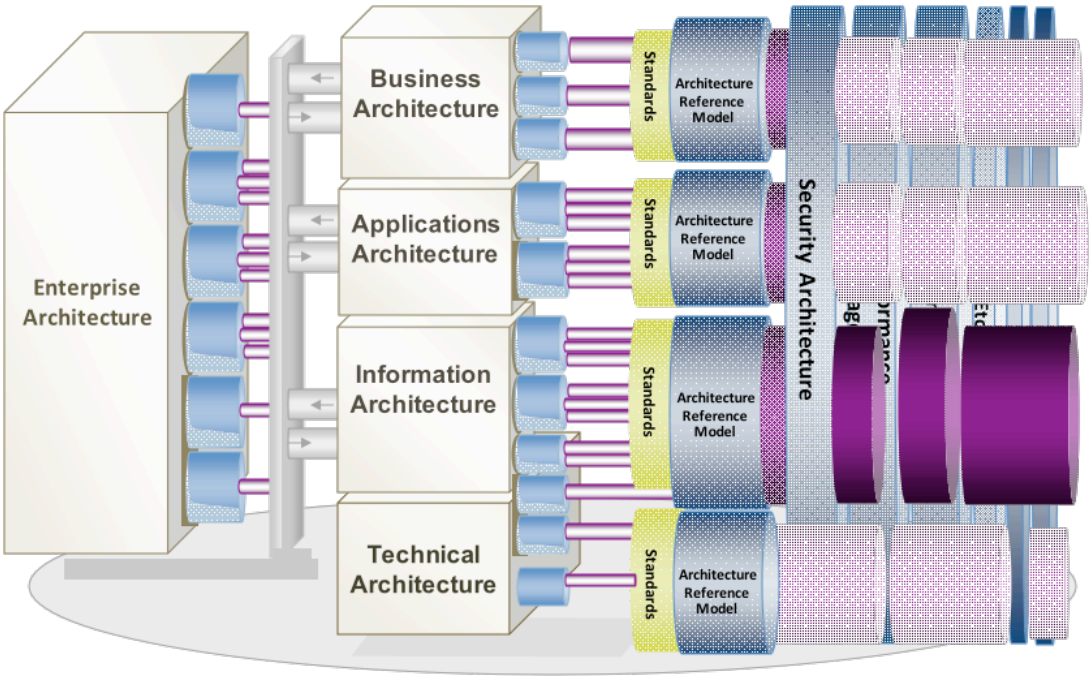


Figure 2: Enterprise Architecture Framework

As illustrated in figure 2 the four main architecture perspectives for the GHS EA are:

- Business Architecture – This describes how the Service's business works. It will include:
  - The GHS's high-level goals and objectives;
  - The GHS's services;
  - The functions and the cross-functional activities embodied in business processes;
  - Major organisational structures and the interaction of all these elements.

  The business architecture includes broad business strategies along with plans for moving the GHS from the current state to the future state.
- Application Architecture - defines the application portfolio. It includes:
  - Descriptions of the automated services that support the business processes presented in the business architecture;
  - Descriptions of the interaction and interdependencies (interfaces) of the organisation's application;

- Priorities for developing new applications and revising old applications based directly on the business architecture.

The application architecture represents the services, information, and functionality that cross organisational boundaries, linking users of different skills and functions to achieve common business objectives.

- Data Architecture - describes what the Service needs to know to run its business processes and operations. It includes:
  - Standard data models;
  - Data management policies;
  - Descriptions of the patterns of information consumption and production in the GHS.
- Technical Architecture - lays out the hardware and software supporting the GHS and the shared services. It includes:
  - Desktop and server hardware;
  - Operating systems;
  - Network connectivity components;
  - Printers;
  - Modems;
  - Other necessary peripheral devices.

  The technical architecture provides a logical, vendor-independent description of infrastructure and system components that is necessary to support the application and information perspectives. It defines the set of technology standards and services needed to execute business goals.

Although there are four perspectives, there is only one GHS EA. The value of the EA is not in any one individual perspective but in the relationships, interactions, and dependencies among perspectives. The development of these four architecture perspectives and the examination of their individual and collective interactions reveal the information that the GHS requires for ICT implementation and purchasing decisions, and provides a powerful communication tool between the ICT and business units of the organisation.

Other areas considered as part of the GHS EA are the Security Architecture and Government Model to support the management of ICT at the Service.

4.1Business Architecture

This section describes the future state of the GHS business architecture.

4.1.1 Business Architecture Principles

1. **Principle: Primacy of principles**

   These principles of information management apply to all organizations within the enterprise.

   Rationale:

   The only way to provide a consistent and measurable level of quality information to decision makers is if all departments abide by the principles.

   Implications:

   - Without this principle, exclusions, favouritism, and inconsistency would rapidly undermine the management of information.
   - Information management initiatives will not begin until they are examined for compliance with the principles.
   - A conflict with a principle will be resolved by changing the framework of the initiative.

2. **Principle: Maximise benefit to the enterprise**

   Information management decisions are made to provide maximum benefit to GHS as a whole.

   Rationale:

   This principle embodies "Service above self." Decisions made from a Service-wide perspective have greater long term value than decisions made from any particular departmental perspective. Maximum return on investment requires information management decisions to adhere to Service-wide drivers and priorities.

   Implications:

   - Achieving maximum Service-wide benefit will require changes in the way the organisation plans and manages information. Technology alone will not bring about this change.
   - Some departments may have to concede their own preferences for the greater benefit of the entire GHS;
   - Application development priorities must be established by the entire GHS for the entire GHS;.
   - Applications components should be shared across organisational boundaries;

3. **Principle: Information management is everybody's business**

   All departments in the GHS participate in information management decisions needed to accomplish business objectives.

   Rationale:

   Information users are the key stakeholders, or customers, in the application of technology to address a business need. In order to ensure information management is aligned with the business, all departments at the Service must be involved in all aspects of the information environment. The business experts from across the Service and the technical staff responsible for developing and sustaining the information environment need to come together as a team to jointly define the goals and objectives of information technology.

   Implications:

   - To operate as a team, every stakeholder, or customer, will need to accept responsibility for developing the information environment.
   - Commitment of resources will be required to implement this principle.

4. **Principle: Business Continuity**

   The Service's operations are maintained in spite of system interruptions.

   Rationale:

   As system operations become more pervasive, the Service becomes more dependent on them, therefore, must consider the reliability of such systems throughout their design and use. Business premises throughout the Service must be provided the capability to continue their business functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop business activities. The business functions must be capable of operating on alternative information delivery mechanisms.

   Implications:

   - Dependency on shared system applications mandates that the risks of business interruption must be established in advance and managed. Management includes but is not limited to periodic reviews, testing for vulnerability and exposure, or designing mission-critical services to assure business function continuity through redundant or alternative capabilities.
   - Recoverability, redundancy and maintainability should be addressed at the time of design.
   - Applications must be assessed for criticality and impact on the Service's mission, in order to determine what level of continuity is required and what corresponding recovery plan is necessary.

5. **Principle: Common use applications**

Development of applications used across the Service and the statutory agencies is preferred over the development of similar or duplicative applications which are only provided to a particular organisation.

Rationale:

Duplicative capability is expensive and proliferates conflicting data.

Implications:

- Departments which depend on a capability which does not serve the entire Service must change over to the replacement Service-wide capability. This will require establishment of and adherence to a policy requiring this.
- Departments will not be allowed to develop capabilities for their own use which are similar/duplicative of Service-wide capabilities. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.
- Data and information used to support Service decision making will be standardised to a much greater extent than previously. This is because the smaller, departmental capabilities which produced different data (which was not shared among other organisations) will be replaced by Service-wide capabilities. The impetus for adding to the set of capabilities may well come from an organisation making a convincing case for the value of the data/information previously produced by its departmental capability, but the resulting capability will become part of the Service-wide system, and the data it produces will be shared across the Service.

6. **Principle: Compliance with Law**

   Information management processes comply with all relevant laws, policies, and regulations.

   Rationale:

   The Service's policy is to abide by laws, policies, and regulations. This will not preclude business process improvements that lead to changes in policies and regulations.

   Implications:

   - The Service must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of data.
   - Education and access to the rules. Efficiency, need and common sense are not the only drivers. Changes in the law and changes in regulations may drive changes in our processes or applications.

7. **Principle: ICT Responsibility**

The ICT department is responsible for owning and implementing ICT processes and infrastructure that enable solutions to meet user defined requirements for functionality, service levels, cost, and delivery timing.

Rationale:

Effectively align expectations with capabilities and costs so that all projects are cost effective. Efficient and effective solutions have reasonable costs and clear benefits.

Implications:

- A process must be created to prioritise projects
- The ICT function must define processes to manage business unit expectations
- Data, application, and technology models must be created to enable integrated quality solutions and to maximize results.

4.1.2 GHS Business Process Model

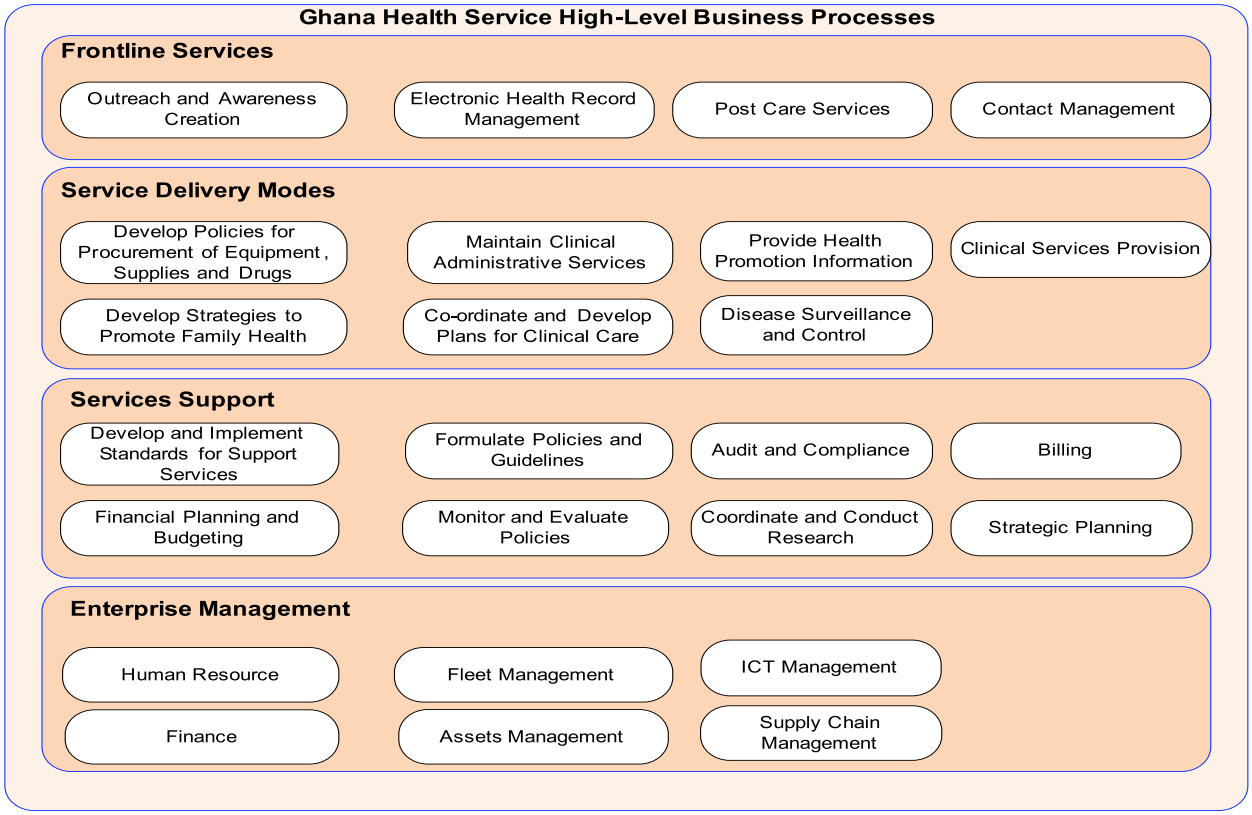


Figure 3: Contextual Business Architecture

Figure 3 depicts the contextual business process model of the GHS. The business processes are based on the 'as is' situation of the Service. The future state process model is identical to the current state. The processes are segmented into Frontline Services, Service Delivery Modes, Service Support processes and Enterprise Management. The high level business processes as defined in the various segments are:

4.1.2.1Frontline Services

Frontline services are business processes that interact more with the customer. Customers' needs and enquiries are captured with the appropriate guidance offered. Campaign and service offerings are promoted and provided. They are:

- **Outreach and awareness creation** – the GHS will produce and manage health information as well as use collaborative strategies to create awareness. The GHS by this monitors the impact of public health field programmes and projects to ensure the dissemination or awareness creation is carried out effectively. They also develop early warning system for epidemics.
- **Electronic Health Record Management** – this is the use of modern information and communication technologies to capture, process and manage health records of citizens, patients, healthcare professionals, healthcare providers, as well as policy makers
- **Post Care Services** – the GHS can collaborate with its clients through the various communication channels to provide post care services such as Billing services, e.g.: patient calls to doctor's office to clarify bill, Follow-up care, e.g. appointment scheduling and appointment reminders, etc.
- **Contact Management** - is the means by which citizens and businesses will contact the GHS about specific programmes or lodge complaints about services provided by statutory health care providers. Contacts will be made via email, telephone, mobile phone and Web Portal.

The desired future state for the Frontline Services will include:

- 100% (or nearly so) paperless Electronic Health Record;
- The patient owns and oversees the content of and access to their Electronic Health Record;
- Standard data model and clinical syntax across the national health system;
- Seamless integration of clinical care activities with data capture and review;
- Thoughtful deployment of edge technologies such as RFID, mobile applications and platforms, biometric authentication, etc.;
- Support for surge capacity and management;
- Integrated patient / caregiver communication and collaboration;
- Predictive modelling tools to enhance care management functions.

4.1.2.2Service Delivery Modes

This category involves the business processes that describe how services would be delivered. Processes here depict the mode of providing the core services the service seeks to offer. They are:

- **Develop Policies for Procurement of Equipments, Drugs and Supplies**: these processes enable the GHS develop long, medium and annual procurement plans consistent with the national GHS strategic plans of action. They also enable the GHS to liaise with both government and international procurement agencies for the purposes of procuring drugs and equipments for the GHS consistent with national and international procurement laws.
- **Maintain Clinical Administrative Services**: the processes enable GHS develop and consistently introduce contemporary administrative systems in collaboration with other Divisions and Regions to enhance institutional efficiency and cost efficiency in GHS. It includes administrative functions such as clinical staff and resource management, inpatient (e.g. nursing), scheduling, workload management; continuing medical education of physicians, nursing, etc
- **Provide Health Promotion Information:** the GHS provide and manage public health information, as a decision support system, for effective decision-making on healthcare in the country;
- **Clinical Services Provision**: the GHS develop standards and protocols to ensure quality, effectiveness and efficient service delivery. The GHS also support, monitor and evaluate quality assurance programmes and projects in collaboration with the Regions, Districts and sub-districts with a view to promoting total quality in program effectiveness and efficiency. This includes diagnosis examination processes and scheduling (e.g. radiology, cardiology, etc), assessments, requests to pharmacy, laboratory testing and reporting, therapeutic support, adverse event management, medication dispensation, clinician consultation, etc.
- **Develop Strategies to Promote Family Health**: the GHS is responsible for the development of strategies and plans for the provision of maternal, adolescent, child and reproductive health and nutrition services through innovative and effective means. It also monitor the implementation of programs and projects with other collaborating partners to ensure consistency and effectiveness
- **Coordinate and Develop Plans for Clinical Care**: at the national level the GHS maintain processes for coordinating, supervising, monitoring and developing clinical services in collaboration with healthcare professionals, professional associations and facility regulatory bodies.
- **Disease surveillance and Control** – the GHS carryout surveillance on disease outbreaks and outline modes of their prevention. This is done by collecting, analysing, interpretation and dissemination of information to the citizens regarding disease outbreak.

4.1.2.3Services Support

These set of business processes support the organisation in delivering service to its customers. This includes processes that are aimed at making sure operations are matched up to standards and also to determine performance level of collection processes and strategic planning. They are:

- **Develop and Implement Standards for Support Services:** the GHS develop standards strategic to the support services to its customers. This is to ensure effective and efficient delivery of services in accordance to best standards available.
- **Formulate Policies and Guidelines:** the GHS ensure the development of comprehensive operational policies, sustainable strategic plans, systems; programmes and budgets to cover all of its activities as well as making sure the policies are consistent with Ministry of Health vision.
- **Audit and Compliance**: The audit and compliance system ensure that policies that are formulated meet required international standards to facilitate quality control and adherence across all channels and monitor integrity.
- **Billing**: the GHS perform all financial transactions that relate to the treasury and Ensure that due process is adequately adhered to in the processing, payment and receipts of all financial obligations of GHS
- **Financial Planning and Budgeting**: the GHS review and develop financial strategies, plan and prepare budgets for all levels. The GHS through its finance division develop and update plans for both capital and recurrent expenditure.
- **Monitor and Evaluate Policies**: the GHS periodically monitor the implementation of health policies, the utilisation of health resources, and the attainment of targets for coverage, utilisation of services and health status. The GHS also co-ordinate the publication of documents relating to Ghana Health Service activities (annual reports and other periodic reports) and ensure that the activities are properly documented and relevant information is disseminated.
- **Coordinate and Conduct Research**: the GHS coordinate and conduct all operations research to serve the GHS and the Health Sector as a whole. It also set up research agenda and assist in the Training and Capacity Building in area of Health Research

  Coordinate Satellite Research Sections (including Regional and District Operational Research Units)
- **Strategic Planning:** the GHS provide support to all levels in the development of comprehensive plans and budget for their various responsibility areas. It will also collate these plans into a comprehensive national operational plan based on the different formats that may be required of it.

4.1.2.4Enterprise Management

- **Human Resource Management** – this function is primarily managed by the Office of the Head of Civil Service but GHS must develop internal processes that will enable the Service to set and efficiently administer talent within the organisation through training. The Service must also develop the necessary mechanisms to attract and retain key performers.

- **Asset Management** – GHS must develop the necessary strategies that make it easy to define and manage assets. All assets must be captured in an inventory and attributes such as activities, or preventive maintenance schedules stored. Purchasing must be integrated with inventory to have a clear view about the approved repairers, suppliers and service providers that the Service usually deals with.
- **Fleet Management** – is the management of the Service's vehicle fleet. Fleet management includes motor vehicles such as cars, vans and trucks. GHS must integrate Fleet management functions such as vehicle financing, vehicle maintenance, vehicle telematics (tracking and diagnostics), driver management, fuel management and health & safety management. The Service must remove or minimise the risks associated with vehicle investment, improving efficiency, productivity and reducing the overall transportation costs, providing 100% compliance with government legislation (duty of care) etc.
- **Finance –** this function includes the preparation of the General Ledger; Accounts Payable; Fixed Assets; Cash Management; Accounts Receivable and Budgeting.
- **Supply Chain Management** - the GHS must streamline the complete procure-to-pay business processes by offering the broadest set of capabilities for procurement professionals, employees and suppliers, including global spend analysis, sourcing, desktop requisitioning and receiving, electronic invoicing, payments, and supplier collaboration.
- **ICT management**: The processes which develop and operate Information and Communications Technology, Systems and Services aligned to business needs.

4.2Applications Architecture

The future state Applications Architecture for the GHS defines an applications portfolio designed to automate the business processes of the Service. It serves to identify and classify the applications components that will support the Service and its interaction with the agencies.

4.2.1 Applications Architecture Principles

1. **Principle**: Technology Independence

   Applications are independent of specific technology choices and are not dependent on specific hardware and software platforms.

   Rationale:

   Independence of applications from the underlying technology allows applications to be developed, upgraded, and operated in the most cost-effective and timely way. Otherwise technology, which is subject to continual obsolescence and vendor dependence, becomes the driver rather than the user requirements themselves.

   Implications:

   - This principle will require standards which support portability. As the GHS will be deploying commercial off the shelf (COTS) applications, there may be limited current choices, as many of these applications are technology and platform dependent.
   - The applications will be Web based and Application Programming Interfaces (APIs) will be used wherever necessary to enable applications to interoperate. Middleware technologies will be used to decouple applications from specific software solutions.

2. **Principle:** Ease of Use

   All applications must be easy to use. The underlying technology must be transparent to users, so they can concentrate on performing business tasks.

   Rationale:

   Ease of use is a positive incentive for use of applications. It encourages users to work within the integrated information environment instead of developing isolated systems to accomplish the task outside of the GHS's integrated information environment. Most of the knowledge required to operate one system will be similar to others. Training is kept to a minimum, and the risk of using a system improperly is low.

   Implications:

   Applications will have a common "look and feel" and support ergonomic requirements. Hence, the common look and feel standard must be designed and usability test criteria must be developed.

4.2.2 Logical Applications Architecture

The GHS's logical architecture defines a multi-channel strategy that addresses the Service's objective of initiating and formulating ICT policies and programmes taking into account the needs and aspirations of the people of Ghana.

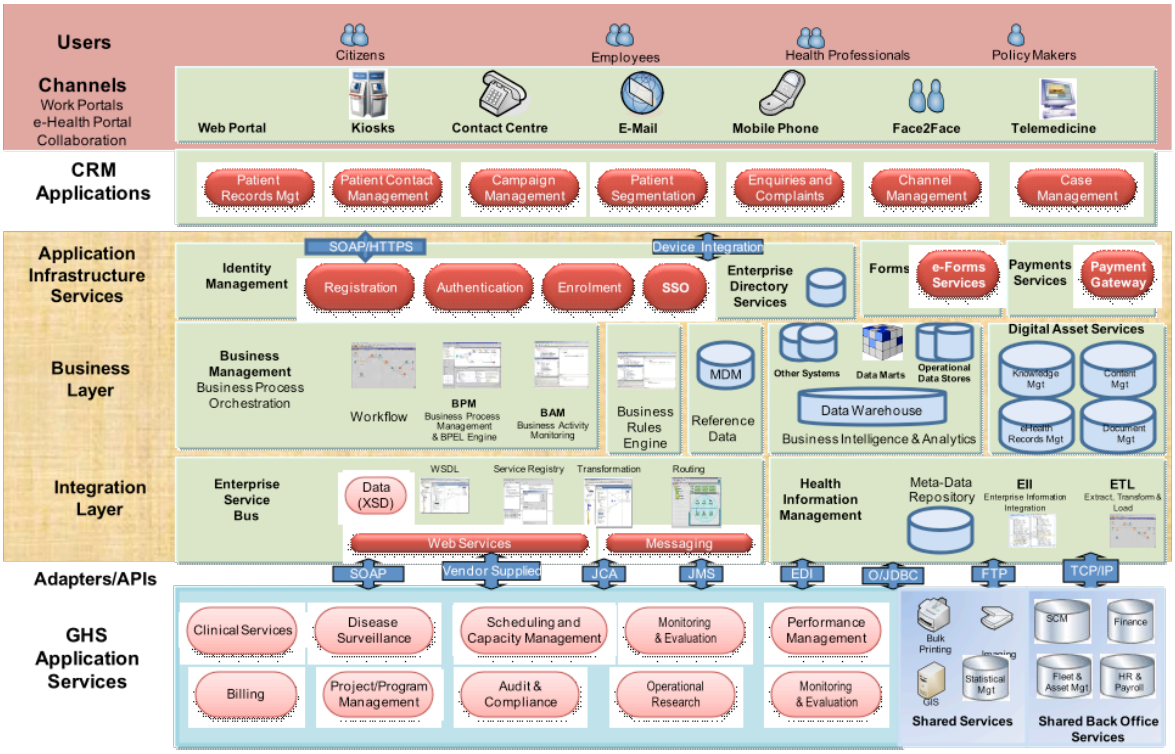


Figure 4: GHS Applications Architecture (e-Health Architecture)

The application infrastructure services layer provides technical and administrative services such as Identity Management and enterprise directory services. The shared infrastructure service layer shows how the Service's assets will be accessed by the various directorates through the registration, authentication, enrolment and Single-Sign On.

The Service integration layer is responsible for exposing the services in the architecture in a consistent manner while enabling services to be implemented in a variety of technologies. The Applications layer shows groupings applications for specific purposes. By leveraging services available in the architecture, applications should generally be quicker to develop and easier to maintain. The architecture also harnesses on the shared application services across government which has already been recommended in the GGEA architecture.

4.2.3 Applications Users

There are effectively four main types of users of the GHS e-Health solutions:

1. Patients are defined as citizens, resident aliens, short term visitors and tourists in need of or receiving medical attention, care, or treatment.

2. Healthcare professionals include doctors, nurses and allied health professionals. Doctors would include general practitioners, physicians and surgeons. Nurses would include hospital, community and specialised nurses, such as cancer care nurses. Allied health professionals, who usually need formal training and accreditation before they are employed, would include, for example, medical assistants, dental hygienists, physio and occupational therapists, laboratory technicians, medical equipment technicians, radiographers, medical secretaries, and medical coders to name but a few.
3. Employees are users who work for the healthcare providers such as hospitals, clinics, medical practices, laboratories and other organizations that accommodate and treat patients. They will provide physical premises and facilities and operate medical and other equipment. They will operate administrative and clinical systems. They will employ healthcare professionals. Policy
4. Makers and Legislators are government, quasi-government organizations and professional bodies responsible for the provision of healthcare services on a national or regional basis. This would include the enactment of legislation, the provision and control of funding and the setting and governance of professional standards of care and process.

Other participants, not shown explicitly in the model for simplicity, include:

- Health plans and insurance companies such as National Health Insurance Secretariat;
- Private healthcare providers and affiliate bodies such as Nurses and Midwives Association, Dental Association, etc.;
- Bio-surveillance, hazard control, population health and intelligence agencies such as the Ghana Statistical Service;
- Medical research bodies such as Centre for Scientific and Industrial Research;

The interaction between these main groups, can be can be categorised as follow:

- **Patient to Doctor Interactions**: typically concerned with episodes of patient care or treatment. These interactions are subject to stringent confidentiality requirements including the observance of specific doctor to patient professional and ethical relationships;
- **Patient to Hospital Interactions**: typically concerned with administrative transactions such as the making of appointments, attendance at out-patient clinics and hospital admissions and discharges;
- **Patient to Government Interactions:** typically concerned with registration for national and regional services and initiatives such as screening programmes and community-based care activities. Citizens often will pay for their health service either through the NHIS or directly;
- **Patient to Patient Interactions**: typically concerned with self-help groups and community-based activities including social services. This group includes charitable groups and activities such as The Ghana Heart Foundation and other tertiary-care

initiatives. We would include insurers in this set of interactions in so far as they trade with citizens and may represent patients in the arrangement of suitable care and treatment.

- **Patient to System Interactions**: typically concerned with the setting and maintenance of patient supplied data such as some demographic details, family information and, importantly, the viewing and variation of consent data for patient data access.
-
- **Doctor to Hospital Interactions**: typically falling into two types – administrative activities around engagement and assignment to particular roles and responsibilities, and clinical activities associated with patient care and treatment such as requests for tests and imaging and the use of specialized facilities and equipment.
- **Doctor to Government Interactions**: under the term government we include not only national and regional bodies but also professional bodies concerned with registration of healthcare professionals and the setting and observance of professional standards of care;
- **Doctor to Doctor Interactions**: typically concerned with the referral of patients for further examination and treatment; case reviews and triage; peer knowledge and information sharing; and the delegation of care as well as the organisation and management of clinical groups and specialist teams.
- **Doctor to System Interactions:** typically concerned with the viewing and maintenance of permissions to access patient data and the creation, updating and audit of the patient care record.
- **Hospital to Government Interactions**: typically concerned with funding and audit, the measurement and improvement of performance and monitoring of standards of care.
- **Hospital to Hospital Interactions**: which are many and varied covering patient administration and clinical care, the management of facilities and the provision of specialist services such as laboratories, imaging systems and specialist diagnostic equipment. Independent services such as dentists, opticians and pharmacies may also be included in this grouping.
- **Hospital to System Interactions**: typically concerned with the recording of activities such as patient attendance; maintenance of waiting lists; the scheduling of teams and facilities; and the recording of examination and test results.
- **Government to Government Interactions**: include the overall definition, planning and execution of national policy; the administration of the national service including the setting and monitoring of national targets and budgets; the definition and management of national programmes; and the definition and monitoring of disease-specific service frameworks and guidelines.

- **Government to System Interactions**: typically concerned with the set-up and maintenance of national administrative facilities; standard procedures and coding systems; and the setting of targets and budgets.

4.2.4 Available Channels

The channel layer highlights the various mechanisms that the Service can deliver services to its recipients. The strategy meets the government's e-Health requirements by providing services that are flexible, accessible, complete, easy and secure from different channels. The implementation of the GHS channel strategy will include user profiling that will show the different segments such as meeting requirements of the uneducated citizen or a disabled person and how a user's channel preferences are influenced by circumstances such as the nature of the service required, or his/her need for direct, person-to-person interaction.

The web Portal will be in two forms: the outer facing Portal which will be used by the public and the Intranet to be used by employees of the Service, healthcare professionals and makers of policy and legislation. The outer facing Portal will provide the public with information about the Service whilst the Intranet will be used by employees to gain access to internal ICT services and applications. The increasing use of wireless technologies can be harnessed for health administrators through the use of PDAs and citizens through mobile telephones. This will enable the decision makers to be able to have access to the Internet and information and also respond to critical issues and make timely decisions.

4.2.5 GHS Enterprise Portal

GHS will develop a secure Intranet using a leading Portal solution that emphasises centralised security for authentication, authorisation and administration. The secure Portal should be able to integrate with applications to automate business processes and enable collaboration between employees and stakeholders such as citizens, businesses and NGOs.

Collaboration will enable interaction between users including e-mail, virtual team meetings, e-learning, instant messaging, and workflow processes.

The Intranet will serve as an employee workplace that focuses on providing employees with a highly efficient work environment characterised by self-service access to business application services, and to collaboration services that improve the ability of employees to collaborate with each other.

It is also important for the Portal to integrate with existing information systems and business applications. Information aggregation will allow users to access and manipulate large amounts of data collected from multiple sources. It brings together data from disparate data sources into a single view, targeted to specific users and groups.

The Internal facing Portal will have the following features:

- **Home page display and user log-in** - a user enters the Uniform Resource Locator (URL) of the Portal and is presented with the Portal front page designed for initial citizen enrolment/registration to use government services online. The Portal will also have a home page designed for unauthenticated users (including a login link). The user uses the login link to provide a user ID and password, and after successful authentication his/her personal Portal home page is displayed based on personal profile information provided for the initial registration;
- **Search for and display content** - the Portal provides the ability to search content provided by various (internal and/or external) sources. The search is carried out on an index that will be pre-built, rather than directly on the content itself. The search can be free-text based, keyword based, or category based. Search results can be filtered based on the user's identified type;
- **Access GHS' applications services and data** - a fundamental concept of the Portal is that it will provide a Single Sign-On (SSO) capability to simplify access to applications and data. The Portal will provide access to the GHS application services and data that is external to the Portal, and has been "registered" with the Portal system as a trusted provider of information and/or application services.
- **User updates personal information** - a user can use the Portal to update some of his/her personal information, such as address, phone number and e-mail address (note that this is personal information, rather than personal preferences). The same actions can also be taken by a Contact Centre staff of the GHS on the citizen's behalf, in which case a chat transcript may be generated and saved;
- **User updates his/her Portal preferences and personalises his/her Portal home page** - the user updates personal preferences in order to make the Portal more effective to use. The user updates personal preferences that control what is shown on his/her Portal home page. An example would be the list of hot links that are displayed on the home page, making the home page more efficient for the user;
- **Submit an inquiry**. - this use case makes use of asynchronous collaboration to allow a user to submit an inquiry such as search for training topics and get a response later without needing to interrupt the flow of their activities. This allows the user to continue with other activities while the inquiry is being handled;
- **Hold an impromptu e-meeting** - The Portal must enable the different project teams, employees and citizens to collaborate through a chat or e-meeting feature. This type of collaboration is synchronous, with users interacting in real time, and requires that all participating users be online and available;
- **Create and manage content –** the GHS will identify key content contributors who will participate in the process of creating and approving content. Display of GHS informational content (text, images and rich media) is one of the major features of the Portal. Depending on the authorisation level of a content "consumer", some or all of a

particular piece of content can be displayed. This personalises the user's experience, and also prevents unauthorised users from accessing certain types of information;

- **Executive dashboards**: presenting scorecards with performance metrics (KPI) sourced from database to expose trends and patterns for consolidated patient and process data and staff administration to monitor training compliance;

- **Collaborative workspaces and portals** - with document and records management; search for secure, real-time access of relevant patient data across multiple departments;

- **Web 2.0** - is a paradigm shift in how the Internet is utilised to provide its service. This new World Wide Web technology refers to changes in the ways in which the Portal will be utilised by the end-users. In essence it will enhance creativity, collaboration and information sharing between government and citizens. Web 2.0 applications include Wikis, Blogs, Mashups, and RSS feeds;

    - Wikis - are virtual workspaces where individuals can access documents, spreadsheets and presentations for various collaborative projects. Wikis enable records management by providing documented logs of revisions, when the revision was made and the name of the person who made the change. Wikis allow edits to be made the second a document is authored;

    - Blogs - (or We**b log**) is a web site that contains regular entries or events and comments as well as other material like graphics or video. Blogs can be on particular subjects or events or simply be personal online diaries. They often combine text, images, links to other blogs, web pages and other media related to its topic;

    - Mashups - is a web application that combines data from more than one source into a "single integrated tool" (Wikipedia). Mashups can be used to gather data from RSS feeds and other origins and deposited into one environment for analysis. This web 2.0 application works best with AJAX;

    - RSS Feeds - (short for Really Simple Syndication) is an XML file that can be read by special feed reading software or a web service. When the address is entered into the address bar, it displays a synopsis of the information and a link to the original page. This reduces the number of visits an end-user will make to the original site.

The external facing Web Portal is the most comprehensive and visible channel of the GHS. The external facing Web Portal will replace existing Web site by introducing additional features such as search capabilities to schedule appointments, place orders and make payments. It will also enable citizens to search for information most up to date treatments and healthcare trends.
Other additional features of the external facing Portal are:

- Delivering customised, targeted and aggregated view of information based on user's identity to generate contextual in-room information and get personalised disease management instructions;
- Automated reminders for users to securely change and modify data, such as rescheduling appointment times;
- Content-centric social computing capabilities and standardised Web conferencing to enable discussions between caregivers and patients;
- Alerts and reminders for making typical test and treatment recommendations and assisting patients in managing scheduled and recommended appointments.

4.2.6 Email

Electronic mail, often abbreviated email, is a means of writing, sending, receiving and saving messages over electronic communication systems. The GHS will utilise the government Secure email infrastructure to communicate internally and with other agencies. Citizens, businesses and other MDAs will have the capability to send, receive, forward, store, display, retrieve, prioritise, authenticate and manage messages, which may include any combination of data, text, audio, graphics, and images.
The GHS will be required to create email mailboxes for departments and projects, where email messages from the users will be delivered.

4.2.7 Wireless Technologies (PDAs and Mobile Phones)

The GHS applications architecture will provide a capability that will enable citizens to communicate with the Service to provide input into policy definition and also enable the Service to disseminate information to citizens. Mobile phone service provision, which is known as mobile government (mgovernment) is particularly suited for Ghana where Internet access rates are low but mobile phone penetration is growing rapidly, particularly in urban areas. Mobile phones are excellent access devices suitable for the transmission of information about services, disease control and general public information to citizens.

In this context wireless encompasses various portable cellular telephones and Personal Digital Assistants (PDAs) to be used by Policy Makers, Health Administrators and Directors of the MoH. The PDA will have emailing capabilities as well as ability to open documents (PDF, Word and Spreadsheets), calendaring, Internet access, etc on the move. This will enable senior officials to have management information at their finger tips for effective and timely decision making.

4.2.8 Self Service Kiosks

The GHS will deploy self service Kiosks to integrate with various information systems and hospital management systems to make the check-in and check-out processes more convenient for patients and to reduce costs and errors for the organisation.
The Kiosks at major regional hospitals will allow patients to confirm their scheduled appointments and to check in. At check out, patients can use the kiosk to schedule future appointments. Some Kiosks have features for payments allowing patients to use a debit/credit

cards to pay their hospital expenses at the Kiosk. This would be ideal if eZwich enabled Kiosks become available in Ghana for patients without NHIS cards to use the eZwich instead for payments.

Kiosks at the hospitals will minimise wait times and congestion at the front desk, reducing the need for clipboards. In addition, the Kiosk lessens the risk of patient misidentification and clerical errors at data entry. Patient check-in features streamline the process of checking patients in for hospital stays, laboratory visits, and/or physician office appointments.

Way-finding kiosks help patients find directions to specific facilities and locations. These Kiosks provide a convenience for patients and their families. The same Kiosk software can be accessed on Personal Computers by volunteers and staff to print easy-to-read directions for those who ask for directions. The Kiosk also provides a convenient channel for the MoH to disseminate information about government disease control programmes.

4.2.9 Telephony (Contact Centre)

This channel utilises the standard telephony device used to transmit and receive sound (most commonly speech), usually users calling specified telephone numbers of the GHS for advice or information.

The GHS will implement a national Contact Centre to handle centralised telephone call services for the GHS, the Contact Centre will deploy the following solutions to provide the services:

- Automatic Number Identification (ANI) – This transmits the citizen's telephone number and delivers it to the Contact Centre's telephone system. ANI can be very valuable because the calling number information can be used to identify citizens and look up contact history before an agent responds. This information will give the caller special treatment as specific cases could be routed to an elite group of agents, for example.
- Dialled Number Identification Service (DNIS) - the telephone network provides you with the number that the citizen dialled.
- Automatic Call Distribution (ACD) – technology is at the core of the Contact Centre service. When citizen calls arrive, they will be delivered to the ACD, which is a phone system that routes a large volume of incoming calls to a pool of waiting agents. It's different from other phone systems in that it makes use of telephone queues instead of extensions.
- Predictive dialling – is a device used to manage and launch large volumes of outbound calls to citizens. The dialler increases agent productivity by placing more outbound calls than the available number of agents. The dialler then sorts out answering machines, busy signals, and other non-human interactions before delivering live calls to the agents.
- Computer/Telephone Integration (CTI) - refers to a system of hardware and software that allows for communication between the telephone system and a computer system. A common and popular CTI application is the "screen pop," in which the system collects

the caller's telephone number and passes this information to the computer/telephone integration system. The CTI system then looks up the customer's information in the database. When a citizen contact detail is found, the CTI system sends the call and the customer information simultaneously to an agent's telephone and workstation.

- Interactive Voice Response systems (IVR) systems present citizens with a series of choices from which he/she can choose. The idea behind automated response is to provide a quick, efficient way for the citizens to get the information needed.
- Speech-enabled systems - allow the system to recognise verbal citizen commands. Traditional automated response systems accept input through touch-tones. Speech-enabled systems, however, can accept human language commands. The immediate benefit of speech-enabled systems is that they are easier and faster for citizens to use. With a larger percentage of the Ghanaian public using mobile phones, it becomes cumbersome to continually look at the keypad and press a number. Speech-enabled systems allow citizens to speak naturally and access the information they want.

4.2.10Telemedicine for e-Health

Telemedicine applications will play an increasingly important role in healthcare in Ghana and provide tools that are indispensable for home healthcare, remote patient monitoring, disease management, rural health and battlefield care.

Advances in technology including wireless connectivity and mobile devices will give practitioners, clinics, and hospitals important new tools for managing patient care, electronic records, and medical billing to ultimately enable patients to have more control of their own well being. As the nation embraces e-Health, the contributions of telemedicine need to be fully understood and appreciated and reimbursement policies must be in place for these applications.

Fourth-generation wireless cellular systems will offer video telephony that can facilitate the transfer of real-time images to help with communications between a patient or a caregiver and a health-care professional.
As wireless technology becomes more ubiquitous and affordable, applications such as video-telephony will gradually migrate towards fourth-generation wireless systems. These techniques promise to greatly improve the cost and convenience associated with long-term outpatient monitoring, and could potentially extend monitoring to the broader healthy population for preventative diagnostics and alerts.

Applications in virtual reality for medicine pertain to the planning of surgeries and use of data fusion, i.e., to fuse virtual patients onto real patients as navigation aid in surgery. Tele-surgery helps surgeons to perform distant operations. Telemedicine technologies also enable remote monitoring of the chronically or acutely ill, allowing early and timely recognition of symptoms, resulting in earlier diagnosis and simpler more effective and lower cost treatment. In the future

patients will be able to monitor their health in their own homes and then send the data by phone, computer or television to a medical centre for checking.
Telemedicine can also be used to advise people, in an interesting and informative way, on health-care issues. Well-informed citizens are less likely to suffer from illnesses caused in part by factors such as over eating, lack of exercise, poor hygiene or smoking.

Telecommunications can be an effective vehicle for training medical personnel and ensuring that wherever they are, and whenever they have need, they can keep abreast of the latest medical breakthroughs and discoveries.
A well informed health professional is more likely to ensure that all Ghanaian citizens receive similar high standards of treatment.

Once e-Health becomes more established throughout Ghana and data protection measures are in place, then any medical centre could, in principle, have access to a patient's medical records when needed.
This will mean fewer worries when travelling as those responsible for medical treatment can check previous health records and medication, and consult with local doctors if necessary. Citizens who need constant checkups and controls will be able to keep in touch with their own doctor or health centre wherever they may be in the country.

In the future, e-Health will ensure that health care and expert medical advice is never far away, even for those living in remote areas, or regions cut off during emergencies. Decisions on utilising limited emergency transport systems can be more sensibly made, based on hard data.
Well-equipped ambulances can be rushed to the scene of a disaster and connected via satellite to medical centres thousands of miles away. Specialist doctors can then advise local medical staff on the best action to take or, when speed is of the essence, even guide them through an emergency operation.

4.2.11Other Channels

Other traditional channels include the use of facsimile machines, postal services and face to face contacts at the offices.

4.2.12Shared Infrastructure Services

The shared applications infrastructure components to be developed as shared services for the agencies include:

4.2.13Identity Management

Designing and implementing robust and secure Identity Management systems for e-Health services is not trivial, especially when the number of potential users may run into hundreds of thousands of healthcare professionals and even millions when patient access is offered. Given the cost and complexity of such systems, they are an obvious candidate for a single common implementation that all services share.

The ability to use a single e-Health credential for accessing multiple target services means implementation of a common user authentication infrastructure that is available to participating services.

Once users have acquired an e-Health credential, making it possible to access multiple services with that single credential is beneficial to, both the user, and in the incremental cost and overhead to Healthcare for enabling access to each subsequent service minimal.

The GHS will utilise the Government's Identity Management shared solution for the registration/ enrolment and authentication of citizens to use government services electronically. The single sign on (SSO) component of the Identity Management solution is required by the Service to provide access to the Service's applications. The SSO solution will be built into a base secure Portal implementation by providing the user with a single sign-on experience. The definition of single sign-on (SSO) is that if a user has successfully authenticated once in a system then that user is not required to present his authentication information again. His established credentials are used to automatically authenticate him to the applications participating in the single sign-on domain.

4.2.14Directory Services

The GHS will build a Directory Service, which is a network service that identifies all resources on a network and makes them accessible to users and applications. Resources include e-mail addresses, computers, and peripheral devices such as printers. The Government ICT infrastructure will make the physical network topology and protocols transparent so that a user on a network can access any resource without knowing where or how it is physically connected. The GHS will use the federated Directory Services.

4.2.15Payments Gateway

Ghanaians are expected to enrol with the NHIS for the payment of healthcare services but the GHS EA identifies bill payments that in many cases cannot be effectively fulfilled by NHIS and traditional payment systems such as cash and cheques. Government as a merchant would like to sell services online and e-commerce technology offers a number of possibilities for creating new payment systems that substitute for existing payment systems, as well as creating enhancements to exiting systems.

The GHS will utilise the GoG's payment gateway to enable patients pay for services online or through a self service device. The Payment Gateway will be developed to be Payment Card Industry standard (PCI) compliant, to meet international security and process requirements. It will also integrate with the GHS billing and accounting systems.

4.2.16 The Business Integration Layer

The Business layer provides the technologies that enable the orchestration of GHS business processes. The layer also includes the requirements and technologies for building analytics and business intelligence capabilities across the Service as well as the management of digital assets.

The GHS business processes span across front, middle and back office functions with multiple applications and systems to automate the business processes. As the GHS goes through Strategic Planning and Budgeting for example the organisation engages people and systems across the enterprise to complete complex processes. Too often, processes are completed inefficiently and at high cost with convoluted manual business processes and mountains of paperwork.

4.2.16.1Business Process Management

The GHS will deploy a Business Process Management (BPM) software suite for modelling, automating, managing, simulating, optimising, and executing business processes across departmental divisions, systems, and applications.

BPM technology will automatically manage processes, allow manual intervention, extract information from databases, and generate transactions in multiple related systems without human intervention when needed. A BPM solution is required to support business process orchestration and automation through workflow management to reduce inefficiencies and errors currently associated with the paper based complex business processes that exist across government.

Support for standards such as the following is critical to the implementation of BPM in GHS:

- Business Process Execution Language (BPEL) - the current WS-BPEL 2.0 standard, commonly called BPEL, has been ratified as an OASIS standard. The WS-BPEL 2.0 standard does not currently have any provision for supporting human interaction. It is more focused on Web Services interaction with the business process. However industry vendors are now working on BPEL4People as an important initiative to standardise the integration of human workflow activities into business processes;
- Business Process Modelling Notation (BPMN) – is a graphical notation that depicts the steps in a business process.
- Unified Modelling Language (UML) – is an Open Management Group's (OMG) specification that addresses the way that Government application structure, data structure and architecture will be modelled.

The value of BPM solutions in the GHS is the ability to orchestrate business processes, integrate them with human interactions and applications services. The BPM solution to be selected for the GHS must include the following features and functionality:

- **Design tools and user interfaces** – to enable business process automation to be designed easily the BPM tools should be intuitive and easy for business users to use. It must have a combination of drag-and-drop and point-and-click capabilities, coupled with graphical interfaces. Once the business user has completed designing the process, the ICT team can then tackle the development of the underlying logic that facilitates the interactions between disparate systems. The BPM solution must serve as a bridge between business and technical users and allow them to work together in a collaborative fashion.
- **API/framework layer** – the BPM solution must offer a well-published application programming interface (API) that will enable the solution to be integrated with a number

of disparate systems. The BPM solution must support Web Services to reduce the complexities of interconnecting the back-office applications.

- **Process automation, workflow, and rules engine** - process automation is a key capability inherent within BPM solutions. Limiting the amount of human involvement is an easy way to streamline processes, where systems automatically handle the handoff and execution of process tasks, based on predefined conditions. Traditional workflow functionality must be an intrinsic part of the BPM solutions. A rules engine is also required to help facilitate the interactions between resources, whether system to system, human to human, or a combination of the two. Business rules are programming code that enables decisions to be made based on predefined conditions that act on data.
- **Data transformation** - interactions between different systems that automate business processes will sometimes require the exchange of data. But in order for the data to be consumed by a system, it must first be converted to a format it understands. A degree of data normalisation, for instance may also have to take place to ensure that inconsistencies between data sets are resolved. The GHS BPM solution must provide necessary data transformation services to help facilitate the exchange of data between systems.
- **Connectivity services** - by a number of technologies, such as adapters, Web Services, integration servers, etc. Ideally, a BPM solution should provide the ability to handle message events captured from a messaging engine with support for transactional integrity and rollbacks. The solution must be able to integrate disparate applications across government together through the proper management of metadata, objects, and transactions.
- **Business Activity Management (BAM)** – is a new addition to BPM solutions. BAM capabilities will allow the GHS to measure the effectiveness of their business processes and provide analysis for improvements. The BAM will enable the GHS track events and activities that are generated from the execution of business processes, with a view towards continuous improvement.

4.2.16.2Master Data Management

Master data (also known as reference data) represents the government's business entities, terminology, definitions and classifications used to describe business information. Due to the autonomous nature of the MDAs, reference data such as accounting codes and other common identifiers such as citizen ID, tax number, etc are inconsistent.

GHS will utilise the central government wide Master Data Management (MDM) solution when it becomes available to manage reference data.

4.2.16.3GHS Business Intelligence (Management Information Reporting)

The Ministry of Health's legal framework for information management in the health sector defines the different reporting levels and the data collection mechanisms for healthcare services and health care providers at each management level.

The different management levels are:

- **Reporting at the community level**: the key health information activities at the community level involve the maintenance of community register of vital events such as Births and Deaths that are compiled at the various facilities

- **Reporting at the sub-district level**: the sub-district is a defined geographical area, where an agreed set of services are provided. Every sub-district maintains an inventory of all health service providers and drug outlets within their catchment area which shall be updated every year. Clinical reports on diseases and submissions are produced monthly.

- **Reporting at the district level**: the District Health Administration has the overall responsibility for the performance of health service delivery at the district level. Budgetary and operational reports on hospitals, clinics, pharmacies, laboratories, diagnostic services and NHIS claims are captured, analysed and reported at the district level.

- **Reporting at the regional level**: the Regional Health Administration has the overall responsibility for the performance of health service delivery at the regional level. To do this the region receives reports and information from various centres, the Regional Hospitals, Health Training Institutions, and Regional Laboratories. Each region has a qualified Health Information Officer and supported by a technical team of statisticians, biostatisticians and data managers. Performance reports on the districts are also produced at the regional level.

- **Reporting at the national level:** The basis of these reports is to demonstrate the performance of the health sector from a programmatic perspective and by the use of the sector-wide indicators. National level reports require that information and data from all agencies are collated and presented in a timely manner so as to meet the deadlines implied by these requirements.

The meet these reporting requirements, the GHS must develop a comprehensive Business Intelligence capability that will replace existing 'manually crafted' reports that are printed and distributed across the different management levels. The requirement is to provide on-demand analytics for both real time and non real time decision making. Such a system will involve the following layers are illustrated in figure 5 below:

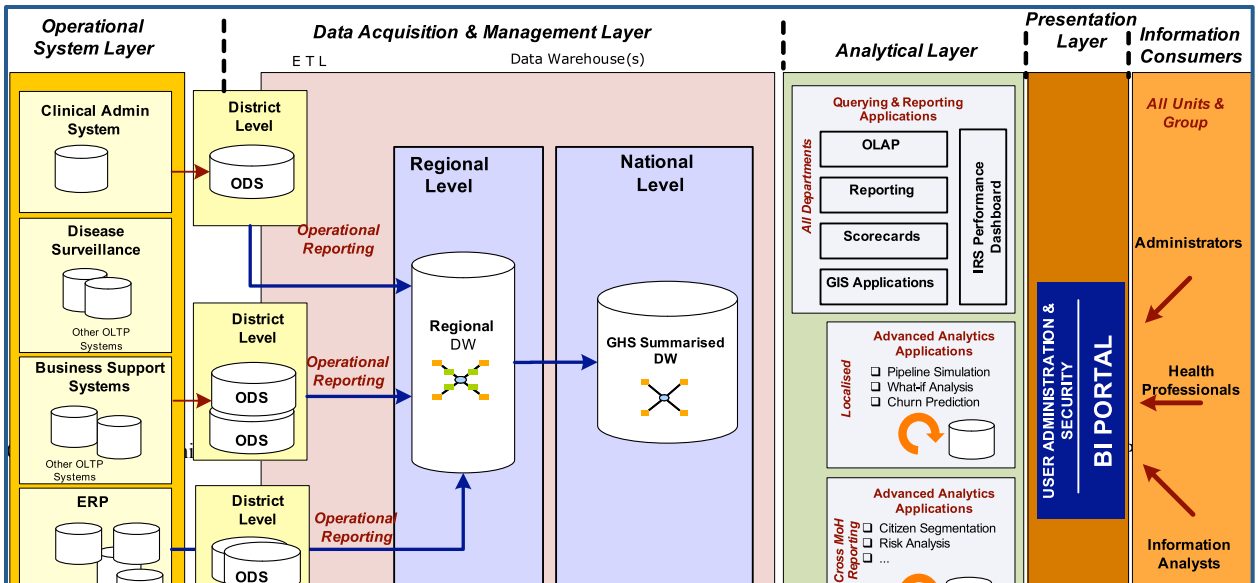


Figure 5: GHS BI Architecture

The different layers of the government BI architecture are:

4.2.16.3.1Operational Systems Layer

This layer involves the systems that will hold data to be extracted for the further analysis. They include the Clinical Administration Systems, Policy Management, Strategic Planning and Budgeting, Audit and Compliance, Enterprise Resource Planning (ERP) and other operational systems to be used by the GHS to run its day to day functions.

Data may be captured real time, daily, overnight, weekly etc. and that will determine the appropriate sourcing strategy to be used by the GHS to capture data for reporting purposes. Patient data will be captured mainly at the community and sub-district levels where events (e.g. births, deaths, admissions, etc) mostly occur.

There are various options available for the transfer of data from the source systems to data warehouses include:

- Enterprise Architecture Integration (EAI) real-time transfer;
- EAI propagation of incremental records;
- Incremental batch transfer;
- Native replication and bulk data refresh;
- Extract Transfer Load (ETL) transfer.

4.2.16.3.2Data Acquisition and Management Layer

This layer involves the physical capture of the data from the source systems into the various staging areas for further processing. Maintaining extract and transformation routines is resource intensive, and coordinating their execution at runtime can be operationally challenging. The solution to this problem is to break the processing into multiple steps. This involves developing a set of routines that extract the source data and load it into shared information staging areas. The detailed data in the staging areas is then used to feed data into independent data marts. As

data flows out of the staging areas, it is enhanced and mapped by Extract Transform Load (ETL) tools into the format required by the target warehouse data store.

Operational Data Stores (ODS) will be created for real time and ad-hoc reporting at the sub-district and district levels. The GHS collates information from various facilities in the districts, (including private self financing facilities). Information captured will include data on service utilisation and intensity of use of health facilities such as:

- Outpatient attendance;
- Outpatient morbidity;
- Inpatient admissions;
- Inpatient deaths;
- Inpatient morbidity;
- Inpatient mortality;
- Hospital bed utilisation;
- etc.

The above information is captured, stored and analysed for each region and where appropriate by age and sex. At the regional level, the information is available by district.

Almost all these indicators are presented by region and by district in some cases. Most of them are collected on routine basis while district coverage surveys are used to verify and validate some of them.

The ODS could also serve as a staging area for the Regional and National data warehouses. As new data marts are added to the data warehousing system, existing extraction routines and staging area data can be reused or enhanced as required. The use of staging areas can also help in the task of fixing source data quality problems. To solve this issue, data profiling tools can be used to analyse and identify problem areas in source data prior to ETL tool processing. If data profiling identifies quality problems in the source data, then data re-engineering tools can be used to fix source data after it has been extracted into the staging areas. Clean and consistent staging area data is then used to populate the various data stores that make up the BI system.

The data warehouse at the GHS Regional level is based on the storage and reporting of data from the district and the regional hospitals. Data collected at this level for the reporting purposes facilitates the assessment of performance of these management units and provides scope for assessing trends and doing comparative analysis.

At the National level, information requires more in-depth analysis to enable the development of policies and standards for health care delivery. Again, it is at this level that outcome and impact of policy is determined indicating the need for a much wider scope of information analysis. The Regions and other tertiary facilities are the primary sources of information at the National level.

Data profiling and warehouse design tools can be used in a series of iterative steps to develop the design of the staging area and to identify the rules for mapping, cleansing and transforming the

source data (from the districts) into the format required by the staging area. The basic design elements of the staging area are business components, which provide a business view of the detailed data in a source system.

After the data has been sourced and extracted, the necessary transformations may be applied as required by the health administrators. These transformations will give the final touches to the integrated data, eliminating any operational inconsistencies to create the 'single version of the truth', that is one and only data store for the publishing layer. This section defines the subsystems for applying the necessary business rules for the captured data. In the BI architecture, the transformation layer is divided into two logical areas:

- Source specific transformations;
- Generic transformations.

The logical grouping of these transformations is to enable source specific transformations to be decoupled from the more generic transformation required by accounting and transaction rules. The split between these areas will make use of staging tables.

The transformation of data is necessary to handle the wide range of platforms, data formats and structures.

4.2.16.3.3Analytical Layer

Analytics is the extensive use of data, statistical and quantitative analysis, explanatory and predictive models, and fact-based management to drive decisions and actions in government. The analytics may be input for human decisions or may drive fully automated decisions. It includes an analysis engine that can generate and/or provide access to current business analyses from any place and at any time. Performance here will largely depend on the amount of data to be analysed and the complexity of the analyses to be performed.

Typical analytics applications include:

- **Activity-based costing (ABC)** - the first step in activity-based management is to allocate costs accurately to aspects of the organisation such as facilities, disease, patients, processes, or service channels; models incorporating activities, materials, resources, and service offering components then allow optimisation based on cost and prediction of capacity needs;
- **Simulation** - a computerised technique used to assess the probability of certain outcomes or risks by mathematically modelling a hypothetical event over multiple trials and comparing the outcome with predefined probability distributions;
- **Capacity planning**: finding the capacity of a supply chain or its elements; identifying and eliminating bottlenecks; typically employs iterative analysis of alternative plans. This analytic is very important for scheduling of equipment, health professionals and beds at the various hospitals and clinics;
- **Modelling**: creating models to stimulate, explore contingencies, and optimise supply chains. Many of these approaches employ some form of linear programming software

and solvers, which allow programs to seek particular goals, given a set of variables and constraints.

- **Strategic forecasting models**: forecast several years ahead the likelihood that districts or regions will fail or will become unstable based on quantitative analysis of social, political, disease, demographic, and economic factors;
- **Operational forecasting models**: monitor, assess, and forecast trends in behavioural interactions between people, organisations, and regions, and predict changes at the event level (for example premature births registered).

To support on-demand analytics, the solution must include parallel processing and integrating analytic capabilities as well as pre-packaged analytic applications that pre-compute business metrics for rapid delivery via a web Portal dashboard. This will include various analytical reports such as Finance, HR, and Supply Chain analytics.

4.2.16.3.4Presentation Layer

The presentation layer delivers the analytics and reports to the end users. Ministers, the Chief Director, the Director General and Health Administrators from the GHS and other stakeholders will use Web based presentation dashboards, reports, spreadsheets, etc for adhoc query and reporting to make more informed decisions.

The key elements of the presentation layer are:

- The provision of a secure, single access point over the Web with a powerful interface for the GHS to gain insight to critical business information.
- Easy access, easy to use, easy to maintain dashboards for performance management and analytics reporting.

4.2.17Integration Layer

The GHS is organised into five distinct levels forming an apparent hierarchy, that is National, Regional, District, Sub-district and Community. However ICT capabilities will be concentrated in the National, Regional and District levels since business activities are concentrated in the tiers. Such intercommunication between systems, require an integration strategy that enables effective health information exchange between the internal administrative functions.

The integration architecture for GHS must be based on a common framework of agreements among the stakeholders. The architecture is based on the tiered management model. Among the important implications of the proposed system for a network of networks is that personal health information would continue to reside where it does now, primarily with hospitals and healthcare providers. According to the patient‘s preferences, relevant health data could be assembled from numerous sources at the point of care, enabling decision making to be informed by past treatment successes and failures and medication history. Both the patient and the clinician could have direct access to this vital information.

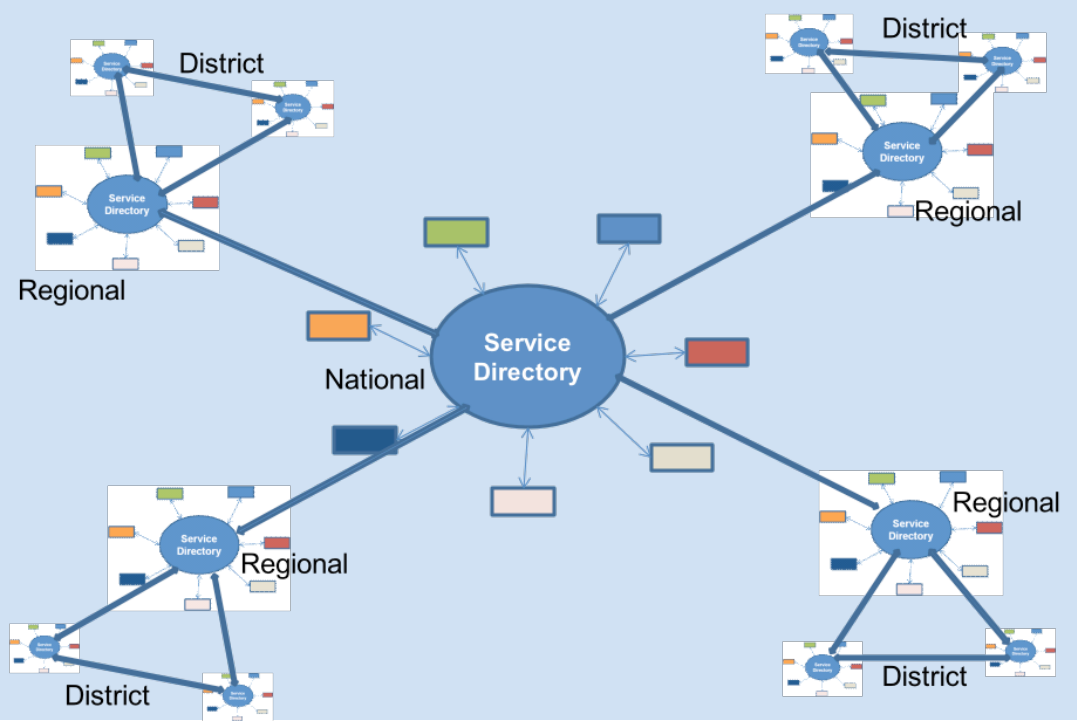


Figure 6: Integration Architecture

The architecture as described in figure 6 above provides a common implementation from the districts, regions and the national levels with a generic integration functionality, which can benefit every remote service. Investing once in the design, development and testing of such a common integration solution, and offering it to affiliated services as a base for their specific integration, can provide significant savings while still assuring the quality of the base solution. The common integration solution can deal effectively with most of the difficult issues around reliable remote communication, security, and other requirements, most of which may require expertise not readily available at the GHS, especially as the spread of e-Health services reaches smaller entities such as the sub-districts.

Service-specific integration, when performed locally to the target system, can be much simpler and easier than full integration all the way to the hub. Combining this architectural approach with the appropriate governance and commercial arrangements, for example, offering a complete base integration solution that includes hardware, software, installation, and support, can be a significant positive driver for the successful adoption of e-Health services in Ghana. The positive experience in several countries demonstrates the advantages of such an approach.

It is recommended that GHS deploys Commercial Off-The-Shelf (COTS) applications to automate business processes. These applications must be seamlessly integrated through a hub to orchestrate the integration of application services across the GHS.

Integration with GHS's back end systems will be based on Web Services standards to aid interoperability. The architecture therefore requires a common integration service platform that will enable both internal and external systems applications to be integrated effectively.

Key to enable easy interconnection and intersystem communication is the ability to connect systems into a plug-and-play infrastructure. This is achieved through the use of system adapters. A system adapter performs four basic functions:

- Message Transport Protocol Translation;
- Message Protocol Implementation;
- Message Mapping
- Message Encryption.

The GHS systems interchange messages based on XML, with the clinical payload within each message following accepted clinical messaging standards whenever one exists, or a pragmatic interpretation of those standards (such as HL7 Messaging). The integration architecture as whole must be designed to allow multiple vendors of specific vendor-types (such as pharmacy) to plug into the plug-and-play infrastructure and register their service as being available. The advantage of this subscription based one-to-many relationship (one instance of the Plug-and-Play Infrastructure to many vendors) is that it helps provide greater interoperability and flexibility of the solution as a whole.

4.2.17.1e-Government Service Bus (e-GSB)

The GHS will utilise the e-Government Service Bus (e-GSB), which will be based on an Enterprise Service Bus (ESB) technology to provide the applications integration and the movement of data among multiple applications services, both within and outside of the GHS. The solution will use open standards to connect, transform, and route documents as XML messages across the channels and the various application services. It will enable monitoring and management of data, with minimal impact on existing applications.

The e-GSB will provide the underlying infrastructure platform for delivering the service-oriented architecture (SOA) and event-driven architecture (EDA) requirements of the GHS.

The e-GSB will include the following functions:

- **Communication** – will supply a communication layer to support service interactions. It should support communication through a variety of protocols. It should provide underlying support for message and event-oriented middleware and integrate with existing HTTP infrastructure and other Enterprise Application Integration (EAI) technologies. The e-GSB should be able to route between all of the different communication technologies through a consistent naming and administration model;
- **Service interaction** – the e-GSB will support SOA concepts. It should support all the shared application services and infrastructure services defined for the GHS EA;
- **Integration** – the e-GSB should support the integration of the various channels and the variety of GHS' systems currently in place as well as new ones to be developed. This includes all internal packaged applications and it will also enable data enrichment to alter data moved across the departments;

- **Management** – as with any other infrastructure component an e-GSB must have administration capabilities to enable it to be managed and monitored and so to provide a point of control over service addressing and naming. In addition, it should be capable of integration into systems management software;
- **Security** – the e-GSB should ensure that the integrity and confidentiality of the services carried are maintained. They should integrate with the existing security infrastructures to address the essential security functions such as:
    - Identification and authentication;
    - Access controls;
    - Confidentiality;
    - Data integrity;
    - Security management and administration;
    - Disaster recovery and contingency planning;
    - Incident reporting.

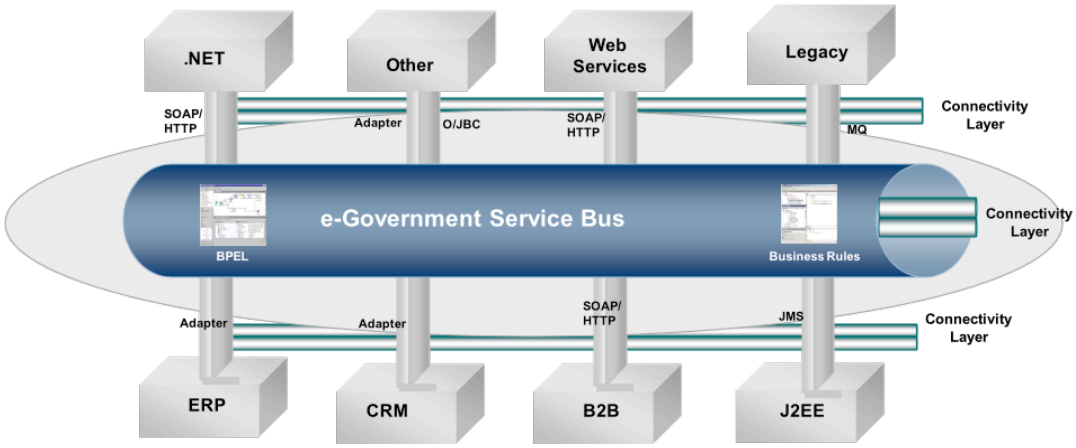


Figure 7: ***e-Government Service Bus Architecture***

4.2.17.1.1E-GSB Connectivity

Connectivity is provided through adapter services and Web Services Simple Object Access Protocol (SOAP) invocation services, which provide connectivity with external SOAP clients, such as the Portal, the BPM engine, .Net, Java components etc as well as back end application services. The e-GSB will receive service requests from such clients or generate calls to them.

The location of a Web Service is determined at runtime by querying the UDDI repository. This preserves one of the core tenets of a service-oriented architecture that is location transparency. The address returned from the query represents the physical location of the Web Service. This may take the form of a HTTP URL if communication with the Web Service is over the HTTP

protocol, but it could equally represent another type of address if a different protocol is used – for example, basic TCP/IP.

A SOAP message that contains a business document should include SOAP headers containing the address of the endpoint that is to receive and process the business document. This endpoint is likely to be the address of a submission service that is responsible for forwarding the message to the target department or utility service.

4.2.17.1.2Messaging & Queuing

The e-GSB will provide Store and Forward of messages services between different clients and the various services performed by the e-GSB, both in synchronous or asynchronous way. The services will include:

- **The Service Registry** – which will be used to provide a controlled point of access to service metadata for all services provided by e-Government;
- **Transaction Management** - transactions are a fundamental concept in building reliable distributed applications over the e-GSB. A transaction is a mechanism to ensure all the participants in an application achieve a mutually agreed outcome;
- **Switching & Routing** - service switching and routing is a key "enabling service" of the e-GSB which ensures that a service is accessed in most efficient and performing manner;
- **Service Provision and Delivery Gateways** - make the services of one application or provider available to others, and vice versa, in a controlled and secure manner. They provide an alternative to client-based or server-based wrappers and instead acts as an intermediary component to translate non-Web Services invocations into Web Services calls and messages, and vice versa.
- **Event Management - t**he e-GSB Event Management Service will enable Event Driven Architecture by providing a standard "push service" that will enable decoupling of clients from consumers of e-GSB events. The various e-GSB components can publish messages into the e-GSB and the Event Management Service will deliver the messages to all the appropriate subscribing users.
- **Channel Interaction Layer** - the Short Message Service (SMS) Gateway will allow the GHS to integrate SMS with their core systems through a single point of entry. The e-GSB will enable all providers and users the ability to simply 'plug in' to the SMS gateway and begin sending SMS messages. The Interactive Voice Response (IVR) Gateway will provide the necessary interaction services to handle telephone callers. Integration with other electronic channels such as the Self Service Kiosk will also be implemented through the e-GSB.

4.2.17.1.3Adapter services

The e-GSB will provide bidirectional, real-time data access to various data sources through adapter services, which either listens for, or polls for events in the source application it supports. When listening for events, an adapter registers as a listener for the application that is configured

to push events to the adapter. The adapter can also poll the back-end application, such as a database or file, for the events required by e-GSB.

Adapter services to be provided with the e-GSB will include:

- **Vendor specific adapter services** – For example SAP and Oracle application adapters services. An inbound vendor adapter sends XML messages to the e-GSB on receiving messages from the vendor application interface. An outbound vendor adapter inserts data from the e-GSB into the vendor applications using APIs and other interfacing methods;
- **File/FTP adapter service** - an inbound file/FTP adapter service reads data from a local/ remote file system transforms the file data into an XML message and sends it to e-GSB when a new text file appears in a local file system. An outbound file adapter service transforms the contents of an XML message to a text file and writes it to a local/remote file system;
- **Database adapter service** - an inbound database adapter service sends an XML message to the e-GSB when a SQL insert, update, or delete operation is performed against a database. An outbound database adapter transforms the contents of an XML message into a SQL insert, update, or delete operation on the target database.
- **MQ adapter service** – ability to integrate legacy system with existing MQSeries support. An inbound Native MQSeries adapter service sends an XML message to the e-GSB when new XML message is received by a queue. An outbound Native MQSeries adapter service writes messages from the e-GSB to a message queue.

4.2.17.2Enterprise Information Integration (EII)

EII the integration of data from multiple systems into a unified, consistent and accurate representation geared toward the viewing and manipulation of the data. The GHS must have the capability to aggregate, restructure and present information in a consistent and secure way to the user. To support the Government's BI architecture there is a need for data integration, which is the extraction, transformation and loading (ETL) of data from disparate systems into a single data store for the purposes of manipulation and evaluation (reporting). Data warehouses and data marts are the data stores and ETL tools are the data integration components. The data transfer techniques available to the GHS include:

- EAI real time transfer – this is application-driven, this option is most appropriate for data transfers where updates to the system of record and the data stores are part of the same transaction. An integration broker receives the transaction that was initiated by the front-end application. After which, it assumes responsibility for propagation of the information to the system of record and the data store/warehouse.
- EAI propagation of incremental records – this approach is also application driven; it is appropriate for lower priority data. The front-end application updates information in the system of record after which this information is propagated to the data store through the integration broker. There are two mechanisms to effect this transfer of information to the data stores: push to Integration Broker and pull from Integration Broker.

- Incremental Batch Transfer (Changed Data Capture) – this approach is data driven, and it is used to move new or changed data periodically from the source to the target data store. This option is applicable to scenarios where it is acceptable for the data updated in the system of record to be provided to other applications after a finite time window (e.g. one day). In such scenarios, the data is transferred on an incremental basis from the system of record to the data stores/warehouse. This data sharing option involves capturing changed data from one or more source applications and then transporting this data to one or more target operations in batch. Typical considerations in this option include identifying a batch transfer window that is conducive to both the source and target system(s) to extract and transport the data.
- Native Replication – this option is also data driven and is especially relevant for high-availability situations. This data sharing option involves the use of native features of database management system (DBMS) to reflect changes in one or more source databases to one or more target databases. This could happen either in (near) real-time or batch mode.
- Bulk Refresh Using Batch File Transfer – this option is also data driven when a large amount of data, like a reference table of product information, needs to be periodically brought into sync with the system of record. This option transfers all data, inclusive of the latest changes, on a periodical basis. All records are extracted from the system of record and refreshed into the data store/warehouse.
- Bulk refresh - is well suited for scenarios where significant overhead is involved in identifying and propagating incremental changes. The incremental approach tends to be more error prone and maintenance intensive. This type of transfer can be accomplished in one of two ways: file extract and program extract.
- ETL Transfer – this option is also data driven and is most appropriate where substantial data scrubbing and transformation are required as data is moved; for instance, in the case of integration into a data warehouse of data mart. This option overlaps with both Incremental Batch Transfer and Bulk Refresh. The difference is that business logic is applied to data while it is transported from source to target systems. An ETL tool will be required for this kind of information transfer. Source data is extract, transformed en route, and then loaded into one or more target databases. The transformations performed on the data represent the business rules of the organisation. Business rules ensure data is standardised, cleaned and possibly enhanced through aggregation or other manipulation, before it is written to the target database(s).

4.2.18GHS Future State Application Services

This section identifies the different application services required to automate the business processes of the GHS. It is recommended that COTS are used as much as possible.

4.2.18.1Electronic Health Records

The GHS will deploy an Electronic Health Records (EHR) system which will contain a lifelong history of a patient‘s health including all relevant identification information, all permanent medical information, and all medical events that have taken place in the patient‘s lifetime. The EHR may be regarded as having four main parts, namely: identification, standing medical information, consents information and the health record itself. The identification portion would contain the primary identifier, which the patient number and include demographic items such as name and address, date of birth, etc. The EHR will be captured and maintained at the point of care.

The standing medical information portion would contain details such as blood type and allergies and such further information as might be useful in an emergency situation. Further it might contain, or point to, information on current medication and indications of relevant prevailing medical conditions such as diabetes or asthma.

The consents portion would contain details of the areas of the patient record to which the patient wishes to restrict access. A number of criteria could be envisaged such as permitting access only by nominated healthcare professionals, restricting access to particular health subjects, limiting viewable data to certain care events, applying time limits and date range restrictions to the lifelong record, and so on.

The patient health record portion contains details of each and every contact and treatment the patient has received in his or her lifetime or a significant portion thereof. The EHR may be recorded to varying levels of granularity. The finest grained entry is usually at the level of an encounter, which is a consultation, examination or treatment provided by a healthcare professional typically at a single session or appointment. The EHR may be held at a higher level of summarisation. For example, a number of encounters may be summarized into an episode of care which covers a specific condition and has a clear start and finish. In turn, a series of episodes of care may be summarised into an event which covers the complete treatment for a particular condition or illness. An event might last for many months or years or, in the case of a chronic condition, the event might be lifelong.

Finally, at the highest level of summarisation, we may have spells of care which may be of long duration and have many events during their currency. Another concept that might be of use is that of a patient problem. This is at an even higher level of abstraction and describes some permanent or chronic condition, diabetes or hypertension might be examples, which are key factors in managing the patient‘s health.

4.2.18.2Scheduling and Capacity Management

Scheduling and capacity management system is to maximise resource utilisation, improve throughput, optimise capacity management, and increase patient, staff and physician satisfaction.

Some of the key features of this system is a visual appointment book that gives a graphical, easy-to-view display of scheduled appointments and resources. This also improves on the access management capability of the system. It allows scheduling of multiple procedures or

appointments at one time and automates the scheduling of repeated events. The system automates the process of scheduling and sequencing multiple events for a particular patient within a single or multiple site facility.

The system will support enterprise-wide and departmental performance improvement by offering:

- Enterprise Scheduling: Helping to connect procedure scheduling and operating suite activity to areas of the hospital that have an impact on efficiency and finances, like supply management and patient accounting.
- Surgery Scheduling: This module will help optimize operating room capacity management and throughput, control resource utilization, lower supply costs, and maximise revenue. All of which improve clinical and financial performance.

4.2.18.3Clinical Services

The GHS monitors and coordinates the activities provided by the district and regional hospitals. As part of their duties, they have oversight responsibilities over health care services provided to the citizens and ensure that service provided matches international set of standards. A clinical services system will effectively manage the relationship between the various wings of the hospitals.

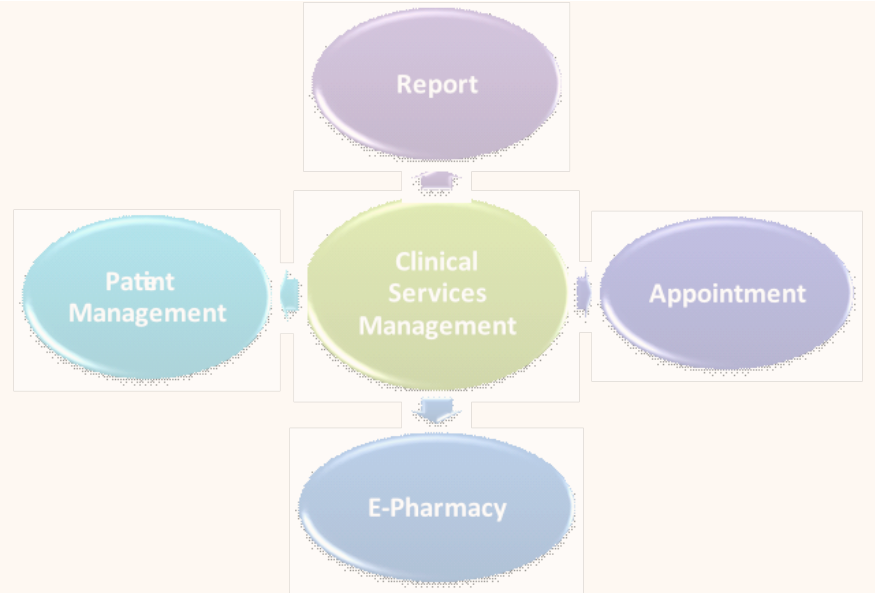


Figure 8: Clinical Services Application Components

The various components of the Clinical Services System and the functions are:

- Patient management: Every patient will be given a unique patient identifier. The unique identifier will match the identifier found on the national health insurance identity card.

This ID will continue to be used to identify the patient throughout the system. Upon registration, a patient's data will be stored in the district hospital data base and later on be dispatched via a batch process into the central data warehouse which will store patient data from all the district and national hospitals. The patient management module will interface with all the modules since it acts as the core of clinical services by housing patients' information.

- E-Pharmacy: e-pharmacy allows prescription sheets for drugs to be sent by the doctor in the consulting room to the pharmacist. In this way, patient drugs will be prepared and sorted out at the counter and all the patient has to do is to pick them up. Additionally it can be linked to main billing. As patient collects drugs from pharmacy shop their charges will automatically transfer to patient billing. Via the web portal, the e-pharmacy module can be extended to cover pharmacies that are outside the confines of the hospital. This will however require that some form of agreement be reached between the GHS and the pharmacies in question. Using the business to business interface of the web portal, prescriptions can be forwarded to those external pharmacies.
- Appointment: The appointment module will cater for all appointments relating to clinical services in the hospital. We propose a web facility to enable citizen's book appointments for laboratories, radiology centres and other departments in the hospital. Citizens can also call the contact centre of the hospitals to book appointments.
- Patient management: Every patient will be given a unique patient identifier. The unique identifier will match the identifier found on the national health insurance identity card. This ID will continue to be used to identify the patient throughout the system. Upon registration, a patient's data will be stored in the district hospital data base and later on be dispatched via a batch process into the central data warehouse which will store patient data from all the district and national hospitals. The patient management module will interface with all the modules since it acts as the core of clinical services by housing patients' information.
- E-Pharmacy: e-pharmacy allows prescription sheets for drugs to be sent by the doctor in the consulting room to the pharmacist. In this way, patient drugs will be prepared and sorted out at the counter and all the patient has to do is to pick them up. Additionally it can be linked to main billing. As patient collects drugs from pharmacy shop their charges will automatically transfer to patient billing. Via the web portal, the e-pharmacy module can be extended to cover pharmacies that are outside the confines of the hospital. This will however require that some form of agreement be reached between the GHS and the pharmacies in question. Using the business to business interface of the web portal, prescriptions can be forwarded to those external pharmacies.
- Appointment: The appointment module will cater for all appointments relating to clinical services in the hospital. We propose a web facility to enable citizens to book appointments for laboratories, radiology centres and other departments in the hospital. Citizens can also call the contact centre of the hospitals to book appointments.

Due to the confidential nature of patient information, roles should be assigned to only the right people who need to use and make use of the information. The system administrator will assign roles and unique identifications to the right users. Using views will allow users to only access the information within their domain.

Various users should be provided with easy to use graphical for easy access to the system.

Alerts and notifications should be provided to remind doctors and health professional of appointments. Must have a specialised view for doctors and front office workers to have a holistic view of scheduled appointments and how to handling those appointments.

4.2.18.4Billing Management System

The GHS will deploy Billing Management systems for each district. The system will be designed to be able to process bills automatically for the NHIS and other third party health insurance companies. The billing Management system will obtain basic account and account balance information from heterogeneous underlying accounting systems for the districts. It will provide:

- Maintenance of billing related information and all the processing required to perform accruals, calculate invoices, review and release invoices for payment;
- Creation of extracts for accounting systems.

The following are the key components of the Billing Management system:

- Account Balances: This component uploads new account information on a daily basis. All account balances are month-end balances. Account balances covering the hospital for any given month can be uploaded many times, initially at the end of the month and subsequently if there are any changes to the balance. It also provides uploading balances such as provisional balances, and then subsequently uploading a final balance that has been reviewed and approved.
- Inbuilt Billing Rules: Once the basic account information has been uploaded, additional billing parameters can be entered directly into BMS in the form of billing rules. These rules define the calculation, billing frequency, in-advance or in-arrears billing, asset bases, minimum/maximum billing limits, discounts, and various other parameters that define billing requirements.

  This module should also provide functionalities to manage both the monthly accruals process as well as the billing process. The system also enable automatic generation and release of invoices at scheduled periods. Numerous work-flow notifications can be used to facilitate operations. The billing rules can be defined at the client, account, or the portfolio level. The rules apply to all entities that roll up to that level;
- Automatic Batch Transfer: This module enable bills of citizens registered on the NHIS to be transferred to the server of the NHIS. This can be done through a batch process file transfer on daily, weekly or monthly basis. This module will solve the problem of late payment of funds to hospitals;

- Flexible Fee Definition: The system administrator can define any number of rules for an account, and therefore, any number of fee types for an account. Each rule can specify its own calculation and billing frequency, asset basis, minimum or maximums, discounts, and so on. Each fee can also be charged to the clients in multiple ways such as direct deduct, hard-copy invoice, etc. And each fee can be presented in a separate invoice, or multiple fees may be combined into one invoice for presentment to the customer.

  Any number of formats can be defined for an invoice and the Billing Management Systems can be configured to automatically send additional copies of invoices to other addresses;

- Cash Flows: This module allows cash flow information to be uploaded from the underlying portfolio accounting system. Portfolios can be marked to reflect the impact of these cash flows on the invoice in multiple ways. An account can be marked to either 'always adjust' for cash flows to 'never adjust' for cash flows or to 'selectively adjust' only if cash flows exceed a definite threshold;

- Audit and Security: The system should provide a flexible set of users and groups and allows different access levels to each group for all functions provided. In addition, an audit trail should be maintained of all activities including any adjustments done to billing parameters or invoices for audit control purposes.

4.2.18.5Disease Surveillance

The threat of high-profile disease outbreaks should draw the attention of decision makers to public health surveillance systems for early detection of outbreaks. The GHS and affiliate bodies should enhance existing surveillance systems and developing new systems to better detect outbreaks through public health surveillance. The GHS Enterprise Architecture report provides adequate information on disease and public health surveillance systems which will go a long way to support disease surveillance: a most important responsibility of the GHS. The purpose of a disease surveillance system is to improve decision-making regarding the outbreak and detection of diseases.

Disease surveillance is the continual and systematic collection, analysis, interpretation, and dissemination of data about health-related events for use in public health action to reduce morbidity and mortality and to improve health. Disease surveillance will serve at least eight public health functions. These include:

- Supporting case detection and public health interventions;
- Estimating the impact of a disease or injury;
- Portraying the natural history of a health condition;
- Determining the distribution and spread of illness;
- Generating hypotheses and stimulating research;

- Evaluating prevention and control measures;
- Facilitating planning.

Another important public health function of surveillance is outbreak detection (i.e., identifying an increase in frequency of disease above the background occurrence of the disease).

Outbreaks typically have been recognized either based on accumulated case reports of reportable diseases or by clinicians and laboratories who alert public health officials about clusters of diseases. Early detection of outbreaks can be achieved in three ways:

- By timely and complete receipt, review, and investigation of disease case reports, including the prompt recognition and reporting to or consultation with health departments by physicians, health-care facilities, and laboratories consistent with disease reporting laws or regulations;
- By improving the ability to recognize patterns indicative of a possible outbreak early in its course, such as through analytic tools that improve the predictive value of data at an early stage of an outbreak or by lowering the threshold for investigating possible outbreaks; and
- Through receipt of new types of data that can signify an outbreak earlier in its course. These new types of data might include health-care product purchases, presenting symptoms to a health-care provider, or laboratory test orders.

The purpose of the system is to provide public health workers with the needed and essential data necessary to detect and track the outbreak of disease for faster action before it evolves into a pandemic. The system will be a long-term one, continually used, will augment data from other sources such as clinical databases. The stakeholders of the system are public health practitioners; health-care providers; other health-related data providers; GHS officials at the district, Regional, and national levels; community residents and nongovernmental organizations.

The ability of a system to reliably detect an outbreak at the earliest possible stage depends on the timely capture and processing of the data produced by transactions of health behaviors (e.g., over-the-counter pharmaceutical sales, emergency department visits, and nurse call-line volume) or health-care activities (e.g., laboratory test volume and triage categorization of chief complaint) that might indicate an outbreak; the validity of the data for measuring the conditions of interest at the earliest stage of illness and the quality of those data; and the detection methods applied to these processed surveillance data to distinguish expected events from those indicative of an outbreak.

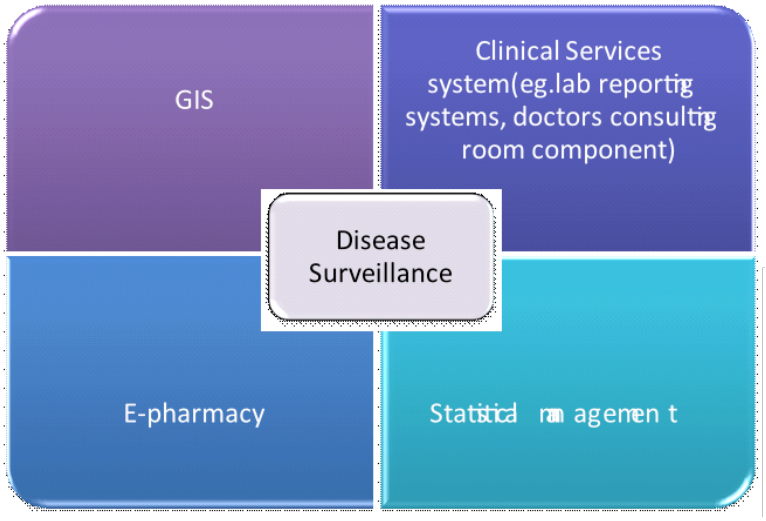


Figure 9: Disease Surveillance System Interfaces

The disease surveillance system should be able to interface with the proposed GGEA shared GIS infrastructure, Clinical services system, the e-Pharmacy system and the statistical management system. An interface with the GIS will give a good understanding of areas where high figures of notifiable outbreaks are being recorded. Thus surveillance information can be matched unto geographical locations and the necessary actions can be taken.

Also the clinical services component and the e-pharmacy systems serves as very good sources of information to the process of disease surveillance. Prevalent cases recorded in the consulting room and the pharmacy counter is useful input to the disease surveillance process. Reports generated for these systems can also be used as data sources for disease surveillance.

4.2.18.6Project/Programme Management

The GHS manage a number of projects each year across the country and therefore require an effective Project Management solution to manage the resources and activities effectively. Project management is the discipline of planning, organising and managing resources to bring about successful completion of specific project goals and objectives. The system will serve as a task manager and collaboration groupware which will enable collaboration and task management by multiple users with simultaneous access to the common database through a network. It will also authorise users to plan, schedule, share, track and report tasks, appointments, projects and any other organizational activity.

Project/Programme Management system will include the following components:

- Employee task planning;
- To do list Management;
- Project Management;
- Employee Time Planning;
- Schedule Management;

- Team Management;
- Employee Task Tracking;
- Workflow Automation;
- Workgroup Productivity Management.

The Project/ Programme Management system will provide a real-time task list, project tree and employee schedule.

4.2.18.7Audit and Compliance

The integration of an Audit and Compliance management system into the architecture of the GHS will enable the Service to ensure that policy stipulations are adhered to. The Audit and Compliance system will ensure that policies that are formulated meet required international standards to facilitate quality control and adherence across all channels and monitor integrity.

The system features will include:

- Create quality and compliance plans;
- Manage resources and projects;
- Write quality and compliance findings directly into the database;
- Perform peer review/approval prior to issuing reports;
- Electronically issue results to a document or web browser;
- Remotely record findings;
- Enter auditor – specific notes;
- Attach supporting evidence;
- Approve reports prior to issue;
- Analyse root causes;
- Perform risk assessment;
- Directly enter and categorise findings;
- Inspections and prosecution module;
- Penalties module;
- Clearance certificate module;
- Standards repository.

4.2.18.8Monitoring and Evaluation

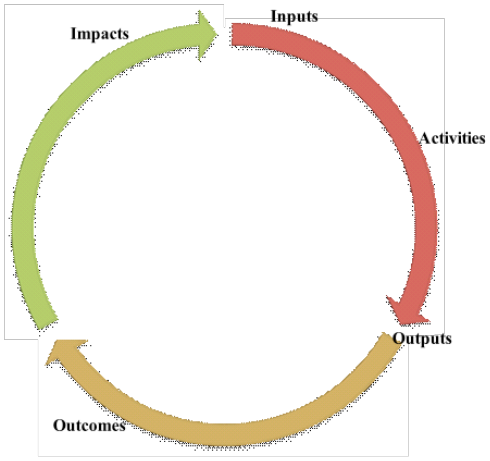


Figure 10: Monitoring and Evaluation System Components

Monitoring and Evaluation is done among MDAs after policies are formulated. As part of the process performance indicators are set and the progress of policies formulated are measured against the key performance indicators.

Monitoring and Evaluation are two closely related, interactive mutually exclusive processes. Through routine tracking of project progress, monitoring present qualitative and quantitative data for evaluation. Thus evaluation supports monitoring.

The monitoring and evaluation solution is an e-governance tool for public sector management to improve its policy/programme/project measurement that specifically targets gathering, collating, analysing and disseminating policy/programme/project information. It should be an easy to use solution with processes combined with various graphics technology, internet technology and modeling tools such as economic analysis without stretching the organisation capacity limitation.

The solution is should be quick and economical to implement on national level, satisfying needs of the national and regional directors. However the implementation process should be able to be customised and quickly adapted to the districts to meet the institutional/capacity development level of the health centres.

The solution should enable the hospital to implement, in the continuously changing environment, within the short time frame, the performance measurement and policy/Programme/project level management information gathering system. It should enhance management capacity through:

- Transparency, Accountability, Flexibility, Adaptability, Participation, Predictability, and Continuity;
- Decentralisation;
- Multiple management objectives;
- Nationwide and grass root solution;
- Organisation Data Architecture and synchronization;
- Commonisation and agreement on performance indicators;

- The logical framework approach.

It is recommended that dashboards and scoreboards technology are used for the evaluating and determining the performance levels of policies nationwide. Data on the impacts of policies implemented will however be gathered nationwide through the issuing of questionnaires or other data gathering techniques. The data will then be fed into a database, cleaned and data quality measures enforced. Using data marts, specific data required to undertake the evaluation process can be accessed and the necessary analysis being done onto the dashboard. The dashboard analysis shows the performance of policies being implemented. These will be measured against the key performance indicators.

4.2.18.9Research and Development

Operational Research is a very important process undertaken by the GHS. It is very important because it informs decision and policy formulation which are key to the responsibilities of the GHS. There are two major types of research: qualitative and quantitative. Qualitative research seeks out the 'why', not the 'how' of its topic through the analysis of unstructured information such as interview transcripts and recordings, emails, notes, feedback forms, photos and videos. Qualitative research does not only rely on statistics or numbers, which are the domain of quantitative researchers.

Qualitative research is used to gain insight into people's attitudes, behaviours, value systems, concerns, motivations, aspirations, culture or lifestyles. It's used to inform business decisions, policy formation, communication and research. Focus groups, in-depth interviews, content analysis and semiotics are among the many formal approaches that are used, but qualitative research also involves the analysis of any unstructured material, including customer feedback forms, reports or media clips.

Quantitative research however deals solely with the collection, gathering, computation and analysis of statistical data to reveal a particular trend or pattern.

We envisage that the GHS will employ both research techniques in undertaking its operational research responsibilities.

Collecting and analyzing unstructured information can be messy and time consuming using manual methods. When faced with transcripts, emails, pictures, diaries and audio or video material, finding themes and extracting meaning can be a daunting task. Collecting, gathering and computing statistics is labour intensive especially when done manually and data has variant sources.

The key features of this system are:

- The research solution should be web enabled to facilitate access from any web browser and also enable field workers to upload data gathered to be uploaded via wireless technologies. Being web enabled, better collaboration can be achieved via video conferencing and messaging tools such as the e-mail.

- Seamless interfacing with shared digital asset services: content management, knowledge management and document management. Interfacing with content management enables research findings and results be published unto the web portal and onto the intranet to be accessed by the citizens and internal workers of the GHS. Interface with the knowledge management will manage results and findings using its internal tools and classification methods. After the research documents have gone through the whole process and cycle of the knowledge management, they are kept in the document management system where they are either archived or kept offline.

The Research management solution will manage, shape and make sense of unstructured information. It must be noted that the solution will not do the thinking; it provides a sophisticated workspace that enables officials to work through information gathered.

With purpose built tools for classifying, sorting and arranging information, Research solution gives more time to analyze materials and discover patterns, identify themes, glean insight and develop meaningful conclusions.

4.2.18.10Performance Management

A Performance Management application is required to help clearly articulate strategy and goals, communicate them across the GHS, monitor key performance indicators, and improve business alignment. It offers complete strategy and accountability mapping capabilities, as well as Web-based message boards, forums and discussion threads. Additionally, the Performance Management application will leverage Business Intelligence capabilities to integrate data from multiple sources and provide dashboards, reporting, and analysis. It will also offer powerful, integrated reporting and analysis tools, including reporting, graphical analysis and an interface built for use by end-users. A common workspace, common security and metadata management will enable a single point of maintenance for reduced cost of administration and ownership.

4.2.18.11Knowledge Management

Knowledge Management is required by the GHS to manage vital knowledge and information possessed by individuals in the Service so that it is effectively shared and used by others in the organisation. Through the effective sharing of intellectual capital, organisational knowledge must be efficiently transformed into business intelligence.

The primary function of the Knowledge Management system is to make information available to authorised users. Capturing organisational knowledge involves more than software and technology, it requires strong document management and cultural transformation of how information is generated, processed, stored, distributed and turned into innovation.

The modules of the Knowledge Management System will include:

- A knowledge web Portal which will serve as an interface for the user and also for the publishing of knowledge. This will be served by the GHS Enterprise Portal.
- Knowledge repositories such as data warehouses that link other operational data stores and appear just to be one big data store provided through the Portal.

The Knowledge Management system will be developed to support and enhance knowledge-intensive processes, tasks or projects. for example creation, construction, identification, capturing, acquisition, selection, valuation, organisation, linking, structuring, formalisation, visualisation, transfer, distribution, retention, maintenance, refinement, revision, evolution, accessing, retrieval and last but not least the application of knowledge, also called the knowledge life cycle.

Users can play the roles of active, involved participants in defined knowledge networks and communities fostered by the knowledge management system. It is designed to reflect that knowledge is developed collectively and that the distribution of knowledge leads to its continuous change, reconstruction and application in different contexts, by different participants with differing backgrounds and experiences.

4.2.18.12Content Management System (CMS)

The GHS will require a Content Management system to help the organisation capture the value and manage volume of structured and unstructured content. It not only assists with managing content across the Service, but also delivers ICT solutions for business process and compliance management. It catalogues content such as policies and procedures (in the form of text, audio, and video), enables sharing and search, facilitates the repurposing of information as well as designed to control content versions.

The application can be used to create, edit, manage, and publish content in a consistently organised fashion. The Content Management system will also help the GHS efficiently organise and manage growing stores of unstructured information like documents, email messages, images, videos and other digital content.

Feature of the CMS will include:

- The ability to assign roles and responsibilities to different content categories or types;
- Definition of workflow tasks for collaborative creation, often coupled with event messaging so that content managers are alerted to changes in content;
- The ability to track and manage multiple versions of a single instance of content;
- The ability to capture content;
- The ability to publish the content to a repository to support access to the content (Increasingly, the repository is an inherent part of the system, and incorporates search and retrieval);
- Separation of content's semantic layer from its layout (For example, the CMS may automatically set the colour, fonts, or emphasis of text.).

Modules of the CMS will include:

- Content Manager: serves as the core content management solution for the system. It combines document management with ready-to-use workflow and process capabilities to drive content-related tasks making it possible to declare a record when a document

reaches a specific point, or when certain process tasks have been completed. The Content Manager manages all types of digitised content across multiple platforms, databases and applications. It will capture computer output and archive scanned documents and will helps organisations gain significant returns on investments by transforming costly high-volume print output to electronic information capture and presentation.

- Image Manager: provides comprehensive image management that will help the GHS control, share and quickly access critical business information. It extends the reach of critical information to all constituents to ensure information accuracy, consistency and timeliness. By integrating critical content with business applications and processes, Image Manager makes the right information immediately available to the people who need it, helping them make better decisions, faster.
- Business Process Manager: automates and optimises business processes by managing workflow and content among people and systems.
- Web Information Integrator: addresses content federation issues including integration, standardisation and consolidation by allowing organisations to access content from numerous heterogeneous repositories and unify it as critical business content.
- Search: a portfolio of scalable search solutions that can turn passive content into active sources of business insight. With a secure search, a managed user experience and content analytics solutions, you can reduce costs by increasing productivity, and turn content information into content intelligence.
- Message Store: E-mail and electronic messaging active archiving module designed to help reduce operational problems introduced by the growing size of e-mail and electronic messaging data stores.

4.2.18.13Correspondence Management

The mission of the GHS is to facilitate the development of a reliable and cost-effective world-class communication infrastructure and services, driven by appropriate technological innovation and accessible by all citizens on order to enhance the promotion of economic competitiveness in a knowledge-based environment. As such the Service engages in extensive communications with its statutory agencies to achieve this mission. A Correspondence Management system will serve as the Service's central system for tracking correspondence including letters and e-mails to and from other MDAs, cabinet and statutory agencies. For example, a Correspondence Management system will track each letter, the type of inquiry, the authority responsible for responding to the inquiry, the intended recipient of the response and the status of the response. The Service will then respond to each inquiry from the office of its statutory agencies or wherever the inquiries are coming from.

The correspondent management component will utilise a database and a set of tools to manage data, security and business rules of the application. Users will be able to access the application through a desktop interface. Security and access rights will be strictly enforced so that only the right people will have the chance to view certain information.

4.2.18.14Case Management

A Case Management system will be a comprehensive, integrated module that will manage and automate every aspect of how cases are managed at the Service. A case is defined as all of the processes, resources, business rules, tasks and analysis as well as the details and evidence that needs to be captured and managed during the case, inquiry, event or investigative management process.

A robust case management solution will also allow the GHS automatically create tasks based on business rules; assign tasks, maintain a single source of truth for each case, log and timestamp all updates, manage attachments including documents, images, audio files, html files and more, set up notifications and alerts for events and create comprehensive integrated reports.

4.2.18.15Strategic Planning

Strategic Planning application will give Directors of the various departments and other decision makers a flexible tool to create joint partner plans and strategies and define specific objectives. Over time, actual performance can be compared to targets and forecasts for variance analysis and evaluation of key success factors, or reasons for underperformance. The Strategic Planning application should have the capacity to interface with Performance Management systems, Finance systems and budgetary systems in to enable strategies to be developed holistically.

4.2.18.16Investment Planning

The Investment Planning system will be a tool for development, coordination and monitoring of investment project budgets. The system will manage investment activities that serve as a basis for executive decision making on project efficiency, elaboration of budgeting and procurement plans. It will automate both workflow processes of budget negotiation and monitoring for individual projects and investment portfolios, and technological process of data consolidation and analysis at multiple levels. The system will be designed as a set of applications with a single database.

Components of the system are:

- Planning and Reporting System: will address the core business functionality of the Service with regards to investment;
- Reference Data Management System: Consist of data on structure of the organisation, employees, types of investment projects and structure of expenses;
- Administration: Will provide information on Access rights, authorisation, authentication and general system administration issues.

Features of the Investment Planning system include:

- Powerful analytical tool enabling full view over budgets in terms of management and finance accounting, per projects or per business units.
- Access to each level of investment project data will be defined depending on functional responsibilities, level in hierarchy of the Service and employees' role.

- Tracking of changes in history, date, time and actions performed by a particular user.

4.2.18.17Policy Management and Administration

As part of the GHS work for promoting Information and Communication Technology in the country, policies are formulated and as such those policies need to be managed effectively. A policy management and administration system will enable policies to be managed effectively and accessed quickly and effectively by all stakeholders. Features of the Policy Management and Administration System include:

- Quick keyword searching of policies eliminating the need to know policies by title or department;
- A built-in approval workflow facilitating timely policy review and approval by key personnel;
- A central policy database promoting consistency and improved outcomes of policies made;
- Powerful reporting delivering timely management information and insight to support effective decision making;
- Data and educational services enabling almost effortless implementation and quick and effective staff utilisation.

4.2.18.18Marketing and Promotion Management System

A marketing and promotion system for the Service will enable other MDAs, citizens, and businesses become aware of the policies and projects defined and implemented by the GHS. For example the GHS have to promote the GGEA and eGIF to ensure their adoption by the MDAs.

Features of the system will include:

- Ability to support hundreds of users, files, projects and lots of contacts;
- Contacts manager: repository of contact details;
- Analytics engine to provide reporting information on the effectiveness of marketing campaigns;
- The system will be able to interface with other systems such as the Content management system which will trigger clients of the Service through emails.

4.2.18.19ERP Shared Services

The underlying technology to support the back office functions of the GHS is the Enterprise Resource Planning (ERP) system.
The GGEA's objective is to accomplish both effectiveness and efficiency gains through unified and well integrated Enterprise Resource Planning (ERP) application as a shared service for government. The ERP solution will support back office functions such as:

- Financial Management;

- Human Capital Management;
- Supply Chain Management;
- Fleet Management;
- Asset/Facilities Management
- Other administrative functions.

4.3Data Architecture

The data architecture provides a standard means by which data may be described, categorised and shared. The purpose of data is to aid decision making. Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. Data is the foundation of decision making, so MDAs must also carefully manage data to assure that they know where it is, can rely upon its accuracy, and can obtain it when needed. The data architecture comprises the relationship model, conceptual model, system interfaces and the process to data elements mapping.

4.3.1 Data Architecture Principles

1. **Principle:** Data is an Asset

   Data is an asset that has value to the Service and is managed accordingly.

   Rationale:

   Data is a valuable resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision making. Accurate, timely data is critical to accurate, timely decisions. Most organisational assets are carefully managed, and data is no exception. Data is the foundation of our decision making, so we must also carefully manage data to assure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.

   Implications:

   - This is one of three closely related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all departments within the Service understand the relationship between value of data, sharing of data, and accessibility to data.
   - Data stewards must be appointed and must have the authority and means to manage the data for which they are accountable.
   - The Service must make the cultural transition from "data-ownership" thinking to "data-stewardship" thinking.
   - The role of data steward is critical because obsolete, incorrect, or inconsistent data could be passed to personnel and adversely affect decisions across the Service.

- Part of the role of data steward, who manages the data, is to ensure data quality. Procedures must be developed and used to prevent and correct errors in the information and to improve those processes that produce flawed information. Data quality will need to be measured and steps taken to improve data quality -- it is probable that policy and procedures will need to be developed for this as well.
- A forum with comprehensive Service-wide representation should decide on process changes suggested by the steward.
- Since data is an asset of value to the entire Service, data stewards accountable for properly managing the data must be assigned at the Service level.

2. **Principle:** Data is shared

   Users have access to the data necessary to perform their duties; therefore, data is shared across business functions and departments.

   Rationale:

   Timely access to accurate data is essential to improving the quality and efficiency of Enterprise decision making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. The GHS holds a wealth of data, but it is stored in hundreds of incompatible stovepipe databases. The speed of data collection, creation, transfer, and assimilation is driven by the ability of the organisation to efficiently share these islands of data across the organisation.

   Shared data will result in improved decisions since the Service will rely on fewer (ultimately one virtual) sources of more accurate and timely managed data for all decision making. Electronically shared data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities.

   Implications:

   - This is one of three closely related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all departments within the Service understand the relationship between value of data, sharing of data, and accessibility to data.
   - To enable data sharing we must develop and abide by a common set of policies, procedures and standards governing data management and access for both the short and the long term.
   - The GHS will also need to develop standard data models, data elements, and other metadata that defines this shared environment and develop a repository system for storing this metadata to make it accessible.
   - For the long term, as legacy systems are replaced, the GHS must adopt and enforce common data access policies and guidelines for new application developers to ensure that data in new applications remains available to the shared environment and that data in the shared environment can continue to be used by the new applications.

- For both the short term and the long term the GHS must adopt common methods and tools for creating, maintaining and accessing the data shared across the organisation.
- Data sharing will require a significant cultural change.
- This principle of data sharing will continually "bump up against" the principle of data security. Under no circumstances will the data sharing principle cause confidential data to be compromised.
- Data made available for sharing will have to be relied upon by all users to execute their respective tasks. This will ensure that only the most accurate and timely data is relied upon for decision making. Shared data will become the Enterprise-wide "virtual single source" of data.

3. **Principle:** Data is accessible

   Data is accessible for users to perform their functions

   Rationale:

   Wide access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. Using information must be considered from an enterprise perspective to allow access by a wide variety of users. Staff time is saved and consistency of data is improved.

   Implications:

   - This is one of three closely related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all departments within the GHS understand the relationship between value of data, sharing of data, and accessibility to data.
   - Accessibility involves the ease with which users obtain information.
   - The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of users and their corresponding methods of access.
   - Access to data does not constitute understanding of the data. Personnel should take caution not to misinterpret information.
   - Access to data does not necessarily grant the user access rights to modify or disclose the data. This will require an education process and a change in the organisational culture, which currently supports a belief in "ownership" of data by functional units.

4. **Principle:** Data Trustee

   Each data element has a trustee accountable for data quality.

   Rationale:

   One of the benefits of an architected environment is the ability to share data (e.g., text, video, sound, etc.) across the Service. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the data trustee make

decisions about the content of data. Since data can lose its integrity when it is entered multiple times, the data trustee will have sole responsibility for data entry which eliminates redundant human effort and data storage resources. (Note that a trustee is different than steward - trustee is responsible for accuracy and currency of the data while responsibilities of a steward may be broader and include data standardisation and definition tasks.)

Implications:

- Real trusteeship dissolves the data "ownership" issues and allows the data to be available to meet all users' needs. This implies that a cultural change from data "ownership" to data "trusteeship" may be required.
- The data trustee will be responsible for meeting quality requirements levied upon the data for which the trustee is accountable.
- It is essential that the trustee has the ability to provide user confidence in the data based upon attributes such as 'data source.'
- It is essential to identify the true source of the data in order that the data authority can be assigned this trustee responsibility. This does not mean that classified sources will be revealed nor does it mean the source will be the trustee.
- Information should be captured electronically once and immediately validated as close to the source as possible. Quality control measures must be implemented to ensure the integrity of the data.
- As a result of sharing data across the Service, the trustee is accountable and responsible for the accuracy and currency of their designated data element(s) and subsequently, must then recognise the importance of this trusteeship responsibility.

5. **Principle:** Common vocabulary and data definitions

Data is defined consistently throughout the Service, and the definitions are understandable and available to all users.

Rationale:

The data that will be used in the development of applications must have a common definition throughout the Service to enable sharing of data. A common vocabulary will facilitate communications and enable dialogue to be effective. In addition, it is required to interface systems and exchange data.

Implications:

- Significant energy and resources must be committed to this task. It is a key to the success of efforts to improve the information environment. This is separate from but related to the issue of data element definition, which is addressed by a broad community - this is more like a common vocabulary and definition.
- The Service must establish the initial common vocabulary for the business. The definitions will be used uniformly throughout the organisation.

- Whenever a new data definition is required, the definition effort will be coordinated and reconciled with the corporate "glossary" of data descriptions. The Service's Data Administrator will provide this coordination.
- Ambiguities resulting from multiple parochial definitions of data must give way to accepted Service wide definitions and understanding.
- Multiple data standardisation initiatives need to be coordinated.
- Functional data administration responsibilities must be assigned.

6. **Principle:** Data Security

   Data is protected from unauthorised use and disclosure. In addition to the traditional aspects of national security classification, this includes, but is not limited to, protection of pre-decisional, sensitive, source selection sensitive and proprietary information.

   Rationale:

   Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information.

   Existing laws and regulations require the safeguarding of national security and the privacy of data, while permitting free and open access. Pre-decisional (work-in-progress, not yet authorised for release) information must be protected to avoid unwarranted speculation, misinterpretation, and inappropriate use.

   Implications:

   - Aggregation of data both classified and not, will create a large target requiring review and declassification procedures to maintain appropriate control. Data owners and/or functional users must determine if the aggregation results in an increased classification level. The GHS will need appropriate policy and procedures to handle this review and declassification. Access to information based on a need-to-know policy will force regular reviews of the body of information.
   - In order to adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level, not the application level.
   - Data security safeguards can be put in place to restrict access to "view only", or "never see". Sensitivity labelling for access to pre-decisional, decisional, classified, sensitive, or proprietary information must be determined.
   - Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorized access and manipulation. GHS information must be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster, or disclosure.

- Need new policies on managing duration of protection for pre-decisional information and other works-in-progress-- in consideration of content freshness.

4.3.2 The Data Relationship Model

The relationship model shows the relationships between the data entities identified to support GHS's business operations. An entity is any real world 'thing' that we want to keep data on. Assets, policy, supply chain, payment, human resource, and finance are all entities. An entity has attributes. Attributes describe the entity. Possible attributes are name, id or date. The Service formulates policies, manages programs, receives and sends request, supervises communication service providers, oversees statutory bodies, makes agreements and interacts with other MDAs. The Service manages employees, bearing in mind that recruiting is done by the office of the head of the Civil Service (OHCS). The recruitment aspect is thus handled in the GGEA report. The Service also manages many physical facilities, such as buildings. It is obvious that these relationships are similar to that which the government as a whole might have with entities which are very similar to these. However this data architecture provides an in-depth understanding of how the entities impact on the processes of the Service.

Figures 8 and 9 describe a conceptual view of the GHS's data model. Detailed Entity Relationship and Process to Data maps are provided in appendix B.

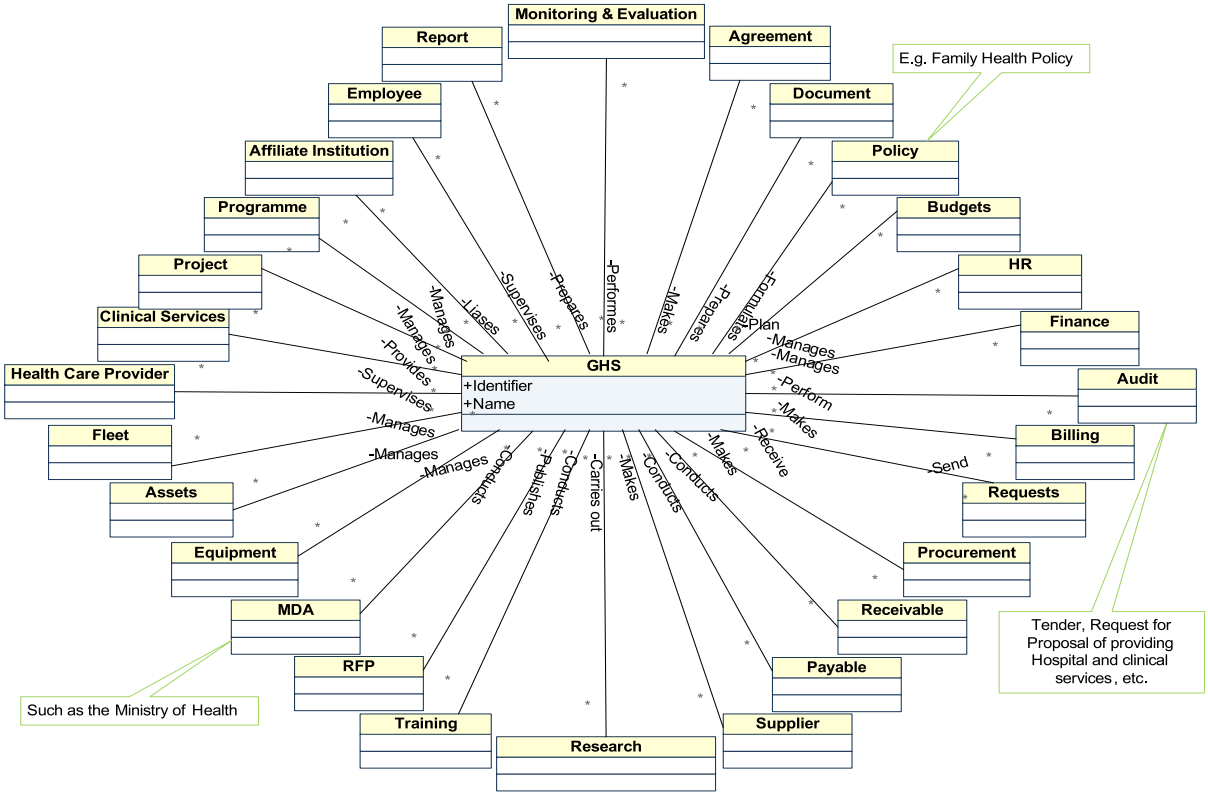


Figure 11: GHS Entity Relationship Diagram

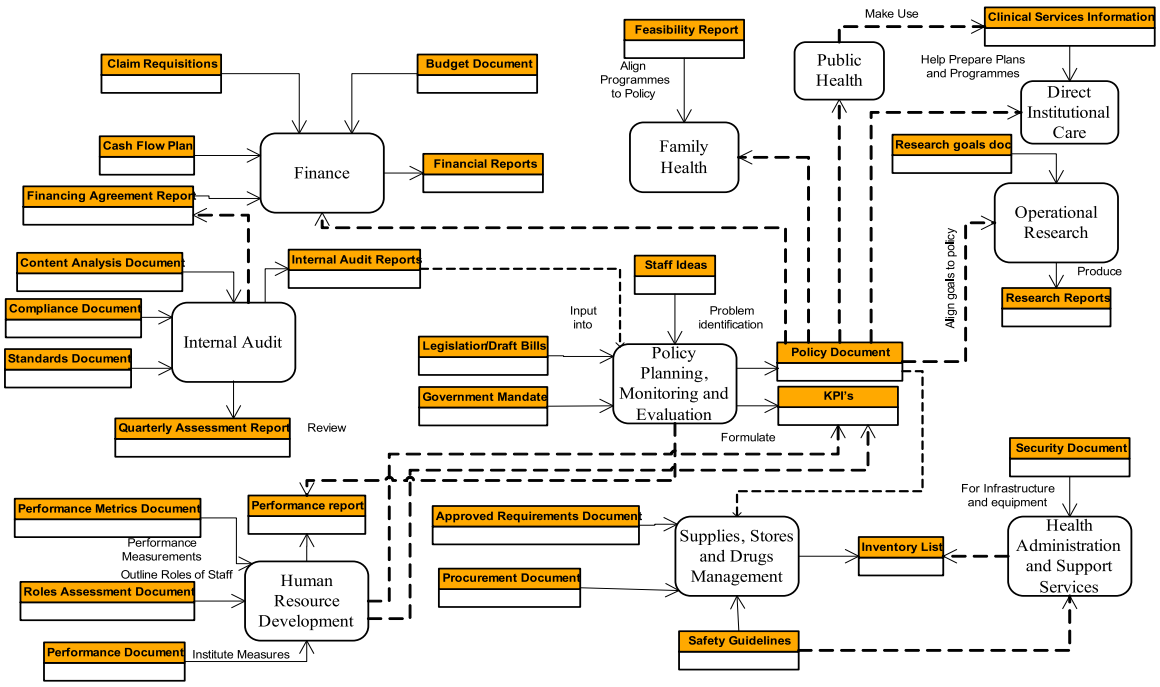


Figure 12: GHS Conceptual Model

The conceptual model describes the relationship between business processes and the various data entities. The model specifies data received into a process and the data output after the process has been carried out. Each entity is involved in one or more business processes. Those are, in turn, related to the functions, sub lines of business and lines of business of the government.

4.3.2.1Policy Entity

The Service maintains many policy documents dating back to the time it was given the mandate to formulate policies concerning the ICT sector. Policies are documents referring to guidelines and blue prints for achieving of a goal. For each policy document a set of metadata is maintained. This metadata includes the author and publisher of the policy document, the subject and keywords, the audience and the type and language of the document.
One important metadata item which must be associated with each document is its protection classification. This is the level assigned to national security information and material that denotes the degree of damage that its unauthorised disclosure would cause to national defence. Examples of possible security classifications are top secret, secret, etc. Another important aspect is its privacy classification, which should be applied to policy documents that are strictly for decision makers perusal and pertains to the degree of potential damage to the Service's privacy, in case the contents of this document would become public or leaked to a 3rd party.

4.3.2.2MDA Entity

MDA (Service Department Agency) is a permanent or semi-permanent organisation in the machinery of government that is responsible for the oversight and administration of specific functions, such as an intelligence agency or government Service. For each MDA we maintain the attributes and relationships common to all organisations such as employees, projects and budget.

4.3.2.3Employee Entity

The two main divisions in the HR are position and employee. An employee is a person who has an agreement with an organisation to perform duties and engage in activities on behalf of the organisation and for specific compensation. An employee fulfils a position. We assume that the master data store containing data regarding all employees and available positions will be maintained by the OHCS in conformance with the GGEA but that the Service will be involved in the recruitment and promotion processes.
An employee is first and foremost a person, and thus the core personal details for each employee, such as his name, Date of Birth, National ID number and current address will be derived from the National Registry population master data store. The National ID number would also serve as the unique key identifying an employee in the government employees master data store. This data store will maintain for each employee data such as her/his employment start date, her/his current position and salary, and her/his education and qualifications.

4.3.2.4Logistics Entity

Like all organisations, a Service needs to procure equipment and services in order to carry out its tasks. The Service when interested in procuring goods or services publishes an RFP. An RFP should be associated with a program, a project, and specific goals. In response to it different suppliers submit proposals. Once a supplier is selected, a fee is agreed upon and a contract is signed. The supplier provides the goods or services, and then submits an invoice. The Service then pays for the goods or services provided. The Service needs also to maintain stock of its existing equipment and perishable goods, through a stock management system. Correspondence should be established with supplier to make sure logistics are managed without any break in the supply chain.

4.3.2.5Asset Entity

An asset can be described as any structure or area that serves as a property (such as building, cars that has a specific use. The Service of communications on its own does not provide for and maintains its own assets. The government is responsible (directly or through private or government owned companies) for the maintenance and development of utilities and infrastructure. The GGEA gives a detailed description of the asset data entity in the Data Architecture Reference Model (DARM).

4.3.2.6Service Entity

The GHS does not provide direct service to the citizens. Its service offerings are done through the statutory agencies. However information on service offerings the GHS oversees needs to be kept to aid in the monitoring and evaluation process. The monitoring entity is linked to the MDA and report entities because monitoring activities are carried out on subordinate MDA after which reports are submitted. Types of services offered are postal and courier services, telecommunications services, Internet services, ICT training services. These services are provided for a fee. In some cases a contract needs to be signed between the customer who may be a citizen and the relevant service provider, in order for the service to be provided. Unlike in the commercial sector, this is the exception, rather than the rule. A service may be composed of multiple actions, spread over time.

4.3.2.7Budget Entity

The finance entity deals with the issue of budgeting with payments being dealt with as a separate entity. In this instance also the Service relies solely on the budgetary allocations form the government. However some of its statutory agencies such as the GIFTEL have their ways and means of raising funds. This is in no way connected to the Service's budgetary allocation. Since the Service has no way of raising funds on its own its finance entity is going to be an instance of the budgetary group in the GGEA. The GGEA DARM gives more detail on the entities in the budgetary group.

4.3.2.8Account Entity

The GHS has payables and receivables. Payables are money that a Service owes to suppliers, but hasn't paid yet, and receivables are amount of money that a person or an organisation owes Service, but has not paid yet. Payables are linked to invoices issued by suppliers, receivables are linked to invoices or payment notifications issued by the Service.

Payables and receivables are recorded together in the finance entity. A Finance entity records the amounts of money owned or owed by or to a particular person or organisation, or allocated to a particular purpose, and is used for managing the day to day finances of an organisation.

4.3.2.9Request Entity

This entity deals with any request that a Service makes. It comprises request for proposals, request for documents, request for budgetary allocations, etc. The other main method through which appropriated money is spent is by issuing RFP's for specific projects, equipment, or services, and than paying the commercial contractors selected during the RFP process. Category identification will be allocated with each request and the meta model of this entity will be hosted by the Service because of the uniqueness of requests.

4.3.2.10Agreement Entity

An agreement in this can be described in this context as a negotiated and typically legally binding arrangement. The Service of communications makes agreements with new service provision companies such as telecom companies. The agreements bother on the regulations and requirements for operations in the country. This is done through the statutory agencies. These agreements are to ensure that citizens have the full value of services that are being paid for. This entity will capture the category of the agreement, parties involved in the agreement and other details of the agreement.

4.3.2.11Programs Entity

The Service, based on its policies executes programmes in order to achieve its targets and goals. Programmes are a set of activities designed to achieve a certain goal. Programmes are subdivided into projects. We define a project as a planned action that represents a set of activities organised and managed to produce a specified product in a specified period of time with specified resources. A project has certain people and departments assigned to it, it has a budget and cost estimates, and is composed of a series of events. An event has a start date and an end date. An action is one, important type of event. An action is an activity, or the occurrence of an activity, that may utilise resources and may be focused on an objective. Thus an action is contained within a project, has a start and end date, and is related to an objective and to the resources it utilises.

Such resources may be personnel or equipment. A task is an action for which the cost can be estimated.

4.3.2.12Supplier Entity

A supplier is an individual or an organisation that makes a good or service available to someone or an organisation. An organisation interested in procuring goods or services publishes an RFP. An RFP should be associated with a program, a project, and specific goals. In response to it different suppliers submit proposals. Once a supplier is selected, a fee is agreed upon and a contract is signed. The supplier provides the goods or services, and then submits an invoice. The Service also maintains specific suppliers from whom logistics and services are procured. Normally these suppliers are contracted over a period.

4.3.2.13Monitoring Entity

The GHS monitors and evaluates the performance of service providers under its authority through the statutory bodies. The criticality of this requires that data be gathered on this process and managed effectively. The statutory agencies will monitor service providers while the Service monitors the statutory bodies. This entity is vital because information on past monitoring and evaluation should be readily available to enhance decision making.

4.3.2.14Organisation Entity

The GHS interacts with other public, private and non-governmental organisations. These organisations are in partnership with the Service to support the Various ICT investment initiatives that the Service undertakes. Data and correspondence needs to be managed effectively to sustain and manage this relationship with these partner organisations.

4.3.2.15Position Entity

A position is a specific job instance requiring an established set of duties and competencies. This entity is dependent on the employee entity. Every employee in the GHS operates in the capacity of a position and it's that position that determines the roles and responsibilities that an employee performs. The position entity will gather information such as the roles attached to a position as well as the privileges that are attached to it.

4.3.2.16Audit

The GHS performs periodic audit among its internal Departments and its statutory agencies. At the end of these audits various reports are submitted. This entity is therefore linked to the report entity which tracks various incoming and outgoing reports.

4.3.2.17Citizen Input

The GHS through its public Affairs department seeks citizens opinions on the impact of policies implemented. They also seek input that will aid in the formulating of policies. These inputs are normally collected through questionnaires or can be captured through various complaints forwarded by staff and citizens of the country. This entity will gather input in this very regard to help the GHS streamline the policy making process to address the needs of Ghanaians

4.3.3 Data Management Strategy

Data Management is an essential discipline for the GHS, as the organisation has to capture, store, analyse and report on a range of data captured and transformed into information for decision making. The organisation generates information on individual patients, populations, outcome of interventions and the state and nature of the infrastructure and systems through which the interventions are applied. Data Management in this context involves the control, information exchange and the management of structured and unstructured data across the organisation. These are supported by the following strategies that enable effective data management.

4.3.3.1Data Governance

Data Governance is the practice of making nation-wide decisions regarding GHS' information assets. Data governance includes the determination of data sources, responsibilities for integrity, defining requirements for business process development and change, and mechanisms of arbitrating differences among stakeholders.

Data governance involves the following:

4.3.3.1.1Email Management

In order to address the growing need for transparency in Government the organisation must retain a greater number of emails than ever before. The GHS needs a standardised, policy-based email retention system that ensures all relevant messages are stored safely and in accordance with any pertinent national laws and governing bodies.

To make email management procedures a cost-effective business asset, the GHS must develop, actively enforce and audit comprehensive retention guidelines. These rules should specify consistent, enterprise-wide data archive windows and define permissions for who can access, change or delete messages, attachments and other records. To this end, GHS should guide staff through the process of developing, implementing, monitoring and auditing a comprehensive email retention policy using the following 10 steps:

1. Define an Email Retention Policy

In order to fully understand its retention obligations, the GHS must first have a clear understanding of the types of content it transmits electronically. To provide this insight, the email retention policy should specify:

- Document types that employees can send via email, as well as the specific files, such as sensitive business contracts, that must be transmitted using a different method;
- Content guidelines defining what should or should not go into emails, including policies around what constitutes sexual harassment or other unacceptable language;
- Enforcement measures and best practices that automatically scan for policy violations and designate an internal authority to periodically review content.

2. Eliminate the Variables Hindering Centralisation

   Without formal archiving guidelines and an automated system to manage the process, employees often save old messages and attachments on local storage systems, such as a PC hard drive. This lack of standardisation makes tracking and protecting archived messages problematic. For example, a judge can request messages saved on personal archives during litigation. But if an employee saves these on a hard drive, which then fails, the information is lost and the GHS becomes vulnerable to legal and regulatory penalties around the spoliation of data.

   Moreover, locating the necessary data on all local hard drives throughout a large organisation is a difficult, time-consuming and expensive process that often fails to discover every message saved on a non-standardised source. To avoid the possibility of missing a message, email retention policies should include specific, centralised archiving methods that prohibit employees from saving messages in personal folders.

3. Educate Employees about the Retention Policy

   Even though a formal email retention policy may be defined and in place, many employees may remain unaware that such guidelines exist. To ensure that archiving rules are followed across the GHS, all employees must be trained on the policy and able to demonstrate that they understand content and storage procedures, as well as any rules restricting the use of personal folders. Moreover, education should:

   - Detail the reasons why these rules are in place;
   - Offer instructions for using any supporting archiving technology;
   - Outline the consequences of noncompliance at both a business and personal level.

4. Incorporate Relevant Regulations into the Retention Policy

   It is critical that all email retention policies incorporate the requirements of the mandates governing the industry sector in which an organisation operates. Although many regulations exist the GHS must ensure the following requirements are key aspect of compliance:

- Data permanence, where data must be in its original state without being altered or deleted;
- Data security, where all retained information must be protected against security threats, including access by unauthorised persons and any outside forces that could physically damage or endanger the availability of archived messages;
- Availability, where organisations must prove that all emails subject to the retention policy can be easily accessed by authorised personnel in a timely manner.

5. Identify Roles with Unique Retention Requirements

   Specific organisational roles have unique archiving requirements, which must be captured in the larger retention policy. It is common practice in most organisations across the globe to save the emails of CEOs/MD/ indefinitely, even after their tenures have ended. GHS's retention policy must ensure that business emails from Ministers and the Chief Director are kept for a very long period.

6. Balance Retention Guidelines and Related ICT Costs

   Though there are many specific legal and regulatory guidelines around email retention, no court or compliance authority demands the archiving of every email ever sent or received. As a result, GHS should implement a retention policy that reduces the storage burden by ensuring that the emails essential to meeting compliance and litigation guidelines are saved, while those that are not needed are deleted. By reducing storage through retention and deletion policies in line with legal and compliance mandates, the ICT department can limit storage-related expenditures and streamline email administration tasks, which often comprise more than 40 percent of total ICT support costs.

7. Provide Employees with Access to Archived Messages

   As GHS establishes overarching policies for archiving and deleting email messages, they must also verify that all employees have access to the electronic assets they need to carry out their business responsibilities. To support productivity, policies should establish rules that enable certain messages to be saved for personal communication, while allowing all other messages to be managed by the default retention strategy. These rules should also allow users to search for all archived email in both production and offline storage systems, and in some cases, enable employees in similar roles to access messages owned by their co-workers.

8. Ensure that Retention Policies Can Accommodate Legal Holds

   Email retention policies must be flexible enough to be suspended if a legal hold is necessary. For example, if an organisation is anticipating legal action, it might choose to retain all emails in order to preserve the information that may be used as evidence during litigation. It is critical that policies accommodate legal holds, because courts can impose sanctions for the spoliation of any messaging content or electronic records that are relevant to a legal proceeding.

9. Validate that All Messages Are Archived

   In order to comply with e-Government and litigation mandates, GHS must confirm and demonstrate that all emails are captured and subject to the retention policy. To support this critical goal and eliminate the possibility that information escapes retention, the GHS should leverage an information governance solution with functionality that provides the live, real-time capture of every message that falls under the rules of the retention policy.

10. Use Technology to Enforce Retention Policies

    To achieve the goals outlined in its email retention policy, the GHS should implement a robust, automated information governance solution capable of enforcing policy guidelines across the business in an efficient, effective manner. Such a solution is the key to improving legal hold management, speeding retention processes and maintaining an archive that preserves necessary messages and purges nonessential emails as necessary. Information governance solutions should help simplify access to archived messages through rules to grant permission by business classification, protect messages as corporate assets and make them available to employees within similar roles.

4.3.3.1.2Data Classification

Data classification is the categorisation of data for its most effective and efficient use. The GHS must classify its data according to the critical value or how often it needs to be accessed, with the most critical or often-used data stored on the fastest media while other data can be stored on slower (and less expensive) media. This kind of classification tends to optimise the use of data storage for multiple purposes, e.g. technical, administrative, legal, and economic.

Data can be classified according to any criteria, not only relative importance or frequency of use. For example, data can be broken down according to its topical content, file type, operating platform, average file size in megabytes or gigabytes, when it was created, when it was last accessed or modified, which person or department last accessed or modified it, and which personnel or departments use it the most. A well-planned data classification system makes essential data easy to find. This can be of particular importance in risk management, legal discovery, and compliance with Government regulations.

4.3.3.1.3Data Quality Management

Poor data quality can undermine the everyday operations and performance of the GHS in multiple ways. It can increase risk by making the organisation vulnerable to defaults and fraud, for example, because the organisation lacks accurate or up-to-date information about the entities receiving assistance.

Poor data quality can also increase the GHS's costs by causing resources to be misdirected (e.g., an inspector visiting the wrong office). Moreover, additional resources may be needed to resolve data inconsistencies or gaps, maintain duplicate source files, rationalise and synthesise data for insight, and address other data problems. The GHS's ability to comply with laws and regulations defining its fiduciary responsibilities is also hampered because poor data quality often leads to overpayments and other improper handling of funds. And poor data quality almost certainly

results in decreased mission performance because the organisation will lack visibility into operations and processes, staff are reluctant to use data they do not trust, and strategic decisions may be based on inaccurate or incomplete information.

The GHS must develop a continuous and iterative framework that can help the ICT departments control the quality of data in the organisation.

The framework must continuously monitor the quality of data and provide necessary inputs to users or systems to take timely actions.

The framework consists of the following four steps:

- Detection: Detecting the data quality issues is the first step towards ensuring quality. Intelligent algorithms and tools are deployed to continuously monitor and report the quality of the data and flag any anomalies in the data elements as erroneous.
-
- Correction: This step involves taking necessary actions to correct the data anomalies. While analytical algorithms are used to auto-correct some of the entries, user intervention is called for when there is more than one choice of action that can be taken.
- Measurement: The measurement step involves measuring the data quality and tracking errors. It ensures that all reported anomalies are corrected and monitored. Key performance indicators such as average cycle rate for error fix, and total error data are captured, trended, and reported to management periodically. Data errors need to be classified as follows to have specific strategy based on classification.

  Type 1 error occurs when relationship is assumed but in fact does not exist. This leads to additional validation and false alarms.

  Type 2 errors occur when no relationship is assumed when in fact it exists. Detecting Type 2 errors is difficult as they require in-depth data analysis. Defining confidence limits of the data errors helps in prioritising the effort that needs to be spent to bring the data quality within control limits.
- Learn: The step involves reviewing the process periodically and enhancing the ability to detect and correct anomalies by deploying additional tools and by reforming business processes. This step ensures that the effort required maintaining the data quality reduces over time.

4.3.3.1.4Data Quality Control Process

Any data quality initiative needs well-defined processes to be followed for maximising the control on quality. The data quality control process involves assessment of data quality issues, cleansing and augmentation of data, and tracking and reporting of data anomalies. The control process consists of:

- Data Assessment - Data assessment phase consists of analysing the data structures and finalising the scope of data quality audits. This is an important phase for data management as priorities of correction efforts is determined in this phase. In data

mapping or the profiling phase, end to end mapping between source system and destination system are carried out. The phase involves detection of errors and correction of data to control the data integrity over time.

- Standardise - The standardising exercise is important to upgrade data content to meet business rules and industry standards. Data must be made consistent across systems, which in turn reduces redundancy. Data standardisation can be done at the following two levels:
    - Coding standardisation involves product codes, financial codes, inventory numbers, model numbers, programme types and so on. For example, all B/W printers from HP are coded starting with BWHP-PRN which makes product recognition easy;
    - Address standardisation involves consistency in the order of various data fields. For example, 9575 N FARM ROAD 173 needs to be changed to 9575 N FARM RD 173.
- Cleanse - The data cleansing and preparation phase fulfils the following objectives:
    - Ensure that the data meets the requirements of future state system;
    - Minimise migration related errors, thus reducing manual data entry effort.

  Cleansing is carried out to ensure integrity of data and to prepare the data for specific migration needs. Some of the constraints that can be enforced are:

  Referential constraints to verify if the key is present in referential master table before transaction record can be built:
    - Unique constraints to ensure that duplicates within an entity are avoided;
    - Default constraints to plug in default values in the absence of user entry in commercial databases.
- Enhance: The enhance phase involves data augmentation by enhancing the information algorithms customised to business scenarios are implemented to detect the violations of the rules. Additional correction procedures are also deployed for rapid error fix. A few instances where cleansing is required are as follows:
    - Inactive master records with no transactions and inspecting them for potential purges;
    - Transaction records with no masters;
    - Invoices with missing Accounts Receivable and vice versa.
- Enforce: Commercial databases can also be leveraged for enforcing referential integrity and constraints. Additional business rules can be enforced using pre-defined triggers on value using internal and external data sources.

Data can also be enhanced by sourcing information from systems within the organisation by matching the required contents across the applications. For example, various customers in database are linked together with information in external database, which resulted in more accurate reporting.

- Consolidate: The consolidate phase involves reducing duplicate or unnecessary information in data store. This ensures that transactions are assigned to correct dimensions making rolling up easier.
- Tracking and Reporting: Monitoring and tracking the data cleansing exercise is important to understand readiness of data and also the progress. It enables users to know if the correction has been successful or not. It provides the ability to prioritise based on severity of data quality issues and trend line. The performance of data quality control teams can be assessed on the action taken on reported quality issues. Tracking also helps identify the most common causes of errors and help explore the possibilities of automating correction procedures.
- Data Quality Verification: Data quality verification focuses on additional efforts to verify the quality of data by performing live tests on the data. The data is tested in cyclic validation runs to test databases and analysis is carried out on the migration to pre-verify the quality of the data. This provides necessary information to the management about readiness of the data in terms of quality.
- Exception Analysis: Data validation or error analysis plays an important role in data migration. It shows the business community the end result of data cleansing being carried out and also gives visibility into the errors, their causes, and the corrective action that needs to be taken. Detailed analysis of errors encountered during migration, statistical summarisation of erred records and tracking of success percentage of each conversion run help reduce chances of errors during subsequent runs and also proactively identify new areas of cleansing for achieving higher conversion rates.
- Reconciliation: Reconciliation is a process through which data from both source and target systems are compared and analysed. Scripts must be run to bring both source and target data into a common framework for comparison. Financial reconciliation, for example, specifically looks at matching revenue and expense related data from source and destination systems to ensure that revenue flow remains constant.

4.3.3.1.5Data Security

Data security is the means of ensuring that data is kept safe from corruption or theft and that access to it is suitably controlled. Thus data security helps to ensure privacy. It also helps in protecting sensitive Government data.

The Security Architecture Reference Model identifies a number of mechanisms to promote data security. Technologies used for data security include:

- Disk Encryption Disk encryption refers to encryption technology that encrypts data on a hard disk drive. Disk encryption typically takes form in either software or hardware. Disk

encryption is often referred to as on-the-fly encryption ("OTFE") or transparent encryption;

- Backups - Are used to ensure data which is lost can be recovered;
- Data Masking - Data masking of structured data is the process of obscuring (masking) specific data within a database table or cell to ensure that data security is maintained and sensitive customer information is not leaked outside of the authorised environment;
- Data Erasure - Data erasure is a method of software-based overwriting that completely destroys all electronic data residing on a hard drive or other digital media to ensure that no sensitive data is leaked when an asset is retired or reused.

4.3.3.1.6Master Data management

Master Data Management is extremely important in ensuring the consistent use of data across Government and details in discussed in the Applications Architecture Reference Model section of this document.

4.3.3.1.7Metadata Management

Metadata is defined as ‘data about data’ and it has been defined to support the e-Government Interoperability Framework (eGIF). The Metadata standards defined by the eGIF provide the structure and rules governing metadata used by the public sector. This standardisation is essential if data is to be truly interoperable, and if citizens are to be able to find Government information and services without a knowledge of the structure of Government and the allocation of responsibilities within it. The eGIF Monitoring and Evaluation and Assessment Methodologies provide the necessary information on how eGIF components such as the Metadata will be managed.

4.3.3.1.8XML Data Management

XML Schemas have been defined by the eGIF and the GoG technical policies for systems data integration and transformation cover XML and XML Schemas for data integration. The eGIF Monitoring and Evaluation and Assessment Methodologies provide the necessary information on how eGIF components such as the XML management.

4.3.3.2Data Sharing

Data Sharing is the practice of provisioning data from an information source to an information consumer in response to a business requirement. A data sharing architecture is a standard, repeatable technical pattern for sharing data. If an MDA can enforce its architecture through a governance process as data is shared to support real business needs, then the MDA has a good chance of creating quality data.

4.3.3.2.1Data Integration

The GHS does not operate in isolation, it shares and exchanges data with citizens, businesses and other MDAs. The data generated by the GHS in some cases have to be integrated and the technologies used include ETL. The Major techniques involved in data integration are data consolidation and data propagation.

Data consolidation involves capturing of data from multiple source systems and integrating into a single persistent data store. The latency of the information in the consolidated data store depends upon whether batch or real time data consolidation is being used and how often the updates are being applied to the data store.

Data propagation involves replicating data in different locations from different sources. Technologies include replication, database log scrapers and change data capture software.

Data Access uses search capabilities to make information accessible to uses via searchable indexes, aggregations and caches using the same type of search technologies that drive Internet search. The application of search technology in an Enterprise is known as Enterprise Information Access.

Details of data integration techniques are provided in section 4.2.7.2.

4.4Technical Architecture

The Technical Architecture is a framework categorising the standards and technologies for the technical infrastructure to support the secure delivery of ICT services for the GHS. It also defines the technical specifications of products, protocols, etc that support the different layers of infrastructure.

4.4.1 Technical Architecture Principles

1. **Principle:** Requirements-Based Change

   Only in response to business needs are changes to applications and technology made.

   Rationale:

   This principle will foster an atmosphere where the information environment changes in response to the needs of the business, rather than having the business change in response to information technology changes. This is to ensure that the purpose of the information support -- the transaction of business -- is the basis for any proposed change. Unintended effects on business due to information technology changes will be minimized. A change in

technology may provide an opportunity to improve the business process and hence, change business needs.

Implications:

- Changes in implementation will follow full examination of the proposed changes using the Enterprise architecture.
- We don't fund a technical improvement or system development unless a documented business need exists.
- Change management processes conforming to this principle will be developed and implemented.
- This principle may bump up against the responsive change principle. We must ensure the requirements documentation process does not hinder responsive change to meet legitimate business needs. Purpose of this principle is to keep us focused on business, not technology, needs--responsive change is also a business need.

2. **Principle:** Responsive Change Management

   Changes to the Enterprise information environment are implemented in a timely manner.

   Rationale:

   If people are to be expected to work within the Enterprise information environment, that information environment must be responsive to their needs.

   Implications:

   - We have to develop processes for managing and implementing change that do not create delays.
   - A user who feels a need for change will need to connect with a "business expert" to facilitate explanation and implementation of that need.
   - If we are going to make changes, we must keep the architectures updated.
   - Adopting this principle might require additional resources.
   - This will conflict with other principles (e.g., Maximum Enterprise-wide benefit, Enterprise-wide Applications, etc.).

3. **Principle: Control Technical Diversity**

   Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.

   Rationale:

   There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. There are further infrastructure costs incurred to keep multiple processor constructs interconnected and maintained.

Limiting the number of supported components will simplify maintainability and reduce costs.

The business advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements. Common technology across the Enterprise brings the benefits of economies of scale to the Enterprise. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

Implications:

- Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle.
- Technology choices will be constrained by the choices available within the technology blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and emplaced.
- We are not freezing our technology baseline. We welcome technology advances and will change the technology blueprint when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated.

4. **Principle: Interoperability**

Software and hardware should conform to defined standards that promote interoperability for data, applications and technology.

Rationale:

Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products, and facilitate supply chain integration.

Implications:

- Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution.
- A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established.
- The existing IT platforms must be identified and documented.

4.4.2 Shared Infrastructure

The key principle that underlines the GGEA Technical Architecture Reference Model is that of a service based approach to the development and deployment of shared infrastructure services for

all MDAs. As such the GHS's technical infrastructure strategy will be based on the GoG's shared services strategy for the Wide Area Network and Centralised Data Centre Services.

4.4.2.1Wide Area Network

The GHS will use the proposed Government shared Wide Area Network (WAN) infrastructure to link the various offices and agencies. The GHS is facilitating the implementation of the GoG WAN (GovNet) and there is required to use it.

As illustrated in figure 10 the GHS Local Area Networks will be connected to the GovNet and the detailed architecture of the GovNet will define the topology and bandwidth requirements for all agencies.

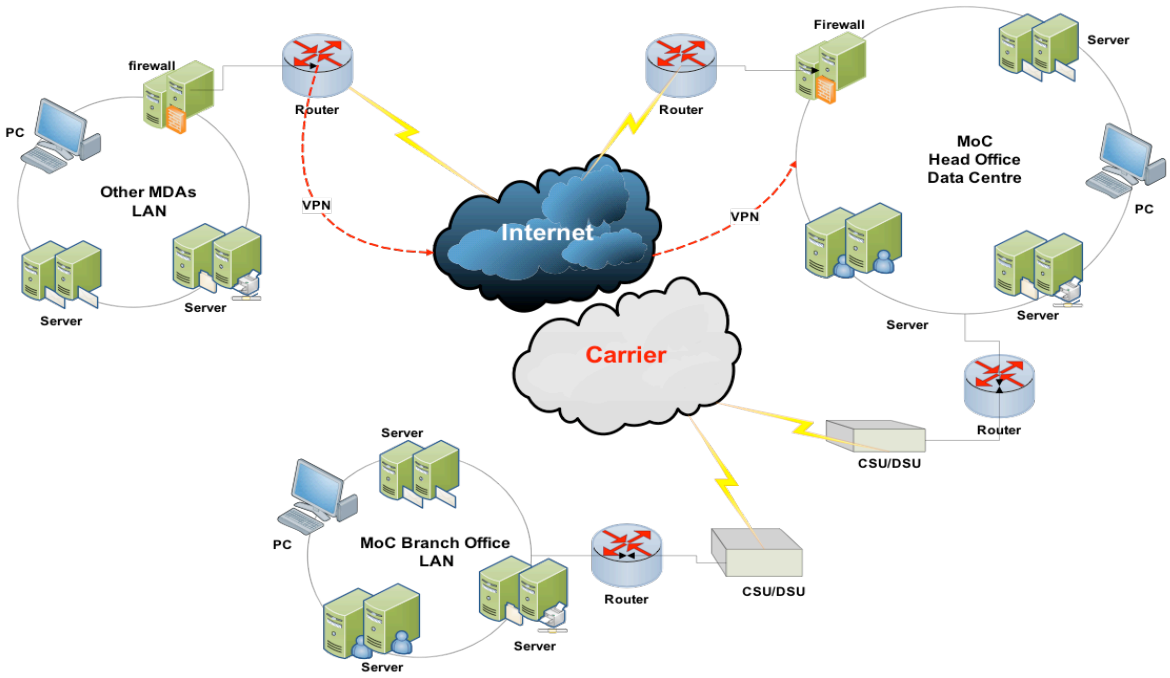


Figure 13: WAN Connectivity Devices

The GovNet solution should be based on carrier-class equipment and should use Virtual Private Network (VPN) technology to create secure networks via the combination of meshed VPN tunnels to form a single routing context. It should enable the creation of logically meshed network environments without physically provisioning individual circuits.

The new converged network should extend the concept of a 'peering point' to form virtual 'peering networks' to enable seamless access to networks, access services like Internet Access and Remote Access, Data Centre Services and other 3rd party services. Common infrastructure drastically simplifies the overall solution and provides the following benefits to the Government:

- Increased reliability and security;
- Increased levels of standardisation and performance to improve the overall consistency of services delivered to the entire organisation;
- Rapid transition and transformation to deliver cost and service benefits as quickly as possible.

The recommendation is for the Government of Ghana to implement a core national backbone layered over the service provider managed network connecting each of the proposed key Government Data Centres. The national backbone would interconnect networks from each of the MDAs to form a coherent, national network. Some of the benefits of this approach are:

- Allowing the Government to chose single national backbone network provider;
- Using IP address summary approach, this will ensure less routing and therefore less overhead on national network.

For future strategy and design, Multi Protocol Label Switching (MPLS) is recommended as being fit for purpose.
MPLS is recommended as the WAN protocol as it delivers the following benefits:

- MPLS can create "any-to-any" VPN without a full mesh of Permanent Virtual Circuits (PVCs);
- With MPLS achieving "Fully-Meshed" VPNs are simpler than many hub-and-spoke configurations;
- Support for voice and video by applying Quality of Service (QoS) to time sensitive packets;
- Switches traffic more rapidly than traditional routing protocols;
- Secure communication;
- Logically separates VPN traffic;
- Connectivity is flexible and uncomplicated.

At a national level, the recommendation is to have a converged network to support data, voice and video. The WAN architecture should be a tiered approach and within this, the GoG Data Centres will form a national backbone and then various agencies with their own WAN and Data Centres connected to the national WAN (GovNet).
GoG should ensure the following are provided by the service provider(s) for national services:

- Privacy – all traffic must be encrypted using high-speed hardware encryption modules to 3DES standard, and the GovNet should have its own private routing environment;
- Resilience – all the major Government Data Centres should be connected to a highly redundant carrier-class equipment and form a fully meshed network;
- High Capacity – all GoG Data Centre nodes should have minimum of 8Mbps access or greater.

- Low Latency –full meshing and hardware encryption should ensure that latency times are low.

Connectivity onto the national network should be through two peering points and these should be located at the GoG Data Centres (locations to be decided, but assumed to be Accra and Kumasi).
GoG should follow industry best practice for implementing end-to-end QoS by identifying the network traffic and its QoS requirements, classifying the network traffic into the appropriate traffic classes and mark the network traffic as close to the source as possible and define the scheduling policy for each traffic class.
GoG should use the following guidelines for deploying end to end QoS to get maximum advantage:

- Achieve the required QoS by managing the delay, delay variation (jitter), bandwidth, and packet-loss parameters on a network;
- Classify and mark traffic as close to the source as possible;
- Ensure that real-time traffic gets priority with minimal delay;
- Ensure that business-critical traffic is correctly serviced;
- Ensure that scavenger traffic (for example, file sharing) does NOT consume too much valuable bandwidth;
- Use link efficiency techniques on WAN links;
- Profile applications to their basic network requirements;
- Do not over engineer provisioning. Use no more than four to five traffic classes for data traffic for example:
    - Mission-Critical: e.g. MDA's defined critical applications;
    - Transactional: e.g. ERP applications;
    - Best-Effort: e.g. email;
    - Less-than-Best-Effort (Scavenger): e.g. Other less critical applications
- Only group applications with common characteristics together into the same class.
- Most applications fall under best effort; make sure that adequate bandwidth is provisioned for this default class;
- Seek executive endorsement of relative ranking of application priority prior to rolling out QoS policies for data.

Figure 11 below shows an overview of the key components of the Ghana Government GovNet network infrastructure design. The design must be based on a modular approach with full resilience built within each module. The different modules are:

- The Internet Hosting Module;
- The VPN and Remote Access Module;

- The Internet Browsing Module;

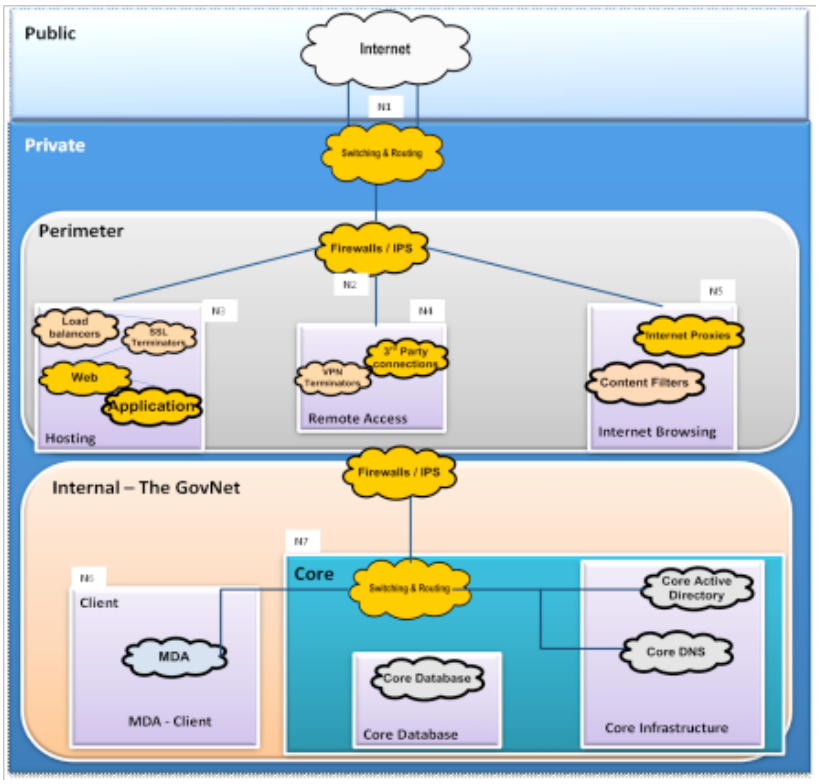


Figure 14: GovNet Infrastructure

The architecture includes:

- **NI – The Public Internet**: two Internet peering connections from two different service providers should be deployed for full resilience. As the main network for e-Government, the availability of its Internet Access shall be of paramount importance. The Internet should connect to the GovNet infrastructure through an additional two screening routers. A bandwidth of 8Mbps is recommended for the initial implementation.
- **N2 – Firewalls & Intrusion Prevention Systems (IPS)**: a Perimeter Firewall services should be implemented to provide the application layer proxy firewall function to control traffic between the Public and Private zones. An Internal Firewall services should be employed to provide application layer access control function between the Perimeter and the Internal - GovNet - core infrastructure.
- **N3 – The Internal Hosting Module:** this module will provide the hosting environment for all the e-Government hosting services. A 3-tiered architecture model is provided, with front-end, application and database layers for secure service deployments. The front-end firewalls will provide Demilitarised Zone (DMZ) connectivity for the front-end Web services, and the Application layer, whilst the back-end firewalls will provide connectivity to the database layer and the Internal GovNet core infrastructure.

There should also be a separate DMZ with a pair of SSL terminators for HTTPS traffic and SSL Offloading from Web services. This will act as the initial point of contact for all inbound connections to the hosting environment. Critical and transactional government services will be based on secure Web services using SSL and XML.

4.4.2.2Data Network Connectivity

The Data Centre will become a 'mission critical facility' that acts as the heart of GHS service delivery in Ghana. The most important asset of GHS is data and as such its availability, security and redundancy must be assured. The GHS will utilise the shared Government Data Centre services to host its applications.

4.4.2.2.1Data Network Elements

The data network elements model is based on a multi-layered model consisting of:

- **Core Layer**
  The core layer represents the network physical entry gateway with external networks (GovNet & Internet). Scalability in the proposed Data Centre solution is achieved by aggregating different Zones into a Core Routing layer. The core routing layer allows the following functions:
  - High speed routing between different Zones
  - Interconnects the Data Centre to the WAN in reliable way
  - Provides traffic control QoS over links toward GovNet
  - Maintain traffic separation between different VPN if required
  - VPN traffic separation might be implemented at L3 by using MPLS VPN technologies.
- **Distribution Layer**
  This layer builds the main skeleton of the data centre data network. Distribution layer provides the following features:
  - Layer3 routing functionality of all LAN subnets/VLANs which represent different virtual security layers and zones;
  - Acts as an aggregation point for all access layer switches/systems. Blocking ratio must be calculated carefully in this point in order to prevent any network bottleneck;
  - Represents the entry point for high-end systems with high-speed Gigabit network interface cards like backend servers and storage servers;

- Provides localised high availability features.

In order to have all the features mentioned above, the hardware used as building units for the distribution layer must have a backplane speed sufficient to handle the huge size of traffic passing through it. Also throughput value (in Million packets per second) is extremely important in ensure the capability of used modules to handle the passing traffic. To ensure redundant solution in the distribution layer, the following features shall be available:

- Two chassis per distribution node/zone fully redundant to each other
- A fully per chassis redundancy in terms of power supplies, processing engine and fans
- Redundant uplinks per chassis to the core layer elements
- Uplinks are aggregated together to act as one virtual high speed link

- **Access Layer**

  The access layer is the end system network layer, which connected all servers to the network through high-density ports architecture. Access layer is a pure layer 2 commodity element which represents the physical separation between different security layers and zones through layer 2 VLAN configuration and trunking the uplinks to the distribution nodes. Both distribution and access layers will be connected to servers based on the tier of the servers as follows:

  - Tier one servers are connected to access layer 2 switches using Fast Ethernet interface;
  - Tier two servers are connected to access layer 2 switches and the high-speed Giga interfaces are directly connected to the distribution nodes;
  - Tier three servers and storage servers are directly connected to the distribution switches through high speed Gigabit and 10 Gigabit Ethernet interfaces.

As illustrated in figure 12 the data network model is a multi-tiered model that will host different servers for the GHS and other agencies in the Government Data Centres. The different tiers are:

4.4.2.3Connectivity Layer

Data connectivity for the various channels will be provided through the Government Secure Intranet using the Internet also the private cellular networks will also be used to support channels such as Mobile Phone and PDAs. This data network tier will serve as a gateway to the Data Centre network with the outside world. All network logical interfaces of GoG secure intranet layer as well as Internet access to hosted systems. This tier handles routing functionality of

external routes (coming from Internet and WAN) and injects them towards the required inside destination as per the approved security policy.

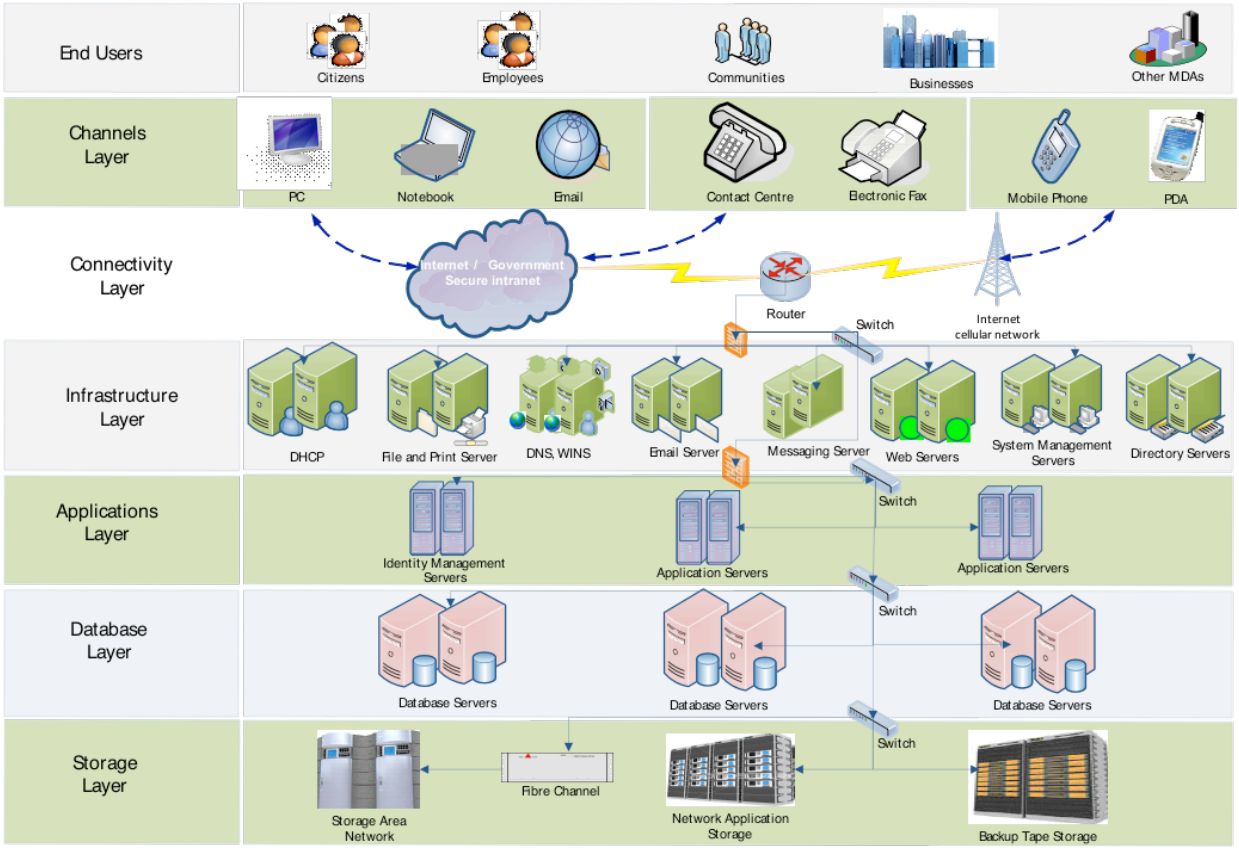


Figure 15: Data Centre Connectivity

4.4.2.4The Infrastructure Layer

The Infrastructure Layer hosts technical and administrative servers such as Identity Management Servers, Directory Servers, DHCP Servers, File and Print Servers, DNS and WINS, E-mail Servers, Messaging Servers, and Web Servers that support the delivery of online services. This layer is hosted in a DMZ for protection. The Infrastructure Layer provides the proxy functionalities, where software or hardware proxy servers are used if needed to serve specific applications in the lower tiers. It also hosts application velocity services used for servers' performance optimisation and offloading through different reverse proxy techniques and products as well as Systems Management servers.

4.4.2.5 The Applications Layer

The Applications Layer is responsible for hosting the specific application servers that need to be deployed to support MDA specific business applications. It will consist of application server instances that will be based on medium sized multiple CPU servers. This tier provides business

logic functionality and processing capabilities and services, such as EJB containers, .Net components, or middleware connector modules that integrate applications. Like the Infrastructure Layer the application servers will also be grouped as server farms, which will be hosted along business criticality and application environment lines.

4.4.2.6The Database Layer

The Database Layer will consist of a set of highly available servers that provides persistent data storage services for critical corporate data. Due to the sensitive nature of the data, this tier will be highly protected in terms of security and availability. The database tier is also structured into server farms for Linux/Oracle, Linux/MySQL and Windows/SQL Server across the Data Centres and the details of the configuration will be provided by the Government Data Centre architecture project. The architecture defines data replication objectives ranging from real-time of mission and business critical copies to daily or weekly copies of non-critical applications, depending on the application capabilities and business criticality requirements.
To meet the reliability and recoverability requirements of the architecture, a traditional cluster solution will be used and the clustered nodes distributed in the Government Data Centres.

4.4.2.7 The Storage Layer

The Storage Layer outlines three major storage modes: Storage Area Network (SAN); Network Applications Storage (NAS); and Backup Tape Storage. Each of these three storages modes will handle different storage needs for GHS.

4.4.2.7.1Network Attached Storage (NAS)

Network Attached Storage as an engineered storage system will provide a flexible and scalable solution to the file-sharing needs of GHS. All user data and file sharing of GHS will be stored on the NAS. It is a server-based storage that runs an operating system specifically designed for handling network file services and has direct storage access to the local area network (LAN) through LAN protocols such as TCP/IP.

4.4.2.7.2Storage Area Networks (SAN)

The SAN will provide access to high performance and availability of storage subsystems. All GHS application and operating system data will be stored on the SAN. The storage subsystems are generally available to multiple hosts at the same time, which makes them scalable and flexible. SAN is connected via a fibre channel thus providing a very fast and easy access and interchange of data. The switches help route storage traffic (in methods that are similar to those used by LAN network switches), disk storage subsystems, and tape libraries.

4.4.2.7.3Backup Tape Storage

Backup Tape Storage will serve as storage server specifically dedicated for making data backups for all GHS files at the Data Centre. It is made up of disk storage subsystems, and tape libraries which it easy to backup file on them.

4.4.2.7.4Direct-Attached Storage (DAS)

Aside the SAN, NAS and backup tape storage systems, Direct-Attached Storages (local disk drives, tape drives, CD drives etc) can be used to store operating system data to enhance quick. The DAS access data through Integrated Device Electronics (IDE) or SCSI interfaces of RAID (redundant array of independent disks) controllers. The main characteristic of DAS is that it provides fast data access to the directly attached serve. The disadvantage to using DAS is that the storage is only accessible by the Server to which it is attached to.

4.4.2.8 Local Area Network (LAN)

In line with the OSI model, LAN connectivity in the GHS should be created by connecting multiple network hosts (PCS, printers, scanners) through a L2 connectivity device or connecting multiple network segments using a L3 connectivity device. The L2 connectivity device uses switches to move data packets at L2 between hosts or devices on the same network segment whilst L3 connectivity devices uses routers or load-balancing devices to move data packets between hosts and/or devices on the same network segment at L3.
The speed of connectivity in the Local Area Network (LAN) should be 10Mbps or higher and a bandwidth size of 100Mbps (a standard speed for normal distributed network connectivity). In the case whereby a high speed application and backbone layer connectivity, the bandwidth should be between 1Gbps to 10Gbps.

4.4.2.8.1Virtual LAN (VLAN)

VLAN technology can also be used to improve network connectivity within GHS. A logically segmented LAN is referred to as Virtual LAN (VLAN). VLAN is created using the same physical network device (switch). A LAN usually has the ports on its segment sharing the same broadcast domain. However a VLAN is made possible where a set of ports on a switch can share the same broadcast traffic and ports outside the set (evening though physically part of the same switch) cannot share it.
VLAN is typically based on L2; however, we can also have L3 VLAN. Some switches can route traffic between VLANs; when this happens, it is usually referred to as L3 VLAN. When L2 VLAN is used, no other segment is routed to or from it at L3. When L3 VLAN is used, other L2 VLANs are routed to or from it within the switch.

4.4.2.9Remote Access

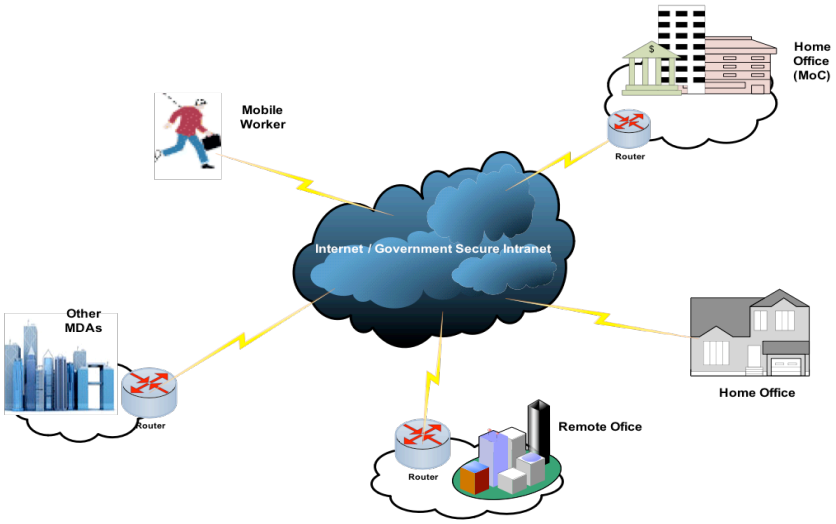


Figure 16: Remote Access Requirements

The remote access functionality provides endpoint connectivity to remote clients or offices. The devices that perform this role generally also perform the routing and firewall services roles for all traffic between the main network and the remote client or site. GHS Branch offices and other users will typically connect to the head office's (GHS) enterprise facilities (Data Centre) through the following:

- **Remote Access Server (RAS)**

  With this application, mobile and remote users use analogue (dial-up modems) or ISDN switched services to get connectivity. This will also help remote offices that do not have a permanent connection to the Government Secure Intranet to get connected. The application will be managed through the RAS server. Users will use analogue (dial-up modems) or ISDN switched services to connect to GHS Data Centre.

  The figure below show how remote users will connect to GHS Data Centre via RAS. This connection will enable e-mail accessibility, file downloading, and access to other GHS system facilities.

- **Virtual Private Network (VPN)**

  A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the MDA's private network to the remote site or employee. It helps distant employees or clients to work together. It provides security, reliability and scalability.

  Some of the benefits of using VPN include: Reduction in the start-up cost associated with a RAS, associated modems, and technical support (installation, configuration, and maintenance of RAS) costs; Replaces long-distance or telephone number services with local ISP connections at remote sites; and gives full access to all data and applications (including e-mail or file transfers) over the Internet.

5. Security Architecture

The Security Architecture for the GHS defines common, industry-wide, open-standards-based technologies and applicable industry best practices as the cornerstone elements required to enable secure and efficient transaction of business, delivery of services, and communications between the GHS and its stakeholders.

The MoH legal framework on the use of data across the sector includes the following provisions:

- Data collection - in line with the principles of information privacy, data collected by the health sector shall be non patient identifiable. This shall be different from the policies on medical records management.
- Data storage - appropriate standards are needed in relation to the condition in which the data is maintained. This includes precautions against fire and other accidents and criminal acts. In the case of computer-based records, the additional question arises as to how the records can be accessed. Because of data sensitivity, appropriate security against unauthorised access and modification is essential.
- Internally used data - medical data should only be used for the purposes for which it was collected, and for additional purposes authorised by law, or consented to by the data subject. The purposes for which health data is collected needs to be clear.
- Disclosure to third parties - since medical data is sensitive, and since a duty of confidence generally applies to data which a health care professional gathers in the course of his relationship with a patient, it is necessary to regard health care data as being unavailable to third parties in the absence of a clear and authoritative reason. In the case of a referral care is needed to ensure that only relevant parts of the patient's history are communicated.
- Data access by subjects - the principle of data ownership is to appreciate that, while the records (the documents or disks) are unequivocally the property of the practitioner or institution, the data is not. Data is not capable of being owned, and many different people have an interest in it, including and especially the person to whom it relates.
- Record transfer - although records are owned by their originator, a patient has a very real interest in having them, or at least an accurate representation of their contents, transferred to his new health care professional. The practice of transferring records when an appropriately documented request is made is therefore highly desirable from a treatment viewpoint.
- Record destruction - patient history is one of the relatively few classes of record for which some genuine justification exists for long-term retention However the volume of information which is generated becomes very large, and much of it does become irrelevant over time, and hence periodic summarisation and destruction of old material should be aimed at.

These provisions generally promote information security management in the GHS in terms of the protection of data and dealing with patient confidentiality and privacy issues.

5.1 SECURITY PRINCIPLES

The GHS will adopt the following security principles as defined by the GGEA:
The principles are:

- **Principle 1 – Security, confidentiality and privacy**

  GHS ICT systems should be implemented in adherence with all security, confidentiality and privacy policies and applicable statutes.

  Rationale:

  The GHS process government information to provide services and also make decisions and all such information must be protected according to government-wide rules, regulations and policies concerning security, confidentiality and privacy of data.

  Implications:

  - Need to identify, publish, and keep the applicable policies current;
  - Need to monitor and enforce compliance to policies;
  - Must make the requirements for security, confidentiality and privacy clear to everyone;
  - Awareness on information security issues such as privacy and confidentiality must become a routine part of normal business processes.

- **Principle 2 – Ability to provide secure e-Government services**

  The Security Architecture must enable the GHS to perform business processes electronically and deliver secure e-government services to the public.

  Rationale:

  The GHS must be able to conduct business processes that provide access to information and resources electronically, while maintaining confidentiality and integrity. A standard set of security services allows the GHS to focus on business goals rather than on the development and implementation of independent security services.

  Implications:

- The implementation of the Security Architecture will:
    - Help protect the GHSs' critical assets of resources and information;
    - Provide a framework and foundation for secure interoperability and flexibility in conducting electronic business across Ghana.

- **Principle 3 – Applying appropriate security levels**

The GHS must be able to apply a level of security to systems and resources commensurate with their value to the organisation and sufficient to contain risk to an acceptable level.

Rationale:

Security is an e-Government and business process requirement with associated costs. Security costs should be rationalised to the intended benefits of the services that are delivered, and appropriate to the level of security required

Implications:

- Implementation of the appropriate level of security will safeguard against security costs that potentially increase beyond mandated requirements and the value of the assets protected.
- Security must be managed to compliment, not unnecessarily impede the GHS's business operations.

- **Principle 4 – Maintain security accountability**

For auditing and reporting purposes, accurate system date and time are essential to all security functions and accountability and must be maintained.

Rationale:

There is a need for accountability from information security standpoint to enable GHS capture information from security logs captured from various storage devices for reporting and auditing purposes. The ability to capture security logs is one of the key benefits of using technology for data processing.

Implications:

- The validity of digital signatures and electronic transactions depends on precise, reliable date and time information.
- Audit accountability relies on placing events sequentially according to date and time.

- **Principle 5 – Must be based acceptable standards**

  The Security Architecture must be based on industry-wide, open standards.

  Rationale:

  The Security Architecture that utilises open standards at all modular levels ensures portability and integration across platforms.
  Open standards-based solutions facilitate inter-MDA communications and data exchange and allow adaptability to migrate to emerging security technologies.

  Implications:

  - Security Architecture services are infrastructure-level services; therefore, to take advantage of security services, application-level security should be designed for open standards.
  - Security services already exist for many common applications; however, products from vendors may be implemented in ways that make it difficult to integrate these products into overall security architecture. Existing application, system, or platform security mechanisms should be used whenever they match Security Architecture target standards. Application-specific security mechanisms should only be developed where necessary.

- **Principle 6 – Protecting government's security assets**

  Utilising defence-in-depth and layered security approaches protects the GHSs information assets.

  Rationale:

  Managing government information security to protect assets must be based on a structured approach.

  Implications:

  - The use of layered security controls across all aspects of network and application better protects resources from various security threats and vulnerabilities, thereby reducing the overall risk of a potential security incident.
  - The use of layered security controls and mechanisms better protects the asset if security controls are circumvented.

- Protection of a resource is best accomplished by placing controls as close to the resource as possible. Additional layers of security help to protect the resource in the event that the primary means of protection fails for any reason.

- **Principle 7 – Interoperability framework**

Security is a critical component of individual GHS systems interoperability.

Rationale:

Open, industry-wide standards-based security solutions support interoperability needs between application systems and position MDAs for future interoperability opportunities.

Implications:

- MDAs should use encryption technologies when sharing sensitive data.
- Web-enabled transactions that require user authentication for transfer of sensitive data or funds should use encryption technologies.

- **Principle 8 – Catering for MDA needs**

Security architecture should accommodate varying security needs.

Rationale:

The GHS requirements for security vary depending upon the nature of communications, the sensitivity of the information, and the risks to the agency. Security needs will change as business requirements and applications change.

Implications:

- Security services should be granular enough to accommodate the different levels of assurance required, and extensible enough to meet future requirements;
- Resetting security assurance levels should not require modification of the Security Architecture.
- Security Architecture must be flexible to support the introduction and/or integration of new technologies, while maintaining appropriate security protection and meeting statutory requirements.
- Whenever security is required, the location in a communications protocol will have an impact on performance, reliance on an underlying network protocol, and on developers. Choosing the appropriate layer in a communications protocol for security will maximise usability and minimise future changes. The performance impact can be

minimised when security services are located in the lower layers of the communications protocol. Services provided at the transport layer have less impact on application programmers than services that run above that layer.

5.2 GHS SECURITY FRAMEWORK

The GHS adopts the GGEA information security framework as illustrated by figure 14 below.

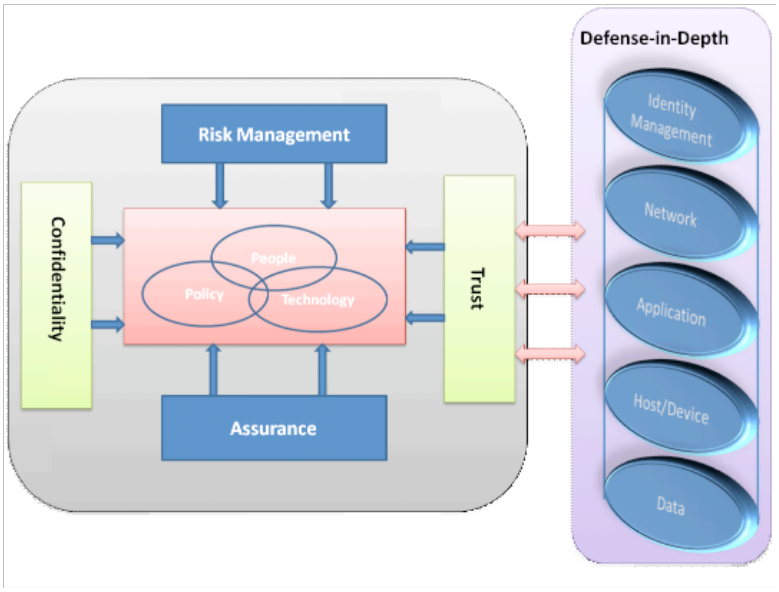


Figure 17: Information Security Framework

The details of the framework are provided in the GGEA but it can be summarised as:

5.2.1 Confidentiality

In the provisioning of GHS services online, it is inevitable that transactions will be conducted which requires confidentiality to ensure that such information is accessible only to authorised users by enforcing the necessary level of secrecy at each stage of data processing and preventing unauthorised disclosure.

A consistent level of confidentiality should be maintained across the GHS in terms of determining the confidentiality levels of information.

The confidentiality levels of GHS information are:

- Level 0 - GHS transactions that involve no private information content - No explicit confidentiality protection is needed though care should still be taken to adopt good system practice.
- Level 1 - GHS transactions in which the information exchanged is client specific but where the impact of public exposure would be a **minor** resource or nuisance impact on one or more of the involved parties - Unpublished private information should be either stored on a system to which only authorised government users have physical access, or else should be password-protected.

- Level 2 – GHS transactions involving private information that could be regarded as sensitive - Data stored in a live environment (*e.*g. on a database) should be protected by strong access control.

5.2.2 Risk Management

The GHS adopts a Risk Management processes for conducting risk assessments and implementing the agreed mitigation strategies. Information security risks are threats that can impact on the availability, confidentially, or integrity of information.

Information Risk Management is about reducing the impact and effect of government information being compromised by unauthorised disclosure, lack of integrity or availability. The process involves identifying information assets, identifying threats, analysing the risks, developing mitigating strategies and contingencies. An Information Risk Management framework is critical to ensure that an adverse impact of the security of information being compromised on the GHS is reduced to acceptable levels. Information Risk Management must be an integral part of day-to-day operational decision making.

5.2.3 Trust

Trust is another element of the Security Framework. The success or failure of many business transactions depends on the levels of trust that the parties involved have for each other.
In order to secure a communication between two parties, the two parties must exchange security credentials (either directly or indirectly). However, each party needs to determine if they can "trust" the asserted credentials of the other party. Citizens, other MDAs and government in general must be confident about the claims (e.g. name, identity, key, group, privilege, capability, etc.) of the individuals that use the electronic government services.

5.2.4 Assurance

Information security assurance is the set of activities that create higher confidence in the system's ability to carry out its design goals even in the face of malicious abuse. These activities are performed by, or on behalf of, an enterprise as tests of the security practices. Activities include penetration testing, code auditing and analysis, and security specific hardware and software controls. The security processes, defence in depth technologies, etc are all built on sets of assumptions; assurance activities challenge these assumptions, and especially the implementations.

Assurance activities should be applied in conjunction with overall risk management goals, for example when the GHS elects to take on a risky integration with a business partner, some of the exposure can be mitigated by increasing assurance activities on the system. Assurance activities

are applied to all of the core security services, which are protection, detection, and response. The Security Architecture should identify areas where assurance services can be leveraged across the multiple projects. For example where multi-factor authentication is federated across domains, or where an XML security gateway provides reusable input validation and authentication services for multiple Web Services.

5.2.5 Identity Management

The GHS will adopt the GoG's Identity Management, which is to provide a combination of processes, standards and technologies to manage and secure access to the e-Government information and resources, whilst also shielding users' details. Identity Management can provide the capabilities to effectively manage such processes both internal and external to particular MDAs for public servants, citizens, business, and even other government applications, and correspondingly, anyone or anything that needs to interact with government services online.
The e-Identity solution should be viewed as primarily a tool for:

- Defining the identity of an entity (a person, place, or thing) for e-Government services;
- Storing relevant information about entities, such as names and credentials, in a secure, flexible, customisable store;
- Enabling secure access to online credentials through a set of standard interfaces;
- Providing a resilient, distributed, and high-performance infrastructure for Identity Management that interacts with all e-government services;
- Helping to manage the relationships to resources and other MDAs in a defined context.

5.2.6 Defence -in-Depth

Defence-in-depth is a multi-layered approach that applies multiple strategies to protect resources from external and internal threats. Sometimes referred to as security-in-depth or multilayered security, defence-in-depth is a term used to describe the layering of security countermeasures to form a cohesive security environment. The deployment of a defence-in-depth strategy includes protective measures all the way from your external routers through to the location of your resources and at all points in between.

Deploying multiple layers of security helps ensure that if one layer is compromised, the other layers will provide the security needed to protect your resources. For example, compromising an organisation's firewall should not provide an attacker unfettered access to the organisation's most sensitive data. Ideally, each layer should provide different forms of countermeasures to prevent the same exploit method from being used at multiple layers.

5.2.7 Physical Security

This section involves physical security elements of the Security Architecture.

5.2.7.1 Access to Data Centre

Information systems (servers, storage, client devices, etc.), media storage areas, and related communication wiring and network devices shall be located in secure locations that are locked and restricted to access by authorised personnel only (facility physical plant permitting). The following security methods shall be implemented:

- Access to secured areas shall only be granted by the facility owner upon written request;
- Facilities containing critical data or information shall be subject to access monitoring that establishes the identity of the person entering/exiting as well as the date and time of the access (e.g., recording badge information, videotaping) and provides data for auditing of physical access;
- Emergency exits to facilities housing critical information systems and related communication wiring and network devices shall be secured for re-entry of only authorised personnel;
- Where locking mechanisms with keypads are used to access secure areas, entry codes shall be changed periodically, according to a schedule defined by the budget unit;
- Where badge-reading systems are employed to log access into and out of a secure facility, "piggybacking" of badge holders shall be prohibited;
- Unused keys, entry devices, etc., shall be secured.

5.2.7.2Environmental Considerations for Data Centre

Information systems, media storage areas, and related communication wiring and network devices should be protected against loss or malfunction of environmental equipment or services necessary for the operation of the facility.

- Appropriate fire suppression and prevention devices should be installed and functioning according to manufacturer's specifications.
- Environmental (A/C) systems should be routinely maintained.
- Environmental facilities (A/C, heating, water, sewage, etc.) should be periodically inspected and reviewed for risk of failure.
- Locations of plumbing system lines should be known, and if possible, not in close proximity to "critical" IT devices, communication wiring, and network devices.
- Uninterruptible Power Supply (UPS) systems and backup generators shall provide a safeguard against loss of electrical power.

6. Enterprise ICT Management

To manage ICT services effectively the GHS must adopt the IT Infrastructure Library (ITIL) framework for the management of ICT services. ITIL provides the MDAs with the following benefits:

- Improved quality because of the standardised framework for service;
- Improved stability and integrity of the environment through automated configuration tools and processes;
- Improved IT services by proven best practice processes;
- Improved end user satisfaction through a more professional approach to service delivery standards and guidance;
- Improved productivity and use of skills and experience;
- Improved delivery of third-party services through the specification of ITIL standards for service delivery in services procurements.

The key ITIL processes to be defined and implemented by the GHS to support ICT service delivery and support are:

- **Service Level Management**: To partner with the customers to define and agree IT services to meet the organization's requirements; to monitor, measure and report on the agreed IT services and to initiate formal actions to ensure service levels are met.
- **Service Catalogue Management**: To ensure that a Service Catalog is produced and maintained containing accurate information on all operational services and those being prepared for deployment.
- **Capacity Management**: To ensure that cost justifiable IT capacity in all areas of IT, always exists and is matched to the current and future agreed needs of the business, in a timely manner.

- **Availability Management**: To ensure that the level of service availability delivered in all services is matched to or exceeds the current and future agreed needs of the business, in a cost effective manner.
- **Service Continuity Management**: To support the overall Business Continuity Management process by ensuring that the required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required, and agreed, business timescales.
- **Information Security Management**: To align IT security with business security and ensure that information security is effectively managed in all service and Service Management activities.
- **Supplier Management**: to manage suppliers and the services they supply, to provide seamless quality of IT service to the business, ensuring value for money is obtained.
- **Event Management**: The basis for Operational Monitoring and Control; the ability to detect Events, make sense of them, and determine the appropriate control action. Events are detectable or discernable occurrences that could impact the management of the IT infrastructure or cause a deviation in the delivery of IT service.
- **Incident Management**: The process for dealing with all failures, questions or queries reported by the users (usually via a telephone call to the Service Desk), by technical staff, or automatically detected and reported by event monitoring tools, with the aim of restoring normal service operation as quickly as possible to minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.
- **Request Fulfilment**: The processes of dealing with requests that are not the result of a problem with the infrastructure to prevent them from congesting or obstructing the normal incident and change management processes.
- **Problem Management**: The process responsible for managing the lifecycle of all problems with the aim of preventing them and resulting incidents from happening, to eliminate recurring incidents or to minimize the impact of unpreventable incidents. Problem Management focuses on root cause and trend analysis in respect of incidents, ensuring that resolutions are implemented through the appropriate control procedures.
- **Change Management**: Is about the controlling of the process which is necessary for applying 'change requests' to a system. This involves assessing the impact, approving or rejecting the change, assigning, scheduling, and the tracking of the change request until it is either implemented or withdrawn.
- **Software Control & Distribution (Release Management):** Software distribution is the control of the packaging, distribution, and installation of software in a Distributed Systems Management environment. It controls the installation of new packages or upgrades to existing applications, or system software releases.

- **Configuration management**: Is an essential part of distributed systems management as it is the process of collecting, recording, maintaining, and the monitoring of the systems inventory within the organisation. All hardware, software and configuration information is recorded in a central inventory catalogue enabling the organisation to administer system resources.

Other non ITIL processes to be implemented are:

- **Single Point Operations and Systems Management:** In order to provide a single point of operations and system monitoring, a common interface to all system facets is required. Controlling, monitoring system status, events and automating the operation of different systems, is the ultimate goal of distributed systems management.

  Platform-specific software will be required to link to a central hub of operations control. From which, the monitoring and control of the various systems, events, and messages can be used to control, by automation or human intervention, the multi-vendor, multi-platform and multi-component operations of an organisation.

  This central point of operation will allow:

  - operators to request status and resource information and will provide, ideally in a graphical format, an instant picture of system status
  - events generated by managed elements or element managers to alert operators, visually and aurally, of unsolicited systems activity
  - the running of automatic recovery actions to restore system status
  - unattended operations monitoring and automatic notification, via an appropriate medium (email, fax, voice) to alert support staff of systems failure if non-automatic recovery is impossible

- **Network Management**: covers the configuration, administration, monitoring and control of local and wide area networks (LAN's and WAN's). This includes all such components as:

  - The network interface;
  - Hardware and software drivers;
  - Routers;
  - Hubs;
  - Switches;
  - Communication lines;
  - Etc.

  Various tools and utilities can be employed to manage the networks and their interfaces to the systems. These should be administered through the single point of operations.

  Network management software should be capable of:

- Sending alerts raised as a result of events which cause a change in the status of the network - component failure, high utilisation, high error rate;
- Supplying status information collected online;
- Activating or resetting line traces;
- Execution of pre-defined actions associated with alerts;
- Enabling network configuration changes;
- Enabling or disabling of connections;
- Fault reporting in the internal and, where applicable, the external fault management system;
- Notification to a (maintenance) supplier of failed network component.

- **On-line Performance Monitoring:** The use of online performance monitoring tools is used to track the various critical system and/or network performance metrics. By monitoring when acceptable threshold levels are exceeded, they allow prompt action to be taken in determining the cause of poor systems performance problems. This means that systems can be proactively managed and service levels maintained.

  Again these tools should ideally have a graphical display and be able to maintain historical performance, tuning and trend analysis charts and figures. Thus the systems performance can be measured over time by maintaining a trace log of specific performance metrics which provides input to Capacity Management.

  Monitoring of resource usage identifies heavy systems users or programs and allows operators to adjust the priorities of running processes, or the temporarily suspending of jobs in order restore system performance to acceptable levels.

  Network metrics enable similar identification and resolution of problems. By measuring performance degradation operators may infer heavy usage, poor line quality or intermittent faults and may be able to boost systems performance by deferring jobs generating a lot of network traffic to a later time.

- **Desktop Remote Control:** provides the ability to work on a desk-top system, usually a PC, by authorised personnel, controlling the screen, keyboard and peripherals from a distant location across the local or wide area network.

  This enables systems or maintenance personnel to:

  - Monitor critical information and systems or program performance;
  - Execute programs on the remote system;
  - Reboot the system if necessary;
  - Simulate keyboard and/or pointing device entries to the system;
  - Instruct remote users in the operation of a system or software.

  For reasons of security and possibly to comply with legal constraints/requirements, remote access will usually require the remote desktop user's permission and the authorisation from an organisations policy monitors.

Once a remote session is initiated, the remote user and the desktop user will share the same view of any screen changes and cursor movements as they happen. Typically the remote desktop user will be informed that a remote session is taking place and may even be required to specifically authorise the connection.

Once the remote access is in session, all keystrokes and cursor movements should be recorded to a log file to allow audit tracing and possible automatic backtracking or replay. All results should be available to the desktop user and forwarded to the remote desktop operator giving the impression of working locally on the remote system.

- **Storage Device Management:** this involves the management of the physical media that is used to backup system software and data, including magnetic tape, cartridge, optical disk, disk mirroring and microfilm. It is concerned with the movement of this medium to off-site locations for the purpose of distribution, archiving or data recovery following a failure.

  The GoG Data Centre may use robotic tape cartridge carousels or mirrored disks at a remote site and are backed up on a regular basis. PC's on the other hand, rely on their user to take backups. Departmental servers need to be treated in the same way as enterprise servers when it comes to backing them up. That is, they must have a backup strategy and schedule and the media must be removable to an off-site facility.

  Media librarians should manage the movement and security of backup media to off-site storage locations and may be responsible for the distribution of machine readable output to third parties.

  The backup of remote servers installed in regional and branch offices should ideally be controlled centrally. Files backed-up to the servers local media should be secured by local system users who would be responsible for its physical handling and storage. Alternatively, network bandwidth permitting, all data could be backed-up to the central location.

  The backup of individual PCs, whether networked or standalone, is typically the responsibility of their users, but remote desktop control could be employed to initiate backup of networked PC's.

  A backup and recovery strategy will determine not only the frequency of backups, the media, the location and storage of them but also the 'shelve life' of the media involved and the replacement and upgrades to that media.

  Whenever a file or database needs to be recovered, there should be easy access to either the original or a copy of the required data. Preferably, this will be on-line or near-line with any necessary library database being used to retrieve the identification and location of the media containing the requested copy. Automation is the key to keeping down-time to a minimum.

- **Database Management:** This deal with all administration related to the successful management of databases facilities, whether on a single platform, or distributed over many. Managing the complexities of modern database systems involves:
    - Provision of an enterprise wide data dictionary;
    - The physical design and location of database areas, files, tables, records, etc. for performance considerations controlled at a local level;
    - Record all mappings between the enterprise wide schema and each local site;
    - The definition, generation and implementation of Data Definition Language statements for new database objects or amendments to existing ones;
    - Consideration and implementation of locking strategies to maximise multi-user availability and to allow on-line backups;
    - Procedures for the recovery of database objects in the event of failure or corruption;
    - Investigation into problems related to the performance of the database and the recommendations for program and database changes.

7.ICT Governance Model

The governance model to support the GHS's EA implementation will involve local capabilities, structure, policies and procedures that must be aligned with the national ICT governance processes. The governance functions include the following:

- The CIO/ICT Director;
- The GHS Enterprise Architect;
- Domain Architects;
- Programme Management Office;
- Service Management

7.1 GHS CIO/ICT DIRECTOR

A Chief Information Officer (CIO) will be appointed at the GHS in consultation with the national CIO. The CIO's role and responsibility will be primarily the implementation of the Service's e-Government strategy based on the local EA and the provision of end to end ICT services to the GHS. The CIO will liaise with key stakeholders throughout Service and other agencies, including Enterprise Architects, Programme and Project Managers, Line of Business Directors, etc. to develop the ICT strategy for the GHS.

The CIO will consider the following when selecting ICT investments for the GHS:

- Delivering services and information to citizens electronically;
- Reducing burden on citizens and businesses;
- Determining that the investment is part of the agency's modernisation blueprint;
- Ensuring interoperability of systems;
- Improving and simplifying business processes;
- Reusing technology where applicable.

Specific CIO requirements include:

- Participating in the functions of the CIO Council;
- Monitoring implementation of ICT standards, including the e-Government Interoperability Framework (eGIF) and government's information security and privacy policies;
- Ensuring ICT Audits are conducted regularly for ICT systems
- Working with the Line of Business Leaders to define Service Level Agreements (SLAs) for end to end ICT services for the MDA
- Developing Operational Level Agreements (OLAs) with vendors and ICT service suppliers to ensure they meet their service commitments to the MDA.
- Ensuring that MDA ICT training programmes is consistent with central government's ICT development provisions.

7.2 THE GHS ENTERPRISE ARCHITECT

The CIO will appoint, with the Chief Director's approval, an Enterprise Architect who will be responsible for leading the development of the GHS's EA work products and support environment. The Enterprise Architect will serve as the technology and business leader for the development organization, ensuring the integrity of the architectural development processes and the content of the Enterprise Architecture products.

The role of the GHS Enterprise Architect will include:

- Liaising with the Line of Business units and ensuring that their business processes are emphasised in the MDA's Enterprise Architecture;
- Responsible for the implementation of the GHS's Enterprise Architecture programme;

- Chairing local MDA Architecture Board to perform technical reviews of projects;
- Facilitate the interaction and cooperation between the business community and ICT organisation;
- Ensure compliance of eGIF and architectural principles, standards and policies;
- Strategic and technical ICT planning, policy development, capital planning and investment control, change management, systems engineering and architectural design;
- The Enterprise Architect will be in charge of the Domain Architects.

7.3 DOMAIN ARCHITECTS

The GHS will appoint Domain Architects (e.g. Business, Data, Technical Architects) will be appointed to provide deep technical design expertise.

The Domain Architects will identify the technologies to be used for their specific areas of expertise and will work with the Enterprise Architect to provide technical input into their areas of expertise. The Domain Architects could be assigned on temporary basis to work as design authorities on projects.

The roles include:

- Presiding over the design and structure to the application, data or technical infrastructure;
- Ensuring that the design is adequately documented and established with design guidelines and best practices;
- The Domain Architects will enforce compliance to standards and policies through Architecture Reviews;
- Ensuring that technical risks for the deployment have been assessed and mitigated and that non-functional requirement are captured and incorporated into the design.

7.4 PROGRAMME MANAGEMENT OFFICE

The GHS's EA implementation will be treated as a formal programme with full sponsorship at the ministerial level. An Enterprise Architecture Programme Management Office (EAPMO) should be established to manage, monitor, and control the development and maintenance of the GHS EA. The EAPMO will be managed an experienced Programme Manager and other staff will include experienced Project Managers, Architects, Financial Managers and Office Assistants. The EAPMO identifies and performs cost analyses of alternative approaches for developing the Enterprise Architecture, and manages internal and external contractor development effort. The EAPMO is also charged with determining needed resources and securing funding and resource commitments.

A primary goal of the EAPMO is to ensure success of the implementation of the Enterprise Architecture. It will oversee the different projects to ensure there is consistency of approach and the use standard of disciplines. The role of the EAPMO includes:

- Enabling more effective delivery of the GHS EA as a government change driver and keeping the focus on the change objectives;
- Providing a framework for senior management to direct the change process;

7.5 Service Management

The GHS will establish a Service Management function to define and maintain required levels of ICT services to the user community. The Service Management function is required to support the implementation of the EA and will focus the needs of the Service as the primary driver for the development of the ICT infrastructure. Rather than arbitrarily deploying computers and networks of various capabilities and capacities, an effective Service Management strategy takes into consideration the needs of the users for any given application area when designing and implementing that portion of the Enterprise Architecture.

Service Management comprises of people, processes and technology and it is recommended that IT Infrastructure Library (ITIL) based Service Management disciplines are employed at the GHS to provide ICT services. ITIL is considered to be industry best practice for Service Management used by thousands of organisations around the world.

7.6 Governance Processes

Governance processes are required to identify, manage, audit, and disseminate all information related to Enterprise Architecture management, contracts, and implementation. These governance processes will be used to ensure that all architecture artefacts and contracts, principles, and operational-level agreements are monitored on an ongoing basis with clear auditability of all decisions made.

7.7 Policy Management and Take-On

All Enterprise Architecture amendments, contracts, and supporting information must come under governance through a formal process in order to register, validate, ratify, manage, and publish new or updated content. These processes will ensure the orderly integration with existing governance content such that all relevant parties, documents, contracts, and supporting information are managed and audited.

7.8 Compliance

Compliance assessments against Service Level Agreements (SLAs), Operational Level Agreements (OLAs), standards, and regulatory requirements will be implemented on an ongoing basis to ensure stability, conformance, and performance monitoring. These assessments will be reviewed and either accepted or rejected depending on the criteria defined within the governance framework.

7.9 Dispensation

A Compliance Assessment can be rejected where the subject area (design, operational, service level, or technology) are not compliant. In this case the subject area can:

1. Be adjusted or realigned in order to meet the compliance requirements
2. Request a dispensation

Where a Compliance Assessment is rejected, an alternate route to meeting interim conformance is provided through dispensations. These are granted for a given time period and set of identified service and operational criteria that must be enforced during the lifespan of the dispensation. Dispensations are not granted indefinitely, but are used as a mechanism to ensure that service levels and operational levels are met while providing a level flexibility in their implementation and timing. The time-bound nature of dispensations ensures that they are a major trigger in the compliance cycle.

7.10 Monitoring and Reporting

Performance management is required to ensure that both the operational and service elements are managed against an agreed set of criteria. This will include monitoring against service and operational-level agreements, feedback for adjustment, and reporting.

7.11 Governance Environment Management

This identifies all the services required to ensure that the repository-based environment underpinning the governance framework is effective and efficient. This includes the physical and logical repository management, access, communication, training, and accreditation of all users.

All architecture artefacts, service agreements, contracts, and supporting information must come under governance through a formal process in order to register, validate, ratify, manage, and publish new or updated content. These processes will ensure the orderly integration with existing governance content such that all relevant parties, documents, contracts, and supporting information are managed and audited.

The governance environment will have a number of administrative processes defined in order to effect a managed service and process environment. These processes will include user management, internal SLAs (defined in order to control its own processes), and management information reporting.

7.12 MDAs EA Assessment Methodology

A detailed version of the EA Assessment Methodology is provided in the GGEA Assessment Methodology document. The EA Assessment framework is based on EA Capability Maturity Model (CMM) to determine the level of an agency's EA maturity. Industry best practice indicates that MDAs should manage their EA efforts according to capability maturity models, which will provide the key ingredients for improving the EA across Government. The methodology will define the evolutionary steps to improve the overall process that starts out in an ad hoc state, transforms into an immature process, and then finally becomes a well defined, disciplined, and mature process.

The EA Assessment Methodology will assess the capability of EA programmes to guide and inform strategic ICT investments. It also helps to better understand the current state of the GHS's

EA and assist them in integrating their EA into their decision making processes. By applying the assessment themselves, MDAs will be able to identify strengths and weaknesses within their EA programmes and adjust them accordingly.

The EA Assessment Methodology will define the frequency and timing for the GHS's EA assessment. It will also describe the self assessment process as well as the external GICTeD evaluation to be conducted at regular intervals.

7.13 New Project Business Case Process

Ensuring the compliance of individual projects with the GHS EA is an essential aspect of EA governance. To this end, the ICT Governance function within the GHS will normally define two complementary processes:

- The Enterprise Architecture function, which will be required to prepare a series of Project Impact Assessments - project-specific views of the EA that will illustrate how the architecture impacts on the major projects within the GHS.
- The ICT Governance function will define a formal Architecture Compliance Review process, for reviewing the compliance of projects to the Enterprise Architecture.

Apart from defining formal processes, the ICT Governance function may also stipulate that the Enterprise Architecture function should extend beyond the role of architecture definition and standards selection, and participate also in the technology selection process, and even in the commercial relationships involved in external service provision and product purchases.

7.14 Architecture Compliance Reviews

An Architecture Compliance Review is a scrutiny of the compliance of a specific project against established architectural criteria, spirit, and business objectives. A formal process for such reviews normally forms the core of an Enterprise Architecture compliance strategy.

7.14.1 Purpose

The goals of an Architecture Compliance Review include some or all of the following:

- First and foremost, catch errors in the project architecture early, and thereby reduce the cost and risk of changes required later in the life-cycle. This in turn means that the overall project time is shortened, and that the business gets the bottom-line benefit of the architecture development faster;
- Ensure the application of best practices to architecture work;
- Provide an overview of the compliance of the GHS's Enterprise Architecture to mandated national standards;
- Identify where the standards themselves may require modification;
- Document strategies for collaboration, resource sharing, and other synergies across multiple architecture teams;

- Take advantage of advances in technology;
- Communicate the status of technical readiness of the project to management;
- Identify key criteria for procurement activities (e.g., for inclusion in off-the-shelf product RFI / RFP documents);
- Identify and communicate significant architectural gaps to product and service providers.

Apart from the generic goals related to quality assurance outlined above, there are additional, more politically oriented, motivations for conducting architecture compliance reviews, which may be relevant in particular cases:

- The Architecture Compliance Review can be a good way of deciding between architectural alternatives, since the business decision-makers typically involved in the review can guide decisions in terms of what is best for the business, as opposed to what is technically more pleasing or elegant;
- The output of the Architecture Compliance Review is one of the few measurable deliverables to the CIO to assist in decision-making;
- Architecture reviews can serve as a way for the Architecture Board to engage with development projects that might otherwise proceed without involvement of the architecture function;
- Architecture reviews can demonstrate rapid and positive support to the GHS's business community;
- The Enterprise Architecture and Architecture Compliance Reviews help ensure the alignment of ICT projects with business objectives.

7.14.2 Timing

The Architecture Compliance Review is typically targeted for a point in time when business requirements and the systems architecture are reasonably firm and the project is taking shape, well before its completion.

The aim is to hold the review as soon as practical, at a stage when there is still time to correct any major errors or shortcomings, with the obvious proviso that there needs to have been some significant development of the project architecture in order for there to be something to review.

Inputs to the Architecture Compliance Review may come from other parts of the standard project life-cycle, which may have an impact on timing.

7.14.3 Governance and Personnel Scenarios

In terms of the governance and conduct of the Architecture Compliance Review, and the personnel involved, there are various possible scenarios:-

- For smaller scale projects, the review process could simply take the form of a series of questions that the project architect or project leader poses to him or herself, using the checklists provided below, perhaps collating the answers into some form of project report

to management. The need to conduct such a process is normally included in overall MDA-wide ICT governance policies.

- Where the project under review has not involved a practising or full-time Architect to date (for example, in an application level project), the purpose of the review is typically to bring to bear the architectural expertise of an Enterprise Architecture function. In such a case the Enterprise Architecture function would be organising, leading and conducting the review, with the involvement of business domain experts. In such a scenario, the review is not a substitute for the involvement of Architects in a project, but it can be a supplement or a guide to their involvement.
- In most cases, particularly in larger scale projects, the Architecture function will have been deeply involved in, and perhaps leading, the development project under review. In such cases, the review will be co-ordinated by the Chief Architect/Enterprise Architect, who will assemble a team of business and technical domain experts for the review, and compile the answers to the questions posed during the review into some form of report. The questions will typically be posed during the review by the business and technical domain experts. Alternatively the review might be lead by a representative of the Architecture Board.

In all cases, the Architecture Compliance Review process needs the backing of senior management, and will typically be mandated as part of the MDAs' IT governance policies. Normally, the CIO will mandate architecture reviews for all major projects, with subsequent annual reviews.

To manage project risks and provide the appropriate levels of control and quality, a Technical Quality Gate process is required to enable quality decision-making control of IT projects and programmes. The Technical Quality Gate process involves a series of well defined checkpoints used to evaluate various activities in a project or projects within an overall programme, as shown in the figure below. This is necessary for joint programmes of work and for providing insight and control over multiple projects.

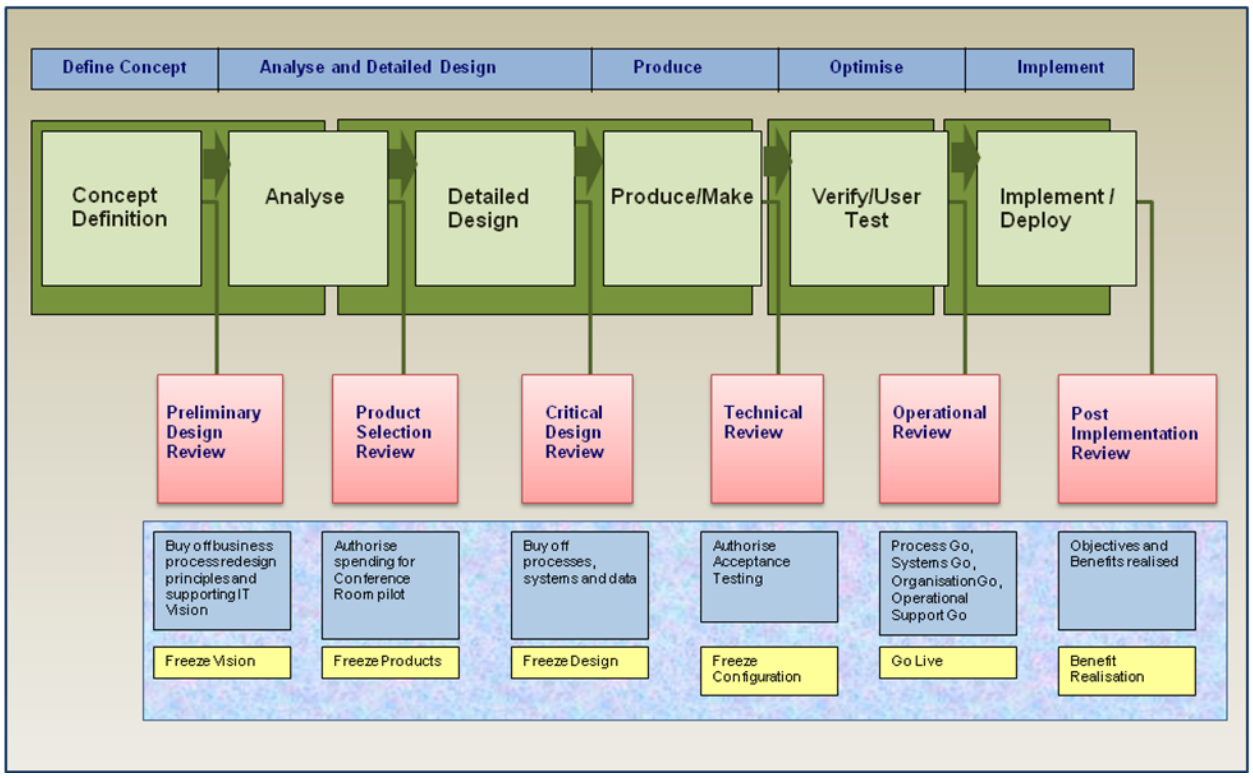


Figure 18: ***Technical Quality Gate Process***

Essentially, the gated review process will support internal policy and standards as well as accepted industry best practices in software engineering methodology. The process will be owned and operated by the GHS's Enterprise Architect.

Run-time governance focuses on controlling deployment through approval processes and on applying runtime access control policies to services. For example, a developer has completed development and testing of a service and submitted the service for approval. After the appropriate people have ensured that the service meets organisational policies, the registrar (a common term for the "super administrator" of the registry/repository) pushes a button and the service is now considered "published."

8. GHS EA Implementation Plan

ID	Task Name
1	**MoC EA Implementation**
2	**Start Project**
3	**Set-Up Program Office**
4	Define Project Scope
5	Validate and Tailor high-requirements(transformation Criteria)
6	Initate risk management procedures and resolution plans
7	Establish other standards and procedures
8	*Program Office Set-up Complete*
9	**Manage Organisational Change**
10	Create Project Awareness
11	Identify Issues
12	Manage Expectations
13	Manage Communication Issues
14	**Business Process Re-engineering**
15	Define Business Areas
16	Assess Change Areas
17	Define Requirements
18	Analyse Requirements
19	Implement Processes, Procedures and Policies
20	*Project Requirements Complete*
21	**Building,Testing and Deployment**
22	**Phase 1: Build Physical Infrastructure**
23	Connect to Government Data Centre
24	Connect to GovNet
25	Enhance Internet Connectivity
26	Implement Remote Access Infrastructure
27	*Phase 1 Complete Checkpoint*
28	**Phase 2: Build MoC Web Technologies**
29	Design secure Intranet and email architecture
30	Build Intranet and deploy portal
31	Implement Content Management
32	Implement Knowledge Management Technology
33	Implement Business Intelligence Analytics(Dashboard,scoreboards)
34	Implement Policy Management Technology
35	Test Solutions
36	Deploy solutions
37	*Phase 2 Complete Checkpoint*
38	**Phase 3: Implement Instances of Shared Back Office solutions**
39	Implement Instance of Finance Solution
40	Implement Instance of Payroll & Finance Solution
41	Implement Instance of Fleet and Asset Management
42	Implement Instance of Supply Chain Management
43	Implement Instance of Statistical Management
44	Test Solutions
45	Deploy Solutions
46	*Phase 3 Complete Checkpoint*
47	**Phase 4: Implement other Solutions**
48	Implement Correspondence Management Solution
49	Implement Case management solution
50	Implement Audit and Compliance Solution
51	Implement Program Management and Collaboration Tools
52	Implement Marketing and Promotion Solution
53	Test Solutions
54	Deploy Solutions
55	***Project Sign-off***

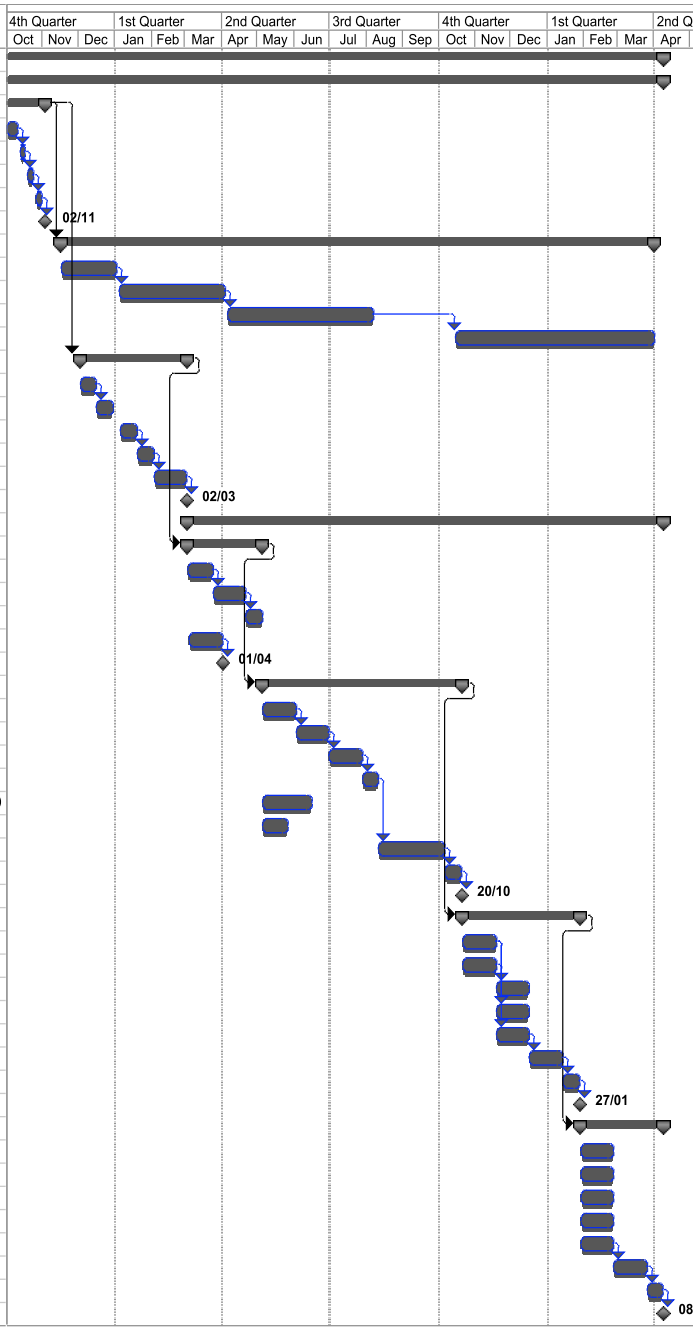


Figure 16: GHS EA Implementation Plan

The high level project plan in figure 16 above is structured to provide maximum benefit to the GHS by prioritising projects, which could be implemented as soon as possible to improve software development and IT operations. The plan is an 18 month programme that will enable a

comprehensive transformation of the GHS. A phased approach has been adopted to reduce implementation risk and provide maximum value to the GHS. The plan assumes that GHS will utilise the proposed Government shared infrastructure services. The GHS must also adopt a piloting strategy wherever necessary to test the effectiveness of the new processes and technologies prior to rollout. It will also allow the organisation to build the knowledge and skills within the GHS necessary for implementing the solution and this should greatly enhance the speed and ease of the roll-out.

Phase 1 is about connecting GHS to the Government Data Centre and Wide Area Network to enable the GHS to utilise the infrastructure to delivery ICT services. If the shared infrastructure services are not ready the GHS should build an interim Data Centre that will host the applications. Phase 2 will enable the GHS to build and deploy composite applications that will provide online presence. Phases 3 and 4 enable the GHS to deploy the remaining systems.

8.1 PROGRAMME MANAGEMENT

The GHS will use a standard programme management methodology to be adopted by the Government of Ghana, which provides a set of logical processes to manage projects of all types and sizes in a structured and standardised manner. It must have a project lifecycle approach, which will enable the capture of all factors from initial analysis to deployment and post implementation review.

The programme will be managed by:

- Steering Committee (GHS Project Director, Programme Manager and other key stakeholders);
- Programme Manager to oversee entire programme;
- Project Managers for the individual projects;
- Programme Office.

8.2 RESOURCE REQUIREMENTS

The resources and skills required for the programme include:

- Project Sponsor
- Chief Architect;
- Project Manager;
- Business Analysts;
- Data Analysts;
- Technical Architects;
- Systems integrators;
- Programme Office Assistants.

Appendices

GHS Future State Business Process with Supporting Applications:

Line of Business	Business Process	Sub Business Process	Activity	Actor	Application to be used
Public Health	Outreach and Awareness Creation	Disease prevention campaign	• Educate citizens on preventive methods for various diseases • Organise health care screening activities for citizens • Disseminate government health care initiatives to citizens and rural folks.	Public Health Administrator	Program Management
Institutional Care Division	Clinical Patient facing	Patient appointment scheduling	• Schedule appointment date • Send reminder notice to patient	Health Administrator	Patient Record Management-CRM
		Outpatient Intake	Registration / Check-in: • Information gathering • Eligibility verification		

Copyright © 2009

		Inpatient Intake	Admissions: • Information gathering • Eligibility verification		
			Discharge: • Discharge planning and instructions for patient • Trigger billing/ claims event in patient accounting • Close encounter		
Institutional Care Division	Post Care Services	Care management	• Health management • Disease management • Case Management	Health Care Professional	CRM
		Follow-up care	• Appointment scheduling • Appointment reminders		

Institutional Care Division	Contact Management	Provide Access channels and contact centres	• Define Contact Strategy • Define Channel Strategy • Implement Contact Centre Infrastructure • Manage Service Quality • Manage Service Accessibility • Manage Responsiveness	Health Care administrator	CRM
Public Health Division		Handle enquiries and complaints	• Capture Enquiries & Complaints • Investigate Complaints • Maintain FAQ • Respond to Enquiries & Complaints • Provide Feedback to Policy and Process Definition • Provide Central Help Desk	Health Care Professional	CRM

PPME		Coordinate with affiliate organisations	• Create Common Interest Forums • Provide Collaborative Working Environment • Share Business Plans • Integrate Business Processes	GHS official	Web Portal
Institutional Care	Maintain Clinical Administrative Services	Clinical staff and resource management	• Staff Scheduling • Workload mgt • Workflow mgt • Equipment and Facility scheduling	Health Care administrator	Scheduling and Capacity Management

	Clinical Services Provision	Diagnosis process	• Summary • Observation • Assessment • Plan • Diagnostic test/exam order • Send medication order / request to pharmacy • Diagnostic exam scheduling (e.g.: radiology, cardiology)	Health Care Professional	Clinical Services System

		Diagnostic tests and exam procedures	• Pre-accessioning (lab) • Accessioning (lab) • Perform test/exam • Document and report test/exam results • Validate test/exam results • Interpret test/exam results • Report test/ exam results / interpretation • Post test/ exam results / interpretation in patient chart / medical record • Log charges on results	Health Care Professional	Clinical Services System

Institutional Care Division		Therapeutic support	• Medication fulfilment • Adverse event management • Verify medication order • Schedule medication administration acts • Health-care professional consultation • Clinical documentation (encounter forms, documents, etc.)	Health Care Professional	Web Portal
		Reference Lab	• Send orders for processing of lab samples (provider acting as reference lab to other providers)		Web Portal

Public Health	Disease Surveillance and Control	Epidemiological Surveillance	• Reportable diseases • Immunizations • Automated Real Time Surveillance - Detect adverse Events and near misses • Detect Disease Outbreaks • Detect Bioterrorism • Disease Registries	Health Care Professional	Disease Surveillance system
PPME	Policy formulation	Formulate policies and guidelines	• Develop strategies to promote family health • Co-ordinate and develop plans for clinical care • Develop and Implement standards for support services	GHS official	Policy Management

PPME		Measure policy impact	• Gather data • Analyse data to reveal trends, patterns • Compare outcomes to previous ones • Measure outcomes against KPI's		
Internal Audit	Audit and Compliance	Perform Audit	• Audits • Reports • Remediation (based on audit outcome)	GHS Audit official	Audit and Compliance system
Internal Audit		Quality Assurance	• key performance indicator measurements – retrospective and concurrent - for clinical care • Benchmarking existing care outcomes against industry best practices		

Institutional Care	Billing	Patient Accounting (charges and coding on patient encounters are linked to billing and claims events)	• Patient bill generation • Payer claim generation • Claim submission to payer	Health Care Administrator	Billing Management system
PPME	Financial Planning and Budgeting	Prepare Expenditure Budget	• Create Budget Forecast • Produce Financial Plan • Acquire Funding • Monitor Cash flow and Expenditure vs. Budget	PPME	Finance system
Operational Research	Research and Development	Conduct Research	• Set research goals • Allocate research grant to research activities • Study results • Publish research results	Operational Research Division	Operational Research
		Provide Health Promotion Information	• Gather statistics from district hospitals •		

PPME	Strategic Planning	Set Corporate Goals / Objectives / Strategies	• Set financial and growth goals and objectives • Set organizational goals and objectives • Set market goals and objectives • Develop strategies	PPME	Finance system
		Execute Strategies	• Initiate strategies • Measure achievements • Refine strategies		
		Monitor KPI's	• Define business performance metrics • Quantify Key Performance Indicators (KPI's) • Monitor performance and quality • Develop performance and quality improvement plans		

		Manage Risk	• Manage financial risk • Manage medical liability • Manage non-medical liability		
Human Resource	Human Resource Management	Align HR to Strategy	• Develop HR Practices, Policy & Direction • Align plans with enterprise targets • Recommend modifications to HR performance • Establish Target HR Attributes • Develop Transition Strategy	HR Division	Human Resource

		Plan HR Composition	• Specify Required Workforce Composition • Assess Potential of HR Pool • Develop Resourcing Plan • Manage Internal HR Pool	
		Adjust HR Levels	• Specify Recruitment Need • Source Candidates • Hire Resource • Induct Resource Onboard • Maintain Employee Information • Maintain Security Clearances • Disengage Resources • Manage Resource Exit	

		Develop Resources	• Identify Development Needs • Provide Education and Training facilities and programs • Assign resources to programs • Evaluate learning effectiveness		
		Assign Job Tasks	• Assign workforce to tasks • Track utilization / realization • Track assignment performance		
Human Resource		Retain Human Resources	• Manage workforce relations • Administer benefits • Administer compensation and incentives • Administer health and safety		

Supplies, Stores and Drug Management Division	Supply Chain Management	Identify Requested Item (Item Master Properties e.g. Group Purchase, Stock Item, Consignment Item)	• Mechanisms - Web Based Catalogs, CDs, • Mechanism - Item Master	Head, Stores	Supply Chain Management system
		Purchase Requisition	• Process Request with Existing (Pre-Contracted) Vendors • Timed • On-Demand • Process Request with New Vendors • Contract with New Vendor		
		Inventory Management	• Place order through EDI mechanism • Receive Order • Distribute logistics • Manage vendor invoice		

Health Administration and Support Services	Asset Management	Provide Fixed Assets	• Establish Asset strategy and policy • Balance asset resources with requirements • Source and Acquire Fixed Assets • Dispose of Assets	Health Administration and Support Services	Asset Management System
Health Administration and Support Services	Facilities Management	Manage Physical plant	• Sterile room preparation • Isolation room preparation • Waste management	Health Administration and Support Services	Scheduling and Capacity Management
		Housekeeping	• Prepare room and bed • Routine Cleaning • Specialised Cleaning		
		Dietary	• Special meals preparation • Routine meals preparation		

Finance	Finance Management	Plan and Budget	• Create Budget Forecast • Produce Financial Plan • Acquire Funding • Monitor Cash flow and Expenditure vs. Budget	Finance Division	Finance Management System
		Perform Management Cost Accounting	• Manage Accounts Receivable • Perform Financial Accounting		
ICT Division	ICT Management	Maintain Business-ICT Strategic Alignment	• Define Enterprise Architecture • Create Business Architecture • Create ICT Architecture • Establish ICT Governance & Control Mechanisms	ICT Division	Web Portal

	Perform ICT Governance	• Manage ICT Governance Activities • Manage Business-ICT Relationships • Manage ICT People & Knowledge • Manage ICT Programs • Manage ICT Projects	
	Manage ICT Services	• Manage Business Continuity • Ensure ICT Security • Manage External Interfaces • Monitor ICT Service Performance	

		Provide ICT Services	• Establish ICT sourcing strategy and policy • Balance ICT resources with requirements • Invite ICT Service Contract Tenders • Select Suppliers and place contracts • Maintain Infrastructure • Maintain Applications	

ICT Division		Manage Transformation Programs	• Manage Integrated Change • Build & Manage Integrated ICT Master plan • Define Engineering Approach • Capture Scope & Requirements • Create Systems Architecture • Design Solution • Build & Test Solution • Migrate Data • Implement & Roll-out Solution • Manage Transition		

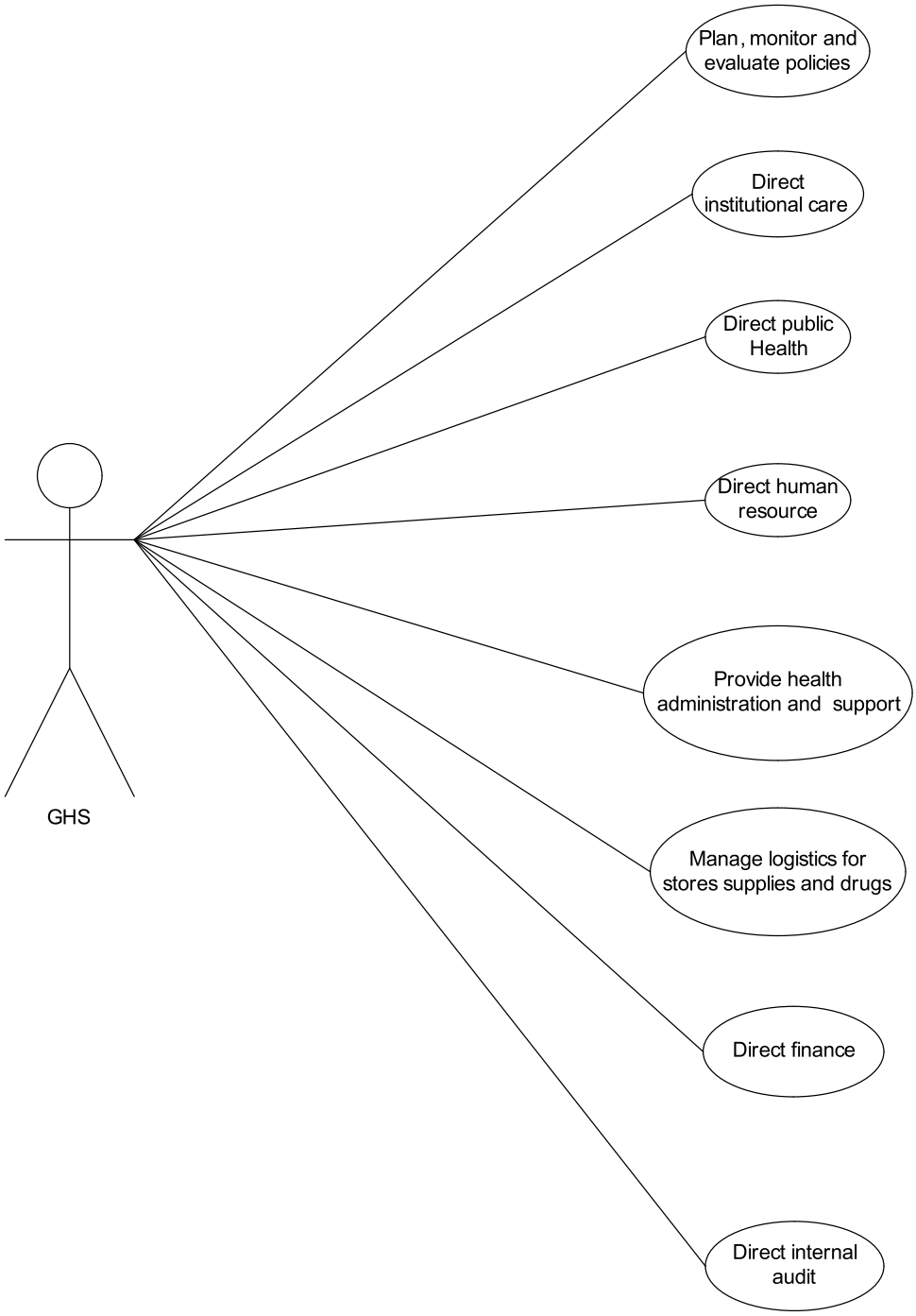
SYSTEM INTERFACES

This table shows the flow of data elements between application system interfaces. The first column in the table consists of applications components recommended in the applications layer in the applications architecture.

System A	Data Element	System B
Policy Planning	Government Mandate Report Staff Ideas Draft Policy Document Revise Policy Document Policy Document	Email To Departments Web Portal
Performance Management	Performance Metrics Document Performance Report Plan Document Budget Document Program Document Requirements Document Key Performance Indicators Roles Assignment Document Quarterly Performance Reports	Email To Administration Web Portal
Human Resource	HR Policy Document	Email To Departments Web Portal
Project /Programme Management	Project Concept Paper Project Preparation Report Feasibility Report Draft Financing Agreement Report Financing Agreement Report	Email To Departments Web Portal
Clinical Services	Policy Document Strategic Plan Document Clinical Services Information Health Policy Review Report	Email To Departments Web Portal

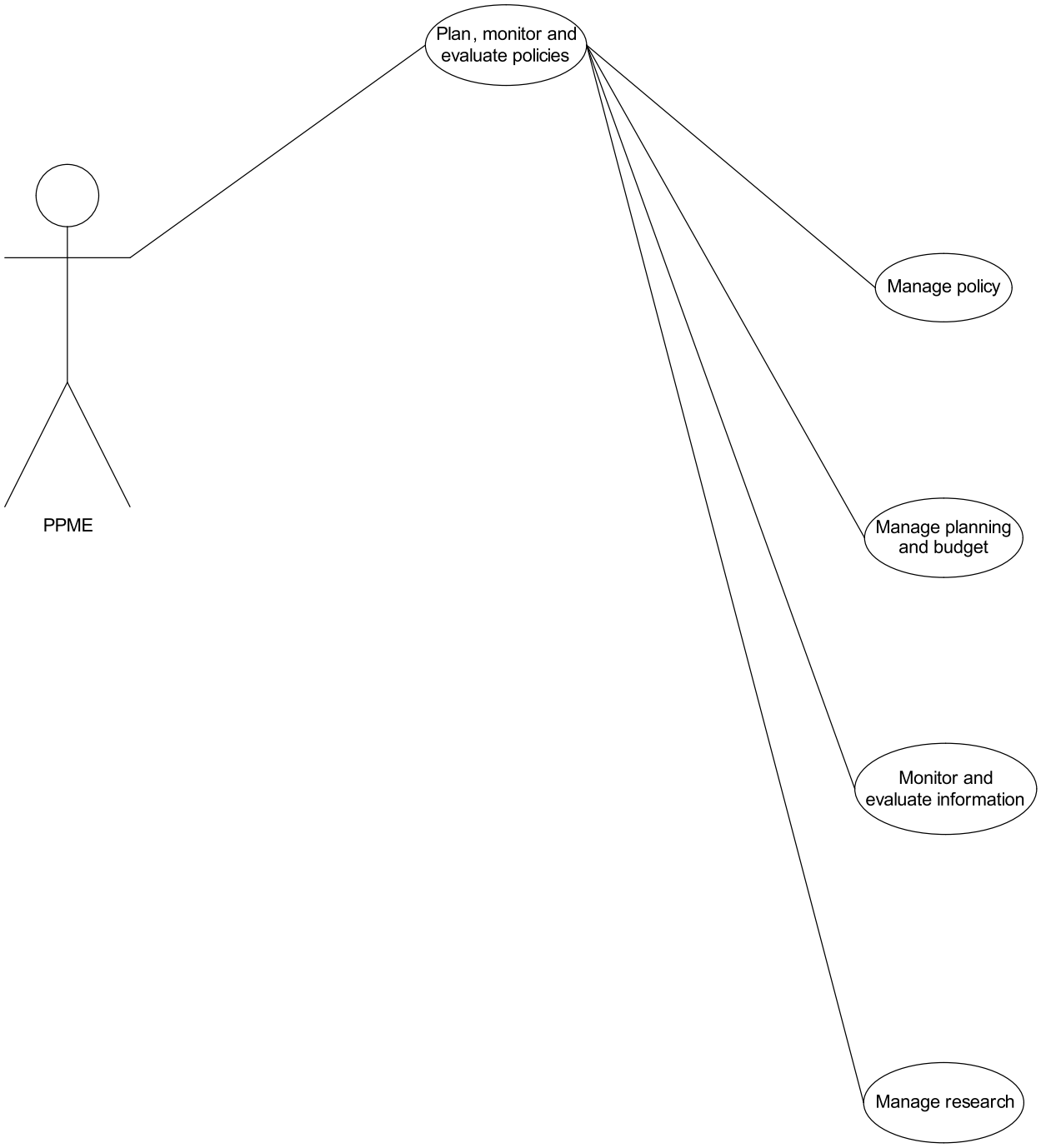
Disease Surveillance	Health Policy Document Strategic Plan Document Project Reports	Email To Departments Web Portal
Asset Management	Policy Document Strategic Report Security Document	Email To Departments Web Portal
Equipment Management	Policy Document Strategic Report Security Document	Email To Departments Web Portal
Fleet Management	Policy Document Approved Requirements List Fleet Management Report	Email To Departments Web Portal
Scheduling and Capacity Management	Policy Document Procurement Document Guidelines	Email to departments
Supply Chain Management	Procurement Report Policy Document	Email To Departments Web Portal
Finance	Cash flow Plan Document Claim Requisitions Financial Reports	Email To Departments Web Portal
Audit And Compliance	Policy Document Internal Audit Reports Operational Reports Financial Reports Compliance Reports Legislation/Draft Bills	Email To Departments
Research and Development	Policy Document Plan Document Content Analysis Document Research Finding Document	Email To Departments Web Portal

GHS HIGH-LEVEL FUNCTIONAL USE CASE:

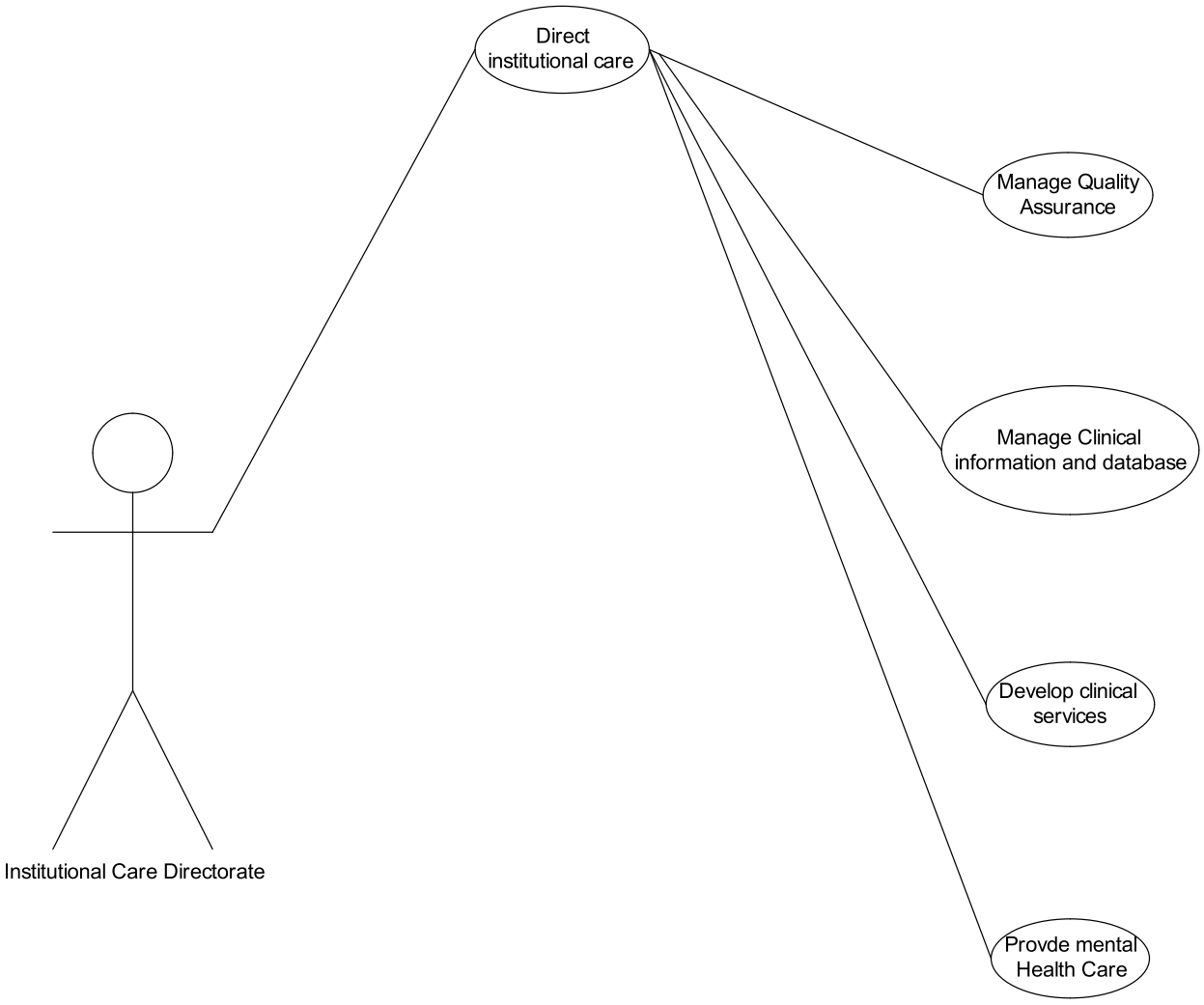


GHS FUNCTIONAL USE CASES:

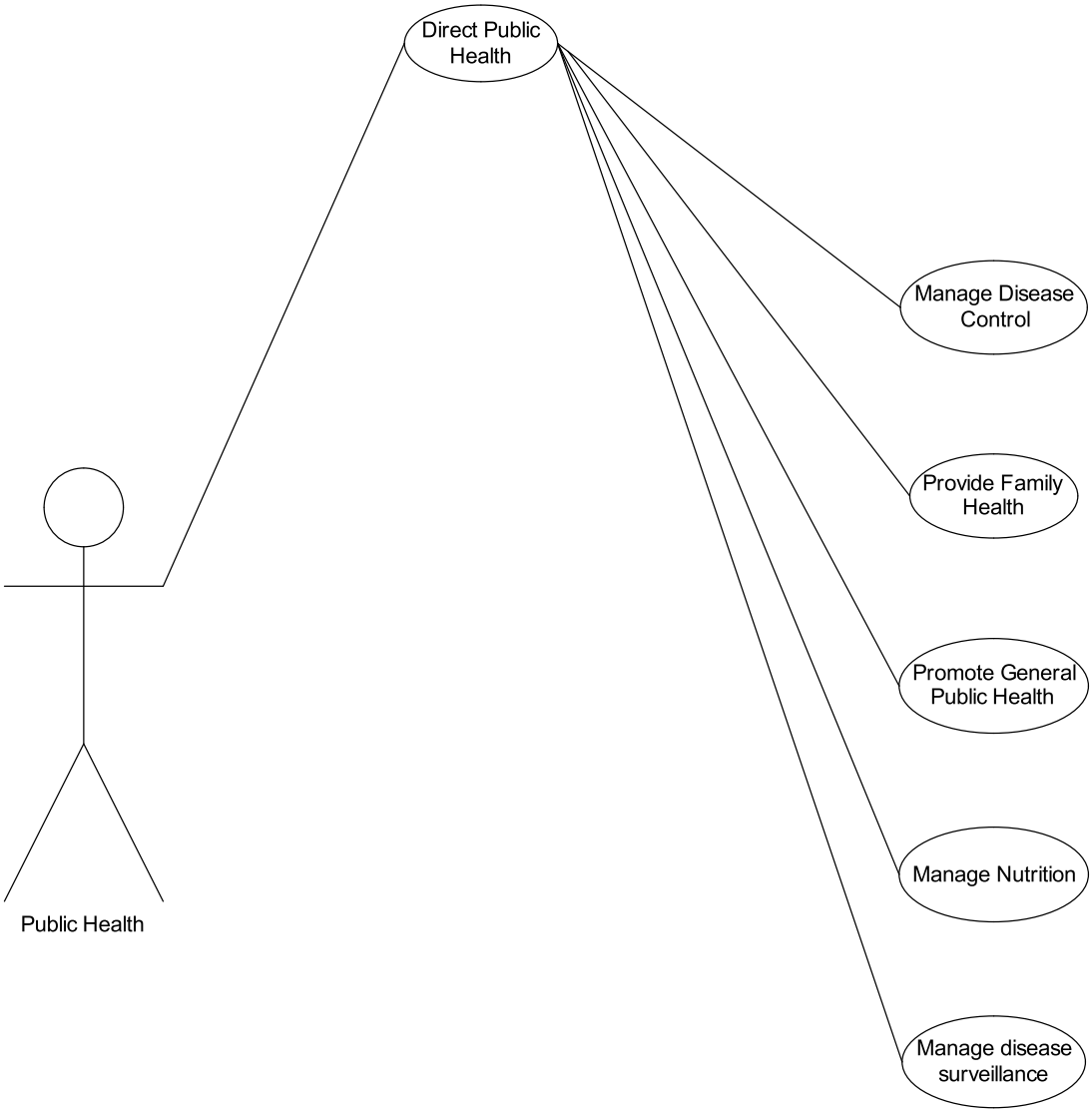
PPME:



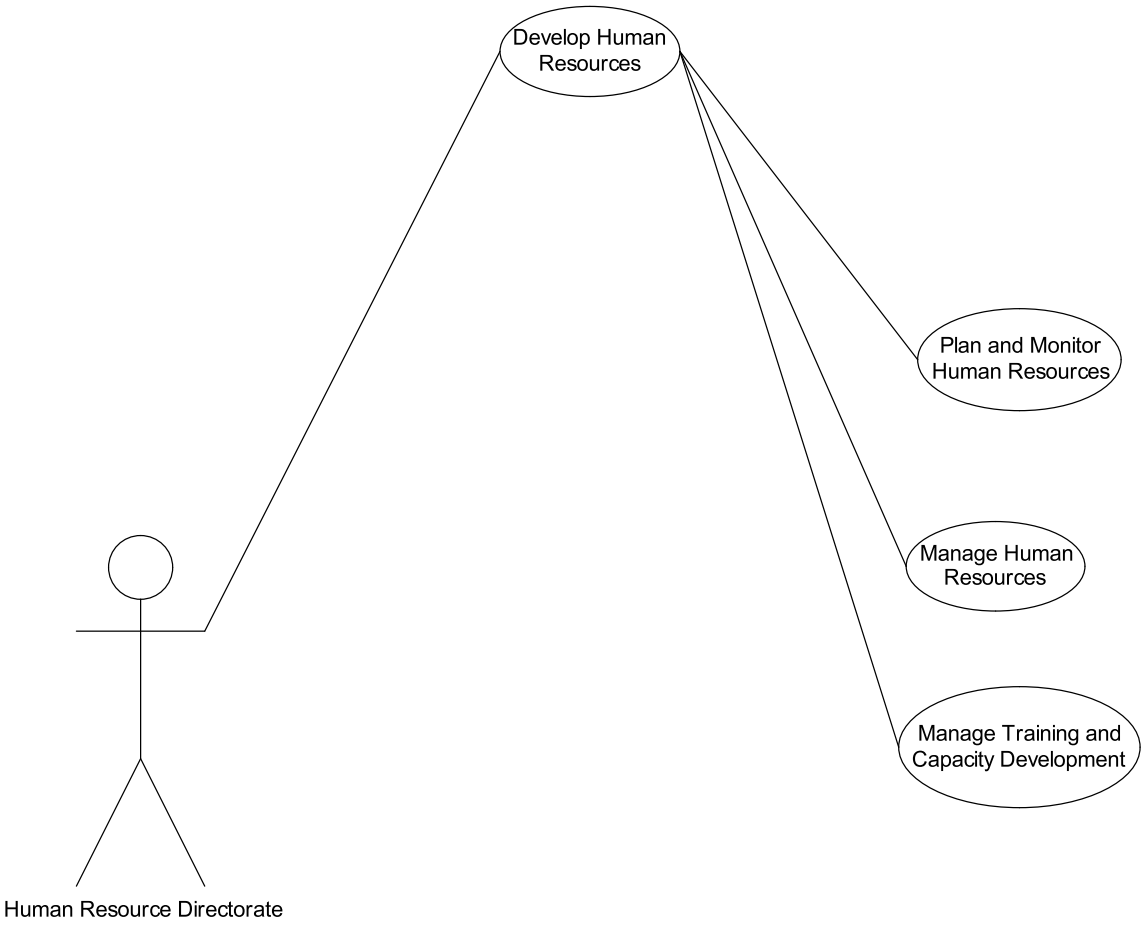
INSTITUTIONAL CARE DIVISION:



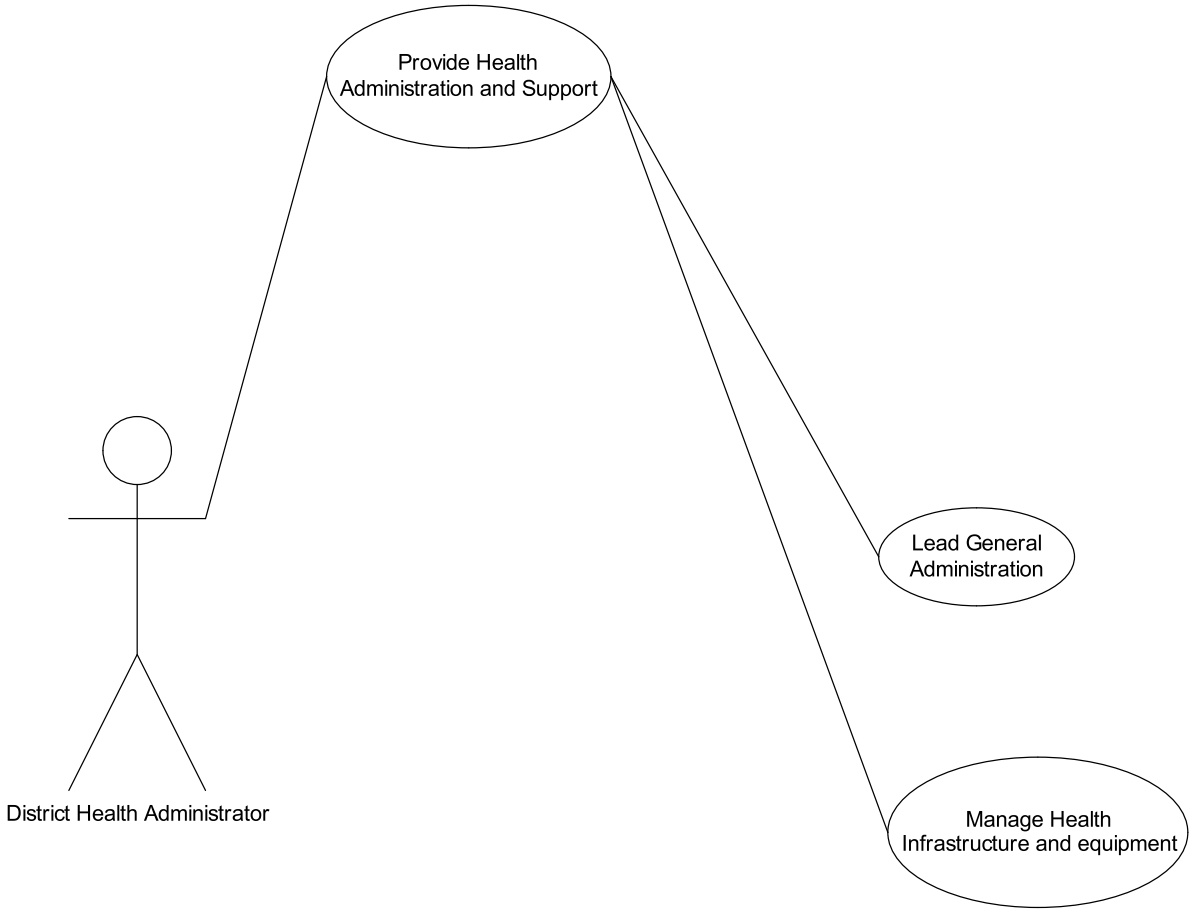
PUBLIC HEALTH:



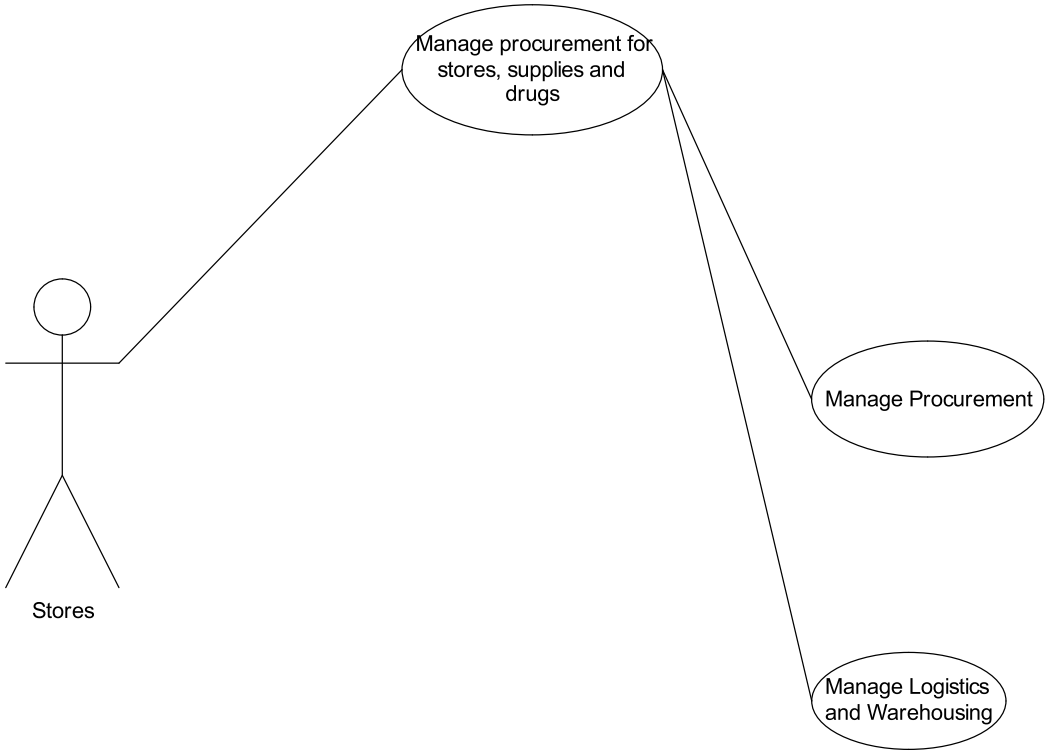
HUMAN RESOURCE DIVISION:


Develop Human Resources
Plan and Monitor Human Resources
Manage Human Resources
Manage Training and Capacity Development
Human Resource Directorate

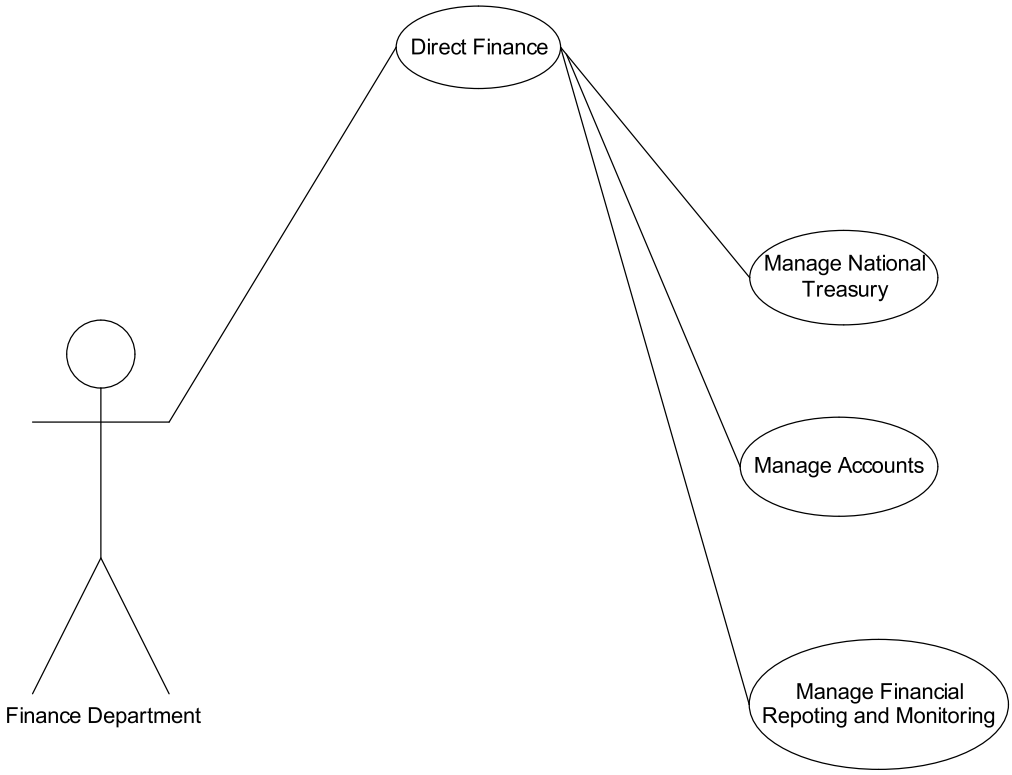
District Health Administrator:



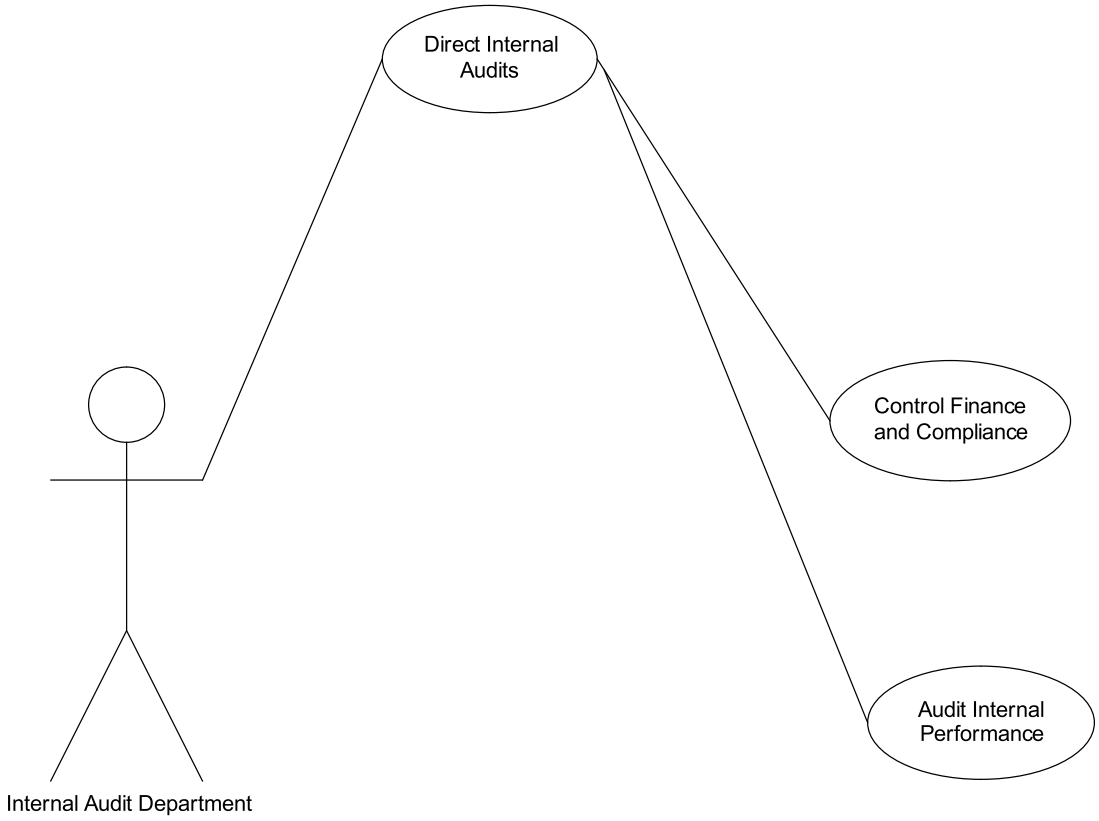
STORES:

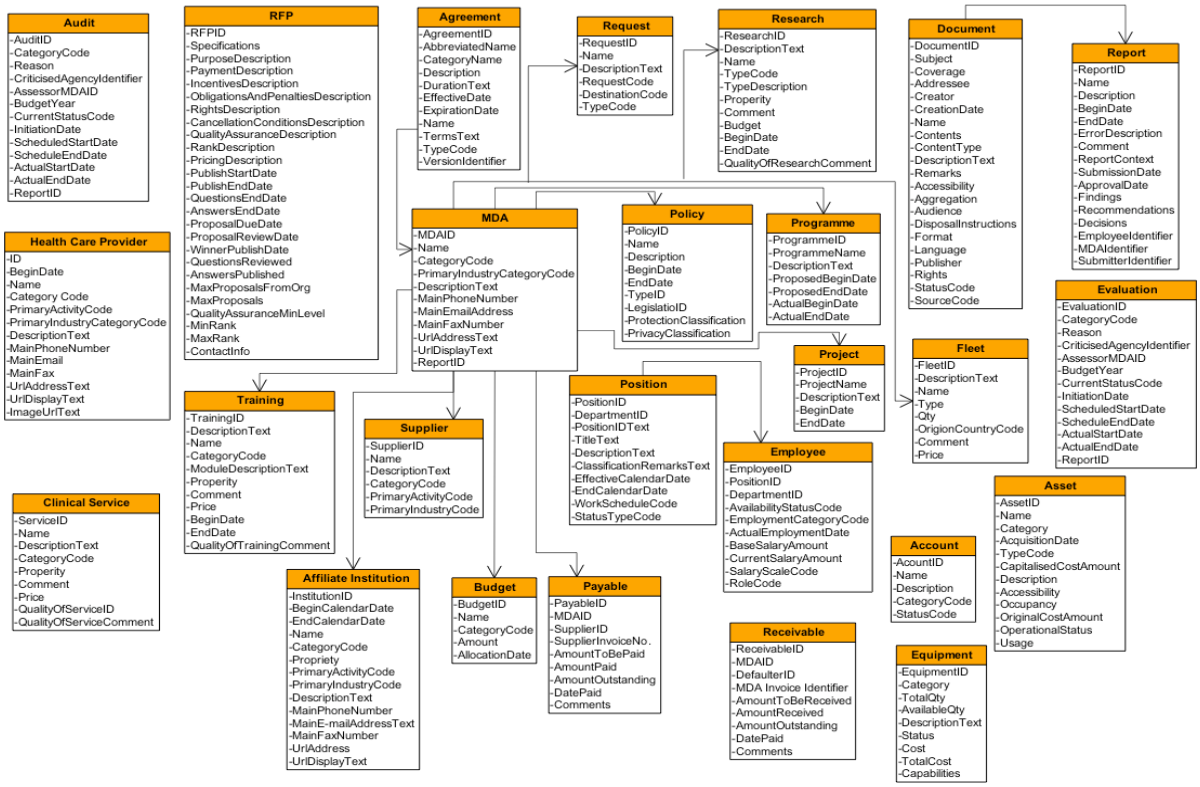

Manage procurement for stores, supplies and drugs
Manage Procurement
Manage Logistics and Warehousing
Stores

FINANCE DIVISION:



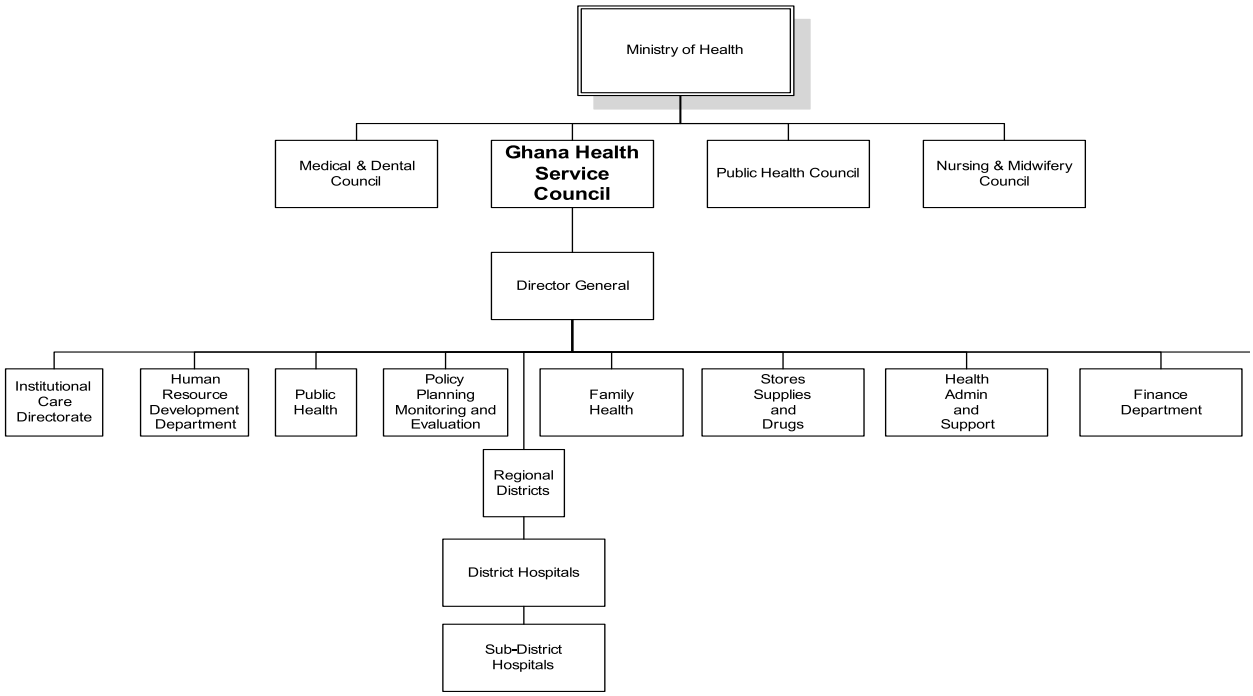
INTERNAL AUDIT DEPARTMENTS:



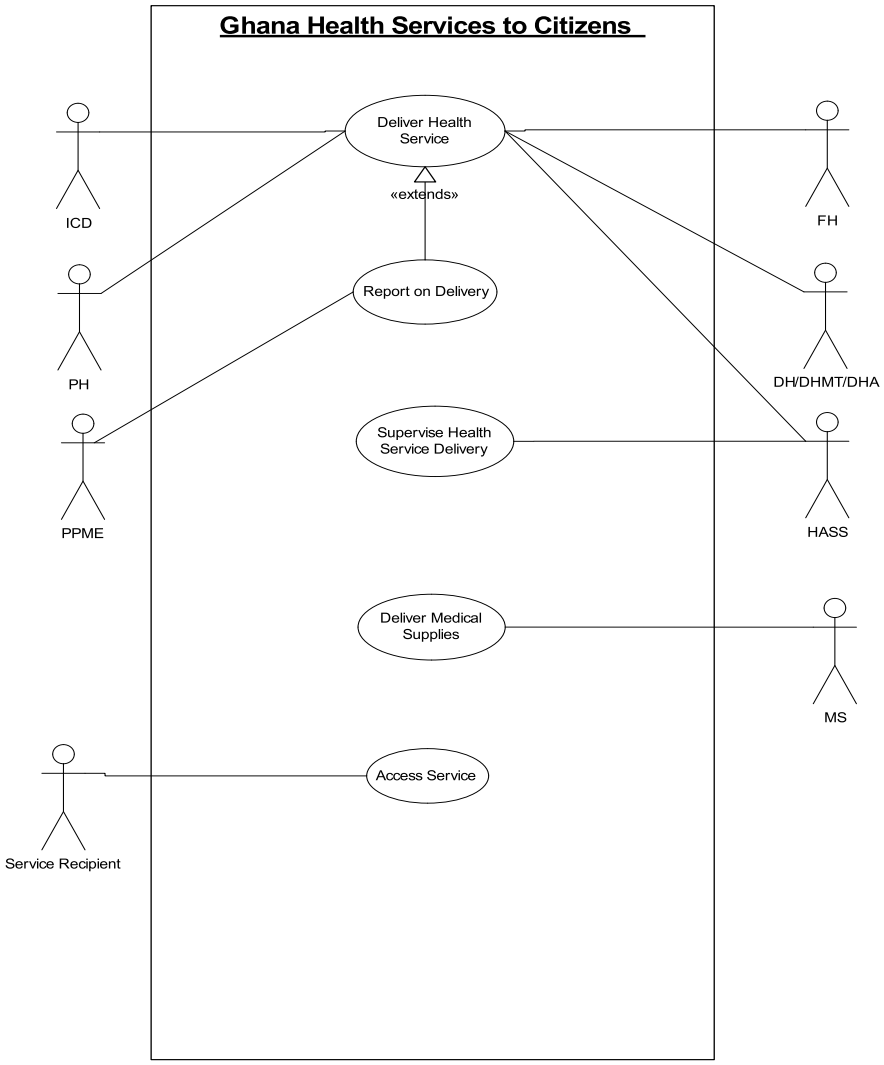


GHS Entity Diagram

GHS FUNCTIONAL ORGANOGRAM:

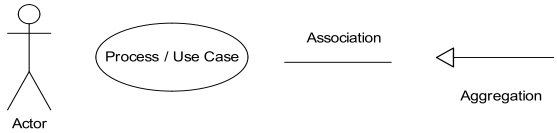


GHS SERVICE TO CITIZENS:



DHMT = District Health Management Team, **DH** = District Hospital, **FD** = Finance Department, **FH** = Family Health, **HASS** = Health Admin & System Support, **HRD** = Human Resource Development, **IAD** = Internal Audit Department, **ICD** = Institutional Care Directorate, **PH** = Public Health, **PPME** = Policy Planning Monitoring Evaluation, **MS** = Medical Supplies (**S**upplies **S**tores **D**rugs), **DHA** = District Health Administrator

Key



 Copyright © 2009