National Health Insurance Council

SOLUTION ANALYSIS AND DETAILED SPECIFICATION AND RECOMMENDATIONS REPORT

Health Insurance Project CR. 4345 – GH Consultancy Services for Conducting ICT Needs Assessment

November 1, 2009

Prepared by:
Telecom/Telematique, Inc.
2737 Devonshire Place, N.W.
Washington, D.C. 20008

CONTENTS

ABBREVIATIONS AND ACRONYMS

ADSL	Asymmetric Digital Subscriber Line
AIM	Adaptive Identification and Mitigation
API	Application Programming Interface
ASA	Adaptive Security Appliance
BCP/DRP	Business Continuity & Disaster Recovery Plan
BOT	Build Operate and Transfer
BP	Business Process
BSS	Basic Service Set
CAPEX	Capital Expenditure
CEO	Chief Executive Officer
CHAG	Christian Health Association of Ghana
CMM	Capability Maturity Model
CMMS	Computerized Maintenance Management System
CNE	Certified Novell Engineer
CPU	Central Processing Unit
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSV	Comma Separated Value
DHCP	Dynamic Host Configuration Protocol
DMHIS	District Mutual Health Insurance Scheme
DMZ	Data Management Zone
DNS	Domain Name System
eGIF	Government Information Framework
EESID	Enterprise Service Set Identifier
EMI	Electro Mechanical Interference
EMR	Electronic Medical Records
FA	Feasibility Analysis
FSC	Forward Schedule of Changes
GA	Government Architecture
GHS	Ghana Health Service
CICTED	Ghana ICT Directorate
G-DRG	Ghana Diagnostic Related Group

GoG	Government of Ghana
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HAMS	Hospital Administration Management Systems
HIMS	Hospital Information Management System
HIP	Health Insurance Project, World Bank
HIPPA	Health Information Portability and Accountability Act
HIS	Hospital Information System
HMS	Hospital Management Software
(HAMS)	Hospital Management System
HTTP	Hypertext Transfer Protocol
IASC	Inter-Agency Steering Committee
ICA	Independent Computer Architecture
ICR/OCR	Intelligent Character Recognition / Optical Character Recognition
ICT	Information and Communication Technology
IDA	The World Bank
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISP	Internet Service Provider
IT	Information Technology
ITAM	IT Asset Management
ITIL	Information Technology Infrastructure Library
ITU	Union-Telecommunication Standardization Sector
ITSM	Information Technology Service Management
KATH	Komfo Anokye Teaching Hospital
KBTH	Korle-Bu Teaching Hospital
LAN	Local Area Network
MAC	Media Access Control
M&E	Monitoring and Evaluation
MCSE	Microsoft Certified Systems Engineer

MOH	Ministry of Health
MPLS	Multiprotocol Label Switching
MTTR	Mean Time To Recovery
MW	Microwave
NCB	National Competitive Bidding
NHIA	National Health Insurance Agency
NHIC	National Health Insurance Council
NHIF	National Health Insurance Fund
NHIL	National Health Insurance Levy
NHIS	National Health Insurance Scheme
NIC	Network Interface Card
NOC	Network Operations Center
OPEX	Operational Expenses
OS	Operating System
PAD	Project Appraisal Document
PC	Personal Computer
PDF	Portable Document Format
PEAP	Protected Extensible Authentication Protocol
PHY	Physical
PoE	Power over Ethernet
POP	Point of Present
PPP	Public Private Partnership
PPME	Policy, Planning, Monitoring and Evaluation
QA	Quality Assurance
QoS	Quality of Service
R&D	Research and Development
RDP	Remote Desktop Protocol
RDBMS	Relational Database Management System
RFC	Request for Change
RTT	Round Trip Time
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture

SOAP	Simple Object Access Protocol
SPM	Service Portfolio Management
SQL	Structured Query Language
SSL	Secure Socket Layer
SSNIT	Social Security and National Insurance Trust
STA	Station
STL	Superlock Technology, Ltd
TIA/EIA	Telecommunications Industry Association/Electronic Industries Association
TCP	Transmission Control Protocol
TLS	Transport Layer Security
T/TI	Telecom/Telematique, Inc.
TOR	Terms of Reference
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VPN	Virtual Private Networking
VSAT	Very Small Aperture Terminal – Satellite terminal
XML	Extensive Markup Language
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WEP	Wired Equivalent Privacy
WPA	WiFi Protected Access

1. INTRODUCTION

This study was conducted to develop the best method for implementing a solution to allow automated member validation and electronic claims submission by Health Providers as a goal of the Phase 2 project for the National Health Insurance Agency. The Gap Analysis portion of this study identified potential methods of providing software, hardware and connectivity to allow Providers to perform these functions.

As part of the Gap Analysis potential Hospital Information Systems (HIS) were identified as being in use within the country. These systems today provide to a few of the health facilities benefits in the day to day management of the facility and Electronic Medical Records (EMR) of the patients. The use of HIS systems as an incentive to the Provider, while also providing the NHIS with their goal of electronic claims is discussed in this report.

This report is intended to recommend potential HIS systems that can be deployed at additional facilities, LAN installation, WAN connectivity, ICT and user training and financial considerations needed to implement a solution. Since no project of this size and scope can be performed without changes to the way work is performed at a Provider, this report will recommend changes to Providers Business Processes (BP) needed to ensure success.

1.1. KEY STAKEHOLDERS

Ministry of Health

The Ministry of Health (MoH) is the sector Ministry for the project and is responsible for the overall coordination through the National Health Insurance Authority (NHIA). The MoH ensures the prompt and efficient implementation of the project. The MoH, through the PPME, is responsible for organizing the Steering Committee and other project-specific review meetings with the necessary reviews and approvals by the Minister.

National Health Insurance Authority (NHIA)

NHIA as the project implementer is responsible for the following:

a) The overall coordination, implementation, financial management, procurement, monitoring, evaluation, reporting and communication of project activities.
b) Ensuring that appropriate policy environment exists to support the project.
c) Carrying out procurement of goods and services in accordance with the Bank's procurement guidelines. In doing so, the NHIA will work very closely with beneficiary institutions.
d) Monitoring overall progress of implementation on a monthly basis and evaluating project performance.
e) Acting as the focal point for communication with the World Bank Implementation Support Missions.
f) Compiling and furnishing Financial Management Reports to the World Bank on a quarterly basis.
g) Communicating project results to the stakeholders, including Steering Committee, donors and the general public.
h) Supporting the Steering Committee through the MoH on technical and operational matters.
i) Review and approval of proposed beneficiary programs to ensure that they conform to the project objectives.
j) Providing assistance to beneficiary institutions on project management, procurement, supervision of implementation, and technical advice as required.

Ghana Health Service (GHS)

The responsibilities of the GHS include:

a) Establishing a Beneficiary Focal Implementation Committee.
b) Developing specifications for procurement of ICT equipment in consultation with the NHIA.
c) Development of the ongoing ICT training program in consultation with the NHIA.
d) Monitoring and evaluation of the related activities in accordance with the established framework.
e) Preparation of the comprehensive semi-annual report showing progress towards outcomes.

The World Bank (IDA)

The World Bank's responsibilities include:

a) Financing the project's components.
b) Monitoring the use of funds and ensure that the project is implemented in accordance with provisions of the FA and the PAD.
c) Organizing the project review missions - IDA would periodically send review missions to the field which will examine the physical progress, including the quality of delivery, the proper accountability of project resources.
d) Ensuring the compliance with the IDA's procurement guidelines and disbursement procedures.
e) Monitoring the progress and performance of the project.
f) Reviewing and issue no objections to proposals submitted as appropriate.

Inter Agency Steering Committee (IASC)

The Steering Committee includes senior officials from beneficiary institutions and is responsible for:

a) Providing the overall policy guidance.
b) Reviewing the progress towards achieving the project's objectives and approve and evaluate the project's annual work program and budget.
c) Coordinating project implementation among all relevant agencies. Organize at least twice a year a joint meeting between the Borrower and the World Bank

NHIA Entity Tender Committee

a) Ensures that at every stage of the procurement activity, procedures prescribed have been followed.
b) Exercises sound judgment in making procurement decisions.
c) Refers to the appropriate Tender Review Board for approval any procurement above its approval threshold.
d) Ensures that procurement packages within the NHIA Entity Tender Committee thresholds are indicated in the procurement plan.

MoH Tender Review Board

a) Ensures that at every stage of the procurement activity, procedures prescribed have been followed.
b) Ensures that procurement packages within the MoH Tender Review Board Thresholds are indicated in the procurement plan.

Providers

Teaching Hospitals

- Teaching Hospital (Korle-Bu)
- Teaching Hospital (Komfo Anokye)
- Tamale Teaching Hospital

Ghana Health Service (GHS)

- Primary care
- Secondary care
- Tertiary care

Ghana Armed Forces Medical Service

Ghana Police Hospital

Christian Health Association of Ghana (CHAG)

1.2. BACKGROUND

The Government of the Republic of Ghana passed the National Health Insurance Act (2003) which established a National Health Insurance Scheme (NHIS) to provide universal health care to the residents of Ghana. This legislation included funding for application software, computer hardware, networking and related services to facilitate the smooth operations of the National Health Insurance Authority (NHIA), District and Mutual Health Insurance Schemes and the Health Service Providers.

Subsequent to the establishment of the NHIS a nation-wide ICT Solution was procured and its implementation began in September 2007 and is currently being implemented in phases. It is planned to be fully operational in February 2010.

This Phase 1 implementation at the current time faces challenges that need to be addressed. The NHIA has contracted T/TI to perform a needs analysis and design of a solution to address these challenges based on the concept of Providers submitting claims electronically.

The challenges that were initially identified to be mitigated in a Phase 2 implementation are:

a) Lack of lasting solution to membership card issuance and robust authentication of benefits eligibility at the point of service delivery;
b) Low use of NHIA provided systems by providers and Schemes.
c) Weak portability of the system (i.e. difficulty in accessing health facilities nation-wide);
d) Weak control of the systems that provide a potential for fraud;
e) Weak enforcement of the gatekeeper system (referral system);
f) High level of providers' claims;
g) Non-uniform Membership Registration processes due to the multiple platforms, which creates avenues for fraud;
h) Inability to effectively monitor and manage service utilization and attendant cost;
i) Inability to gather timely data on prevalence of the diseases/illnesses in different parts of the country leading to suboptimal proactive national health interventions;
j) Manual processing of claims leading to delays in payment of the claims.

Based on these and additional challenges identified as part of this study, T/TI will produce solutions to accomplish the goal of Provider based electronic claims submission.
The vision of the stakeholders in the national health insurance area is to have a seamless nationwide ICT platform that links the NHIA, the Schemes, the Providers and members of the NHIS for an effective, efficient and cost effective health delivery system in the country.

For this purpose, T/TI was awarded a contract to determine the ICT needs, document the requirements as an input to the RFP for the acquisition of the solutions that will address the gaps that are left by the ongoing nationwide NHIS ICT Solution.

The T/TI consultants undertook several trips to sites in Ghana and conducted meetings with the Ghanaian Providers and Schemes on local and regional levels as well as with the major stakeholders. T/TI reviewed ICT systems available at the Provider sites, assessed their adequacy for effective NHIS membership eligibility determination, tracking of patients, bulk

billing, electronic submission of claims and other standard accounting and financial management functions.

T/TI also reviewed the ongoing Nationwide ICT Solution for the NHIS with the purpose to identify gaps that will hinder seamless interfacing of the NHIA systems with those of the Providers' for the purposes of NHIS membership eligibility determination, tracking patients, bulk billing, electronic submission of claims and other standard accounting and financial management functions.

Therefore, this report will propose solutions that will meet the NHIS's goal of improving the electronic claims submission while enhancing the overall operations at the nation's Health Care Providers.

1.3. THE PURPOSE OF THE REPORT

This Phase 2 study was conducted to identify ICT systems, which if installed at Provider locations, would fulfill the goals of the NHIA as to member validation and electronic claims submission. A part of this goal is to provide ICT infrastructure, application software, LAN and sufficient WAN bandwidth to allow not only these functions, but to also add value for the Providers. The added value being in the form of a Hospital Information System (HIS) system for the use in all departments within the healthcare facility.

In order to allow the member validation and electronic claims submission functions of the various existing HIS systems in use today in Ghana, an interface has been designed that will allow developers of the HIS applications to communicate with the NHIA central database.

In order to implement these goals the study will identify ICT technical personnel required for the management of the Provider based systems as well as required training of the application users. This will be encompassed in an implementation plan that covers all aspects of a successful implementation.

While the study focuses on the Providers' needs, the needs of NHIA to support the Providers on a continuous basis will be addressed. This part of the study will discuss changes to the existing NHIA ICT operational structure focusing on support, ICT operational management, and the required ICT personnel.

The recommendations made in the study will be supported by tools that allow for developing budgetary costs for implementation at Provider facilities as well as recurring maintenance costs. In addition to the costing tools the study will define the technical requirements section for inclusion in any RFPs issued to procure systems for the Providers.

1.4. APPROACH TAKEN IN THIS STUDY

During the first week of the study the key stakeholders were visited and their comments on the study and suggestions were recorded. These initial interviews were used to form the basis of the subsequent interviews in the following weeks. The stakeholders interviewed included:

- Mr. George Dakpallah, Director, PPME, MoH

- Dr. Afisah Zakariah, MOH
- Honorable Dr Benjamin Kunbour, Acting Minister of Health
- Mr. Sylvester A. Mensah, (CEO), NHIA
- Mr. Ben Kusi, Director of ICT, NHIA
- Mr. Phillibert Kankye, Executive Secretary, Christian Health Association of Ghana
- Mr. Alhaji Muniru Mohammed,Project Coordinator, NHIA
- Mr. Philip Akanzinge, NHIS National Coordinator for GHS
- Mr. Daniel Osei, (PPME), GHS
- Mr. Sam Quarshie, Finance/ICT, GHS
- Ms. Laura Rose, Task Team– HIP, World Bank

The T/TI team of consultants spent two and a half (2.5) weeks interviewing representatives from a cross-section of medical facilities and schemes in the country. During these interviews the team gathered data on the operation of those facilities as it relates to the NHIS. Using a previously defined interview template the team gathered data on the way that patients are registered and claims are processed currently as well as the degree of computerization at the facility.

In order to develop a cross section of the types of facilities found in the country we visited facilities under the control of various stakeholders in this project. During this period the team visited four of the regions. In each region the T/TI team visited district, regional and teaching hospitals as well as schemes and regional NHIS offices. The regions visited included the Greater Accra, Central, Ashanti and Northern Regions. The facilities visited included:

Greater Accra Region

- Korle-Bu Teaching Hospital (KBTH)
  - Mr Narteh Abrakwa, NHIS Coordinator
  - Dr Ben Annan, Director of Clinical Services
  - Mr. Charles Anachanser, Director of ICT
- Ghana Armed Forces Medical Service
  - Dr. Wisdom Atiwoto
  - Col. Francis Kwashie
- Police Hospital – Richard Gueilla
- Alpha Medical Center
- Osu Klottey, Mutual Scheme
- Kpeshie Mutual Health Scheme

Northern Region

- Tamale Teaching Hospital – Dr. Ken Sagoe
- Tamale Mutual Health Scheme – Mr. Aminu Tuferu
- Savelugu Nanton District Hospital

Ashanti Region

- Komfo Anokye Teaching Hospital (KATH) – Dr. Nsiah Asare
- Ashanti Mampong District
- Mutual Scheme

Central Region

- Cape Coast Hospital
- Cape Coast Municipal Scheme

Other

Christian Health Association of Ghana (CHAG) - Phillibert Kankye, Executive Secretary

During week 4 of the in-country interviews, we visited with NHIA personnel having a stake and interest in the areas that this study covers. Meetings were conducted with:

- Mr. Sylvester A. Mensah, CEO of NHIA
- Mr. Nathaniel Otoo, Director of Administration and General Counsel, NHIA
- Alhaji L.Mohammed- Muniru, Project Coordinator, Health Insurance World Bank Project
- Ben Kusi, Director of ICT, NHIA
- Dr. Nicholas A. Tweneboa, Director of Operations, NHIA
- William K. Sarpong, Senior Internal Auditor, NHIA
- O B Acheampong, Director of R&D, NHIA
- Ahmed A. Imoro, Director of Finance & Financial Controller
- Thomas A. Adobe , IT Infrastructure / Project Manager
- Joseph Annor, National ICT Coordinator, Schemes

At the meetings with the NHIA personnel the T/TI team shared our preliminary views on what our recommendations will be for improving the submission of claims electronically through provider based Hospital Information Systems (HIS). Their opinions on these initial concept and recommendation were solicited. The T/TI team also learned about the needs of their departments that might be assisted through this proposed approach.

Meetings were also conducted with Superlock Technologies Ltd (STL) on current operations and current challenges. Follow-up meetings were conducted to solicit their recommendations for an interface between Provider-based HIS systems and the central NHIA system. Detailed technical information was requested during these meetings.

1.5. THE SCOPE OF THIS STUDY

This study builds on the previously conducted Gap and Needs Analysis report and seeks to define recommended solutions for the goals of Phase 2 of automating member validation and electronic claims submission by Health Care Providers. Covered under this study are selected Health Facilities and the NHIA supporting structure needed to implement Provider based systems to accomplish this goal.

This study incorporates the “people” side of implementation and does not just address the ICT requirements, but the planning for success. The steps necessary to implement Phase 2 are addressed including business process change at the Providers and the NHIA.

A review of the existing NHIA claims and membership management system necessary for a successful Phase 2 implementation was also conducted. The stability and completeness of the

Phase 1 project directly affects the potential success of Phase 2. Those risks associated with Phase 1 were previously identified in the Gap Analysis report previously submitted. These risks associated with a successful Phase 2 project are discussed in the current report.

2. SOLUTIONS ANALYSIS

The goal of study clearly identifies the need for solutions that meet entering 60% of claims in an automated fashion. It is clear that in order to do that, within a limited budget, it is necessary to target the facilities that will quickly attain that objective. Based on these budget limitations the study has defined required outputs that will serve as guidelines that can be used over time to bring automation to all facilities.

Based on our analysis of the existing healthcare facilities we have concluded that no one solution will accomplish this goal. A mix of solutions will need to be used in order to input all claims into the NHIA system. Each of the suggested models will need to be evaluated against the needs of each facility in order to reach the best choice for that facility.

We have identified the following options for claims submission:

1. Install an HIS system at Provider's facility which has the ability to submit claims electronically to the NHIA central system.
2. Use ICR/OCR forms as an interim method while HIS systems are installed and for facilities that are too small to justify an HIS implementation.
3. Manual submitted claims entered at a regional or central NHIA claims center.

All these options are discussed in detail in this report.

2.1. EXISTING PROVIDER ICT INFRASTRUCTURE

Our team's visits to the provider sites reveals that the current networks in the Ghana Health Service hospitals are at diverse levels of completion and quality. The network infrastructures for most of the hospitals visited where quite different. Some of the hospitals use fiber optics cable, while others still use the Unshielded Twisted Pair (UTP) cable as a backbone. Most of the hospitals network analyzed can be categorized as Flat network, this is because there is no routing taking place, and the whole network consist of the switches. Below is a detailed description of the ICT infrastructure in selected GHS hospitals:

2.1.1. TEACHING HOSPITALS
KORLE BU TEACHING HOSPITAL

The Korle Bu Teaching Hospital Local Area Network is segregated along the lines of individual departments/clinics which have varied levels of completion, connectivity and access points. Whereas the central administration block, main pharmacy, central stores, child health and maternity are fully networked, the medicals, accident centre, exchange and central Lab have varied degrees of completion for the LAN.

All the buildings are fully networked with the exception of the polyclinic. The individual buildings' LAN is characterized by a combination of wireless and wired network. All the LANs were laid within the last three years with about 70% of the switches in good condition.

The absence of a centralized and integrated Hospital Information Software (HIS) has reduced the use of the LAN in most of the departments to Internet connectivity. Radiology, Pharmacy and Central Administration are the only departments with a central management and sharing of information resources through Active Directory and other applications.

With the exception of the exchange, plastic and central lab all the departments have separate broadband access (with varied bandwidth sizes) to the Internet using Vodafone. The bandwidth sizes ranges from 1mbps at the Central Administration to 256kbps at child health.

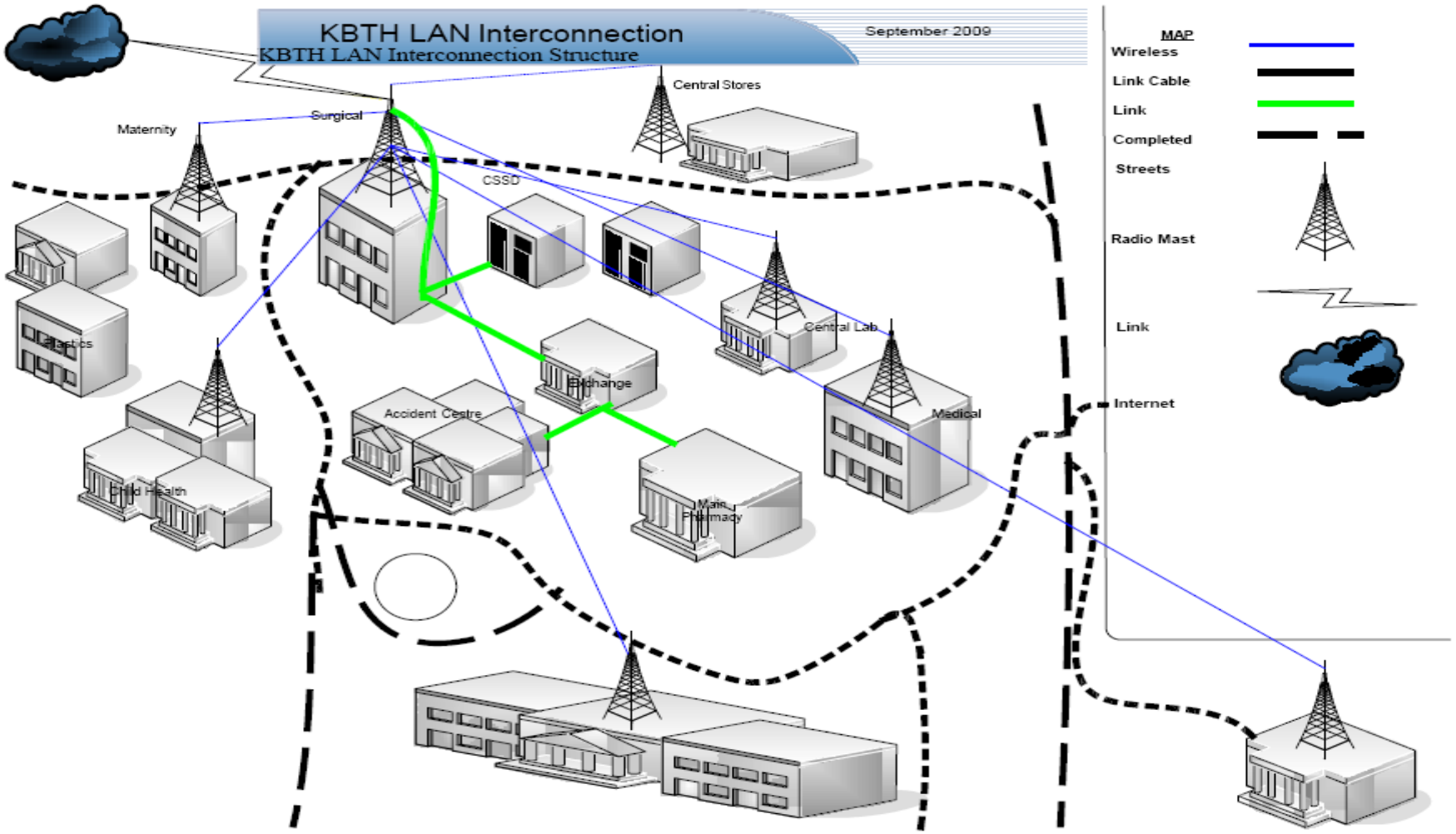


Figure 1 Korle Bu - Physical Topology

The figure 1 above shows the current level of backbone connection that exists between the various clinics and departments of the Korle Bu Teaching Hospital. Currently, there is no backbone connectivity between the buildings except those indicated with a green line on the diagram. The green line backbone link is a temporal link created using a cat 6 UTP cable. The proposed radio link connectivity is yet to be installed.

2.1.2. KOMFO ANOKYE TEACHING HOSPITAL

Konfo Anokye Teaching Hospital has an almost connected Local Area Network with the following features:

Komfo Anokye Teaching Hospital		
Box 1934, Bantama , Ksi	**Tel:** 051 02821	**Fax:**
Key contacts	**Position**	**Telephone**
Mr. Gyima Offin	Head of Administration	05102821
Ms Dufie	Secretary to Head of Administration	05122301
Dr. Nsiah Asare	Chief Executive Officer	051223010-3
Carl Wemengah		
IT Infrastructure		
• Networking of the entire hospital is about 90% complete. • Fiber Optic Links are used to connect the various clinics and buildings • A mixture of managed and un-managed switches (Cisco, DLink and 3com switches) is used. • A single physical layer network separated logically using IP Addresses. • The Local Area Network is internally managed • Kaspersky Anti-Virus is installed on all workstations and servers.		

The Komfo Anokye Teaching Hospital's network is characterized by 250 Workstations, a fully configured Microsoft Active Directory and two Data Servers. Domain Users and group profiles are used for authentication and access to various resources.

A Hospital Information System (HIS) from a local company, Pro-Resolve is being used by the hospital. Currently, the records, pharmacy and claims modules are fully developed and used. Further work is required before the medical and clinical modules can be used.

A 1Mbps dedicated broadband internet link is provided by a local Internet Service Provider – Africonnect. Workstations, which are allowed to connect to the internet, are logically separated from the rest of the network using a separate IP address. The Internet Access is mainly used for research purposes.

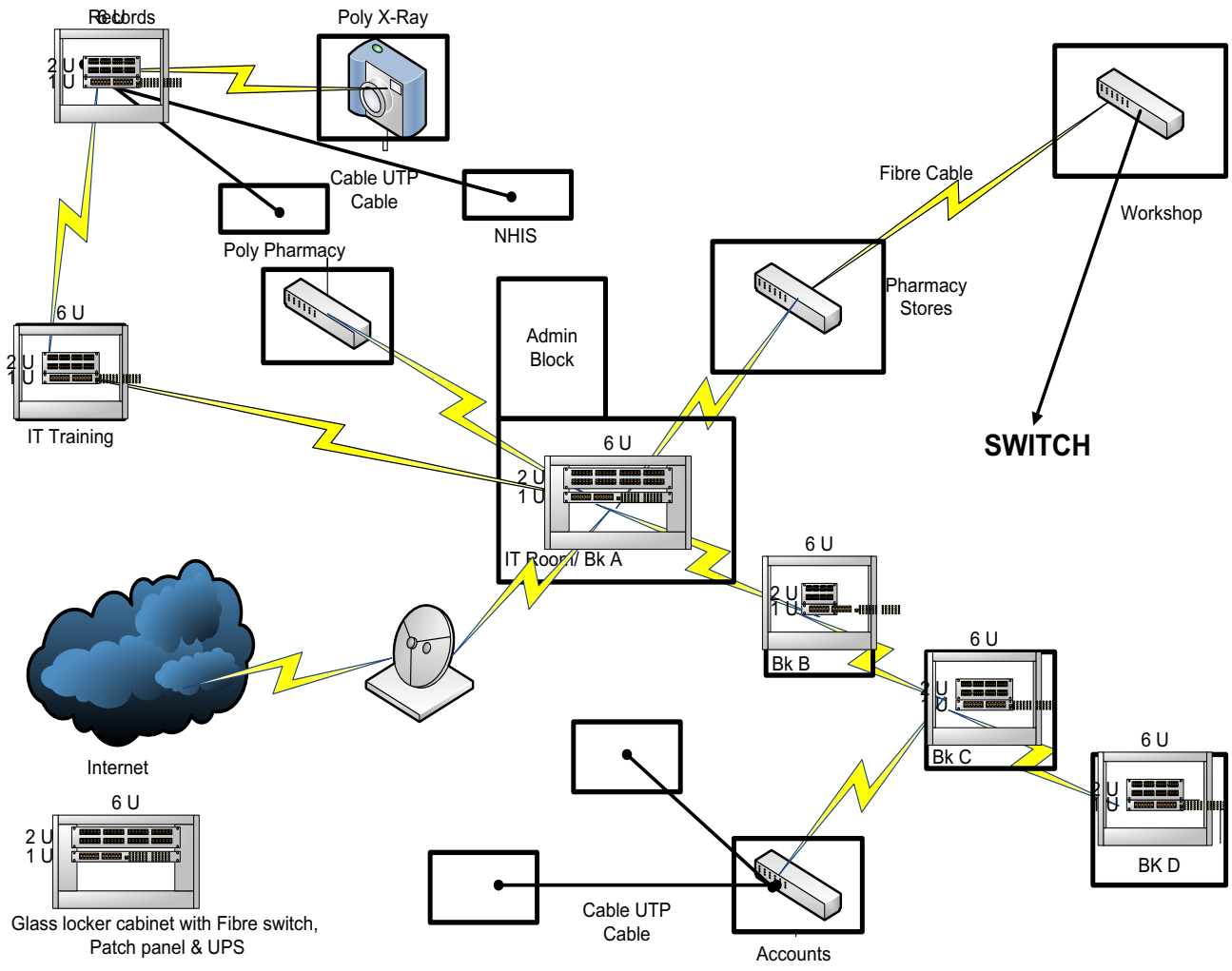


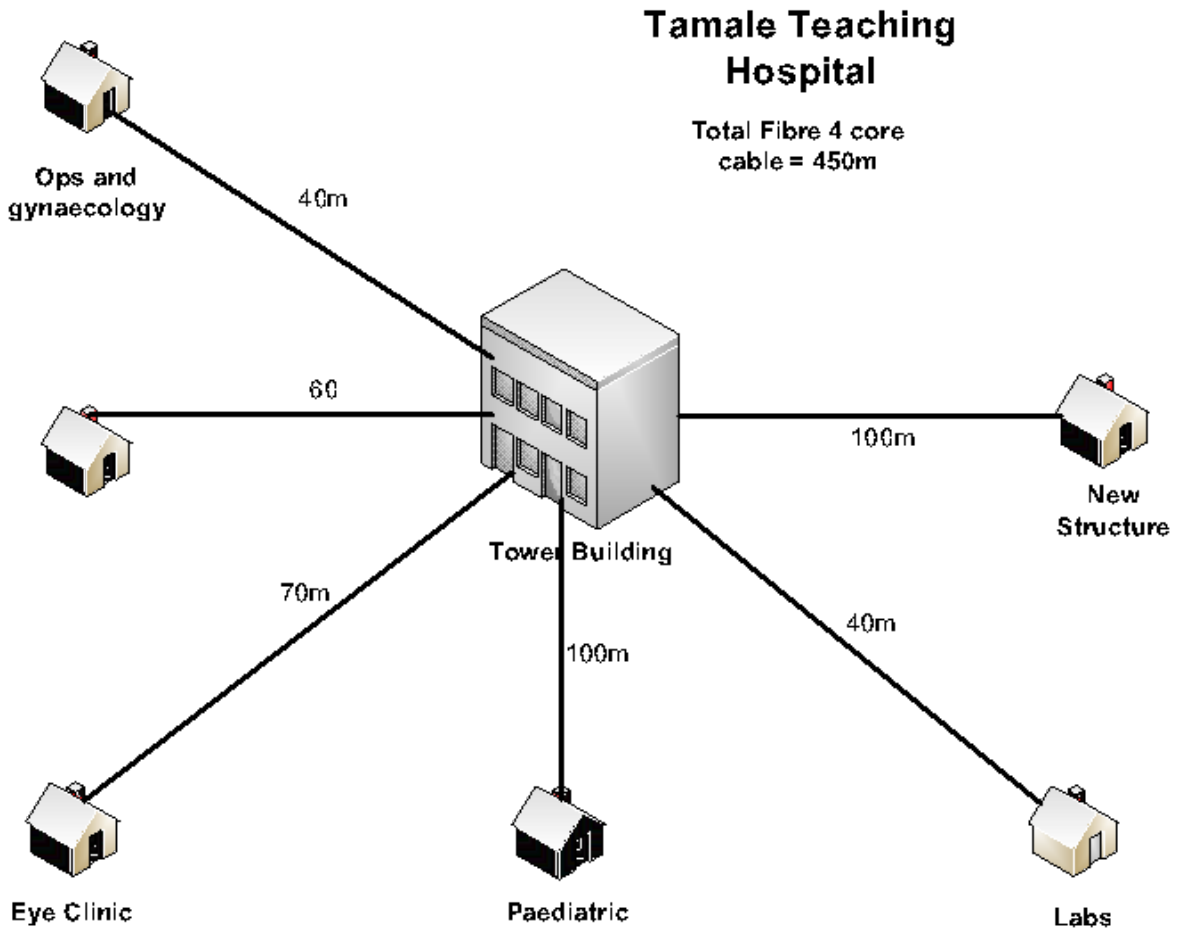
Figure 2 Komfo Anokye Physical Topology

As shown in **figure 2** above, the Komfo Anokye Teaching Hospital has about 90% fiber optic backbone network which stretches across the hospital. It also has point of entry and exit into the network. However, it is also characterized by a flat network. It may be necessary to introduce network segmentation in the future to reduce the broadcast domains.

2.1.3. TAMALE TEACHING HOSPITAL

The Tamale Teaching Hospital has no ICT Infrastructure except for a few computers used for recording patient data at the records section. Also, there are a few computers scattered across the hospital with no define management, maintenance or monitoring plans. Also these computers are not connected for any form of resourcing sharing. A complete ICT Infrastructure may be required to have full use of our recommended HIS solution.
Below is a not-to-scale diagram showing the buildings in the hospital and their respective distance from the central tower building:

Northern Regional Hospital, Tamale.		
Box 16. Tamale	**Tel:** 07122505	**Fax:** 07122505
Key contacts	**Position**	**Telephone**
Mr. K.K Boachie	Head of Administration	0244830382/0208174340
IT Infrastructure		
▪ LAN not Present ▪ Hospital Information System not present ▪ Scattered PCs and printers used mainly for basic Microsoft Office packages.		



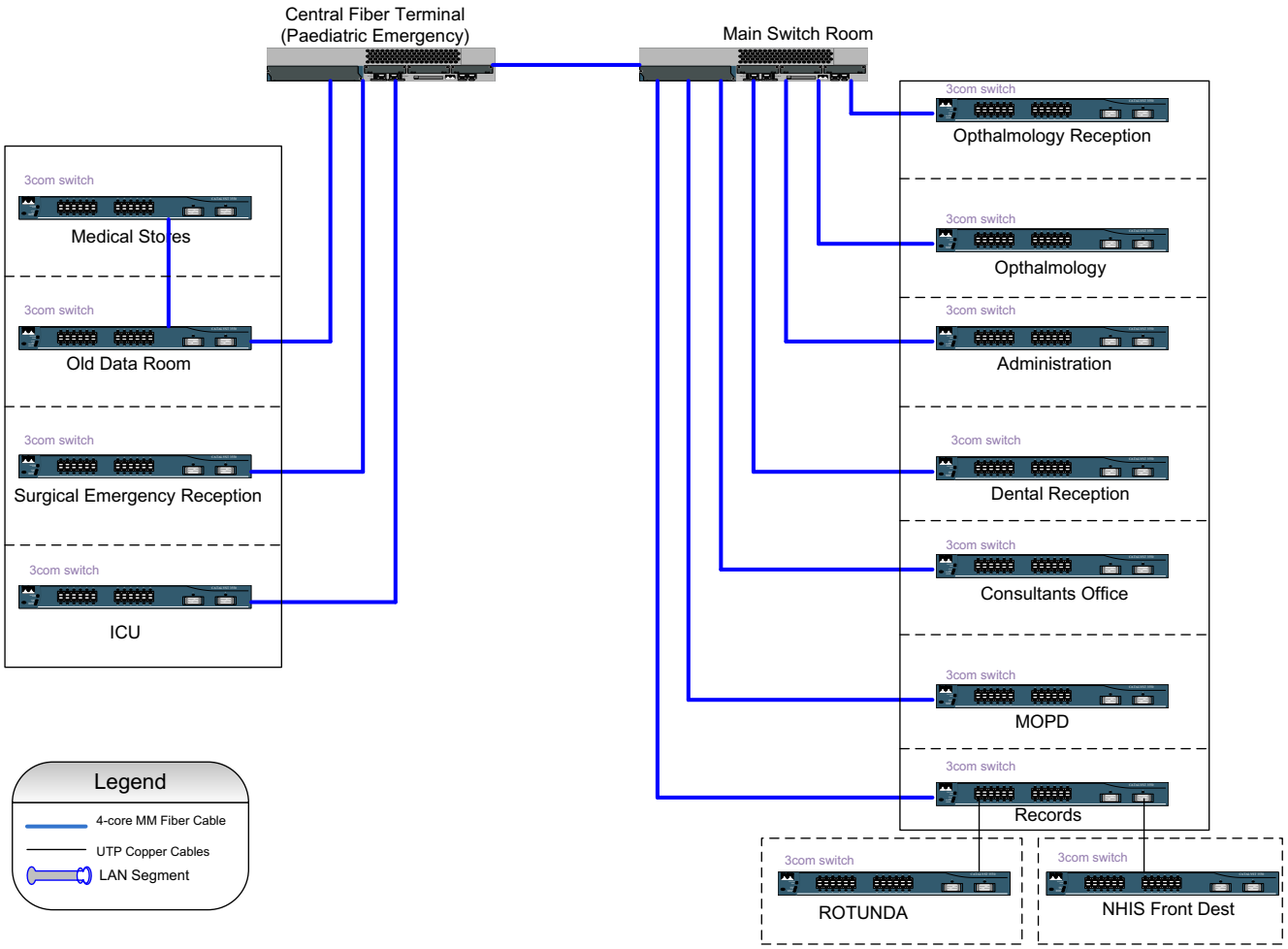
2.1.4. 37 MILITARY HOSPITALS

The 37 Military Hospital is characterized by a cat 5e cabled network in all the building in the facility with fiber optic backbone connectivity. It is currently configured as a flat network with no segmentations (one large broadcast domain). However, most of the switches on the network are old with no maintenance or support contracts.

There is a team in charge of the ICT infrastructure headed by Dr. Wisdom Atiwoto.

37 Military Hospital, Accra		
Key contact	**Position**	**Telephone**
Dr. Wisdom Atiwoto	Head, IT	0244 333223
IT Infrastructure		
• There is a Local Area Network in most parts of the hospital • Existing network is based on a Microsoft Active Directory domain with effective resource sharing and access control mechanisms. • There is an internal Information Technology team in place who supports the day to day operations of the ITC Infrastructure. • The current network is a flat network with no managed switches or routers for segregation • There is partial fiber optic backbone connectivity between the buildings. Connectivity between some of the buildings is based on cat 5e cables. • The 4 core fiber backbone can be configured for link redundancy.		
Physical & Logical Network Diagrams:		
Please find below the physical topology of the 37 Military Hospital's network.		

37 Military Hospital
Existing Network Diagram



2.1.5. POLICE HOSPITAL

Police Hospital, Cantonments		
Key contact	**Position**	**Telephone**
Inspector Adjei	Administrator in charge	0274322317
IT Infrastructure		

- There is no form of computerization in the hospital, there are pockets of LAN cables found in some parts of the building but could not traced to any aggregation point.
- Existing network is based on some form of peer – to – peer connection with no formal method of resource sharing and access control mechanisms.
- There is no internal Information Technology team in place and support depends solely on ad hoc contract with external partners for support.
- A small number of unmanaged switches were identified.

Physical & Logical Network Diagrams:

There were no physical or logical network diagrams in place.

Most of the departments at the Police Hospital are within close proximity with the exception of the Annex which is about hundred meters away.
There is also a new uncompleted block opposite the current main block (about 20 meters apart)

2.1.6. REGIONAL HOSPITALS

2.1.6.1. HO REGIONAL HOSPITAL

Volta Regional Hospital		
Box 49, Ho	**Tel:** 091-27321	**Fax:** N/A
Key contacts	**Position**	**Telephone**
Mr. Alex Amenu	Head of Administration	0244529794
Dr. Nyanuame	Chief Medical Officer	091-27321
Mr. Benjamin Amedumah	Head of Medical Records	0244751967
IT Infrastructure		

- Local Area Network (LAN) present, the hospital is fully networked. The LAN is configured as a flat network with a single IP Address for all the buildings, there are no routers on the network.
- There is a complete networking facility with Microsoft Active Directory present. The facility uses DHCP and DNS Servers for local device connectivity.
- There is complete fiber connectivity between the main buildings in the facility.
- Internet facility is available at most of the offices. The hospital is connected to a local ISP with a shared 512mbps internet access.
- An Anti-Virus product is currently installed on all computers at the facility.
- There are no internal Information Technology personnel at the facility. The external consultant used in developing the LAN is on yearly renewable maintenance and support.

2.1.6.2. SUYANI REGIONAL HOSPITAL

Sunyani Regional Hospital		
Box 27, Sunyani	**Tel:** 061-2846160	**Fax:**
Key contacts	**Position**	**Telephone**
Mr. Thomas Tawia	Head of Administration	061-2846160
Mr. Yakubu Abdulai	IT Officer(Record section)	0244068553
Dr. Dan Asare	Medical Director	031-23157
IT Infrastructure		

- Local Area Network (LAN), there are 40 PCs connected to 17 unmanaged switches.
- Microsoft Active Directory for Resource Management and user access right and permission.
- Connected 26 buildings for data connectivity using cat 5e.
- Currently using a Hospital Management System (HMS) – HAMS.
- Internet present
- Some form of Computerization is currently being provided by Finalyst Ghana Ltd.

2.1.6.3. UPPER EAST REGIONAL HOSPITAL

Upper East Regional Hospital, Bolgatanga		
PMB, Bolgatanga	**Tel:** 07222461/2	**Fax:**
Key contacts	**Position**	**Telephone**
Mr. George Atampugri	Head of Administration	0244180195
Dr. Amiah	Medical Director	072-22461
IT Infrastructure		
▪ Local Area Network (LAN) was not visible ▪ According to Mr. Atampugri some form of Computerization is currently being installed for the pharmacy department.		

2.1.6.4. WA CENTRAL HOSPITAL

Wa Central Hospital , Wa		
PMB, Wa	**Tel:**0756-22664	**Fax:**
Key contacts	**Position**	**Telephone**
Mr. Roger Gaalee	Head of Administration	0243586733
Dr. Ababresse	Medical Director	0756-22664/0243586733
IT Infrastructure		
▪ Local Area Network (LAN) present ▪ Internet present ▪ Will review our proposal and make a decision		

2.1.6.5. CAPE COAST REGIONAL HOSPITAL

Central Regional Hospital		
Box 1363, Cape Coast	**Tel:** 042-34010	**Fax:** N/A
Key contacts	**Position**	**Telephone**
Mr. Ofori	Head of Administration	O42-34010
Dr. Ekenam	Chief Medical Officer	O42-34010
IT Infrastructure		
▪ Local Area Network (LAN) present, hospital is fully networked. ▪ Internet facility available at most of the offices ▪ Extent of computerization was not immediately known and officials were unwilling to provide us with the further information		

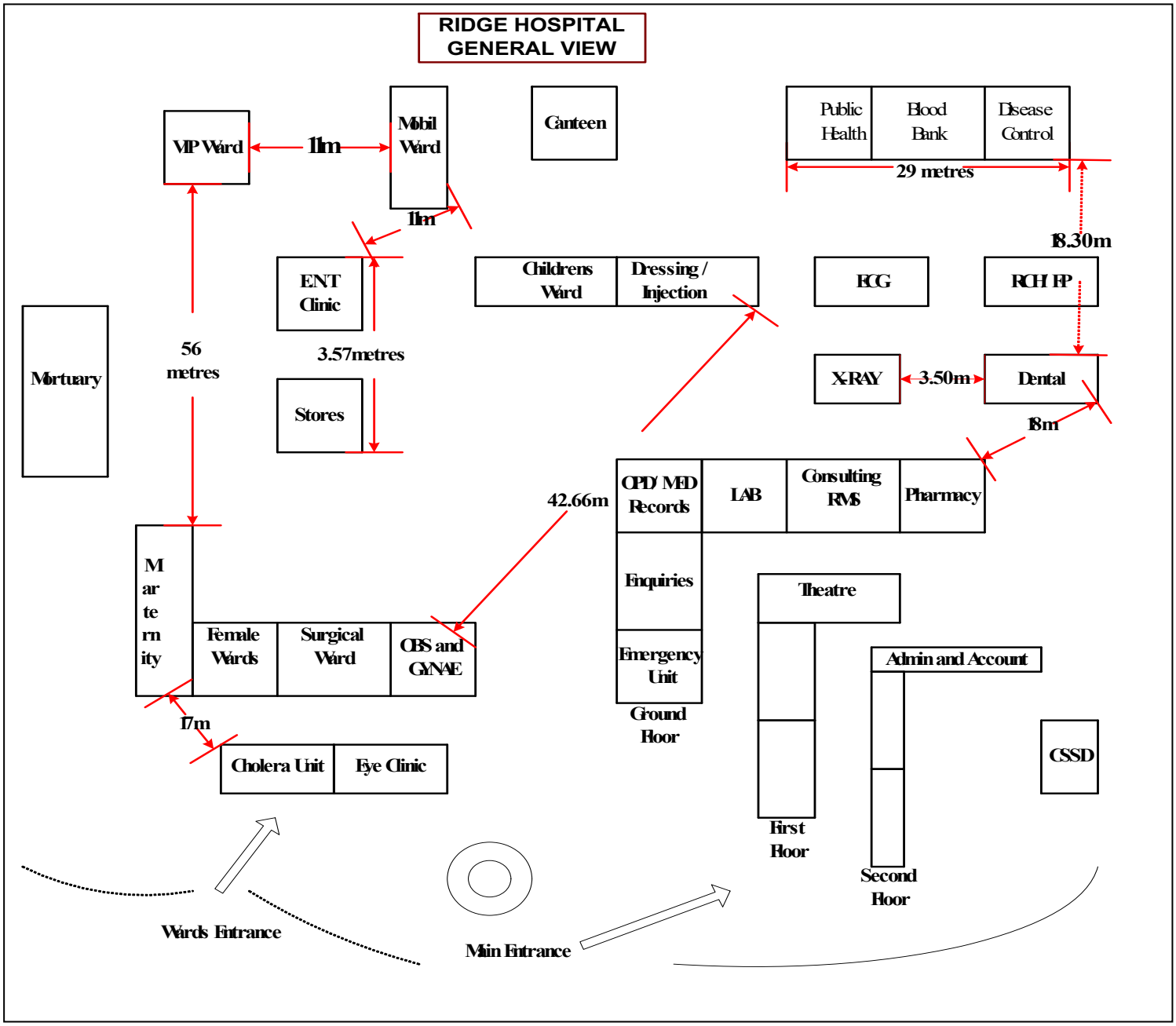
2.1.6.6. EFFIA NKWANTA REGIONAL HOSPITAL

Effia Nkwanta Regional Hospital		
Box 229,Sekondi	**Tel:** 031-23157	**Fax:** N/A
Key contacts	**Position**	**Telephone**
Mr. Osei Boateng	Deputy head of Administration	0244718670
Mr. Asare Bediako	Head of Administration	031-23157
Dr. Paul Ntodi Kwao	Chief Medical Officer	031-23157
▪ Proposal submitted to Mr. Osei Boateng (Deputy head of Administration)		
IT Infrastructure		
▪ Local Area Network (LAN) partially done ▪ Some form of Computerization is currently being provided but		

2.1.6.7. RIDGE GENERAL HOSPITAL

The Ridge General Hospital has a very limited ICT infrastructure. It is characterized by number of computers that is scattered across the various buildings in the hospital.

Ridge General Hospital



2.2. EXISTING WAN

In the period of August 17 - 25, 2009 the team visited Superlock Technologies Limited for detailed discussions regarding the installed WAN.

Items discussed included:

1. The installed network, and details of design, security, and quality assurance.
2. Existing network design vis-à-vis planned.
3. Challenges from users (especially providers and schemes).
4. System documentation and change control.
5. Possible upgrades and changes in designs.
6. The Network Operating Center (NoC) operations and maintenance.
7. Degree of usage of WAN infrastructure and level of support provided by STL.

Their comments were recorded and verified. The staff of STL interviewed includes Mr. Zino the Project Implementation Manager and Mr. Oz.

In order to broadly categorize the types of installed systems we grouped the installed sites into VSAT sites and Radio sites.

Reviews of technical documents were conducted where available to assess the capacity of the current WAN network to support Provider based solutions.

The WAN Needs Assessment covers the following areas:

- Review the entire WAN systems (available at the Provider sites, NOC and Scheme sites) and assess their adequacy for effective communication between the various stake holders.
- Review WAN operations to identify gaps that require attention.
- Provide recommendations as to how gaps identified will be filled with a view to ensuring the high availability network for NHIS operations.

2.3. CENTRALIZED INSURANCE PROCESSING

Centralized Insurance Processing is a critical component to efficient patient registration and claims processing. Centralization allows for consistency in processes and procedures, efficiencies in HR hiring and monitoring, effective oversight of the program and eliminates redundancy.

A solution that allows for 60% automation of claims processing, requires a rules based system that allows for minimal intervention when claims are submitted. It also requires a change in philosophy in how claims are handled both pre and post processing.

Based upon the goals of the project, interviews with key stakeholders and meetings with the schemes and providers, the following structure is recommended for addressing patient registration, claims processing and reconciliation.

Assumptions:

1. Infrastructure supports data entry 99.95 % of the time.
2. A rules based system is in place that supports maximum claims processing without manual intervention.
3. System supports user friendly interfaces that are easy to read and streamline data entry.
4. System supports post payment audits of both member registration and claims by generating statistically valid audit samples.

Roles and Responsibilities:

NHIA Central Office

1. Administration
2. Member registration processing
3. Member ID Card generation
4. Member validation during provider registration
5. Data entry of paper claims
6. Claims processing, payment and reconciliation
7. Auditing of member registration and claims

Regional Office

1. Training
2. End-user support
3. Technical support
4. Paper claims collection point
5. Provide workspace to auditors

Schemes

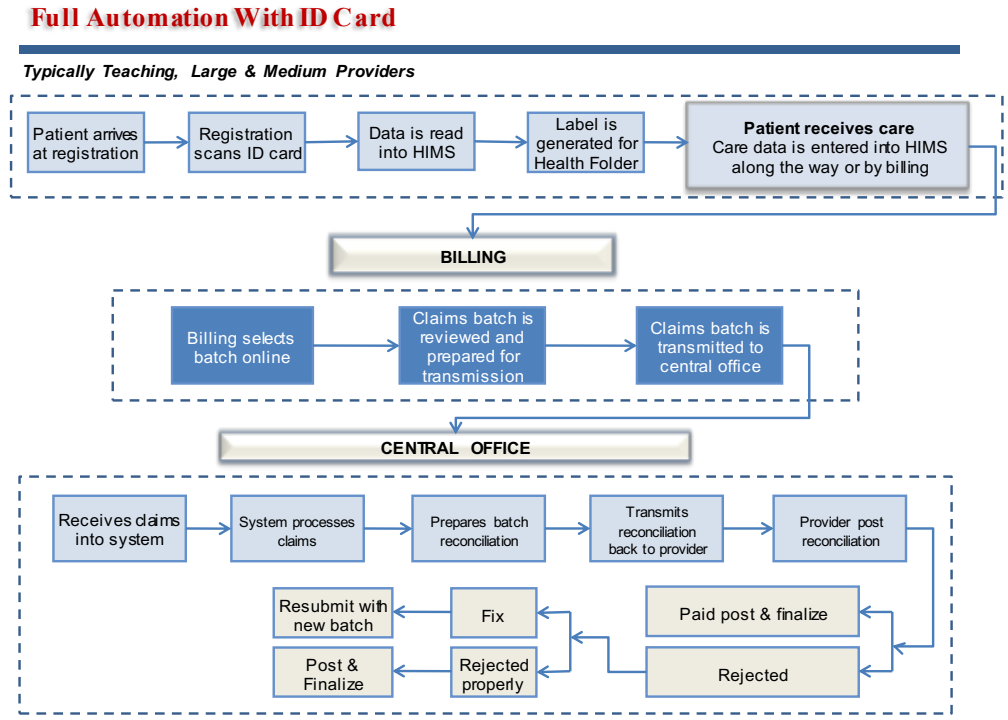
1. Marketing for new members
2. Member registration
3. Accounting
4. Card distribution
5. Member renewals

Providers

1. Member verification at the time of registration
2. Claims preparation and submission
3. Claims reconciliation

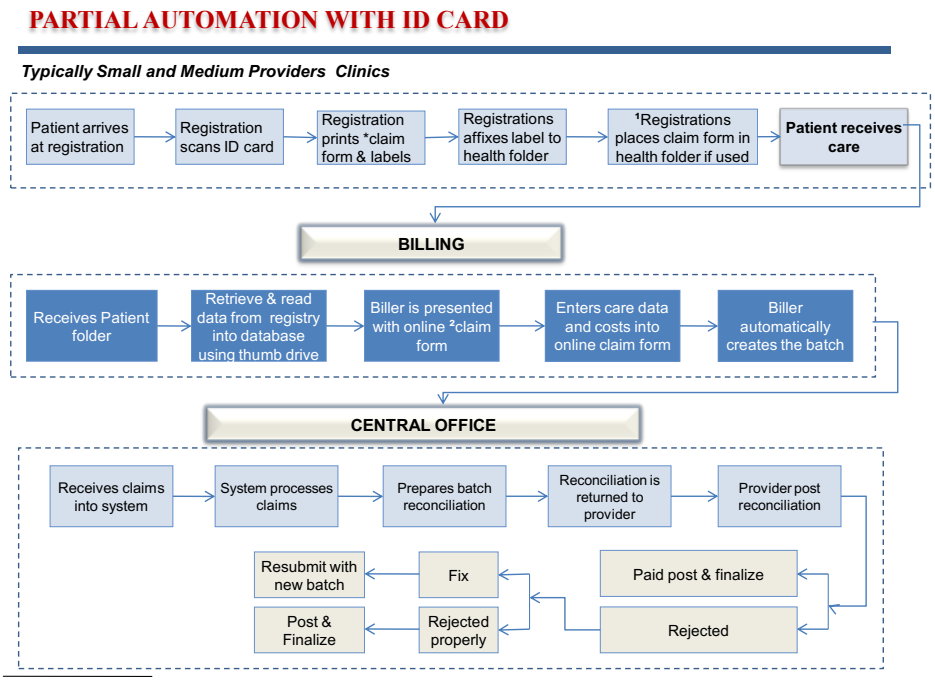
Providers are responsible for registering patients, submitting claims for reimbursement and reconciling once claims are processed. In order to meet the needs of the various providers, the following approach will be taken:

1. Teaching hospitals and larger providers will be provided with automated solutions for all three processes.



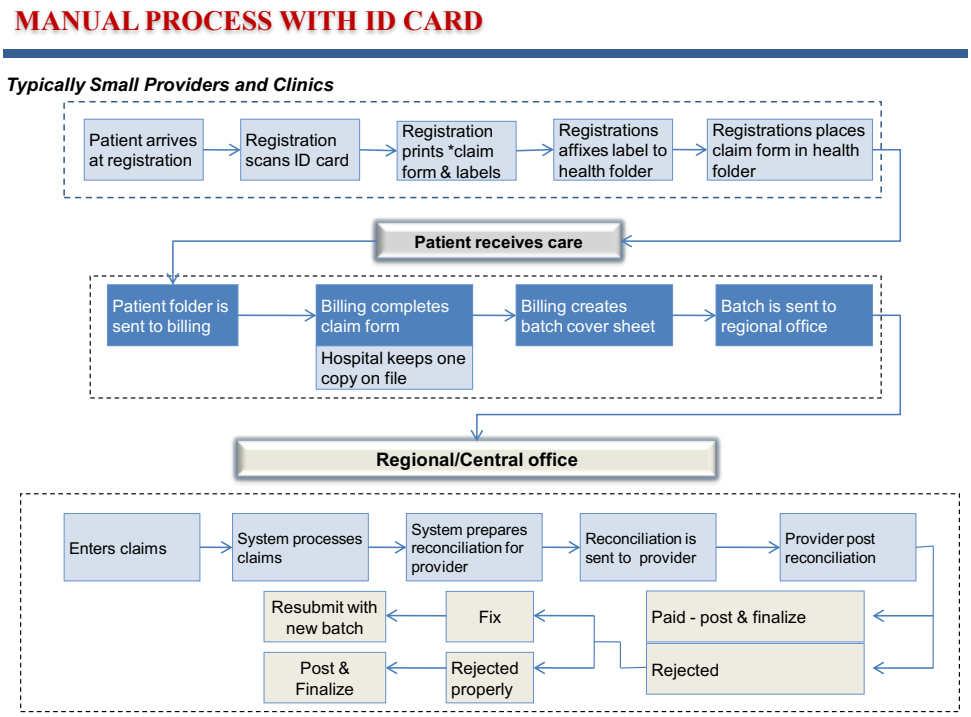
Note: Claim form is optional in this process
Claim form has patient registration data complete

2. Small to mid-sized will be provided automated solutions for patient identification and will be offered an automated claim form that can be completed and electronically submitted for processing.



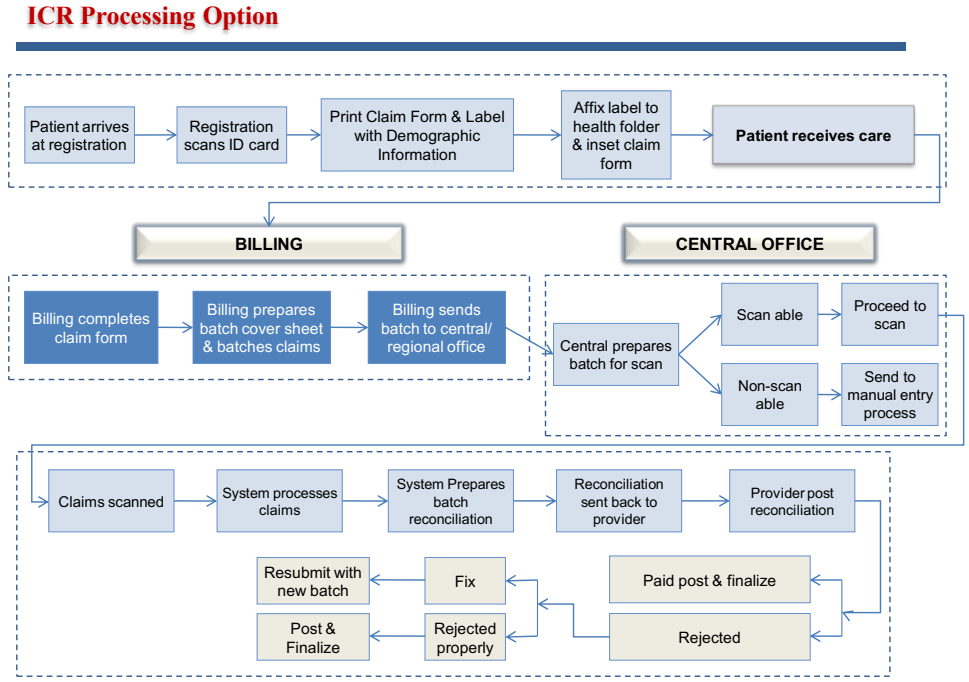
Note: ¹Claim form is optional in this process
²Claim form has patient registration data complete

3. Smaller providers will be provided automated solutions for patient identification and will complete two-ply paper claim forms that will be used for claims processing, the provider will retain one copy and the other submitted for payment.



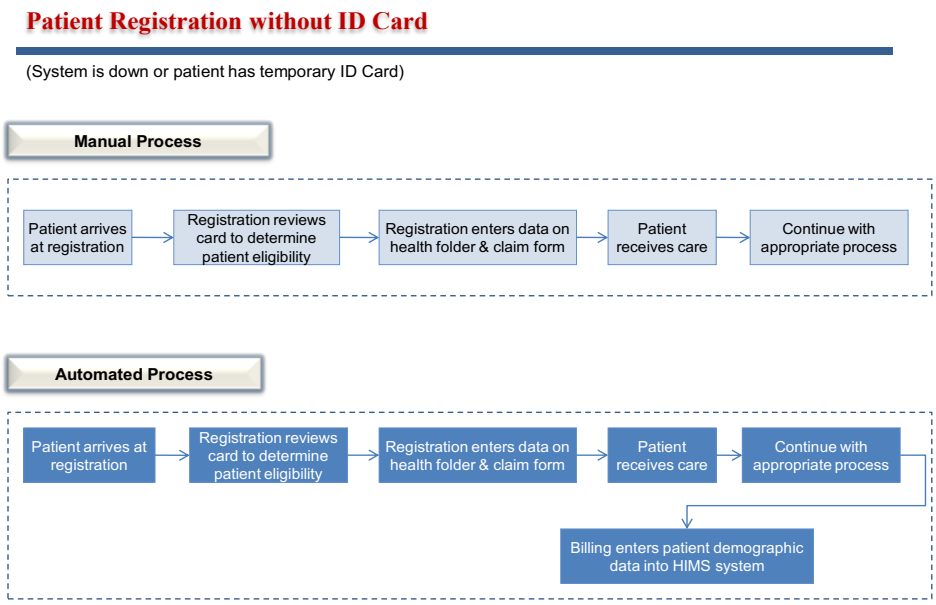
Note: * Assumes 2 ply claim form otherwise photocopy is needed

4. ICR Processing is an option that allows for partial automation. The claim completed at the provider site is completed according to specific guidelines which allow the claim to be scanned in a machine readable format for processing. This alternative would require that the IRC claim forms be 2 ply or provisions made for photocopying before submission so that the provider maintains a record of the claim.



Note: Claim form is optional in this process
Claim form has patient registration data complete

5. Although the planned infrastructure calls for the system to be available 99.95 % of the time, provisions need to be in place for manual processing of registrations in the event the system is down or when the patient has not received a permanent ID Card.



Note: Claim form is optional in this process
Claim form has patient registration data complete

NHIA Regional Offices are responsible for training, technical and customer support and collecting and sending paper claim forms to the central office for processing. Although comprehensive training and education will take place during the implementation, ongoing training and support is needed to ensue provider employees are fully capable of using the solutions, the equipment and software. They also need to know how to maintain the equipment in working order. Paper based providers must also have processes and procedures in place to ensure timely submission of claims. Although the Regional office will not be directly responsible for auditing, they will provide office space to the auditors assigned to that territory.

Schemes, using their own personnel and agents, will be responsible for patient registration, this includes: marketing to obtain new members, screening members when they apply for insurance, collecting insurance premiums, taking required photographs, entering the data into the registration system, submitting it to the Central office for processing and distributing cards when they are issued. They will provide detailed accounting data regarding insurance premiums to the Central office and reconcile premiums with the central office based upon an agreed upon formula.

The NHIA Central Processing facility has four main functions: overall management of the patient registration and claims processes, processing patient registration and producing identification cards, claims processing and reconciliation and auditing of patient registrations and claims.

The overall management function in the central office ensures that the same processes and procedures are being used throughout the system. They monitor statistics, customer support queries, and make recommendations and changes as needed.

The central office will receive all patient registrations, process the requests, produce cards and send the cards back to the Schemes for distribution. They will ensure quality and timeliness of processing.

Claims processing at the central office will accommodate all types of claims submissions and will be staffed with qualified claims analysts and data entry personnel. The claims will be processed and claims reconciliation will be returned to the provider. They will ensure quality and timeliness of processing.

The audit staff reporting to the central office will be responsible for conducting random audits generated by the system to ensure accuracy and validity of patient registrations and claims being submitted for processing.

2.4. SOLUTION OPTION ANALYSIS

The Government traditionally evaluates new IT projects on a “buy” basis. The new model of Public Private Partnerships needs to be added to this traditional method of procurement options. This study evaluates all of these options as a possible method to implement new systems and business process for the identified Health Providers.

Our analysis is based on defining the required functionality needed by Providers in order to submit electronic claims. Since implementation of all Providers will take years to accomplish and may never be accomplished at some of the smaller facilities we have also identified interim recommendations. These recommendations have been designed to significantly improve the claims process and provide simplification of the Provider business process while providing a semi-automated process for claims.

After considering the possible solutions for improving processes at the Providers we have concluded that no one solution fits all Providers. We are not making a recommendation of a specific HIS system that should be used country wide but instead offer choices that can be used. The selection of the specific solution for any individual facility needs to be made at the facility level by the administration of the facility based on their needs.

It is a positive situation that choice is available in Ghana. The competition leads to better systems over time as each competitor adds functionality to their products in order to retain or acquire new customers.

The Defined Outputs section of this report identifies selection criteria that can be used to determine that a HIS vendors solution meets the basic requirements for use in interfacing with the NHIA main system. It is the Provider that needs to determine if the vendor's solution meets their specific needs at their facility. NHIA should not under any circumstance force a facility to accept NHIA's desires as to a specific HIS system

2.4.1. DEFINED OUTPUTS

In order to evaluate all options on an equal basis T/TI has developed required Outputs that all of the solutions must provide.

2.4.1.1. COMMON OUTPUTS

DATACENTER CONSTRUCTION – OPTIONAL

- Necessary Servers for system operation
- Necessary Routers for system network
- Necessary Firewalls for system data security
- Load balancing hardware need for rapid response times
- Redundant Servers, Routers, Firewalls and Load Balancers for fail safe operations
- Spare parts
- Sufficient Air Conditioning to support 150% of the initial datacenter cooling load
- Centralized UPS sufficient to support 200% of the initial load
- Electrical generator sufficient to support 300% of initial load and backup generator
- Sufficient data circuit bandwidth to support a 99.99% availability under load

DATACENTER OPERATION - OPTIONAL

- Policy and Operations policy and procedures
- ITIL complaint Change Management, Configuration Management, Problem Management policies and procedures
- 24x7 Network Operations Center (NOC) located in Ghana.

- Certified MCSE and CNE technicians
- Service Level Agreement (SLA) for 99.95% availability
- Disaster Plan
- Security Plan and Audits
- Active network monitoring system
- Trouble Ticket system
- Hands on Government staff training in all operational aspects of the datacenter
- Fuel for power generators

REPORT AND QUERY SERVICES

- Report generator service to process requested reports
- Available as a Web service by all applications
- Support for both blocking and non-blocking request modes
- Request priority support
- Selection queries to be in SQL format
- Saved report support
- Scheduled report support
- Queue and report management via browser interface

2.4.1.2. COMMON OUTPUTS FOR ALL APPLICATIONS

- Full Ghana e-GIF compliance
- User Interface to be simple and easy to use
- Context sensitive on-line help
- Multi currency support with an inbuilt currency converter but should maintain a one currency (GH ¢) database. (This will facilitate processing of foreign currency denominated purchases and payments).
- Session logs
- Transaction logs
- Simple page display times to be less than 6 seconds
- Complex queries to be optimized for optimal response times
- Context sensitive menus

2.4.1.3. NHIA CENTRAL SYSTEM CHANGES

In order for any Provider HIS system to interface with the NHIA central system changes will be required at the current central processing system. These changes will need to be made to allow the HIS systems to interface for member validation and claims submission. Currently all transactions for these purposes are performed by applications created by STL as part of the Phase 1 contract.

The current method of member validation is a dedicated PC at the Providers that queries the central NHIA system to check the current member status. This process currently interfaces with no other processes at the Provider and is viewed as extra work by the personnel at the health facility.

Claims are currently submitted at the Schemes via a forms entry process developed by STL which allows for entry of claims one at a time. This method is not applicable to the Phase 2 model of bulk claims submission by the Providers. A central system function will need to be developed that posts bulk claims to the main databases.

In addition, a process for transmitting bulk claims will need to be developed. This can be an integrated process within the NHIA central system or an out-of-band process that operates independent of the central system and is used to place batch claim data into a location where STL processes can post the claims to the central system.

The interface between the Provider HIS systems and the NHIA central system will need to be based on best practices for moving data between health related organizations that is:

- Secure transmission
- Ensures patient privacy
- Resilient to power and communication link failures
- Simple to implement at the Provider locations
- Adds value to the Provider

As of the writing of this report we have not been able to evaluate the difficulty of STL to implement this interface methodology. The NHIA system is a proprietary system owned by STL. NHIA has purchased the use rights to use this system and has no ownership rights as to the source code that the system is written in. In order to determine the cost STL will charge for the required changes the NHIA will need to submit a change request for pricing by STL.

The optimum method of implementing the inclusion of the required interface would be to negotiate with STL technical personnel the best methods to use to assist them in implementing the required changes. Using a consultative process will allow STL to advance their preferred methods and allow for the modification of the proposed methods to assist them.

2.4.1.4. NHIA CENTRAL SYSTEM OUTPUTS

In order for any interface to work between the Providers HIS systems and the NHIA central system there are some required functions that need to be implemented. These are:

- Real-time query for member validation. This process will query the NHIA system and return the information contained in the Membership Tables or an invalid member response. For new patients at a facility the NHIA membership information would be used to create a new patient account within the HIS system.
- Download tables:
    - Diagnostic codes, description, reimbursement rate and rule linage definitions
    - Treatment codes, description, reimbursement rate and rule linkage definitions
    - Laboratory codes, description, reimbursement rate and rule linkage definitions
    - Drug codes, description, quantity limits, reimbursement rate and rule linkage definitions
- Bulk Claims Submission in Batch – Once uploaded from the Provider HIS system the claims will be available for posting to the NHIA central system. Our proposed format would be XML but could support a Comma Separated Value (CSV) format.

- Claims Submission must be batch transmission
    - Claims Submission must be capable of restarting from last checkpoint
    - Transmission to be encrypted
    - Must compare batch totals and hash counts at batch completion
    - Codes to be used for submission rather that text fields. Currently STL feels that codes should not be used but text descriptions instead. We disagree with this method but have designed the interface based on STL's desires. This will result in substantial increases in transmission times.
- Rejected Claim Notification – The NHIA system would extract all original submitted claim information along with error codes indicating the reason for rejection that would then be downloaded by the Provider HIS system the next time a connection is made.
- Claim Batch Status query – This needs to be a real-time link to the NHIA system from the Provider system to retrieve the status of claims batches previously submitted. The status information on the batch would be returned on the query.
- All tables to be coded with valid start dates to allow for multiple revisions to tables. Treatment date determines which table revision to use for drugs, treatments and diagnostic pricing and validation.
- Business rules to be used for claims vetting rather than manual prepayment vetting.
- System must support random claims selection for post-payment audits.
- Retrieval of rejected claims must be supported
- Resubmission of rejected claims must be supported
- Real-time retrieval of claims batch status to be retrievable
- Graphic document attachment and viewing to Member Registration. Storage type to be PDF or alternative standard.
- All interface APIs to be SOAP using XML formats

2.4.1.5. PROVIDER HIS OUTPUTS

As part of the Phase 2 solution is the goal of Providers submitting claims electronically. In order to accomplish this goal the Providers need a method of submitting the claims. The majority of the existing hospitals in Ghana do not have any HIS systems in their facilities.

We have identified four (4) vendors currently marketing HIS systems in Ghana. Further discussion on the vendor systems can be found in Section 3.1 Existing HIS Systems in Ghana in this document. In order to modify those systems to use the defined interface required for the claims submission and vendor validation the following defined Outputs.

- Capable of implementing the NHIA interface using SOAP / XML.
- Have provision for querying the NHIA central databases for member validation in real-time as part of the patient registration process.
- HIS application has provision for:
    - Patient Registration
    - Patient Electronic Medical Record (EMR)
    - Clinical care departments
    - Pharmacy
    - Laboratories

  - Radiology
  - Stores / supplies
  - Billing / Claims / Reconciliation
  - Accounting
- Supports batch submission of claims via NHIA interface that is re-start enabled ever n transactions.
- Supports retrieval of rejected claims and resubmission after correction
- Supports query to NHIA central database to retrieve status on claims batch
- Support downloading of supporting tables from NHIA system for updating HIS tables:
  - G-DRG or other coding structure
  - Drugs
  - Treatment
  - Laboratory
- Use same table format as NHIA tables for:
  - Diagnosis
  - Drugs
  - Treatment
  - Laboratory

Note: Dependant on STL supplying table formats used.

- Have Rules for the validation of claims data
- Have report generator for creation of reports
- Have Identity service for user authentication
- Have configuration items for Provider Identity information needed to identify the facility on the NHIA system
- Provide Disaster recovery process as part of the system
- Support data encryption of all transmitted data
- Provide manual outage process with post incident recovery of data entry
- Be configurable as to which departments are implemented at a facility.
- Be capable of being used with a minimum of registration and claims departments being implemented for claims submission. In this configuration claims should be allowed to enter missing data on a single form / page without having to use multiple forms

2.4.1.6. PROVIDER HARDWARE INFRASTRUCTURE OUTPUTS

2.4.1.6.1. PROPOSED PROVIDER SOLUTION

As part of the Gap Analysis, our team identified that any solution that will encourage providers to use the NHIA infrastructure in patient verification and claim submission must provide some incentive to encourage the provider to use the system. We identified the implementation of a Hospital Information System as a key incentive.

Geographically dispersed clinics need Local Area Network for various reasons. Among them are instantaneous access to patient information, access to medical information, and access to the Internet. These and other communication needs of providers also require the

development of hospital management application software backed by electronic patient record systems. Design of such communication networks will also require the understanding of organizational structure of the clinics involved in the network.

To be effective, a HIS requires a Local Area Network (LAN) and a Hospital Management Software (HMS) which covers the core business of hospital including but not limited to identification, records, medical, labs, pharmacy and stores. We therefore proposed that all the hospitals chosen to constitute the first 60% claim submission target should be configured with a working LAN to facilitate the use of the HMS.

A detailed study about specific hospitals and polyclinics, their locations relative to the nearest access point to existing ICT infrastructure, traffic load and its characteristics, security, LAN/WAN protocol, topology and bandwidth requirements and utilization, allocation of bandwidth etc, have to be considered while trying to design any Hospital Information System.

2.4.1.6.2. PROVIDER LAN DESIGN PRINCIPLES

For the purposes of this report our team believes its best to group the hospitals' LAN solutions into Large, Medium and Small categories. The Large LAN Solution covers the Teaching Hospitals, Regional Hospitals and the Military and Police Hospitals. The Medium LAN Solution covers the General Hospitals, District Hospitals and Polyclinics. The Small LAN Solution should cover all the other providers which do not fall under the other classifications. However, the fundamental principles behind the proposed LAN design are the same irrespective of the hospital's classification.

The proposed LAN will follow the hierarchical structure of the hospital. The decision to make the selection between the various LAN technologies was done based on:

- Expected application to run on the network and their traffic patterns.
- Physical locations of the offices and users to be connected in campus.
- The rate of network growth.
- The abundance of the network technology in the market.
- Simplicity of installation and maintenance.

Principle 1. Expected application to run on the network and their traffic patterns.

Currently we expect a web-based HIS application to run on the network. The application will use a central database server where all the user and patient information will be stored. The type of data to be transmitted on the network shall be in the text and image formats. Since all communication shall be through the server, the traffic pattern around the centre is expected to be heavy. Higher speed devices will be used at the centre of the LAN where there will be servers.

Principle 2. Physical locations of the offices and users to be connected in campus.

As shown in figure 1 above, the Korle Bu hospital has about 15 buildings including the central administration. Though we could not get the exact figure, the 15 buildings are clustered around a square kilometer area. Most of the buildings have their own set of

switches and routers with access to the Internet. Having routers switches in each of the departments is ideal to design a high speed and expandable LAN, but makes it expensive. A cost effective choice is to put switches per building and then have the departments be connected and form groups by using Virtual LAN technology.

Principle 3. The rate of network growth.

The rate of the hospital LAN growth depends on the level of computerization in the hospital. Currently in the hospitals, there are LANs that connects few offices and a computer room. The network uses star topology, using a centrally located hub and Unshielded Twisted Pair (UTP) cables forming a peer-to-peer LAN. The purpose of this LAN in most cases is to provide access to the Internet to hospital staff. A further usage we have identified is the Hospital Management System (HMS) usually limited to records, pharmacy and stores. However in designing the proposed solution it is necessary to consider future usage of the network. The future use of the LANs may include but not limited to following; telemedicine, VoIP and video conferencing. The switches/routers selected in this design should have many free ports to help cascade the growing number of connections in the future.

Principle 4. The abundance of the network technology in the market.

Our proposed design is based on availability of network technology in our local market. Currently, Ethernet technology is common in most organizations that implement computer networks in Ghana and it is also the most likely technology used currently. Also, the use of fiber optics for backbone is identified as most reliable and durable.

Our proposed topology is extended star topology that uses standard UTP cables for within building cabling and extends fiber optic cables for vertical cabling (backbone cabling) between buildings that belong to the various departments. Where an aggregation link is required to connect one part of the building to another, we proposed a fiber cable to be used. Such horizontal backbone cabling provides interconnection between wiring closets and Point of Present (POPs). The zones that fall within area of department were served by internetworking devices such as switches and UTP cables. Wireless LAN is considered in the design to cover areas were the laying of cables will not feasible.

It was also identified that, since such networks dominate the Ghanaian network market, network technology devices and support can be found from limited number of vendors.

Principle 5. Security

Network is designed with standards that ensure confidentiality and security of data as a high priority. Since this network is going to be used to transmit sensitive patient information, security is paramount in the proposed solution.

Principle 6. Convergence Solution

Networks should be designed to support converged services while accommodating traditional data, voice, and video services and to be “application aware” in the delivery of business-critical application systems.

Principle 7. Simplicity of installation and maintenance.

To design the LAN architecture we have selected the hierarchical model. It enables us to design and arrange the inter-network devise in layers. It is a model preferred by most of network design experts for its ease of understanding, expandability and improved fault isolation characteristics. The model required the following three layers

- ***Layer One (Core Layer)***

Core layer high performance switches that are capable of switching packets as fast as possible should be deployed. This layer connects the LAN backbone media. It also connects to the outside world to WAN via a firewall. In this design the devices in the core layer will be placed at a central location in the hospital. The devices in this layer will be connected with high-speed cables such as fiber optics, or fast Ethernet cables. The servers will be connected to switches in this layer shielded by a firewall.

Our team recommends the DGS-3627G xStack Managed 24-Port Gigabit SFP Stackable L3 Switch, 4 Combo 1000Base-T Ports, 3 10GE Slots, IPv6 switch for the core layer of the large regional and teaching hospitals. An all fiber port switch will connect the various buildings to a central location. This switch or its equivalent must have Layer 3 capabilities for routing between the VLANs. This will be most suitable for providers with more than 12 buildings that need to be connected. Currently the Korle Bu and Tamale buildings will be the most appropriate.

- ***The second layer (Distribution Layer)***

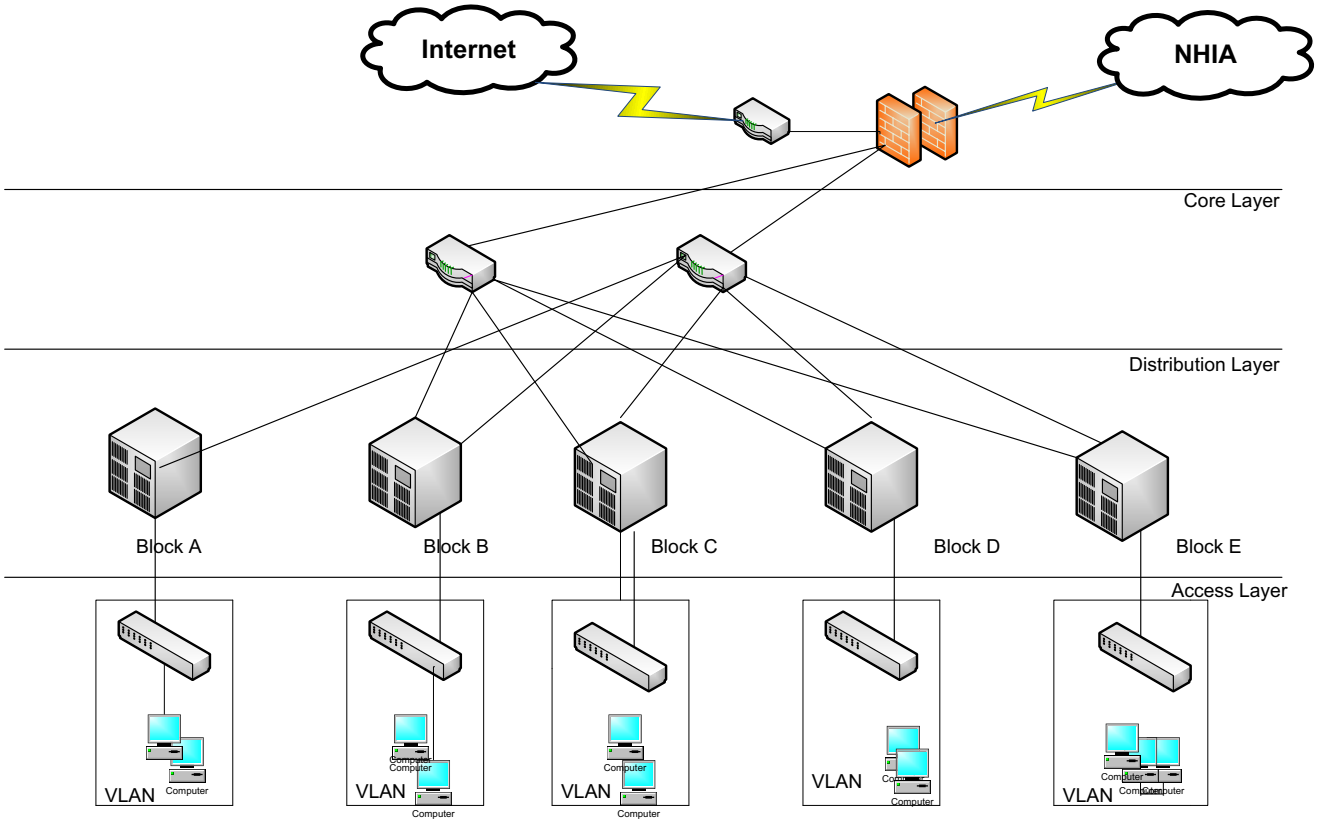
Distribution layer will contain switches and routers capable of VLAN switching and allow defining departmental workgroups and multicast domains. The devices should also support connectivity of different LAN technologies since they also serve as the demarcation point between the backbone connections in the core layer and the access layer. In this hospital LAN design the distribution layer represents switches/routers at each building connected to the core layer on the one end and to the access layer on the other end. Use of redundant links will be used for maximum availability. The departments could be grouped forming their own Virtual LAN.

Our team recommends the DLink DGS-3426P Managed 24-Port Gigabit L2 PoE Switch, 4 Combo SFP, 2 10-Gig Slots for the distribution layer switches. This switch or its equivalent must have at least 2 combo SFP slots for the fiber uplink to the core switches. In small to medium providers this switch could be appropriate as core switches. As stated earlier, the smaller the broadcast domain the better, therefore were necessary a building may be divided into several VLANs. In which case a Layer 3 switch may be required for routing between the VLANs.

- ***The third layer (Access Layer)***

Access Layer is where the end users are allowed in to the network. This layer contains switches from which workstations in each department get access to the Hospital LAN. The

number of switches per department depends on the number of terminals, which in turn will have redundant links to more than two of the switches in the distribution layer.



2.4.1.6.3. STRUCTURED CABLING SYSTEMS

Cabling installations for new buildings, major cable plant additions or modifications, building renovations or remodeling, shall meet all minimum requirements and mandatory criteria addressed in Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) Commercial Building Telecommunications Standards 568, 569, 606, 607, and applicable electrical codes.

- Cabling installations must comply with Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) Commercial Building Telecommunications Standards 568, 569, 606, 607, and applicable electrical codes.
- Cabling categories before 5e do not provide the convergence principle required in the network design and should not be used for any new installation.
- The management of telecommunication infrastructure should comply with the TIA/EIA 606 standard.
- TIA/EIA 607 standard provides grounding and bonding requirements for telecommunications circuits and equipment.
- UTP shall be used unless specific issues exist, such as high EMI or long transport distances.

2.4.1.6.4. COPPER NETWORK CABLING

Structured Cabling System installations for new and/or renovated buildings without cabling shall be Category 6 Unshielded Twisted Pair (UTP) as specified by TIA/EIA 568-B.2.1 Commercial Building Telecommunications Cabling Standards.

- UTP shall be used unless specific issues exist, such as high EMI or long transport distances.
- Category 6 cabling is certified to carry up to 10 Gbps of data up to 100 meters. The cabling industry, TIA, and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) support Category 6 cabling or better as the optimal choice to develop the Institute of Electrical and Electronics Engineers (IEEE) 10 Gbps Ethernet standard based on the rapid growth of Category 6 cabling installations in the marketplace.
- Category 5e cabling is acceptable when incremental additions to existing Category 5e cabling for major cable plant modifications and/or additions due to building renovations or remodeling are necessary.
- Category 6 link and channel requirements are backward compatible to Category 5e.
- Category 6 cabling, and existing Category 5e cabling, installed per TIA 568-B.2.1 standards, to the desktop allow most IP platform devices requiring power to operate without supplemental AC power in accordance with IEEE 802.3af Power over Ethernet (PoE) requirements.
- Category 5e patch cables used to connect platform client devices to Category 6 Structured Cabling Systems where throughput performance is constrained by the platform client device interface are acceptable.

2.4.1.6.5. FIBER NETWORK CABLING

Structured Cabling System installations for new buildings, major cable plant additions or modifications, building renovations or remodeling shall be either multi-mode or single-mode, depending on business unit requirements, as specified by TIA/EIA 568-B.3 and ISO/IEC 11801:2002 Commercial Building Telecommunications Cabling Standards.

- TIA/EIA-568-B series standards specify 50/125 micron multi-mode fiber for horizontal subsystems. 50/125 micron multi-mode or single-mode (8/125 micron) fiber is specified for vertical subsystems.
    - Multi-mode fiber transmits up to 10 Gbps Ethernet a distance of approximately 35 meters to 300 meters (50/125 micron), depending on the specific fiber and the Ethernet port characteristics. Single-mode (8/125 micron) transmits up to 10 Gbps Ethernet a distance of 2, 10, and 40 kilometers, depending upon specifications.
    - Single-mode fiber network cabling subsystems between buildings allow up to 10-Gbps Ethernet transmission rates over greater distances, as specified by the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) Series G.652 and ISO/IEC 60793 standards.

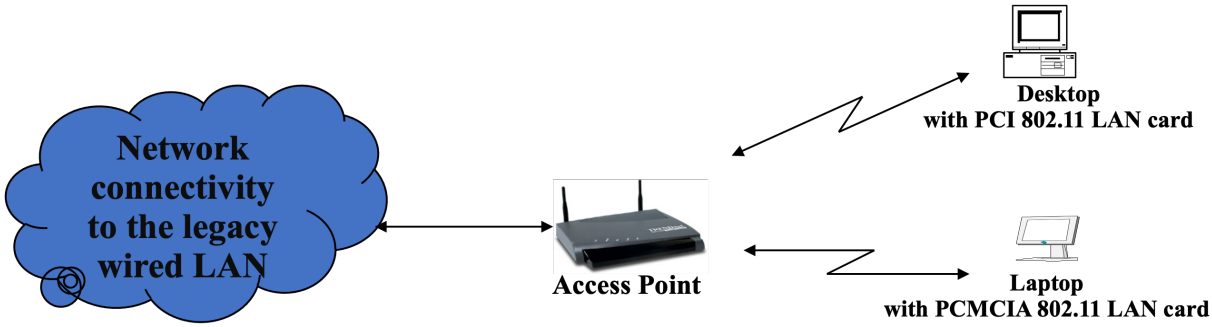
2.4.1.6.6. NETWORK LINK LAYER ACCESS PROTOCOL

Shall be Ethernet, IEEE 802.3, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method.

- Ethernet is scalable, with current versions able to manage the increase of data flow and provide the bandwidth and “end-to-end” Quality of Service (QoS) necessary to support the requirements of multimedia and converged voice, data, and video applications.
- The IEEE 802.3 Ethernet standards provide 10 / 100 / 1000 (1 Gbps)/10,000 (10 Gbps) Mbps operation progressively providing higher bandwidth and improved performance.
- The IEEE 802.3 standards provide an upgrade path resulting in a consistent management model across all operating speeds.
- Full-duplex mode of Ethernet allows a simultaneous flow of network traffic from one workstation to another without collision issues.
- The IEEE 802.3af PoE standard allows most IP platform devices requiring power to operate without supplemental AC power.
- Network design, installation, and maintenance costs are minimized by preserving network architecture, management, software, and structured network cabling.

2.4.1.6.7. WIRELESS LOCAL AREA NETWORK (WLAN)

The demand for WLAN as an alternative to ubiquitous wired-LAN connectivity has been on the increase over the last few years. The design of a wireless LANs should primarily ensure security, convenience, cost efficiency, and ease of integration with other networks and network components.



In 1997 the IEEE adopted IEEE Std. 802.11-1997, the first wireless LAN (WLAN) standard. This standard defines the media access control (MAC) and physical (PHY) layers for a LAN with wireless connectivity. It addresses local area networking where the connected devices communicate over the air to other devices that are within close proximity to each other.

2.4.1.6.8. THE IEEE 802.11 WIRELESS LAN ARCHITECTURE

The 802.11 architecture is comprised of several components and services that interact to provide station mobility transparent to the higher layers of the network stack.

Wireless LAN Station

The station (STA) is the most basic component of the wireless network. A station is any device that contains the functionality of the 802.11 protocol, that being MAC, PHY, and a connection to the wireless media. Typically the 802.11 functions are implemented in the hardware and software of a network interface card (NIC).

A station could be a laptop PC, handheld device, or an Access Point. Stations may be mobile, portable, or stationary and all stations support the 802.11 station services of authentication, de-authentication, privacy, and data delivery.

Basic Service Set (BSS)

802.11 defines the Basic Service Set (BSS) as the basic building block of an 802.11 wireless LAN. The BSS consists of a group of any number of stations. The BSS is not a very interesting topic until we take the topology of the WLAN into consideration.

The standard is similar in most respects to the IEEE 802.3 Ethernet standard. Specifically, the 802.11 standard addresses:

- Functions required for an 802.11 compliant device to operate either in a peer-to-peer fashion or integrated with an existing wired LAN
- Operation of the 802.11 device within possibly overlapping 802.11 wireless LANs and the mobility of this device between multiple wireless LANs
- MAC level access control and data delivery services to allow upper layers of the 802.11 network
- Several physical layer signaling techniques and interfaces
- Privacy and security of user data being transferred over the wireless media

2.4.1.6.9. WIRELESS LAN RECOMMENDATIONS

Implement a layered approach to wireless security.

- Security is being addressed in the transmission layer with the IEEE 802.11i standard and at the IP applications layer with standards- and policy-based authentication and access control. The Wired Equivalent Privacy (WEP) algorithm, which is part of the 802.11x standard, is susceptible to compromise; therefore, improved security methods should be considered. The WiFi Protected Access (WPA) standard and Protected Extensible Authentication Protocol (PEAP) with the IEEE 802.1x Network Port Authentication standard provides interim, improved security until approval and widespread adoption of 802.11i. In addition, vendor-specific, proprietary, security solutions may provide more enhanced interim security prior to approval and widespread adoption of 802.11i.
- Change the default Enterprise Service Set Identifier (ESSID) on wireless access points.
- Filter based on Media Access Control (MAC) address of the client.
- Firewall technologies must be implemented at connection points between wireless and wire-based LANs additionally to reduce unauthorized access to internal networks.
- Require user authentication and authorization in order to gain access to the wireless network.
- Utilize Virtual Private Networking (VPN) where strong security is required.
- Provide application level security such as application authentication and authorization as well as SSL.

Develop a shared key distribution process prior to implementation.

- The Wired Equivalent Privacy (WEP) standard uses a shared key system. The WEP standard does not, however, include a process for distributing pass-phrases, hex keys, or ASCII strings that represent a wireless encryption key. Therefore, a secure process for the distribution and maintenance of shared keys must be developed in advance of implementation in order to ensure the security of the data.

SNMP must be disabled on wireless networking and communications devices unless explicitly required.

- SNMP vulnerabilities may cause denial-of-service conditions, service interruptions, and in some cases may allow an attacker to gain access to the affected device.

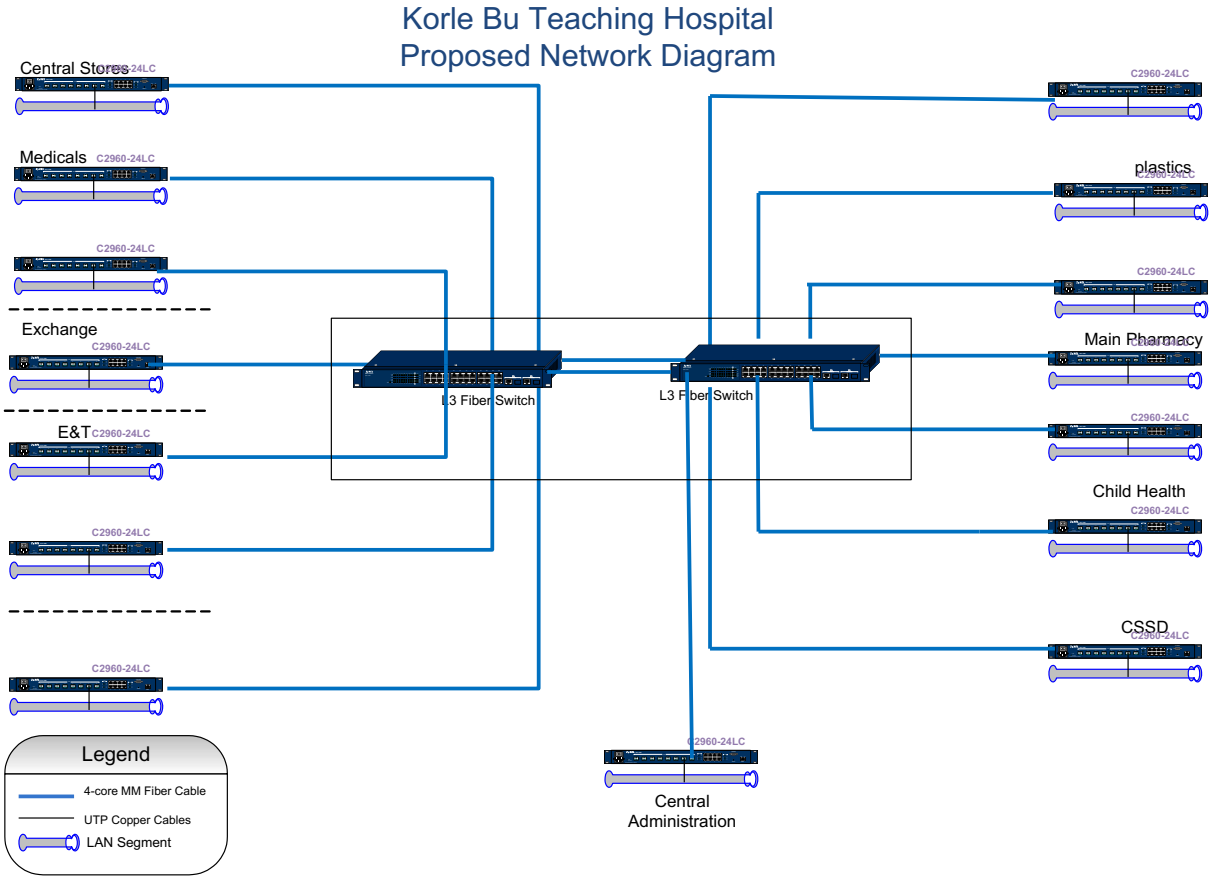
General Wireless Standard Considerations

- Mobile IP provides an efficient and scalable mechanism to allow users to seamlessly roam among wireless networks. Using Mobile IP in applications such as VoIP, media streaming, and virtual private networking can be supported without service interruption when users move across network boundaries.
- Wireless Profiled TCP (WP-TCP) provides connection oriented services for developing applications that operate over wireless communication networks via the Wireless Application Protocol (WAP). Wireless Profiled TCP is optimized for wireless environments due to the emergence of high-speed wireless networks (e.g., 2.5G and 3G) and provides for large data transfers, end-to-end security (using TLS) and convergence with IETF protocols.
- The IEEE 802.11x standards form a family of specifications that define how WLAN equipment should be produced so equipment from different manufacturers can work together.
- The IEEE 802.11b and .11g standards operate in the unlicensed radio 2.4 GHz frequency band and provide up to 11 Mbps and 54 Mbps transmission speeds, respectively, for wireless connectivity.
- The IEEE 802.11g is backwards compatible with .11b allowing .11g and .11b devices to coexist in the same network (.11g devices' performance declines based on distance and number of wireless devices).
- The IEEE 802.11f Inter Access Point Protocol ensures interoperability between access points from multiple manufacturers.
- The IEEE 802.15.3 standard is designed for short-range (up to 50 m), very-low-power operation from 11 to 55 Mbps. The standard will provide quality of service, connection management, and advanced power management modes. The IEEE 802.15.2 standard addresses coexistence between WLANs and WPANs operating in the 2.4 GHz frequency band.
- The IEEE 802.16x standards address the "first mile/last mile" connection broadband wireless access for Metropolitan Area Networks, providing up to 155 Mbps transmission speeds. These standards provide for interoperability and coexistence of fixed broadband wireless access systems from multiple manufacturers in both licensed and unlicensed frequency bands. The IEEE 802.16x standards provide for quality of service to support the needs of different applications. IEEE 802.16 WMAN can coexist with IEEE 802.11x WLAN to provide a viable, last-mile, backhaul solution.
- The IEEE 802.17x standards address the Resilient Packet Ring which can handle multiple gigabit transmission speeds in opposite directions. This dual ring technology can be used in MAN and WAN networks.

2.4.1.7. LAN RECOMMENDATIONS

2.4.1.7.1. PROPOSED LAN SOLUTION – BACKBONE NETWORK

Below is a typical network diagram for a large provider network backbone. Using Korle Bu as an example, a large provider with multiple buildings will require a fiber connectivity between the buildings at the distribution layer. Every building will be equipped with a fiber enable switch which will provide connectivity between the buildings through a core layer. A pair of layer 3 switches will be used to provide routing between the VLANs.



Hospitals	Cabling	Switches	Remarks
Korle Bu	As stated earlier the Korle Bu Teaching Hospital has most of its building cabled for Local Area Network. For Hierarchical Campus Network, each building should be configured as a VLAN. A 4 core fiber cable should be used for the backbone cabling. Certain connectivity will require 8 core cabling a further assessment of the hospital would be necessary to determine the exact cabling method.	An additional managed gigabit switch with a fiber port per building is the minimum requirement. 15 gigabit switches with a fiber port. An additional pair of Layer 3 switches will be needed at the central site (i.e. surgery building).	The four core fiber cable shall be used for link redundancy.
Komfo Anokye	Komfo Anokye is almost fully networked with a fiber backbone. It requires about 100m fiber cable to complete. However, it is a flat network with all the switches on one single IP subnet. Reconfigure network to include a VLAN for each department.	A pair of layer 3 switches should be installed to provide routing between the proposed VLANs. Alternatively, a pair of routers configured with appropriate routing protocol will provide the required routing.	Ensure that existing switches are of good quality. The four core fiber cable shall be used for link redundancy.
Tamale Teaching Hospital	There is no networking at Tamale Teaching Hospital. A total of 700m of cat 6 UTP cable and 450m of fiber core 4 network the hospital.	A pair of layer 3 switches (core layer) should be installed to provide routing between proposed VLANs. 6 additional 24 (distribution layer) port managed switches with a fiber port to connect the buildings to the central tower. An additional 8 24 ports access layer switches will be distributed across the building for data connectivity.	A further assessment may be required before implementation. This should be considered for similar implementation at larger District and similar regional hospitals.
37 Military Hospital	The 37 Military Hospital is fully networked with a fiber backbone. However,	A pair of layer 3 switches should be installed to provide	The proposed solution shown in figure 6 below will provide

	it is a flat network with all the switches on one single IP subnet. Reconfigure network to include a VLAN for each department.	routing between the proposed VLANs. Alternatively, a pair of routers configured with appropriate routing protocol will provide the required routing.	faster uplink and redundant link for the distribution and core layers. All security and packet filtering will be done at the distribution layer.
Sunyani Regional Hospital	The Sunyani Regional hospital is fully networked with a fiber backbone. However, it is a flat network with all the switches on one single IP subnet. Reconfigure network to include a VLAN for each department.	A pair of layer 3 switches should be installed to provide routing between the proposed VLANs. Alternatively, a pair of routers configured with appropriate routing protocol will provide the required routing	
Ho Regional Hospital	The Ho Regional hospital is fully networked with a fiber backbone. However, it is a flat network with all the switches on one single IP subnet. Reconfigure network to include a VLAN for each department.	A pair of layer 3 switches should be installed to provide routing between the proposed VLANs. Alternatively, a pair of routers configured with appropriate routing protocol will provide the required routing	Flat networks have a single but large broadcast domain which usually slows down the network. It is therefore necessary to divide it into VLANs.
Koforidua Regional Hospital	The Koforidua Regional hospital is fully networked with a fiber backbone. However, it is a flat network with all the switches on one single IP subnet. Reconfigure network to include a VLAN for each department.	A pair of layer 3 switches should be installed to provide routing between the proposed VLANs. Alternatively, a pair of routers configured with appropriate routing protocol will provide the required routing	Flat networks have a single but large broadcast domain which usually slows down the network. It is therefore necessary to divide it into VLANs.

Backbone Equipment List

Hospitals	Cabling	Router	Switches	Remarks
Korle Bu	5km of fiber optic 4 core cable.	1 router (3 Fast Ethernet ports) 1 Application Layer Firewall.	16 Gigabit Fiber Optic port Switches 24 port Fiber Switch	The four core fiber cable shall be used for link redundancy. +/- 10% on the cable
Komfo Anokye	200m fiber optic 4 core cable	1 router (3 fast Ethernet ports) 1 application layer firewall.	5 Gigabit fiber switches	Ensure that existing switches are of good quality. The four core fiber cable shall be used for link redundancy.
Tamale	450m fiber optic 4 core cable	1 router (3 fast ethernet ports) 1 application layer firewall	2 layer 3 fiber port switches, 6 switches for the distribution layer 8 24 port switches for the access layer	This is an approximate network requirement for hospitals of similar sizes.
37 Military Hospital	Already installed fiber cable is 4 years old. May require change of cable.	1 router (3 fast Ethernet ports) 1 application layer firewall		The total equipment list according to the proposed diagram may be required.
Police Hospital	150m fiber optic core cable required.	1 router (3 fast Ethernet ports) 1 application layer firewall	2 Gigabit fiber switches	Most part of the building is connected and may require only 150m of fiber to connect the main hospital with the annex building.
Sunyani Regional Hospital	Fully networked.	1 router (3 fast Ethernet ports) 1 application layer firewall	A pair of layer 3 switches for routing between VLANs	
Ho Regional Hospital	Fully networked.	1 router (3 fast ethernet port) 1 application layer firewall	A pair of layer 3 switches for routing between VLANs	
Koforidua Regional	Fully networked.	1 router (3 fast ethernet port)	A pair of layer 3 switches for	

Hospital		1 application layer firewall	routing between VLANs	
Efia Nkwanta Regional Hospital	450m fiber 4 core cable	1 router (3 fast ethernet ports) 1 application layer firewall	2 layer 3 fiber port switches, 6 switches for the distribution layer 8 24 port switches for the access layer	This is an approximate network requirement for hospitals of similar sizes.
Ridge General Hospital (Greater Accra Regional Hospital)	450m fiber optic 4 core cable	1 router (3 fast ethernet ports) 1 application layer firewall	2 layer 3 fiber port switches, 6 switches for the distribution layer 8 24 port switches for the access layer	This is an approximate network requirement for hospitals of similar sizes.

Price of 4-core Loose Tube Fiber Cable [62.5/125 (OM1) & 50/125 (OM2)] is $3.00 per meter

2.4.1.7.2. RECOMMENDED NETWORK SWITCHES

Access Layer Switch

D-LINK WEB SMART DES-1228

Summary

D-Link is an industry pioneer, market leader, designer and true manufacturer of networking communications and digital home electronic products. Excellence in manufacturing, innovation and a commitment to quality has allowed D-Link to produce cutting-edge, high-performance products within standard-based technologies. The company continues to offer the best value in the connectivity market today by combining high-quality products with the most affordable price point. PRODUCT FEATURES: 4 Gigabit Uplinks; Versatile SmartConsole Web-Based Management; VLAN Traffic Segmentation & Priority Queue QoS; Network Access Security; Built-in SNMP MIB-II.

Features

- **Product Description:** D-Link Web Smart DES-1228, switch, 24 ports
- **Device Type:** Switch
- **Form Factor:** External, 1U
- **Dimensions (WxDxH):** 17.3 in x 5.5 in x 1.7 in
- **Weight:** 4.6 lbs
- **Ports Qty:** 24 x Ethernet 10Base-T, Ethernet 100Base-TX
- **Data Transfer Rate:** 100 Mbps
- **Data Link Protocol:** Ethernet, Fast Ethernet
- **Auxiliary Network Ports:** 2x1000Base-T/SFP (mini-GBIC)(uplink),2x1000Base-T(uplink)

- **Remote Management Protocol:** SNMP 1, Telnet, HTTP
- **Features:** Flow control, full duplex capability, layer 2 switching, auto-sensing per device, DHCP support, auto-negotiation, VLAN support, IGMP snooping, port mirroring, store and forward, MAC address filtering, Broadcast Storm Control
- **Compliant Standards:** IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.1x

Price per Unit: $250.00

DISTRIBUTION LAYER SWITCH

Depending on the number of devices connecting at the access layer, the access layer switch can also act as a distribution layer switch as well. Where there are more than 4 24 port access layer switches in the same building a distribution layer switch with high speed gigabit ports may be preferred.

Summary

Cisco Catalyst Express 500 Series switches deliver best-in-class networking that is designed to meet the needs of growing businesses with up to 250 employees. This family of Layer 2-managed Fast Ethernet and Gigabit Ethernet switches offers non-blocking, wire-speed performance and provides a secure network foundation optimized for data, wireless, and IP Communications. The Cisco Catalyst Express 500 also offers options for Power over Ethernet (PoE) to help reduce the cost and complexity of IP Communications and enable new uses for the Ethernet network.

Features

- **Type:** Switch
- **Form Factor:** External
- **Max Data Transfer Rate:** 1 Gbps

- **Ports**: 12 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
- **Slots**: 4 x shared SFP (mini-GBIC)

Price per Unit: $1200.00

CORE LAYER SWITCH
Cisco Catalyst 3750 Metro Switch

Summary

The switches feature hierarchical quality of service (QoS) and traffic shaping, intelligent 802.1Q tunneling, virtual LAN (VLAN) translation, Multiprotocol Label Switching (MPLS) and Ethernet over MPLS (EoMPLS) support, and redundant AC or DC power. They are ideal for service providers seeking to deliver profitable business services, such as Layer 2, Layer 3, and MPLS VPNs, in several bandwidths and with different service-level agreements (SLAs). With flexible software options, the Cisco Catalyst 3750 Metro Series offers providers a cost-effective path for meeting current and future service requirements from enterprises and commercial businesses. As an addition to Cisco's metro Ethernet access switching portfolio the Cisco Catalyst 3750 Metro Series provides enhanced QoS, broader Layer 2 and Layer 3 VPN offerings, and power redundancy for carrier-class metro Ethernet services with service-quality guarantees. By using Cisco Catalyst 3750 Metro Series switches for metro access along with Cisco Catalyst 6500 and 4500 series switches and Cisco 7600 Series routers in the aggregation/core layers, service providers are able to build a flexible, integrated network with intelligence from end to end.

Features

- **Product Description:** Cisco Catalyst 3750 Metro, switch, 24 ports
- **Device Type:** Switch, stackable
- **Form Factor:** Rack-mountable, 1U
- **Dimensions (WxDxH):** 17.5 in x 14.7 in x 1.7 in
- **Weight:** 12.1 lbs
- **RAM:** 128 MB
- **Flash Memory:** 32 MB
- **Ports Qty:** 24 x Ethernet 10Base-T, Ethernet 100Base-TX
- **Data Transfer Rate:** 100 Mbps
- **Data Link Protocol:** Ethernet, Fast Ethernet

- **Empty Slots:** 4 x SFP (mini-GBIC)
- **Remote Management Protocol:** SNMP 1, SNMP 2, RMON, Telnet, SNMP 3
- **Features:** Layer 3 switching, layer 2 switching, DHCP support, VPN support, trunking, MPLS support, VLAN support, IGMP snooping, traffic shaping, dynamic DNS server, manageable, stackable, IPv6 support
- **Compliant Standards:** IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s

Price per Unit: $4000

RECOMMENDED APPLICATION LAYER FIREWALL

A firewall is required for the connectivity to the NHIA WAN. This will shield the NHIA infrastructure from any locally compromised security at the provider site. For the large Provider sites, the core switches will be connected to the firewall for both access to the Internet and the NHIA WAN.

At minimum, the firewall must have 3 ports for the proposed architecture. The firewall policy should only allow the application server from the provider site to access the NHIA Data Centre. Specific application ports should be considered for access further restricting any unauthorized access.

FOR LARGE PROVIDERS

The Cisco ASA 5510

Summary

The Cisco ASA 5510 Adaptive Security Appliance delivers a wealth of advanced security and networking services for small-to-medium businesses and enterprise remote/branch offices in an easy-to-deploy, cost-effective appliance. These services can be easily managed and monitored by the integrated, Web-based management application, Cisco Adaptive Security Device Manager, thus reducing the overall deployment and operations costs associated with providing this high level of security. The Cisco ASA 5510 Adaptive Security Appliance provides high performance firewall and VPN services, three integrated 10/100 Fast Ethernet interfaces, and optional high-performance intrusion prevention and anti-x services via a Security Services Module making it an excellent choice for businesses requiring a cost-effective, extensible, DMZ-enabled security solution.

Features

- **Type:** VPN/Firewall
- **Form Factor:** Rack mountable, 1U
- **Connectivity Technology:** Wired
- **Data Transfer Rate:** 10Mbps Ethernet, 100Mbps Fast Ethernet
- **Features:** Firewall protection, VPN support, VLAN support
- **Warranty:** 90 Days Limited

Unit Price: $2000

FOR SMALL/MEDIUM PROVIDERS

Summary

Cisco ASA 5500 Series adaptive security appliances are purpose built solutions that combine best of breed security and VPN services with the innovative Cisco Adaptive Identification and Mitigation (AIM) architecture. Designed as a core component of the Cisco Self Defending Network, the Cisco ASA 5505 50 User Firewall Edition Bundle provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network security appliance family that provides the security breadth and depth for protecting home office, branch office, small and medium-sized business, and enterprise networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.

Features

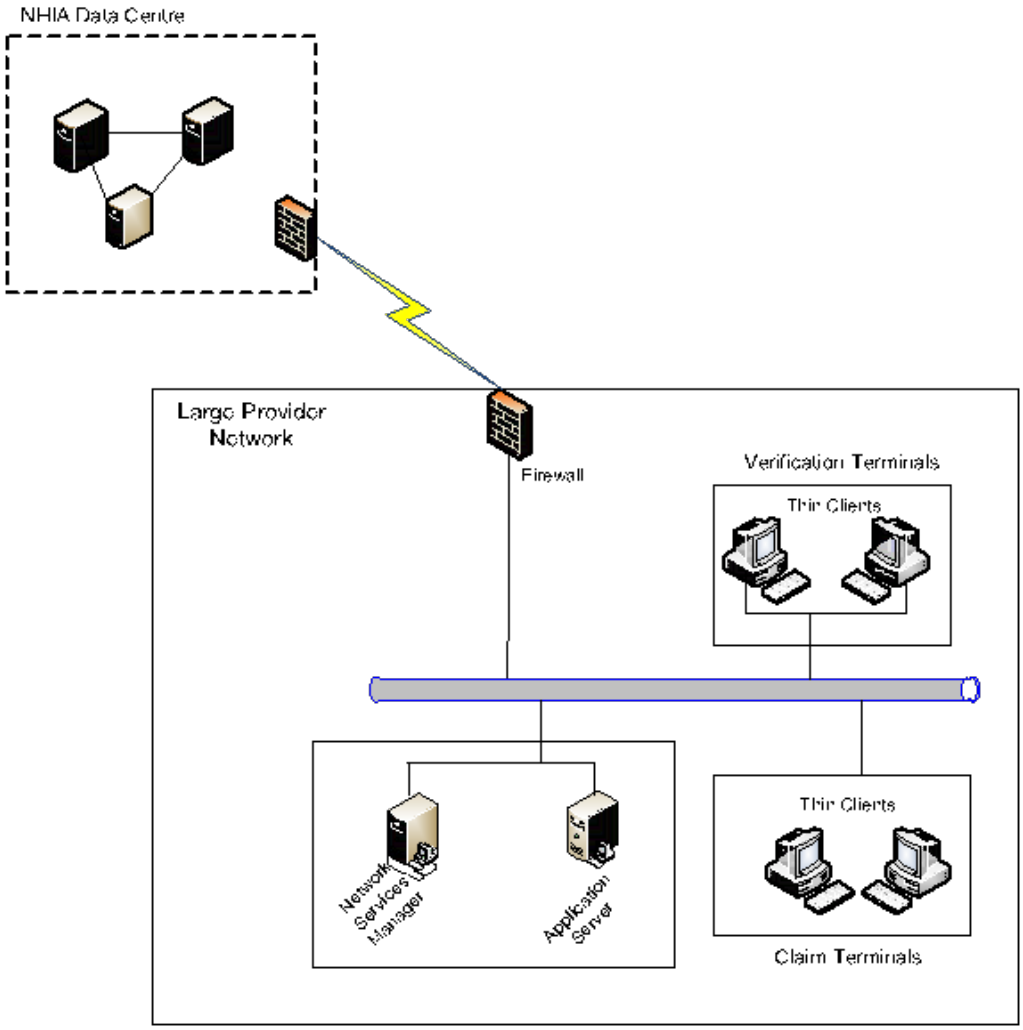
- **Device Type:** Security Appliance
- **Enclosure Type:** External
- **License Qty:** 50 users
- **RAM:** 256 MB

- **Flash Memory:** 64 MB
- **Data Link Protocol:** Ethernet, Fast Ethernet
- **Network Protocol:** IPSec
- **Weight:** 4 lbs

Unit Price: $500.00

LOCAL AREA NETWORK SERVICES

IT departments spend a lot of valuable time on their employees' computers and the providers are no exception. Fixing computer hardware, installing updates and patches, keeping everything current and running correctly requires a lot of IT budget which is not readily available in most of the hospitals. We therefore proposed a thin client solution for the provider sites. This will cover the verification and claim systems.



LAN EQUIPMENT LIST

Hospitals	Servers	Thin Clients	Remarks
Korle Bu	2	30	Teaching and Regional Hospital should be given 2 Servers. Separating the application server from the thin client management server.
Komfo Anokye	2	25	
Tamale	2	20	
37 Military Hospital	2	20	
Police Hospital	1	15	
Sunyani Regional Hospital	2	18	
Ho Regional Hospital	2	18	
Efia Nkwanta Regional Hospital	2	20	
Ridge Hospital	2	20	

2.4.1.7.3. RECOMMENDED LAN EQUIPMENT

Benefits of Thin Client Technology

The Thin Client solution offers several key benefits:

Easily Managed Infrastructure

- **Easily deployed** – New applications, patches and upgrades are easily deployed at the server level. Speed, stability and security are all easily maintained.
- **Easily managed** – This architecture is purpose built to provide a greater centralized management function than possible with a PC-based deployed infrastructure. By moving management to the data center, standardized management processes may be applied to applications and data at a single centralized location instead of individual workstations.
- **Easily controlled** – The Thin Client Management Services solution provides flexibility of management, instant load balancing and real-time failover, and rapid recovery for most types of applications – performance that has never been possible using PC devices at the desktop.
- **Reduced complexity** – The solution centralizes the application so that a common image across all users of similar profiles is enforced. Different users may require different features, and this is easily managed centrally.
- **Optimized to preserve bandwidth –** Mouse movements, keystrokes and screen updates are not transmitted back to the remote server resulting in optimization of bandwidth.
- **Improved scalability** – Thin Client Management Services adopters enjoy quicker deployments of new applications without need for engineering and regression testing code for individual end user platforms. Rather, the end user device is simply a protocol layer, abstracted by design within the system. New applications scale easily and require less testing, saving time and money in rolling them out.

Reduced End User Costs

- **Reduced user hardware costs** – Thin client devices cost about one-third of the purchase price of PCs.
- **Reduced overhead cost** – The Thin Client solution uses less power, generates less CO2 and heat, and occupies smaller space footprints than their PC counterparts. This allows facility managers to cut overhead costs and CO2 emissions through the conservation of space and energy.
- **Less hardware support** – Decreased break/fix, service desk and warranty support reduces total operating costs over time.
- **Reduced administrative costs** – Management is carried out almost entirely using remote server-based interfaces.
- **Decreased support and maintenance costs** – Due to the solid state structure of end user thin client devices.

- **Simpler new application deployment** – Changes and installations are required only at the server rather than on each user device.

Reduced Risk/Increased Security

Unlike PCs, thin clients have no local storage. As a result, they are not vulnerable to viruses and other malware as long as the servers are protected. Since there is no way to store and remove proprietary information from thin clients, the data remains safe on the server and compliant with privacy regulations.

HP Thin Client t5540 - FQ799AT

Summary

The HP t5540 Thin Client delivers a great desktop experience for general office applications or your specific line of business software. This unit's enhanced features make it ideal for mainstream business use, with support for legacy ports, ICA, RDP, terminal emulation, Windows Media Player, and basic web browsing. The t5540 is designed for more secure, convenient access to traditional Terminal Services/Citrix solutions, Virtual Desktop Infrastructure (VDI), HP Blade PCs, and HP Blade Workstations.

Features

- **Product Description:** HP Thin Client t5540, Eden 1 GHz
- **Type:** Network computer
- **Form Factor:** Tower
- **Dimensions (WxDxH):** 2 in x 8.5 in x 8.7 in
- **Weight:** 3.3 lbs
- **Localization:** English / United States
- **Processor:** 1 x VIA Eden 1 GHz
- **RAM:** 512 MB DDR SDRAM
- **Flash Memory:** 128 MB

- **Monitor:** None.
- **Graphics Controller:** VIA Chrome9 HC3
- **Audio Output:** Sound card, stereo
- **Networking:** Network adapter, Ethernet, Fast Ethernet, Gigabit Ethernet
- **Power:** AC 120/230 V (50/60 Hz)
- **OS Provided:** Microsoft Windows CE 6.0
- **Manufacturer Selling Program:** HP Smart Buy
- **Manufacturer Warranty:** 3 years warranty

Unit Price: $400.00

HP ProLiantDL360 servers

Summary

Combining concentrated 1U compute power, integrated Lights-Out management, and essential fault tolerance, the DL360 is optimized for space-constrained installations. What's more, the DL360 G5 steps up the fault tolerant in an ultra dense platform with redundant power, redundant fans, mirrored memory or online spare memory, embedded RAID capability, and full-featured remote Lights-Out management.

Features

- **Product Description:** HP ProLiant DL360 G5 Performance, Quad-Core Xeon E5450 3 GHz
- **Type:** Server
- **Form Factor:** Rack-mountable, 1U
- **Dimensions (WxDxH):** 16.8 in x 27.8 in x 1.7 in
- **Weight:** 27.6 lbs
- **Localization:** United States
- **Server Scalability:** 2-way
- **Processor:** 2 x Intel Quad-Core Xeon E5450 / 3 GHz (Quad-Core)
- **Cache Memory:** 24 MB L2 cache
- **Cache Per Processor:** 12 MB (2 x 6MB (6MB per core pair))
- **RAM:** 4 GB (installed) / 32 GB (max), DDR2 SDRAM, Advanced ECC, 667 MHz, PC2-5300

- **Storage Controller:** RAID (Serial ATA-150 / SAS), PCI Express x4 (Smart Array P400i) ; IDE (IDE/ATA)
- **Server Storage Bays:** Hot-swap
- **Hard Drive:** None.
- **Optical Storage:** CD-RW / DVD-ROM combo
- **Monitor:** None.
- **Graphics Controller:** ATI ES1000, 32 MB
- **Networking:** Network adapter, PCI Express x4, Ethernet, Fast Ethernet, Gigabit Ethernet, Ethernet Ports : 2 x Gigabit Ethernet
- **Power:** AC 120/230 V (50/60 Hz)
- **Power Redundancy:** Yes
- **Manufacturer Warranty:** 3 years warranty (on-site)

Unit Price: $4500.00

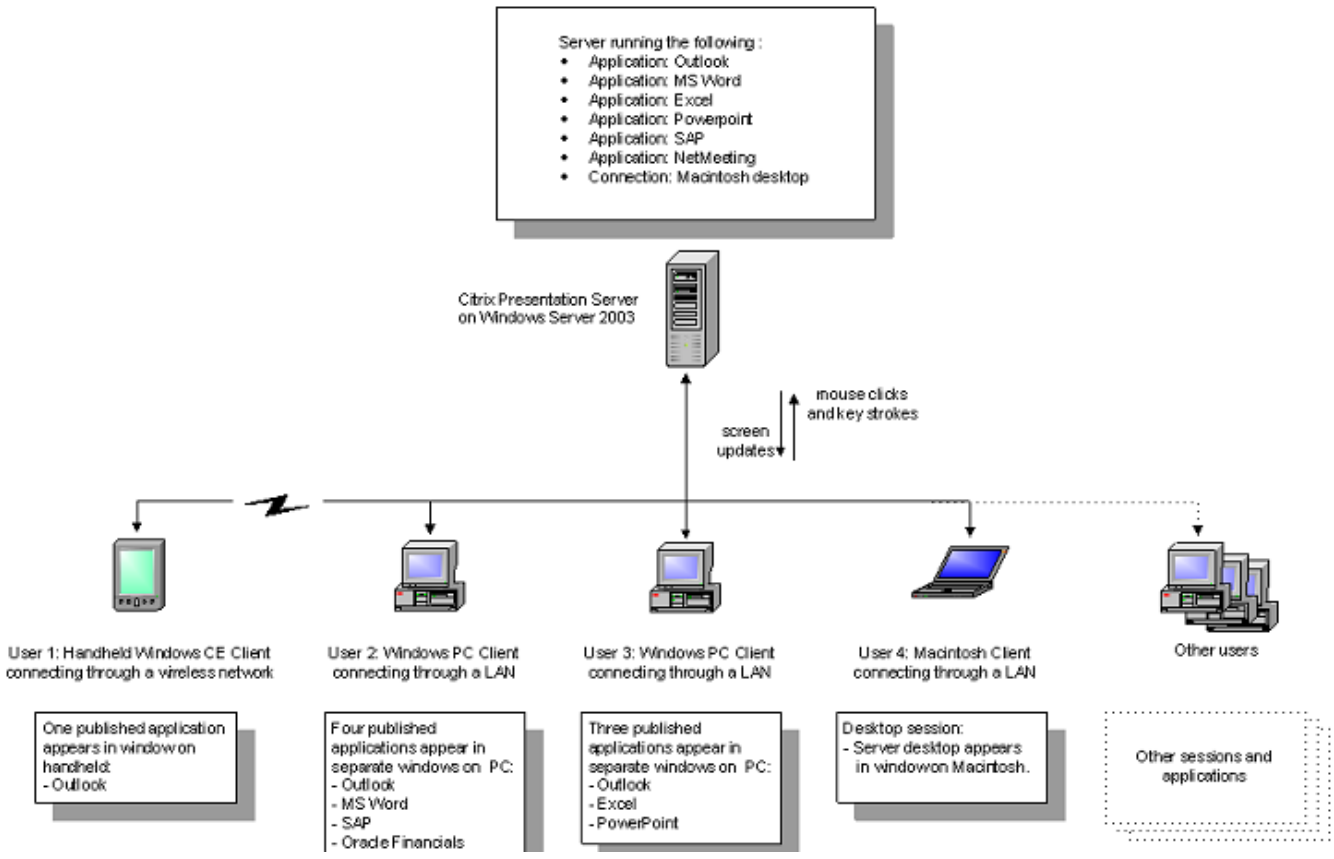
Citrix Presentation Server

Presentation Server allows delivery of applications as a service—providing on-demand access to users, while affording the flexibility to leverage future application architectures.

Citrix Presentation Server is the industry standard for delivering Windows applications at the lowest cost—anywhere. Its application virtualization and application streaming delivery methods enable the best access experience for any user, with any device, working over any network. Presentation Server allows delivery of applications as a service—providing on-demand access to users, while affording the flexibility to leverage future application architectures.

Whether your users rely on Windows or Macintosh PCs or laptops, UNIX or Linux workstations, thin-client devices, Windows-based terminals, wireless devices, or other network appliances, you can use Citrix Presentation Server solutions to:

- Provide tailored secure access control in any access scenario
- Deliver continuous access across devices, networks, and locations
- Provide scalability and continuous availability for any business scenario
- Protect information through a multidimensional secure architecture
- Observe, monitor, and measure access infrastructure resources



2.4.1.8. WAN INFRASTRUCTURE OUTPUTS

A careful study of operations of the Providers provides some assumptions and considerations for WAN system as follows:

1. Bandwidth distributed to each site would not exceed 128Kbps per site, except for large providers like Korle-Bu Teaching Hospital, and 10Mbps aggregate channel capacity to Data Centre. The aggregate channel will be required to accommodate concurrent connections from the various providers. This link capacity would be made scalable to be able to expand with growing capacity demands.
2. Other commercial terrestrial solutions, that are more reliable and with higher availability than VSAT (e.g. fiber optic or regional MW), would be employed. These solutions promise to be much less expensive than VSAT.
3. Sites that are difficult to connect with any terrestrial solution would be connected with VSAT. VSAT to be deployed as last resort.
4. All links will terminate at the Data Centre (proposed to be NHIA-designated location), and Backup data Centre. Connection to the backup data centre could be in two ways; either creates a backup routing system in a backup site, or direct duplicate links to Data Centre to the backup site. The former solution is less expensive, but less efficient, and depending on system availability requirement a decision has to be made to choose one.
5. NHIA central location to be connected via dedicated E1 data circuits. Additional capacity may be required based on estimated usage.
6. Remote agencies offices to be connected via wireless “last mile” technology.
7. Backup Data Centre is proposed to be at different physical location from primary.
8. All the over 700 Sites, and any new sites would be connected, even if in the long term.
9. WAN Security shall be implemented using contemporary solutions available.
10. A VPN node shall be provided at NHIA central location (offices) for Network monitoring and assist in systems audits. This link would have data capacity of 256Kbps minimum (E-1 preferred)
11. WAN usage policy should be adopted to enhance WAN usage and improve connectivity and also optimize the use of WAN resources.
12. Backup Narrowband Network proposed for redundancy of key network sites would be considered.
13. WAN is IP based and uses RJ-45 (Ethernet) interfaces
14. General Practice of 6% of volume of installed equipment should be stocked as spares.

2.4.1.9. PROVIDER HIS TO NHIA SYSTEM INTERFACE

A crucial element in implementing Phase 2 is an interface between Provider HIS systems and the NHIA core claims system. The requirements of this interface are:

- Web based service
- Service Oriented Architecture (SOA) compliant
- Simple Object Access Protocol (SOAP) compliant
- Use Extensive Markup Language (XML) formats for data

- Contain functions and attributes for:
  - Member validation
  - Claims submission
  - Claims rejection
  - Claims re-submission
  - Claims batch status from NHIA system
- Retrieve latest drug, diagnostic and treatment tables from NHIA system
- Be resilient to power failures
- Operate on data connections of 256K or greater
- Auto restart on communications link failure or power outage
- 100% data security
- Be auditable
- Meet Ghana Government Information Framework (eGIF) standard
- Meet Ghana Government Architecture (GA) standard

We believe that the designed interface meets all of these criteria and is implementable within any Provider HIS system in use in Ghana today. Based on meetings with the companies supplying HIS to facilities today we are confident that they can do the needed modifications to use the interface.

The funding for the implementation of the interface is currently shown as a total of US$900,000 spread between GHS, CHAG, Teaching and Military Hospitals. What does not seem to be covered is the funding for changes required to the central NHIA system to incorporate this interface. STL will need to modify their software to do this. A detailed discussion of the financial considerations can be found further in this report.

2.4.1.9.1. HEALTH PROVIDER RECOMMENDATIONS

The prime objective of this study was to determine viable alternatives to the current validation of member status and electronic submission of claims by the Health Provider. While conducting interviews with Providers it became obvious that the current processes and procedures in place at the hospitals was in most cases manual and in addition to the normal processes used by the facility outside of NHIS requirements. Many of these risks are detailed in the previously submitted Gap Analysis Report.

The study team does believe that a possible solution exists that mitigates the identified risks and also serves to improve the health care management in Ghana. At various facilities visited we viewed Hospital Information Systems (HIS) in use. These HIS systems were supplied by various in-country vendors and could provide the necessary interface capabilities needed to transmit claims to the NHIA system electronically.

These systems provide additional value to the Health Center in the management of the facility as well as Electronic Medical Records (EMR) of patients. Where the administration of the facility showed commitment to the implementation and use of these systems the acceptance and use were evident. Some of the facilities are using only portions of the HIS systems but plan of implementing other departments over time.

The departments needed for implementation for use as a solution for the NHIS electronic claims submission method are:

- Patient Registration – Front Desk
- In-patient or Out-patient Care – This can be optional with diagnostic and treatment coding being done by the Billing & Claims departments
- Laboratory – Lab tests
- Pharmacy - Medications
- Billing / Claims

The viewed HIS systems also provided additional services for

- Stores
- Purchasing
- Billing
- Radiology
- Others

We did note that even where these systems are in use many of the old manual processes are still being used in parallel with the HIS systems. This dual process method produces duplication of effort and the human reaction of "why should I do it both ways?" We believe this challenge can be overcome with proper training and follow up.

One other reason for this duplication of electronic and manual systems is the reliability of the HIS systems and their supporting systems. We believe that through proper backup power systems and a workable technical support plan this obstacle can be overcome.

2.4.1.9.2. PROVIDER OFFICE UPGRADES

Many of the facilities visited were not suitable for implementation of HIS systems. Of concern was the condition of the electrical wiring and the lack of clean air conditioned space for server and LAN/WAN equipment. While these concerns will have to be improved before the installation of any HIS systems they are not covered in this study and are not included in any cost analysis.

The majority of the large and medium health facilities were in better condition than the smaller district facilities. The cost of upgrading the larger facilities wiring and air conditioning will be less as a percentage of any HIS implementation than the smaller facilities. Since we believe that the goal of 60% electronic claims can be met with just the larger facilities we do not believe that the costs associated with those facilities improvements will effect implementation.

3. SUITABILITY FOR A PROVIDER IMPLEMENTATION

Our site visits to both Providers and Schemes indicated various reasons for the low usage of the Phase 1 implementation. From the lessons learned from Phase 1 it is clear that the underlying shortfall was in not having a complete implementation plan in place. Many of the problems identified in the Gap Analysis could have been mitigated had such a plan in place that considered all aspects of the project.

We believe that it is possible to reach a significant level of electronic claims submission by the Providers. This will require a well thought out and executed implementation plan that starts at the planning stage and carries through the support of the Providers in the use of the system. As part of this study we have produced a preliminary plan that will lead to success of Phase 2.

The recommended Implementation Plan can be found under Section 4.6 in this report. The critical steps in this plan are:

- Partnering with Providers in getting administrative support.
- Partnering with Provider groups such as GHS and CHAG
- Professional Project Manager full-time during the complete project
- Provider incentives both positive and negative
- On-site training of all involved Provider personnel
- Strong and timely support for all infrastructure and users once installed
- NHIA management of Data Center to control SLAs with Providers

3.1. HIS SOLUTION OPTIONS

We believe that any of the vendor solutions could fulfill the goal of automated member validation and electronic claims submission. Based on interviews with each of the companies we believe that all vendors should be allowed to compete in the free market to supply solutions to the Providers. We therefore have made no one-solution recommendation.
All of the interviewed vendors expressed interest in including an automated ability to verify membership and electronically submit claims. They agree that a Web SOAP XML interface is a good solution for doing this.

We learned during the study that GHS has already made a decision to use the IHost system in its facilities. This however does not prevent other vendors from supplying systems to other Providers in Ghana.

The NHIA has already embarked on a project to implement OCR readable forms as a method of submitting claims. A discussion of this method is also included below as a possible solution for smaller facilities where communications is not available today.

Pertinent marketing materials for each vendor who supplied information is available as separate attachments to this report. The following description of each vendor's system is briefly described.

3.2. EXISTING HIS SYSTEMS IN GHANA

HOSPITAL ADMINISTRATION MANAGEMENT SYSTEMS

Hospital Administration Management Systems (HAMS) is a software system developed by Infotech dot Net Systems Limited in Ghana that is being used by few hospitals. The software was developed in Ghana and is sold as use licenses. Its architecture is client server with the application running on each PC with the database on a dedicated server. It currently is not browser based.

We have viewed a successful implementation at Alpha Hospital, a CHAG facility. In documenting the processes in use at the facility as the patient proceeds through the facility we received positive statements from the personnel involved with the system. In general the usability seems satisfactory and the systems key functions fit the workflow of the facility.

Our team met with the company that has developed the system in Kumasi. From our discussions with the company we were informed that the software is currently being used by 4 regional hospitals and 26 other district and private hospitals in Ghana. The Software is developed in C# on the Microsoft .Net platform.

With the addition of the use of a standard set of interfaces to the NHIA central system this system could be used to automate claims submission. Since its establishment in 2004, InfoTech has developed a number of software solutions for schools, churches and other organizations.

GHS IHOST

IHost is an open source system acquired by GHS for implementation at their facilities. GHS has contracted a local development company to modify the system to meet the needs of their facilities. The system is currently installed at a number of hospitals.

The design of the system is browser based and implementable in phases by enabling its use in specific hospital departments. Its current configuration is more suitable to larger facilities but could be simplified for use at smaller facilities also.

We viewed the system in use and found that it contains all of the functions necessary to generate automated claims. As with HAMS, the implementation of the standard NHIA system interface to be proposed by this study, IHost could automatically verify NHIS membership at the front desk and electronic claims submission at the claims department.

DISTRICT HEALTH INFORMATION SYSTEM (DHIS)

The District Health Information System (DHIS) is currently being used by a number of District and Regional Hospitals to collate statistics about patients for their monthly report. The DHIS is based on Microsoft Access Database with forms for gathering data and reporting features. It is quite easy to use and does have authentication features for confidentiality of information.

HOSPITAL INFORMATION MANAGEMENT SYSTEM (HIMS)

Another Hospital Management System is from an organization called Samtech. The features of Samtech HIMS are very similar to HAMS:

- Client / Server architecture
- Based on Microsoft .Net Platform using Visual Basic
- Covers most Hospital Management Modules – i.e. Records, Clinic, Labs, Pharmacy and Claims

The system seems complete and covers all of the hospital departments. The interface is intuitive and requires basic computer skills to use. During a meeting with the company we discussed the possibility of their incorporating a standard NHIA system interface in order to perform member validation and electronic claims submission. They felt that this could be done. They also expressed a willingness to convert the GUI to a browser based solution.

PROPOSED SCAN ENABLED FORMS

The ability of systems to read hand printed and computer printed text has been available for over a decade. These systems have been used with varying success in capturing data that a human has printed on a form and converting it to electronic data. These systems provide a way to eliminate the manual process of typing in data.

The use of this technology can be implemented in a number of ways for use in capturing Member Registration and Claims. The technology could be implemented at the Provider location, Scheme location or a centralized data capture center administrated by the NHIA.

We understand that preliminary testing of this new method was done and that greater than 90% accuracy was achieved. These levels of results were achieved using human entered data carefully on forms that were clean and not mutilated. The person also filling out the forms was careful in writing the characters in the style required and in the boxes.

This level of clerical accuracy cannot be attained in the facilities we visited. The risks to this becoming successful for the purposed use within the NHIS process are substantial based on observations we have made during the study.

- Conditions of forms at the schemes and providers – Forms are torn, stained, wrinkled and stapled to other documents.
- More manual rewriting of forms – Will require them to write all of the information again (See existing Work Flows).
- More work for scheme or provider – without an identifiable incentive to the scheme or provider the systems use is in question.

In evaluation of this method we believe that there are some of the Phase 1 challenges that will need to be addressed. These are:

- Lack of Provider administration “buy in” causing their lack of commitment to claims administration since there is no incentive to the facility

- Lack of process integration of Phase 1 processes at the Provider operation causing no "buy-in" by the staff, just "more work".
- Card swipe step adds work and is therefore not being used
- Card swipe systems not being used
- VSAT links not operational frequently causing users to discontinue use
- Claim forms add to the manual process requiring another form that must be filled in
- Looking up diagnostic codes and drug codes adds to workload
- Creating batch cover sheets for sending with claims batches creates another manual step.
- Final review of claims before submission to Schemes adds to workload
- Larger facilities cannot identify how to distribute reimbursements to the providing department

It is the opinion of the study team that the implementation of using scanned forms for automated entry of claims data requires further evaluation. We believe that real world testing must be done before implementation of this option be considered as an option. We understand that a pilot project consisting of 10 facilities in the Greater Accra area is planned. Specifically we recommend:

1. A selection of the 10 providers from small, medium and large facilities should be chosen for the pilot.
2. Each of the test provider's administration should select the personnel that they wish to test the process.
3. On-site training of the employees that will perform each of the entry processes should be done prior to the testing phase. The training should be given using the implementation plan developed for the general rollout of the system.
4. The forms should be used through the various stages of the hospital process with the information available at each stage being entered at that stage.
5. A system containing the software that is used to process the scanned forms should be taken to a site other than STL. After training on the use of the system at the work location the trained employee should do the processing of the forms.
6. Technical assistance to the testers should be provided in the same manner as defined in the implementation plan in order to closely as possible simulate the designed support plan.
7. Statistics should be gathered on:
    - the number of technical assistance requests received
    - number of forms requiring manual verification
    - number of forms whose physical condition does not allow scanning
    - total forms processed
    - time to process the forms,
8. Gather comments from provider personnel involved in the testing.

The recommendation of this testing method will duplicate, as closely as possible, the conditions that can be expected if the scanning of forms was put into production and can serve as guidance in changes needed to the implementation plan should the testing prove successful. Using providers in the 3 size categories will serve to evaluate if this method applies to all sizes of providers or would be useful only within certain size organizations.

The use of this method of data capture should also be evaluated against the Provider based HIS systems identified as part of the study.

INTERIM SOLUTION FOR SMALL PROVIDERS

Not all healthcare facilities are suitable for a full HIS system. Some of the facilities are small with no space to locate computer equipment and lack suitable facility infrastructure to support systems. In these cases we are recommending that either the facility submit forms manually for entry by a regional or central NHIA claims center or the use of ICR/OCR scanable forms.

As the Government improves the existing hospital infrastructure these smaller facilities can benefit from HIS system implementations. The added value of electronic patients records and inventory control are that serve to increase the quality of patient care as well as reduce costs.

3.3. STRATEGY ON SELECTION OF HIS SOLUTIONS

As described above there are currently four (4) separate HIS solutions in use in the country. In keeping with an open competitive market for Ghanaian software companies we are recommending that NHIA/NHIS not select a single vendor for all facilities under the Phase 2 implementation.

It has already been decided by GHS to standardize on one of these products for all of their facilities. The software they have chosen is an Open Source product called IHost. GHS has contracted a local software development company to maintain this software. Talks have been opened between GHS and CHAG for CHAG to also standardize on IHost and to share in the maintenance costs of the applications.

Since a major risk to the successful implementation of Phase 2 is the buy-in of the Providers we believe that the administrators of the facility be allowed to decide if they wish to continue using their existing HIS solution, if any, and that if they do wish to continue that the vendor be allowed to participate in funding for interface implementation. The NHIA may chose to set a low limit on the number of facilities using a vendors HIS product that below which no funding would be supplied.

It would be the responsibility of the Provider's administrator to sign a compliance letter stating that the HIS vendor's software is in use in at least three (3) departments in the facility and that they wish to continue the using the software. Where the facility is under the umbrella of a parent organization, such as GHS, the parent organization should make this decision.

In Section 3.4 Tiered HIS Compensation Model of this report we are proposing a tiered payment method to compensate HIS vendors for implementing and retraining existing facilities on the changes made to support the NHIA interface. This tiered method will only cover those HIS systems in use at least 3 facilities and would compensate vendors with the largest installed base at the highest rate commensurate with the additional updating and retraining required.

We believe that allowing all existing vendors to participate in the funding to implement the required interface will have the least impact on facilities already using a HIS application.

Another option that is already in the pre-testing stages is the OCR forms. This option, once tested and being an acceptable process for entry of claims, should be put into use both as an interim method of claims collection pending the implementation of HIS systems at a facility but also as a method for smaller facilities where a HIS system is not practical.

3.4. TIERED HIS COMPENSATION MODEL

As described in the previous section we are recommending a test of desirability of a particular HIS solution by health facilities to decide if the HIS vendor's would be eligible for payments for implementing the new NHIA interface and retraining of hospital staff. The minimum number of hospitals that are using a particular HIS system is set at three (3) in order to be considered.

Vendors that meet the minimum number of facilities need to be compensated based on the effort they will need to expend in order to implement the needed software changes and to retrain the hospitals staff in system use. The greater the number of facilities needing retraining, the greater the effort required. We believe the following levels of compensation are reasonable for this purpose:

- 3 to 5 systems $7,000
- 6 to 10 systems $10,000
- 11 to 30 systems $15,000
- 30 or above $25,000

Before any program begun to compensate vendors these values will need to be discussed with all of the vendors that qualify. A simpler model using $1,500 per facility may be more acceptable to the vendors involved. Further discussions will be needed before a final approach is determined.

3.5. GENERAL DESIGN HIS/NHIA INTERFACE

In order for any Provider based HIS system to be useful for the submission of electronic claims and member validation, a real-time and batch submission interface need to be implemented. Electronic claims are a by-product of the hospital process and not an added workload process to the hospital.

The design of this interface requires that the Admission/Front Desk of the hospital as part of entering a patient into the HIS system automatically connects to the central NHIA system for validation of the members' status. This process should be transparent and not require a separate step such as is currently required in Phase 1.

As the patient progresses through the facility additional information is gathered on the diagnoses, treatment, laboratory tests and drugs used in the treatment. Once the patient is released the creation of the NHIS claim is created as a by-product of the previous steps.

At each stage of treatment entered data is verified as to correctness using rules contained in the HIS system. These rules are based on the same criteria a human claims person would use to vet a claim. An example is the prescribing of drugs not acceptable for the treatment of the identified condition are not allowed at the point of entry. This allows for the correction of the data at the point of entry eliminating the manual correction later on in the process.

The proposed interface will use the tables that the central NHIA system uses in order to assure that the claim contains the correct codes when submitted. The interface will contain an automated process to download the latest tables for diagnoses, treatments, laboratory procedures and drugs assuring that the claims when submitted are acceptable.

The final stage of the HIS process is the submission of claims using a batch oriented model. This process requires the claims manager selecting to submit a group of claims and can be done at any time that the manager feels is acceptable.

This batch submission process is fail-safe, secure, and encrypted. Should the WAN communications link fail or the hospital losing power the process can be re-started from the last checkpoint. This process can support low and high speed connects with no loss of data.

Once the data has been received the posting of the data to the NHIA databases takes place. STL has indicated that they wish to post this data at night so as to not overload the system's capacity. This is not the most efficient method but can be accommodated in the design.

Once posted into the central system the vetting rules of the system can be used to auto-vet the claims. This process should be the same set of rules that were used in the Providers HIS system for the same process. The design assumes that all of the rules used in the NHIA central system will also be implemented by the HIS system vendors. They all already have rules that their systems use today and they have agreed to modify the rules to agree with the NHIA's system.

Any claims rejected by the NHIA system will be sent back to the Provider's system using the same batch methodology. The claim data will be a copy of the original claim along with the error code information so that the HIS system claims personnel can review the rejected claim and make any necessary changes for resubmission.

Following the submission of claims the Provider's HIS system will have the ability to query the current status of their previously submitted claims batches. This is an important function to the hospitals in order for them to control their cash flow needs.

The interface design uses current standards of Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML) for the methods and data formatting. These standards are implementable in all current programming languages and are widely used in the industry. They are a defacto standard for most Governments as part of their Government Information Framework (GIF) standards. This is also the GoG's proposed standard as part of the e-Government project.

It should be noted that in discussion with the five HIS system vendors in Ghana all agreed that this was a preferred interface standard that they would recommend. They also agreed to implement this interface into their products.

3.6. HIS SYSTEM INTERFACE DEVELOPMENT

It will be necessary to assist the vendors with financial and technical support in the modification of their products to conform to the defined NHIA interface. The HIP budget contains funding for this process.

The technical assistance will be in the form of professional advice on the implementation of SOAP XML in their product, testing facilities allowing them to test against sample data contained at the NHIA DC and Compliance Certification of their implementation for use.

NHIA will need to hire or contract a programmer capable of assisting vendors in the implementation of the interface. It would not be feasible to have STL perform this function from Israel since they have no software people in Ghana.

A person will also be needed to certify the compliance of HIS vendors interface implementation as to conformity with the defined standard and interoperability testing. This can be the same programmer that is used to assist the vendors with their questions.

The needed changes are:

- System table definition changes for information needed by NHIA system to identify the institution.
- Real-time link from the HIS system to the NHIA central system for verification of membership.
- The use of NHIA tables for diagnostic, treatment, laboratory and drugs as a replacement for their existing tables. All of the existing systems have their variation of these tables already.
- Implementation of the same rule set used by the NHIA system for automated vetting of claims. All have their own rule sets today and would modify them to conform to the NHIA rules.
- Bulk Claims submission using the prescribed interface. All of the systems currently print a NHIA Claim Form indicating that they have the needed data within their systems.
- Rejected Claim Processing for claims rejected by the NHIA system. This would retrieve claims that were rejected, reduce the batch total for later payment reconciliation, interpret error codes to descriptions, and place corrected claim into next batch for resubmission.
- Query Claim Batch Status

In order to make the necessary changes varying amounts of work will be required by the vendors to implement these changes. Current HIP funding has budgeted for the changes necessary on the HIS systems to conform to the desired interface.

We believe that a method needs to be developed to fairly compensate the vendors for their effort. This compensation needs to be judged against the value of each of these HIS systems to the NHIA goal on electronic claims submission. To that end we have proposes the following evaluation method for this compensation.

1. Vendors system must be currently used or committed to at 3 facilities in Ghana.
2. The certification of the use or proposed use at facilities documented via a signed form from the Chief Administrator at the health facility.
3. Compensation based on the number of installed systems using a stepped payment schedule.
4. Seminar on implementing the interface
5. Test system and support for interface testing
6. Help Desk support with implementation questions.
7. Interface Certification

3.7. INTERFACE DESIGN

As of this time we are unable to define a detailed technical specification for the HIS to NHIA system interface. We believe that an optimum design requires that the parties to the interface be involved in its design. The following are some of the reasons we are not able to supply a detailed technical specification as of now:

- No qualified software development personnel exist at the NHIA.
- No in-country programmers or software analysts are located in Ghana.
- STL software is proprietary.
- Numerous requests for detailed database table definition from STL have not been fulfilled in our opinion.
- Discussion between STL and the HIS vendors is needed.

In lieu of a detailed technical definition of the interface, we are including a high level requirement that can be used for the basis of the design when the above mentioned obstacles have been resolved.

NHIA CENTRAL SYSTEM CHANGES

In order for any Provider HIS system to interface with the NHIA central system, changes will be required at the current central processing system. These changes will need to be made to allow the HIS systems to interface for member validation and claims submission. Currently all transactions for these purposes are performed by applications created by STL as part of the Phase 1 contract.

The current method of member validation is a dedicated PC at the Providers that queries the central NHIA system to check the current member status. This process currently interfaces with no other processes at the Provider and is viewed as extra work by the personnel at the health facility.

Claims are currently submitted at the Schemes via a forms entry process developed by STL which allows for entry of claims one at a time. This method is not applicable to the Phase 2 model of bulk claims submission by the Providers. A central system function will need to be developed that posts bulk claims to the main databases.

In addition, a process for transmitting bulk claims will need to be developed. This can be an integrated process within the NHIA central system or an out-of-band process that operates

independent of the central system and is used to place batch claim data into a location where STL processes can post the claims to the central system.

The interface between the Provider HIS systems and the NHIA central system will need to be based on best practices for moving data between health related organizations that is:

- Secure
- Ensures patient privacy
- Resilient to power and communication link failures
- Simple to implement at the Provider locations
- Adds value to the Provider

As of the writing of this report we have not been able to evaluate the difficulty of STL to implement this interface methodology. The NHIA system is a proprietary system owned by STL. NHIA has purchased the use rights to use this system and has no ownership rights as to the source code that the system is written in. In order to determine the cost STL will charge for the required changes, the NHIA will need to submit a change request for pricing to STL.

The optimum method of implementing the inclusion of the required interface would be to negotiate with STL technical personnel the best methods to use to assist them in implementing the required changes. Using a consultative process will allow STL to advance their preferred methods and allow for the modification of the proposed methods to assist them.

NHIA Central System Outputs

In order for any interface to work between the Providers HIS systems and the NHIA central system, there are some required functions that need to be implemented. These are:

- Real-time query for member validation. This process will query the NHIA system and return the information contained in the Membership Tables or an invalid member response. For new patients at a facility, the NHIA membership information would be used to create a new patient account within the HIS system.
- Download tables:
    - Diagnostic codes, description, reimbursement rate and rule linage definitions
    - Treatment codes, description, reimbursement rate and rule linkage definitions
    - Laboratory codes, description, reimbursement rate and rule linkage definitions
    - Drug codes, description, quantity limits, reimbursement rate and rule linkage definitions
- Bulk Claims Submission in Batch – Once uploaded from the Provider HIS system the claims will be available for posting to the NHIA central system. Our proposed format would be XML but could support a Comma Separated Value (CSV) format.
- Claims Submission must be batch transmission
    - Claims Submission must be capable of restarting from last checkpoint
    - Transmission to be encrypted
    - Must compare batch totals and hash counts at batch completion
    - Codes to be used for submission rather that text fields
- Rejected Claim Notification – The NHIA system would extract all original submitted

claim information along with error codes indicating the reason for rejection that would then be downloaded by the Provider HIS system the next time a connection is made.

- Claim Batch Status query – This needs to be a real-time link to the NHIA system from the Provider system to retrieve the status of claims batches previously submitted. The status information on the batch would b returned on the query.
- All tables to be coded with valid start dates to allow for multiple revisions to tables. Treatment date determines which table revision to use for drugs, treatments and diagnostic pricing and validation.
- Business rules to be used for claims vetting rather than manual prepayment vetting.
- System must support random claims selection for post-payment audits.
- Retrieval of rejected claims must be supported
- Resubmission of rejected claims must be supported
- Real-time retrieval of claims batch status to be retrievable
- Graphic document attachment and viewing to Member Registration. Storage type to be PDF.
- All interface APIs to be SOAP using XML formats

Required Functions

Member Validation

Fields:

FIELD	DATATYPES	NULLABLE	Notes
MEMBER NUMBER	VARCHAR2(30)	N	Main Key
MEMBER_FULL_NAME	VARCHAR2(360)	N	Not Used
MEMBER STATUS CATEGORY(LOV)	VARCHAR2(150)	Y	Status Active and Inactive (I , A)
SPECIAL CONDITION (LOV)	VARCHAR2(150)	Y	'Pregnant Woman' and 'Security Service'
COMMUNITY_CODE	VARCHAR2(150)	Y	
SSNIT_NUMBER	VARCHAR2(150)	Y	
SCHEME_CODE	VARCHAR2(150)	Y	
ID CARD SEARCH	VARCHAR2(150)	Y	
PERSON_FIRST_NAME	VARCHAR2(150)	Y	
PERSON_MIDDLE_NAME	VARCHAR2(60)	Y	
PERSON_LAST_NAME	VARCHAR2(150)	Y	
PERSON_TITLE	VARCHAR2(60)	Y	
COUNTRY	VARCHAR2(60)	Y	
ADDRESS1	VARCHAR2(240)	Y	
ADDRESS2	VARCHAR2(240)	Y	
ADDRESS3	VARCHAR2(240)	Y	
ADDRESS4	VARCHAR2(240)	Y	
CITY	VARCHAR2(60)	Y	
STATUS	VARCHAR2(1)	N	
EMAIL_ADDRESS	VARCHAR2(2000)	Y	
DATE_OF_BIRTH	DATE	Y	DD-MON-RRRR
GENDER	VARCHAR2(30)	Y	
MARITAL_STATUS	VARCHAR2(30)	Y	
START_DATE	DATE	N	DD-MON-RRRR
END_DATE	DATE	Y	DD-MON-RRRR
PICTURES	BLOB	N	

Query

MEMBER NUMBER

Return

MEMBER NUMBER
MEMBER_FULL_NAME
MEMBER STATUS
CATEGORY(LOV)
SPECIAL CONDITION
(LOV)
COMMUNITY_CODE
SSNIT_NUMBER
SCHEME_CODE
ID CARD SEARCH
PERSON_FIRST_NAME
PERSON_MIDDLE_NAME
PERSON_LAST_NAME
PERSON_TITLE
COUNTRY

ADDRESS1
ADDRESS2
ADDRESS3
ADDRESS4
CITY
STATUS
EMAIL_ADDRESS
DATE_OF_BIRTH
GENDER
MARITAL_STATUS
START_DATE
END_DATE
PICTURES

Settable Parms

Timeout	smallint	seconds
IP Addr	varchar2(25)	Addr of Service IPV4 or IPV6

Table Download

Fields

FIELD	DATATYPES	NULLABLE	Description
G-DRG / CODE	VARCHAR2(40)	N	For example: Drugs , Diagnostics , Treatments , Investigations
DESCRIPTION	VARCHAR2(240)	N	
UNIT_PRICE	NUMBER	N	

Query

Table_Name	varchar2(100)	Drugs, Diagnostics , Treatments , Investigations
Check_Point	smallint	Record ID at this value. 0 if from the beginning

Return

Record_ID	smallint	Sequence # of returned record. Used as Check_Point for next query

G-DRG/CODE
Description
UNIT_PRICE
Return code

Settable Parms

Timeout	smallint	seconds
IP Addr	varchar2(25)	Addr of Service IPV4 or IPV6

Notes

1. Process to get 1 record per query.
2. Previous Record_ID used as Check_Point value for next record
3. Need return code. Also use to indicate EOF

Transmit Batch Claims Header

Claims batches will have 1 header per batch.

Fields:

FIELD	DATATYPES	NULLABLE	VALIDATION
Health Provider Name	VARCHAR2(240)	N	LOV from Health Provider Table
Batch Number	VARCHAR2(20)	N	
Submission Date	VARCHAR2(150)	N	
Status	SmInt	N	1=New, 2=Delete, 3=Restart from checkpoint
Total Amount Diagnostic	Number	N	
Total Amount Labs	Number	N	
Total Amount Drugs	Number	N	
Total Amount	Number	N	

Post

All Batch Header Data

Return

Return code

Settable Parms

Timeout	smallint	seconds
IP Addr	varchar2(25)	Addr of Service IPV4 or IPV6

Notes

1. Process to post 1 record per batch transmission.
2. Previous Record_ID used as Check_Point value for next record

Transmit Claims

Fields:

FIELD	DATATYPES	NULLABLE	VALIDATION
Claim Header			
Claim number	VARCHAR2(20)	N	Generated by the System
Health Provider name	VARCHAR2(240)	N	LOV from Health Provider Table
Claim Status	VARCHAR2(25)	N	Generated by the System
Physician id	VARCHAR2(30)	Y	
Member Number	VARCHAR2(30)	N	
Claim Date	VARCHAR2(150)	N	
1st visit	VARCHAR2(150)	N	Cannot be higher than Claim Date
2nd visit	VARCHAR2(150)	Y	Cannot be higher than 1st visit
3rd visit	VARCHAR2(150)	Y	Cannot be higher than 2nd visit
4th visit	VARCHAR2(150)	Y	Cannot be higher than 3rd visit
Date Received	VARCHAR2(150)	Y	
Type of Service(a)	VARCHAR2(150)	N	LOV (Diagnostic , In-patient , Outpatients)
Type of Service(b)	VARCHAR2(150)	N	LOV (All Inclusive , Unbundled)
Outcome	VARCHAR2(150)	N	LOV (Absconded / Discharged, Died, Discharged, Transferred out)
Type of Attendance	VARCHAR2(150)	N	LOV (Emergency Acute Episode, Chronic Follow-up)
Claim Lines	Repeated 10 times		
D-GRG Code	VARCHAR2(40)	Y	LOV From Items table
Quantity	NUMBER	Y	Number of items
Charge	Number	N	Dollar amount of charge

Post

All Claims Data

Return

Record_ID smallint Sequence # of returned record. Used as Check_Point for restart
Return code

Settable Parms

Timeout smallint seconds
IP Addr varchar2(25) Addr of Service IPV4 or IPV6

Notes

1. Process to post 1 record per transmission.
2. Previous Record_ID used as Check_Point value for next record
3. Claims Lines are repeated 10 times. May be NULL
4. Send end of claims as all 9s in Claim Number

Retrieve Rejected Claims

Fields:

FIELD	DATATYPES	NULLABLE	VALIDATION
Claim Header			
Batch Number	VARCHAR2(20)	N	Original Batch Number
Claim number	VARCHAR2(20)	N	Generated by the System
Health Provider name	VARCHAR2(240)	N	LOV from Health Provider Table
Claim Status	VARCHAR2(25)	N	Generated by the System
Physician id	VARCHAR2(30)	Y	
Member Number	VARCHAR2(30)	N	
Claim Date	VARCHAR2(150)	N	
1st visit	VARCHAR2(150)	N	Cannot be higher than Claim Date
2nd visit	VARCHAR2(150)	Y	Cannot be higher than 1st visit
3rd visit	VARCHAR2(150)	Y	Cannot be higher than 2nd visit
4th visit	VARCHAR2(150)	Y	Cannot be higher than 3rd visit
Date Received	VARCHAR2(150)	Y	
Type of Service(a)	VARCHAR2(150)	N	LOV (Diagnostic , In-patient , Outpatients)
Type of Service(b)	VARCHAR2(150)	N	LOV (All Inclusive , Unbundled)
Outcome	VARCHAR2(150)	N	LOV (Absconded / Discharged, Died, Discharged, Transferred out)
Type of Attendance	VARCHAR2(150)	N	LOV (Emergency Acute Episode, Chronic Follow-up)
Reject Codes	VARCHAR2(100)	N	Comma separated list of reject codes. If errors are in Claim Lines code here is 1000.
Claim Lines	Repeated 10 times		
D-GRG Code	VARCHAR2(40)	Y	LOV From Items table
Quantity	NUMBER	Y	Number of items
Charge	Number	N	Dollar amount of charge
Reject Codes	VARCHAR2(100)	Y	Comma separated list of reject codes. Codes may be null if Claim Line is not in error.

Query

Health Provider name varchar2(240)
Claim Date varchar(150) Start date to check rejected claims from.
Check_Point smallint Record ID at this value. 0 if from the beginning

Return

All Claims Data Fields
Record_ID smallint Sequence # of returned record. Used as Check_Point for restart
Return code

Settable Parms

Timeout smallint seconds
IP Addr varchar2(25) Addr of Service IPV4 or IPV6

Notes

1. Process to post 1 record per transmission.
2. Previous Record_ID used as Check_Point value for next record
3. Claims Lines are repeated 10 times. May be NULL
4. Send end of claims as all 9s in Claim Number from central system

Query Batch Status

Fields:

Batch Number	varchar2(20)	N
Batch Status	smallint	0= No such batch
		1=Batch posted
		2=Batch vetted
		3=Estimated payment date set
Batch Payment Date	varchar2(150)	only if status = 3

Query

Batch Number	varchar2(20)

Return

Batch Number
Batch Status
Batch Payment Date
Return Code

Settable Parms

Timeout	smallint	seconds
IP Addr	varchar2(25)	Addr of Service IPV4 or IPV6

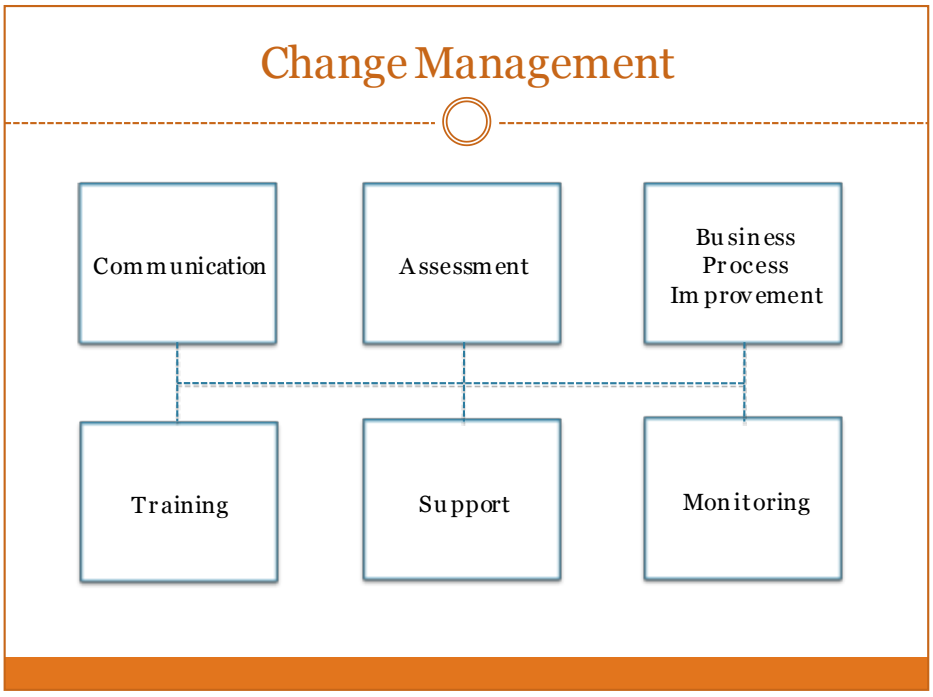
This high level description is based on the available information at this time. It should be noted that a most of the fields defined are currently text based (varchar2). All lookup fields such as drug codes, procedure codes as well as other should be numeric codes that are used in the NHIA central claims system rather than long text fields. We were not able to get the numeric coding structure from STL. This would substantially reduce the amount of data that needs to be transmitted.

4. QUALITATIVE FACTORS

A major objective of this project is the restructuring of the business processes used within the Provider facility to ensure a successful implementation. As identified in the GAP Analysis, Integrating *people and technology* and establishing *effective business processes* is a complex process. It requires a well thought out *Change Management Plan* and a comprehensive *Implementation Plan* including: incentives, a comprehensive *End-to-End* process, clearly defined roles and responsibilities, an organizational structure that supports the *End-to-End* process, comprehensive job descriptions, training and monitoring.

4.1. CHANGE MANAGEMENT

To begin, a Change Management plan must be developed and implemented. The Change Management Plan is designed to ensure that all stakeholders and end-users are ready to provide full support to the project and the changes required to make the implementation successful.



4.2. THE CHALLENGE

NHIA is seeking to implement technical solutions to ensure the fast, efficient, and accurate patient registration and claims preparation and submission within the hospital setting. Phase I of the project, essentially resulted in the status quo. The vast majority of providers are still using paper-based tools for these functions. If change cannot be affected in Phase II, the hospitals will continue to use paper-based systems and NHIA may lose their support for future technology solutions.

4.3. CHANGE READINESS

NHIA needs to conduct a formal Change Readiness Assessment. During the GAP Analysis, the T/TI project team determine that the Hospitals are in fact interested in automated solutions; however, they have little confidence that the technical infrastructure is in place to support this type of change. In addition, the hospitals have demonstrated that while they implement new tasks, they do not evaluate their current processes and procedures to streamline existing work processes. This results in duplicate work.

4.3.1. CHANGE READINESS ASSESSMENT METHODOLOGY

A Change Readiness Questionnaire will be developed to determine readiness to change within multiple levels of the hospital and other agencies involved in the project, including NHIA. Hospital representation included in the survey should include: Executive Management, Operations Management and End-Users.

4.3.2. CHANGE CAPABILITIES

Once the Change Readiness Assessment is completed, the results should be compiled outlining the strengths and challenges to implementing this change. This report should include:

- Stakeholder Readiness – including motivators to support or resist change and strategies to mobilize supporters and mitigate the resisters.

- Key contacts in each hospital and the role they will play during the planning and implementation of the project.

- Change management strategy including:

    - Value based messages for stakeholders
    - Stakeholder support messages for operations managers and end-users.
    - Project progress communications – meetings, newsletters, etc.
    - Clearly defined processes and procedures
    - Roles and responsibilities that support the new processes and procedures
    - Job Descriptions with performance measurements
    - Training
    - Support/Monitoring
    - Incentives
    - Success Criteria

4.3.3. IMPACT OF THE CHANGE

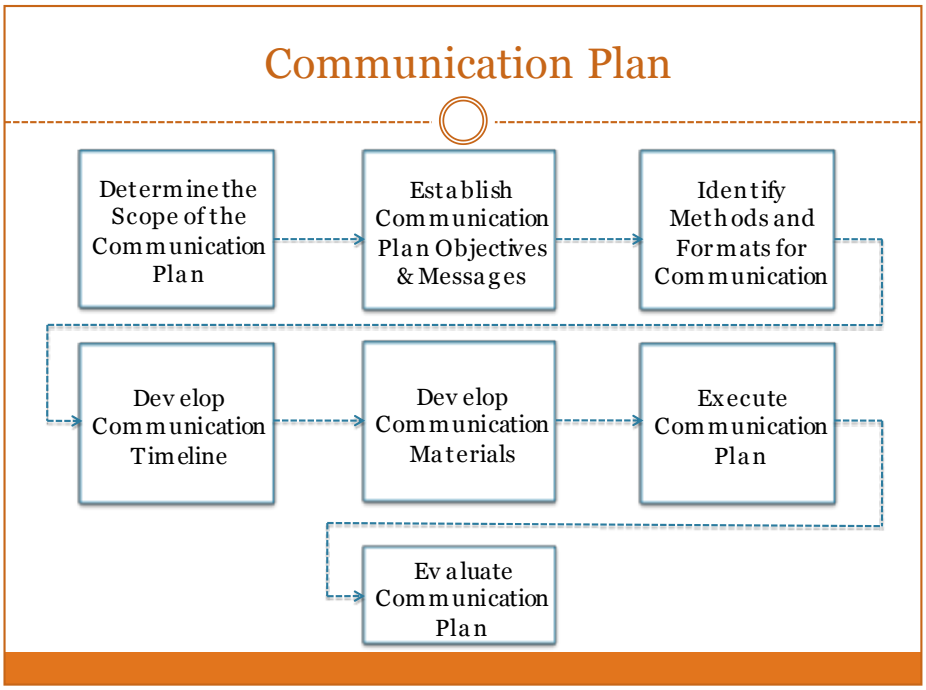
The results of the Change Readiness Assessment should also identify issues that need to be addressed regarding processes and procedures, location, care of and environment for equipment, software interfaces. It should also identify resources issues due to conflicting projects and workloads.

4.3.4. CHANGE MANAGEMENT PLAN

It is important to develop a comprehensive Change Management Plan that addresses: change readiness, communications, business process improvement, training, support and monitoring. The Change Management Plan must include a clear explanation of the project. It needs to define the changes that will take place and the benefits that will be derived from those changes. This plan will be used to ensure that all involved parties are prepared and ready to adopt the enhanced/new processes and procedures being implemented.

4.4. COMMUNICATION PLAN

The communication plan is designed to accomplish several goals. First, it needs to communicate the overall project goals and progress to the stakeholders and end-users. Next it needs to generate stakeholder and end-user support and enthusiasm for the project. Finally, it is used to communicate project progress, issues and deliverables among project team members.



Communication

- Determine the scope of the communication plan
  - Stakeholders
  - End users
  - Project team
- Communication plan goals and messages
  - Project value
  - Project progress
  - Project reports
- Determine communication methods, formats and frequency
  - Email
  - Meetings
  - Brochures
  - Etc.
- Develop communication timeline
  - What needs to be communicated when and in what format
- Develop the communication content
  - Write materials and obtain approval
  - Set meeting agendas and develop meeting materials

Communication

- Execute communication plan
  - Ensure that each communication is distributed to the appropriate audience
- Evaluate communications
  - Conduct surveys to determine the effectiveness of the communications (oral or written)
  - Evaluate survey results
  - Publish results
  - Modify communication plan as needed

Scope

This communication plan addresses the communication needs of stakeholders, end-users and the project team.

Objectives

This communication plan is designed to ensure that stakeholders, end-users and project team members are kept informed of the following, as appropriate:

- Stakeholders and end-users - Project Goals and Value
- Stakeholders and end-users – Project Status and next steps as they involve the stakeholders and end-users
- Project Team:
    - Project Status Reports
    - Team Project Reports
    - Milestone Progress
    - Issues/concerns

Methods/Formats

First and foremost, the project must be branded so that anytime someone sees the "brand", they will associate it with the project. For each type of communication recipient, it is important to identify the most effect means of communicating information. For example, not all end users in the hospital setting have access to email, therefore, it is important to identify various means of communicating with them that conveys information and generates excitement. Meetings can be held to discuss needs, impacts and progress. In addition, fun updates can be developed employing hospital related formats, i.e. a progress report in the form of a patient record or on a plaster motif.

Suggested formats:

- Stakeholders
    - Meetings
    - Emails
    - Project Report Card
- End-users
    - Meetings
    - Fun paper based communications
    - Project Promotions – pads of paper or pens with project logo or theme.
- Project Teams
    - Meetings
    - Emails
    - Reports
    - Intranet

4.5. ROLES AND RESPONSIBILITIES

Communications Team Manager: This position will be responsible for interacting with the overall project team. They will attend meetings, gain a clear understanding of the communication objectives and needs, manage the communication needs assessment, oversee the identification and development of communications materials, and monitor and report on communications progress.

Needs Assessment Analyst: This position will develop the needs assessment screening tool, conduct the needs assessment and produce a report identifying the types and levels of communications required to ensure the successful implementation of the project.

Communications Materials Development Team: The individuals in this position will be responsible for developing the communications materials and evaluation forms required to effectively design and implement the materials needed to communicate with all involved parties.

Consultants: In order to prepare effective communications materials, the communications team will need access to and support from vendors and NHIA project team members to design, develop and produce the required communication materials.

Communications Evaluation Committee: This committee is responsible for determining Communication plan evaluation criteria, evaluating completed forms and suggest modifications to the communications plan and/or materials.

Note: one person may be responsible or assist with multiple functions.

Communication Timeline

It is important to begin communications at the inception of the project and continue them throughout the project implementation and monitoring. The communication timeline should be designed to ensure effective communication of:

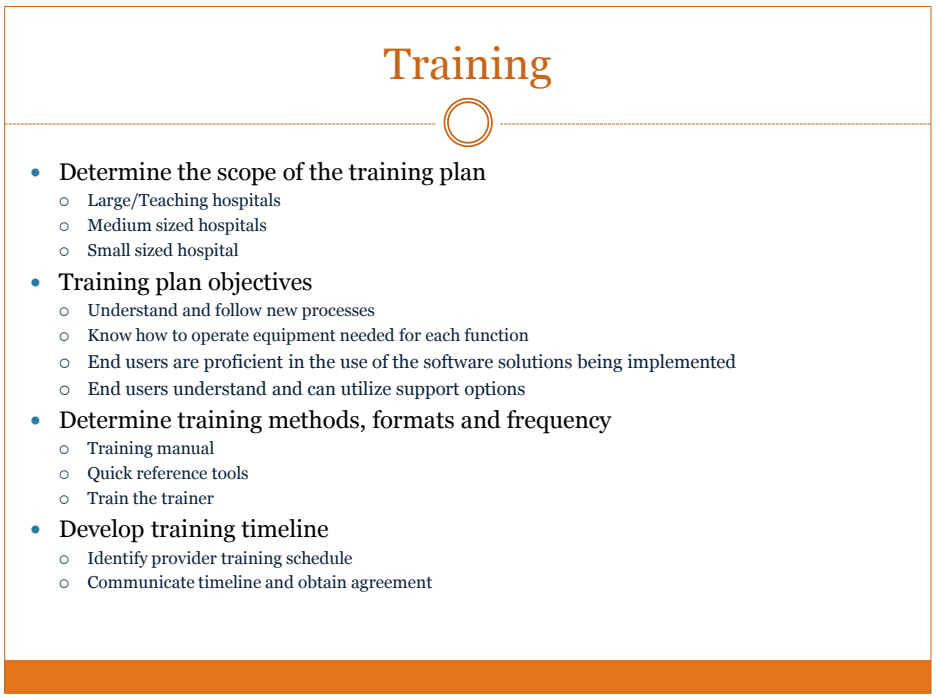
- Value messages
- Project status and accomplishments
- Success stories and end user
- Best practices

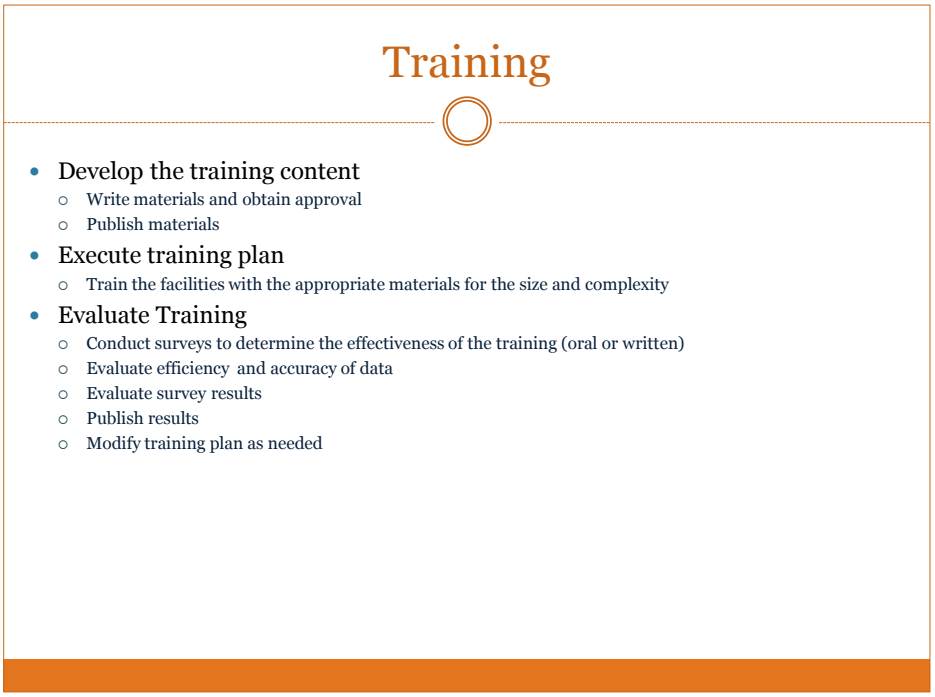
Communication Evaluation

Although the above-mentioned communication formats are effective in most circumstances, they are not always effective. Periodically, the stakeholders, end-users and project team members should be randomly contacted to determine the effectiveness of the communications. Also, unsolicited feedback should be considered and incorporated into the communication plan as appropriate.

4.6. TRAINING PLAN

The training plan is designed to ensure that all end-users are fully trained and able to effectively utilize the processes and procedures, technology and application being put into place on the "Go Live" date.





Scope

This training plan addresses the training needs of large, medium and small-sized hospitals.

Objectives

This training plan is designed to ensure that hospital end-users are proficient in the following:

- Understanding and are able to follow the processes and procedures regarding the full Hospital Information System and at a minimum, patient registration, claims submission and claims reconciliation.
- Know how to operate the equipment needed to perform the functions associated with the new system.
- Are proficient in the use of the software solutions being implemented within the hospital.
- Understand and can utilize the end-user support options available to them while performing these function.

Background

NHIA is standardizing the processes that will be used for patient registration and claims submission and reimbursement. Patients with health insurance are issued cards with magnetic strips carrying all of their demographic and enrolment information. These cards are swiped at the time of registration to ensure the patient is eligible for health insurance at the time the service is being rendered. Once the service(s) is rendered, the claim is prepared and submitted to NHIA in a specific file format. The claim is process and the disposition is returned to the provider in a specific file format.

Training Requirements

The work environment within the hospitals varies greatly depending upon the size of the hospital and the services offered. In larger hospitals, there may be several points of registration, while in medium sized hospital, there may only be one point of registration. Some hospitals are using HIMS throughout the hospital while others only use HIMS in specific departments. As a result of the unique processes within the hospitals, initial training must take place in each facility.

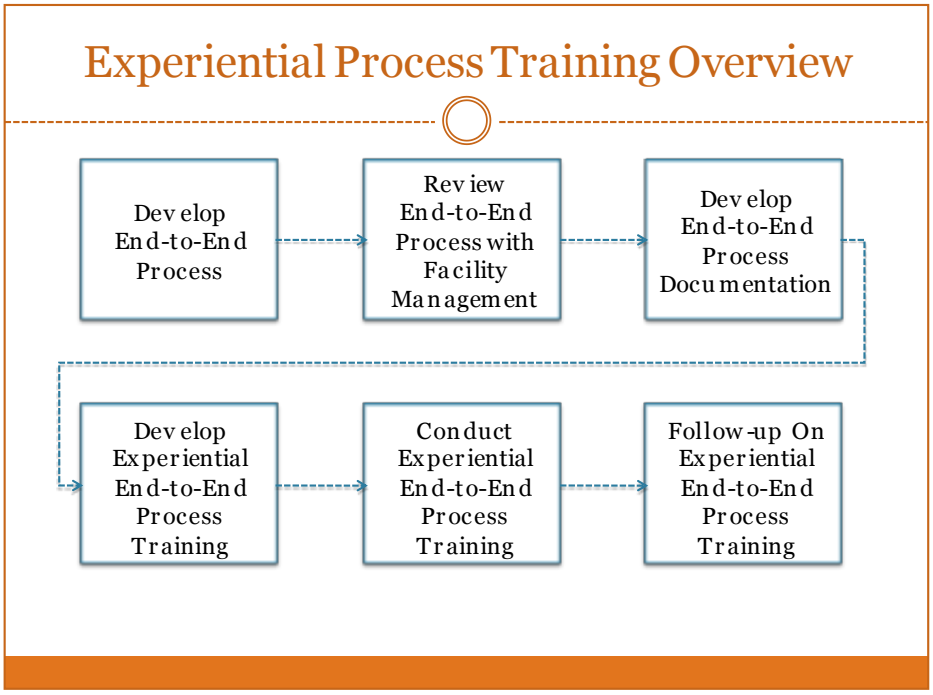
Within each hospital, several levels of training will be required. First, Executive Management must have a clear understanding of the overall project, an understanding of how the project will affect their hospital and be committed to supporting the project by sending supportive messages and mandates to employees.

Next, operational managers must understand the project, how it impacts their processes and procedures and their employees. They must understand and be able to monitor the specific steps required by their employees to support the new processes and procedures. They must also know how to operate the hardware and software used in support of this initiative. *Experiential Process Development* is an effective tool for this process.

Finally, the employees must understand the project goal, the processes and procedures they will use to accomplish the goal and how to use the equipment and software installed in support of the goal. The employees must also be able to adapt their current processes and procedures to accommodate the new requirements. *Experiential Process Development* is an effective tool for this process.

4.6.1. EXPERIENTIAL PROCESS TRAINING

Experiential Process Training is a methodology used to assist in the integration of people and technology thus ensuring the most effective and efficient use of both personnel and technology. It allows the employees involved in new processes to evaluate the overall goals, identify a workable process, evaluate existing processes against proposed processes and make the necessary changes in policies and procedures. It ensures understanding and buy-in to the new process and facilitates change.



Experiential Process Training

- Initial training is conducted at each facility.
- Training is conducted by function.
- All employees involved in the function should participate in the training if possible.
- Review objectives with participants.
- Work with participants to layout the existing work process on a “Sticky Wall”.
- Lay out the new End-to-End Process on the “Sticky Wall” and review with participants.
- Work with participants' to develop a detailed work process, for their function, that supports the End-to-End process.
- Work with the participants to ensure that the new work process does not have a negative impact on the patient or other functions.
- Formally document the process.
- Implement the process.
- Monitor the process

Roles and Responsibilities

In order for training to be successful, the training team must be staffed properly. The roles and responsibilities that must be filled for this project are as follows:

Training Team Manager: This position will be responsible for interacting with the overall project team. They will attend meetings, gain a clear understanding of the training objectives and needs, manage the training needs assessment, oversee the identification and development of training materials, including quick reference guides, lesson plans and resource allocations and monitor and report on training progress.

Needs Assessment Analyst: This position will develop the needs assessment screening tool, conduct the needs assessment and produce a report identifying the types and levels of training required to ensure the successful implementation of the project.

Curriculum Development Team: The individuals in this position will be responsible for developing the training materials, quick reference guides, frequently asked questions, training feedback and evaluation forms, train-the-trainer materials and lesson plans required to effectively train the various constituents within the hospital.

Trainers: These individuals are responsible for training the hospital personnel in all aspects of their responsibilities as they related to the project goal.

Consultants: In order to prepare effective training materials, the training team will need access to and support from technology resources, both hardware and software, NHIA project team members and hospital staff the assist with processes and procedures.

Training Evaluation Committee: This committee is responsible for determining training evaluation criteria, evaluating completed forms and making recommendations on modifications to the training program.

Note: one person could be responsible or assist with more than one function.

Training

Training for Phase I of the NHIA project was conducted at a central location. Since the time of training for Phase I, adoption has been slow if at all. The initial training for Phase II will take place at each hospital. By doing the initial training at the hospital site, the training can be customized to ensure each user understands how to incorporate the changes into their routine and sees the relevance and impact to their day-to-day processes and procedures. At least two people will be trained on the equipment, software and each process and procedure to ensure back up in the event one person is not available. Of course, the Hospital may elect to have additional people trained as long as the number is agreed upon up front and can be accomplished during the normal training program.

Once the initial training is complete, refresher training and new employee training will be conducted at a regional location. The hospital may elect to have further on-site training for a fee, negotiated in advance, depending upon the complexity of training required.

Training Sources

Training will be developed and conducted by a combination of permanent training staff and consultants. Since the majority of training resources are used during the development and initial training stages, it does not make sense to "staff-up" for the initial implementation. Permanent staff should be hired for ongoing regional training and support and curriculum maintenance. Once the initial implementation is completed, consultants would be used on an as needed basis.

Dependencies, Constraints and Limitations

In order to develop effective training programs, the processes and procedures, software and hardware attributed to the project must be clearly defined. While some development of the curriculum may take place during the project planning stage, the vast majority of work will not be completed until right before the pilot begins.

It should also be noted that while the training curriculum will be geared toward the processes and procedures used in the hospital but cannot be designed to cover the specific nuances of each hospital.

In addition, the hospital will be provided with clear, minimum capabilities of the potential end-user. If the trainees do not meet these minimum criteria, the success of the training cannot be guaranteed. Also, success cannot be guaranteed if the trainees do not participate in the entire training program,

Training Materials

The training materials developed may include visuals for overhead projectors, handouts, workbooks, manuals, computerized displays and hands-on demonstrations.

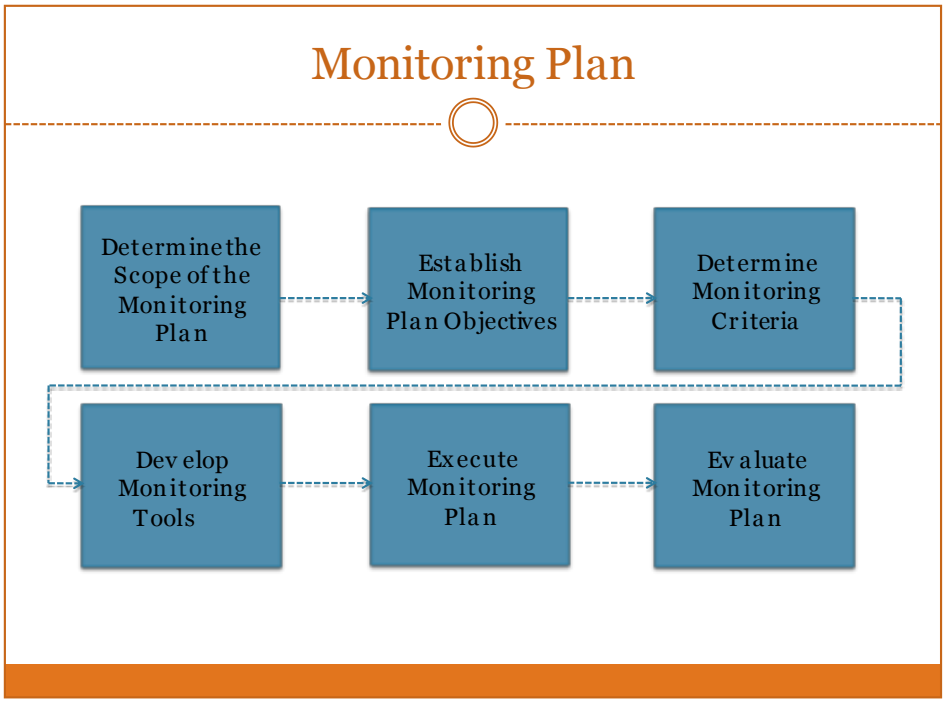
Update/Revise Training Materials

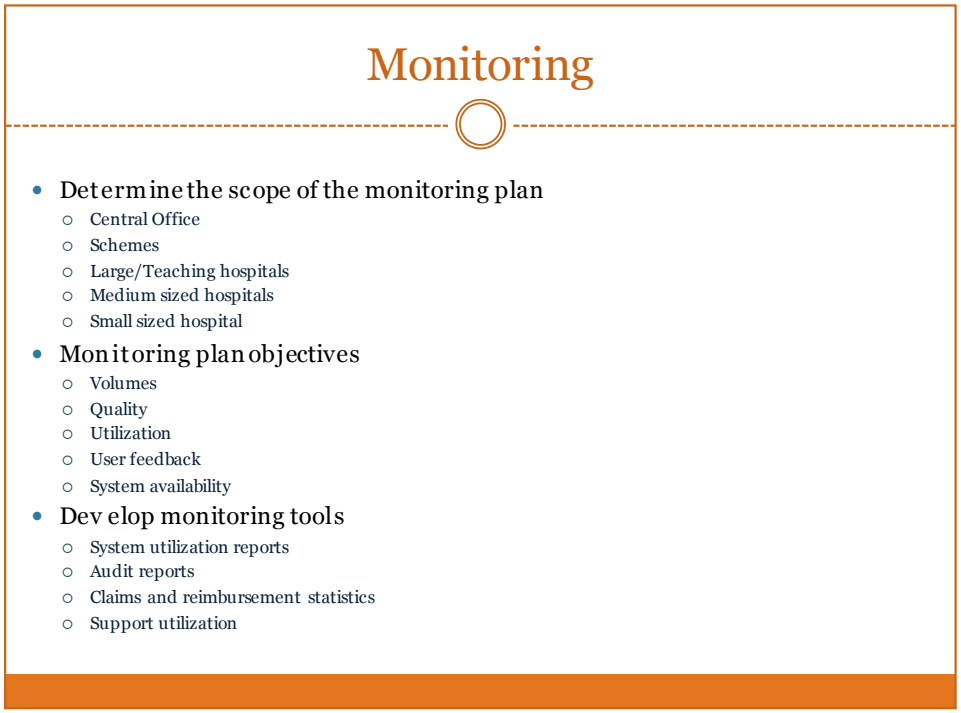
Once training materials are developed and tested, they must be thoroughly documented and updated and revised as necessary. Training materials should remain current with system enhancements. To accomplish this, the training team should be included in distributions of release changes and provided sufficient time to update training materials before the next scheduled user training.

Training Evaluation

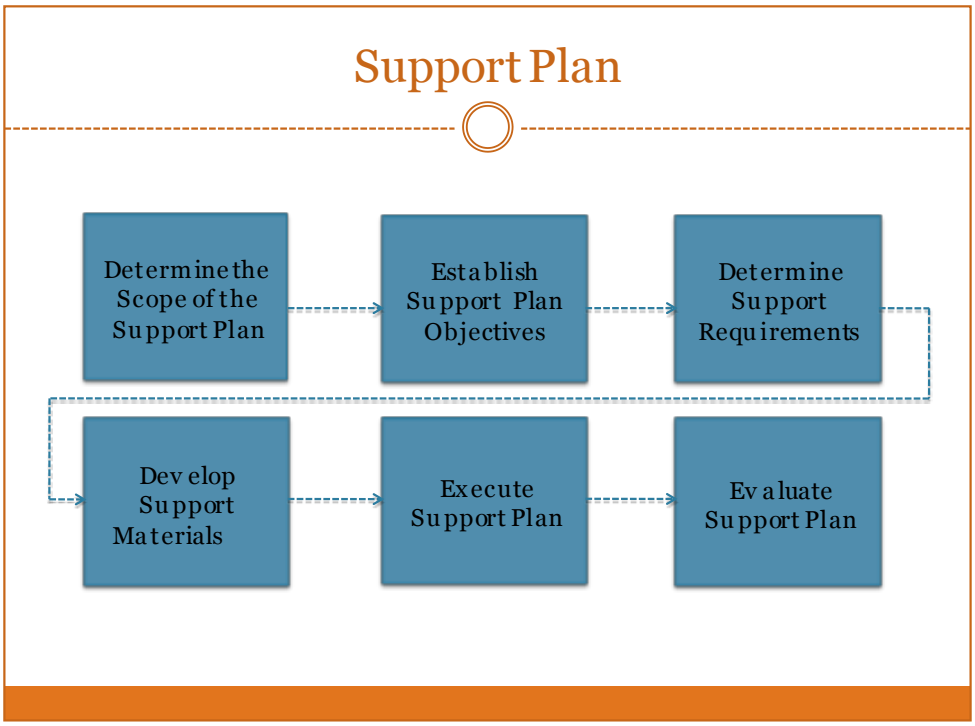
At the end of each training program, the participants will be asked to complete a training evaluation and suggestion form. The forms will be collected and the Training Evaluation Committee will review the feedback and determine if changes are needed to the existing training program. If changes are required, the committed will send the changes to the curriculum development team for them to make the necessary changes and disseminate the changes to the trainers.

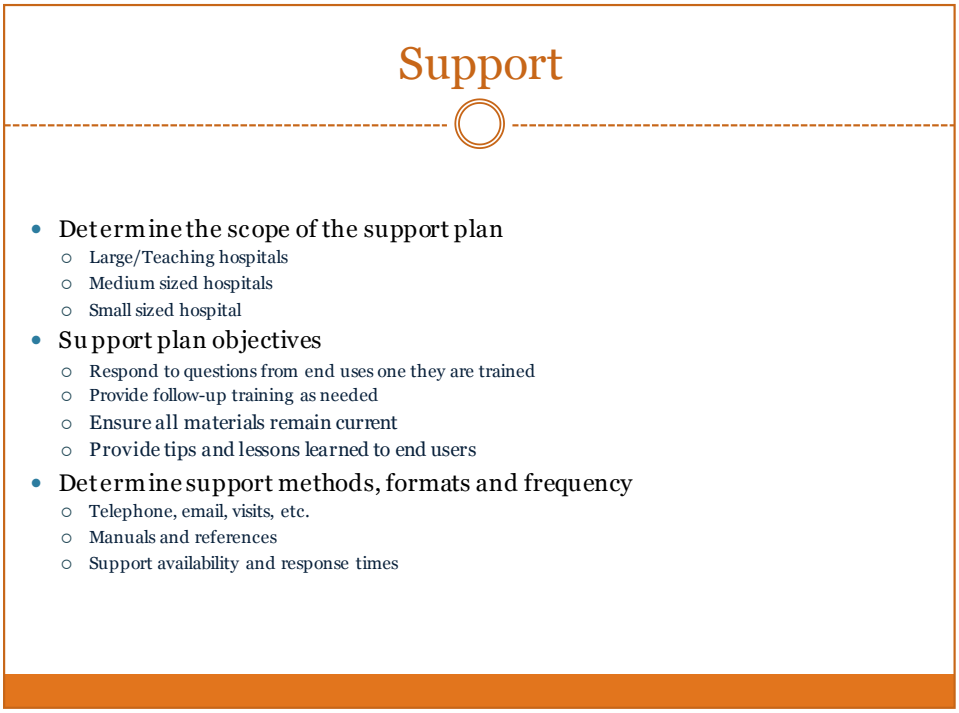
Monitoring Plan





Support Plan





4.7. IMPLEMENTATION PLAN

In order to plan for the success of implementing Phase 2 a well defined and implementable plan must be devised. The objective of any implementation plan is the anticipation and understanding of each step required to reach the project goal.

The concept of "Think before you act" is the basis of creating any project's implementation plan. Every step in the process needs to be evaluated as to what it needs to accomplish, who is responsible, and what are the outcomes. No plan is too detailed since most plans that fail have failed because of unforeseen needs that haven't been defined in advance.

Implementation planning is not something to be viewed as just a process that has to be done because best practices dictate one should be done. Business implementation planning is no different than a carpenter creating a diagram of a piece of furniture before starting to build it. The carpenter makes sure that they have all of the measurements detailed, how the pieces go together and how the final piece is going to look. Failure to do that could result in the final piece of furniture having doors that don't match or other imperfections.

Since having an implementation is critical to success the preliminary Implementation Plan included in this document is intended to be a guide for the development of a comprehensive plan. . Using this high level plan the NHIA and stakeholders can refine each of the steps through consultation and create a plan for success of Phase 2.

We have attached as an electronic attachment our preliminary Implementation Plan. This plan can be used as a starting point of a more detailed plan.

5. CONTINUING MANAGEMENT AND MAINTENANCE ICT INFRASTRUCTURE

One of the chronic problems associated with large scale GoG ICT projects is the lack of maintainability once the original funding is exhausted. The existing HIP funds available are targeted to the CAPEX expenditures needed to install solutions at Providers and are not sufficient to manage the continuing operations once installed.

It is our opinions that these Phase 2 projects will ultimately fail due to lack of maintenance unless a funding model is found to provide the equipment and personnel necessary for operations. The lack of any ICT items in the MoH budgets clearly illustrates the problem.
To install new systems without a clearly defined model for maintaining the systems, training and payments for WAN connectivity will result in future system failure.

Discussions on funding issues is more clearly defined in later sections of this report. Presentation of potential funding mechanisms will be discussed.

Based on the critical nature of the need for the Phase 2 improvements we believe that the Government will reach a solution to the funding issues. Based on that belief we have defined a model for maintaining and managing infrastructure at Providers with a view to cost minimization.

Operational cost mineralization can be accomplished by sharing of technical personnel on a regional basis with lower cost personnel being responsible for day-to-day equipment swap and maintenance procedures and more expensive network personnel being located at a regional facility. We believe that a regional monitoring and network maintenance person in some regions should be sufficient to handle all of the district and regional hospitals.

This type of technical management can be done by incorporating software management tools and qualified personnel. Shown below are recommended staffing models for a regional/district and teaching hospitals.

5.1. GHS AND CHAG FACILITIES

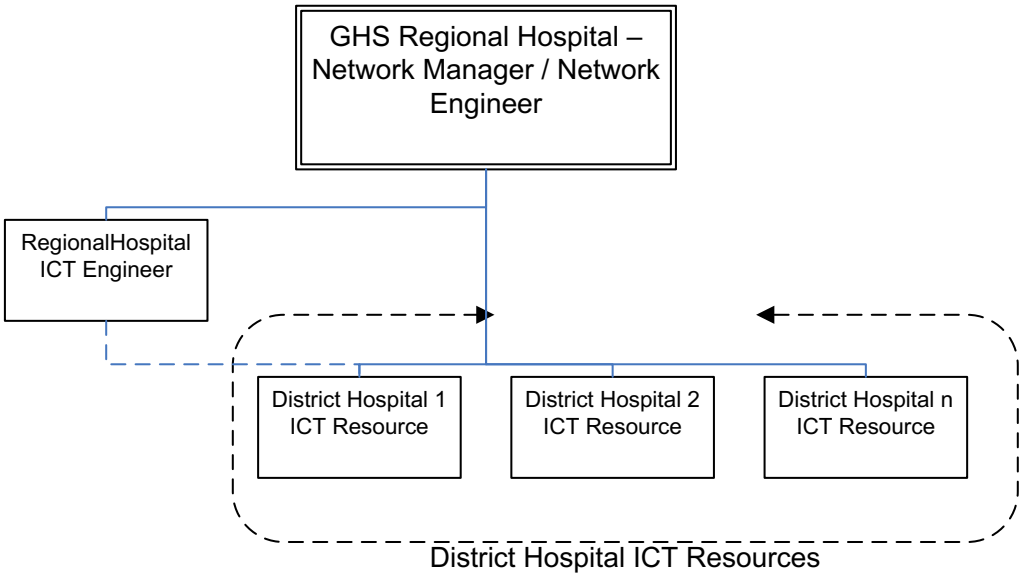


Figure 1 GHS & CHAG Support Model

5.2. TEACHING HOSPITALS

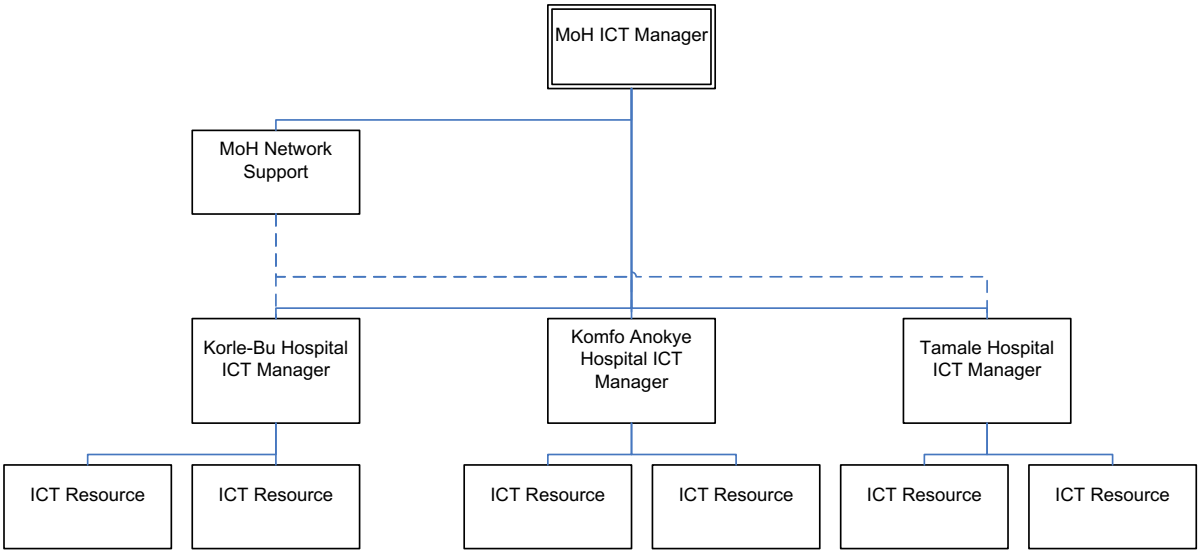


Figure 2 Teaching Hospitals Support Model

5.3. FIELD TECHNICAL PERSONNEL JOB DESCRIPTIONS

Network Field Engineer

The primary responsibilities of the Network Field Engineer will be the diagnosis of network infrastructure and system configuration problems and their resolution for the regional and district health facilities. They will apply firmware updates after approval by the QA department and perform routine maintenance on network systems. They will work with the Field Technicians in communicating with customers on the status of problem resolution.

Additional responsibilities will require running diagnostics and other key performance indicators on all network connected devices. They will mentor other field personnel in advancing their skills on networks.

- Maintain and Install new LAN/WAN network infrastructure
- Level 2 support for regional and district network problems
- Analyze network statistics to identify potential future problems
- Work closely with the Security Specialist on policies and procedures to ensure the Provider's networks are secure
- Assist in coordination of regional ICT tasks and resolving network repairs tickets
- Understand and debug network related issues on network hardware and OS
- Resolve technical challenges of managing networks in multiple geographical locations
- Develop and maintain network automation and installation tools

- Create documentation to streamline and improve upon best practices
- Identify opportunities for process improvement, plan, and implement changes.
- Performs other duties as requested

Field Technician

The Field Technician will be responsible for the general maintenance of all ICT infrastructure at facilities assigned. They will identify ICT equipment problems and repair or replace failed equipment under the supervision of the Network Field Engineer. The Field Technician will be responsible for periodic visits to all assigned facilities on a scheduled basis to perform routine maintenance and testing of ICT equipment.

- Maintain and Install new PC, printer, scanner infrastructure
- Level 1 support for regional and district ICT infrastructure problems
- Install authorized software on PCs
- Report the use of un-authorized software installed on PCs
- Work closely with the Network Field Engineer on policies and procedures to ensure the Provider's networks are secure
- Assist in coordination of regional ICT tasks and resolving repairs tickets
- Create documentation to streamline and improve upon best practices
- Identify opportunities for process improvement, plan, and implement changes.
- Performs other duties as requested

5.4. NHIA DATACENTER AND OPERATIONS

5.5. MANAGEMENT MODEL

5.5.1. PROCESSES

5.5.1.1. PROCESS MATURITY ASSESSMENT

Definition

The Capability Maturity Model (CMM) is a "process" capability maturity model which aids in the definition and understanding of an organization's processes. Ratings are defined indicating an organization's relative stability and process execution. Level 1 represents an unstable and ad hoc environment up through Level 5 indicating a stable and continual process improved environment.

Although CMM comes from the area of software development, it is applied as a generally applicable model to assist in understanding the process capability maturity of organizations in diverse areas including information technology (IT). The CMM levels are defined below.

- **Level 1 – Initial -** Processes are usually ad hoc and the organization usually does not provide a stable environment. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes.

- **Level 2 – Repeatable -** At maturity level 2, processes performance is repeatable. The processes may not repeat for all the projects in the organization. Process discipline helps ensure that existing practices are retained during times of stress. When these practices are in place, projects are performed and managed according to their documented plans.

- **Level 3 – Defined -** The organization has a set of standard processes, which is the basis for level 3, is established and improved over time. These standard processes are used to establish consistency across the organization.

- **Level 4 – Managed -** Using precise measurements, management can effectively control process performance.

- **Level 5 – Optimized -** Maturity level 5 focuses on continually improving process performance through both incremental and innovative technological improvements.

The NHIA should use this Capability Maturity Model industry benchmark to help the NHIA better assess their current process maturity level and to provide a realistic goal and timeline for what level they should strive to reach. We will discuss the process maturity of the NHIA as part of each ITIL IT Service Management framework area in the following sections to help ascertain the "right" CMM level for optimal service and IT alignment.

Findings

The current overall IT process Capability Maturity Level for the NHIA is assessed as "Level 1 – Initial". For this level of maturity, the processes are typically ad hoc. The organization as a whole does not provide the processes required for a stable environment. It relies upon the competence and heroics of the people in the organization and not on the use of proven processes.

While the NHIA is currently pursuing standards as outline by the Information Technology Infrastructure Library (ITIL) model, they have not reached the next maturity level. At this next level ("Level 2 – Repeatable"), repeatable processes are implemented to ensure that defined practices are followed during times of stress. The use of proven processes provides a much more stable environment.

When the recommendations included in this report are implemented, a NHIA data center should realistically reach the goal of "Level 2 – Repeatable" within 2 years. As continued program improvements are implemented, a capability maturity "Level 3 – Defined" should be attained, reflecting a consistent deployment of IT services across the enterprise.

Recommendations

Although higher capability maturity levels are achievable for an organization comparable in size and function, striving for higher levels of IT program maturity may not be compelling nor yield an attractive return on investment.

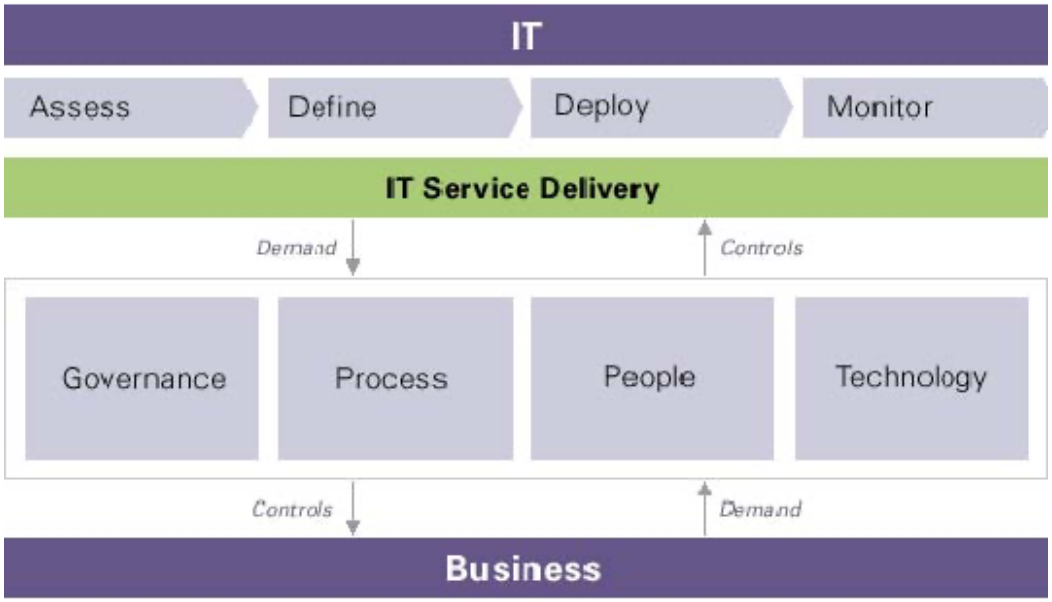
Recommendations	Suggested Timeline
Execute process improvements to move toward a Capability Maturity Model of "Level 2 – Repeatable"	1 – 2 years

5.5.1.2. IT PROCESS FRAMEWORK

Definition (ITIL v2)

The Information Technology Infrastructure Library (ITIL) is defined as a customizable framework of best practices designed to promote quality computing services in the information technology (IT) sector. As an IT Service Management (ITSM) framework, ITIL provides a systematic approach to the provisioning and management of IT services, from inception through design, implementation, operation and continual improvement. In ITIL v2, IT Service Management is grouped into a collection of practices focused on Service Delivery and Service Support. This framework is shown in the figure below.

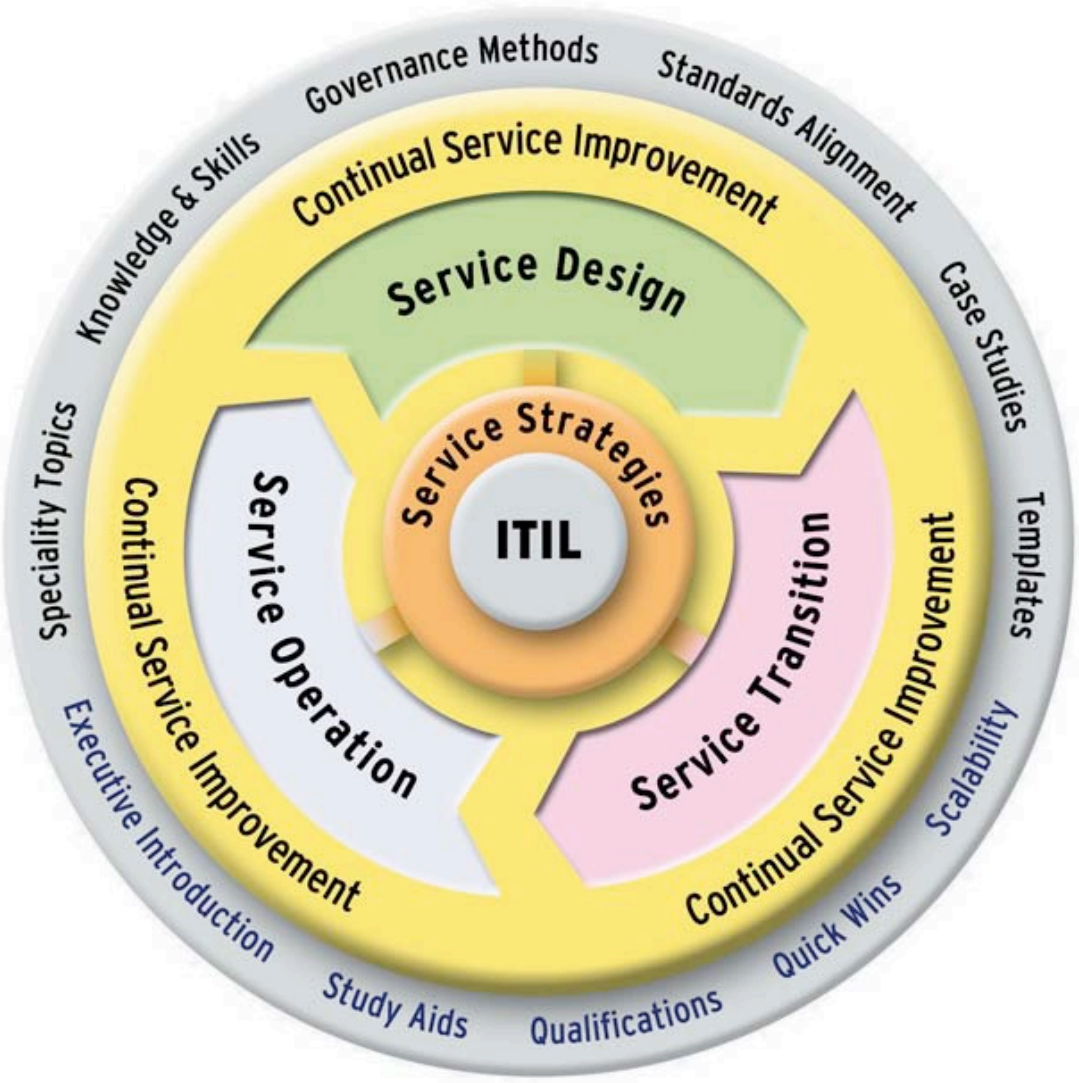
The "Business", representing the NHIS enterprise, sets the IT service expectations or "demand". The functional IT roles establish the "controls" necessary to satisfy the IT demand. The roles are: governance, process, people and technology. Together, the IT processes are operated to deliver the requested level of service. A feedback loop provides the "Business" with insight into process efficiencies and business opportunities.



In 2007 ITIL v3 adopted an integrated service lifecycle approach to IT Service Management. This updated approach repositioned the ITIL v2 framework, which emphasized process lifecycle and alignment of IT to "the business", to the management of the lifecycle of the services provided by IT and the importance of creating business value rather than just the execution of processes. This is a perfect opportunity for the NHIA to update its IT roadmap through the adoption of ITIL v3. This will help focus limited IT Service Management resources to take advantage of best practices that will provide greater return on investment.

Definition (v3)

ITIL v3 breaks down the IT Service Management framework into five categories as shown in the figure and descriptions below. This report aligns our observations and recommendations for the NHIA along these lines.



- Service Strategy focuses on the identification of market opportunities for which services could be developed in order to meet a requirement on the part of internal or external customers. The output is a strategy for the design, implementation, maintenance, and continual improvement of the service as an organizational capability and a strategic asset. Key areas of this volume are Service Portfolio Management and Financial Management.

- Service Design focuses on the activities that take place in order to develop the strategy into a design document which addresses all aspects of the proposed service, as well as the processes intended to support it. Key areas of this volume are Availability Management, Capacity Management, Continuity Management and Security Management.

- Service Transition focuses on the implementation of the output of the service design activities and the creation of a production service or modification of an existing service. There is an area of overlap between Service Transition and Service Operation. Key areas of this volume are Change Management, Release Management, Configuration Management and Service Knowledge Management.

- Service Operation focuses on the activities required to operate the services and maintain their functionality as defined in the Service Level Agreements with the customers. Key areas of this volume are Incident Management, Problem Management and Request Fulfillment. A new process added to this area is Event Management, which is concerned with normal and exception condition events.

- Continual Service Improvement focuses on the ability to deliver continual improvement to the quality of the services that the IT organization delivers to the business. Key areas of this volume are Service Reporting, Service Measurement and Service Level Management. ITIL v3 uses the word "continual" as opposed to ITIL v2's references to "continuous" service improvement (CSIP). Continual implies an activity that is undertaken on a phased, regular basis as part of a process. Continuous is more suitable for the definition of activities intended to operate without pause, such as the ultimate goal of availability.

The NHIA/NHIS model will need to focus on providing continual quality improvement in its ICT Service Management and will benefit by following the latest Information Technology Infrastructure Library (ITIL) framework. The latest version of ITIL is version 3. This new standard promotes the adoption of an integrated process approach to the effective delivery of IT services and sets guidelines for quality in IT Service Management (ITSM).

While the scope of ITIL is all encompassing it is designed to be adaptable to businesses of all sizes and complexities. Each of the areas requires evaluation as to how it fits the individual business. It does not mean that all of the responsibility areas require staffing since many areas can be administered by a single individual.

There is a clear need for ITIL to be implemented immediately for the management of the DC at STL's offices. This model can form the basis for the actual implementation of the new DC and can then be used for the continuing operations when operational.

We are recommending that the DC be operated using this overall model. In order to effectively accomplish this implementation we believe that the designated Infrastructure Manager or a separate ITIL Manager be the overall administrator of the ITIL implementation and continuing management. To accomplish this manager will need to either need to have ITIL Foundation Certification or have read and understand all of the 5 volumes that comprise the guidelines. These books are available at www.amazon.com or www.ITIL.org. The complete set of 5 guides is entitled ITIL Lifecycle Suite and is currently available for US$470 from Amazon. There are also good introductory books available that can assist the manager in becoming familiar with what ITIL is about and how it functions within an enterprise.

5.5.2. SERVICE STRATEGY

Definition

The Service Strategy provides guidance on how to design, develop, and implement service management not only as an organizational capability but also as a strategic asset. This guidance is used to set objectives and expectations of performance towards serving customers and market spaces, and to identify, select, and prioritize opportunities.

Service Strategy is about ensuring that organizations are in a position to handle the costs and risks associated with their Service Portfolios and are set up not just for operational effectiveness but also for distinctive performance. Decisions made with respect to Service Strategy have far-reaching consequences including those with delayed effect.

Key areas include:

- Strategy Generation and Financial Management
- Service Portfolio Management and Demand Management

5.5.3. STRATEGY GENERATION AND FINANCIAL MANAGEMENT

Definition – Strategy Generation

Service Strategy involves four key areas:

- Defining the market – set of opportunities to provide services of value to the business or customers
- Developing the offerings – focus on opportunities of greatest values
- Develop strategic assets – creating efficiencies through automation or otherwise adding value or facilitating revenue generation
- Prepare for execution – determine critical success factors of product or service and leverage existing where feasible

Definition – Financial Management

Financial Management is the discipline of ensuring IT infrastructure is obtained at the most effective price (which does not necessarily mean cheapest) and calculating the cost of providing IT services so that an organization can understand the costs of its IT services. These costs may then be recovered from the Customer of the service. Costs are usually broken down into equipment, software, organization (staff, overtime), accommodation, and transfer (costs of third- party service providers).

Definition – Governance

The discipline of information technology governance derives from corporate governance and deals primarily with the connection between business focus and IT management of an organization. It highlights the importance of IT related matters in contemporary organizations and states that strategic IT decisions should be owned by the corporate board, rather than by the IT managers.

The primary goals for information technology governance are to assure that the investments in IT generate business value and mitigate the risks that are associated with IT. This can be done by implementing an organizational structure with well-defined roles for the responsibility of information, business processes, applications, infrastructure, and so on.

Findings

The NHIS has formed and is operating a Steering Committee which meets on a regular basis to address strategic needs. Although this is a good first step, the need for more detailed product and service definition, development of the offering, and true determination of its value to the business must be clearly understood before a service should be added to the portfolio.

Recommendations

Recommendations	Suggested Timeline
Create a more formal governance organization made up of members of each of the secretariats/agencies represented	0 – 30 days
Review and, where possible, renegotiate current contracts with vendors	3 – 6 months
Requests for new services should go through a preliminary design phase before being added to the service portfolio	Ongoing

5.5.4. SERVICE PORTFOLIO AND DEMAND MANAGEMENT

Definition – Service Portfolio Management

Service Portfolio Management (SPM) involves the proactive management of the investment across the service lifecycle, including those services in the concept, design and transition pipeline, live services, and retired services.

Definition – Demand Management

Demand Management is a critical aspect of service management. Excess capacity generates cost without creating value. The purpose of Demand Management is to understand and influence customer demand for services and the provision of capacity to meet these demands. Projects for each of the secretariats/agencies should be prioritized and added to the IT Service Portfolio as a result of the Demand Management process.

This process balances the strategic needs of the NHIS with day to day services, staffing levels, and feature sets delivered by IT. Assuming that the proper technical input, requirements, and forward thinking by the IT staff are present, a successful IT governance process result would help keep projects in line. This allows IT to better serve its customers with a more consistent service level.

While the "bottom-up" approach can play a role in IT Demand Management, this approach is limited to the prioritization of existing, or immediate initiatives based on IT resource limitations. When incorporating a "top-down" perspective to Portfolio Management, the movement towards shared responsibility for IT Demand Management becomes apparent. This strategic alignment becomes a prerequisite to successfully implementing IT Demand Management.

Findings

Our study could not identify a formal IT Services Portfolio. It was also determined that there was little or no coordination of services between the various organizations, so there is no consistent methodology being employed to identify new IT initiatives.

Based on input from the key stakeholders, there does appear to be a combination of strategic input and tactical requirements being gathered, albeit on a user level rather than across the organization as a whole.

Recommendations

Recommendations	Suggested Timeline
Require more detailed design and cost information before prioritizing and adding items to the service portfolio	Ongoing
Coordinate requirements across the entire organization rather than at NHIA agency level	Ongoing

5.5.5. SERVICE DESIGN

Definition

Service Design focuses on the activities that take place in order to develop the strategy into a design document which addresses all aspects of the proposed service, as well as the processes intended to support it.
Key areas include:

- Service Catalog Management
- Capacity Management
- Continuity Management
- Availability Management
- Security Management
- Supplier Management.

5.5.6. SERVICE CATALOG MANAGEMENT

Definition

A Service Catalog is a menu of IT services. It describes features, components, charges and so on and provides details of Service Level Agreements between the organization, its customers and suppliers. Typically, an internal Service Catalog is accessed via the Intranet Portal and provides internal customers with an end-to-end service view of the IT services available to an organization.

From the Service Catalog, internal customers can perform a number of tasks such as requesting a service, reporting an incident against the service and so on. Customers can track requests for service and add additional information as it comes to hand. For Business Managers, Service Level Management reports can be published to the Intranet Portal, providing ease of access to performance information. In addition, availability of services can be tracked and their performance analyzed.

Findings

No service catalog was observed for any of the agencies interviewed.

Recommendations

Recommendations	Suggested Timeline
Create a service catalog	Ongoing

5.5.7. CAPACITY MANAGEMENT

Definition

As the usage of IT Services change and functionality evolves, the amount of processing power, memory, and other key performance indicators also changes. If it is possible to understand the demands currently being made and how they will change over time, planning for IT Service growth becomes easier and less reactive. If there are spikes in processing power at a particular time of the day, for example, it proposes analyzing what is happening at that time and making the appropriate changes such as increasing the existing infrastructure, tuning the application or moving a batch cycle to a period with less demand.

Capacity Management work is proactive rather than reactive in nature and is responsible for optimizing performance and efficiency. It is also used to plan for and justify financial investments. Capacity Management activities include:

- Monitoring, analyzing, tuning, and implementing necessary changes in resource utilization; i.e., performance and throughput or load on a server
- Managing demand for computing resources; i.e., performance analysis of measurement data, including analysis of the impact of new releases or service on capacity
- Understanding the demands on the Service and future plans for workload growth (or shrinkage)
- Application sizing to ensure required service levels can be met; i.e., performance tuning activities to ensure the most efficient use of existing infrastructure
- Understanding the demands on the Service and future plans for workload growth (or shrinkage); i.e., storage capacity
- Influences on demand for computing resources; i.e., producing a capacity plan that documents current utilization and forecasted requirements, as well as support costs for new applications or releases
- Developing a plan for the Service; i.e., building the annual infrastructure growth plan with input from other teams

Findings

No formal process for capacity management was observed at the NHIA.

Capacity management depends heavily on (1) the ability to measure the current resource utilization in order to analyze the growth of current applications and (2) the ability to determine the impact of new services and applications on the current load. Where monitoring tools were in place, they were of a reactive nature, providing alarm notification only.

There were no tools in place to capture the data needed to provide accurate capacity planning management. There did not appear to be a formal process in place at STL or the NHIA to be able to assess the impact of new applications.

Fundamentally, capacity management does not appear to be a focus of the organization today. Implementing capacity management could reduce the amount of reactive incidents and significantly reduce the amount of rework for technology deployments.

Recommendations

Recommendations	Suggested Timeline
Implement monitoring capabilities in the data center. At a minimum, power and environmental (temperature) data should be collected in order to assess the current load on the infrastructure	6 - 12 months

5.5.8. CONTINUITY MANAGEMENT

Definition

Continuity Management, often labeled Disaster Recovery or Business Continuity, is the process by which plans are implemented and managed to ensure that IT Services can recover and continue should a serious incident occur. It is not just about reactive measures, but also about proactive measures to reduce the risk of a disaster. Continuity Management is so important that many organizations will not do business with IT service providers if contingency planning is not practiced within the service provider's organization. It is also a fact that many organizations that have been involved in a disaster where their contingency plan did not exist or failed ceased existence within 18 months following the disaster.

Continuity Management is regarded as the recovery of the IT infrastructure used to deliver IT Services. Many businesses today practice the much farther reaching process of Business Continuity Planning (BCP) to ensure that the whole end-to-end business process can continue should a serious incident occur.

Symantec Corporation's annual "IT Disaster Recovery" survey reveals the "rising DR [disaster recovery] pressures on organizations caused by soaring downtime costs and more stringent IT service-level requirements to mitigate risk to the business."

The June 2009 survey of 1,650 Enterprise IT professionals involved in disaster recovery in companies of at least 5,000 employees worldwide reported that 93 percent of organizations have had to execute their disaster recovery plans. The cost per incident averaged $287,000 (costs were higher on average in the health care and financial services sectors). The median cost for North American enterprises can be as high as $900,000.

The median time to recover to "skeleton operations" was three hours; four hours were needed to return to "normal operations." According to a release, "This is dramatically improved over the 2008 findings, where only 3 percent of respondents reported that they could achieve skeleton operations within 12 hours, and 31 percent believed they would have baseline operations within one day." The leading reasons given for executing their recovery plan included computer system failure (hardware or software), external computer threats (viruses, hackers) and natural disasters (fires, floods).

Continuity Management involves the following basic steps:

- Prioritizing the businesses to be recovered by conducting a Business Impact Analysis (BIA)
- Performing a Risk Assessment (sometimes called Risk Analysis) for each of the IT Services to identify the assets, threats, vulnerabilities and countermeasures for each service
- Evaluating the options for recovery
- Producing the contingency plan
- Testing, reviewing, and revising the contingency plan on a regular basis

Findings

Several of the stakeholders expressed concern regarding the current level of Disaster Recovery readiness. The primary disaster recovery efforts were focused on localized system or device failures and not on site disasters.

Our observations noted that Business Continuity was not part of the overall IT strategy. Considering that the data center is currently under control of STL and contains the entire mission critical services portfolio for the NHIS (network tunnel terminations, VPN access, financials, key applications, and so on), the emphasis should be on replicating the data and services to another data center for business continuity. In the event that a natural or man-made disaster destroyed or severely disabled the STL site, the ability of the NHIS stakeholders currently using these services and applications to continue operations from another location would be severely diminished.

Recommendations

Recommendations	Suggested Timeline
Formalize all sites in hub and spoke topology for email, file replication and failover sites	2 – 4 months
Analyze network bandwidth requirements between hub sites to accommodate load and Business Continuity plans.	2 – 4 months
Analyze alternative WAN VPN providers	2 – 4 months

Analyze existing backup and restoral processes	1 – 2 months
Develop a formal business continuity plan for the NHIS	4 – 6 months
Evaluate potential hot backup sites for data center to ensure business continuity	3 – 6 months

5.5.9. SERVICE TRANSITION

Definition

Service Transition focuses on the implementation of the output of the service design and the creation of a production service or modification of an existing service. There is an area of overlap between Service Transition and Service Operation.

Key areas are:

- Change Management
- Configuration Management
- Asset Management
- Release Management
- Service Knowledge Management.

5.5.10. CHANGE MANAGEMENT

Definition

The goal of Change Management is to ensure that standardized methods and procedures are used for efficient handling of all changes, in order to minimize the impact of change-related incidents and to improve day-to-day operations.

Change Management compliments Incident Management by:

- Providing the Service Desk with information on current and future change activity, as well as change history
- Minimizing disruption of services by providing controlled implementation of changes
- Providing up-to-date information to customers on progress of change
- Reduction of back-out activities
- Better economic utilization of resources involved in the change

Ideally, a *Request for Change (RFC)* form is used to record details of a request for a change and is sent as an input to Change Management by the Change Requestor. As a result, a *Forward Schedule of Changes (FSC)* schedule is produced that contains details of all the forthcoming Changes which can be distributed to the end users and posted accordingly.

Findings

Change management processes are inconsistent or non-existent within the NHIA. On the whole, change management has not been formally defined. Maintenance activities are performed and changes are introduced into the environment on a frequent basis. No tools, such as a Computerized Maintenance Management System (CMMS), are currently in place to manage preventive maintenance of critical infrastructure equipment

Recommendations

Recommendations	Suggested Timeline
Implement formal Change Management Process	5 – 8 months
Evaluate CMMS systems to manage preventive maintenance of infrastructure at data center	3 – 4 months

5.5.11. CONFIGURATION MANAGEMENT

Definition

Configuration Management assists Incident Management by:

- Providing valuable information on how much of the IT infrastructure is affected by the Configuration Item (CI)
- Identifies the nature and importance of relationships between assets (CIs)
- Providing up-to-date information on customers, owner and status of CIs
- Assisting with identification of incidents of similar CI type

Findings

Configuration management processes are inconsistent or non-existent within the NHIS. On the whole, configuration management has not been formally defined.

Recommendations

Recommendations	Suggested Timeline
Implement formal Configuration Management Process	3 – 6 months

5.5.12. ASSET MANAGEMENT

Definition

IT Asset Management is the discipline of managing finances, contracts, and usage of IT assets throughout their lifecycles for the purpose of maintaining an optimal balance between business service requirements, total costs, budget predictability, and contractual and regulatory compliance. Traditional ITAM activities include the management of inventory, software licenses, vendors, procurement, leases, warranties, cost accounting, retirement and disposal.

Findings

No tools are currently in place to assist in the management of assets. Implementing an asset management system is a time-consuming system, but is easiest to do in a new data center because the workflow management functionality in the system can be used to add the new hardware as it is moved into the data center. This will also provide the best opportunity to start with an accurate view of assets as well as to implement the workflow management processes that are crucial to keeping the asset records accurate.

Industry studies of data centers typically find 10% or higher instances of "ghost servers". These are idle servers that are not being used to perform any work (processing) but are still powered up and using valuable resources (power, cooling and space) in the data center. Asset management and real-time monitoring systems can help to identify these "ghost servers", often paying for much of cost of the system in reduced energy costs.

Recommendations

Recommendations	Suggested Timeline
Evaluate asset management tools for the data center	3 – 6 months

5.5.13. SERVICE OPERATION

Definition

Service Operation focuses on delivery of agreed levels of service to users and customers, and to manage the applications, technology and infrastructure that support delivery of the services. It is only during this stage of the lifecycle that services actually deliver value to the business, and it is the responsibility of Service Operation staff to ensure that this value is delivered.

It is important for Service Operation to balance conflicting goals:

- Internal IT view versus external business view
- Stability versus responsiveness
- Quality of service versus cost of service
- Reactive versus proactive activities

For each of these conflicts, staff must maintain an even balance, as excessive focus on one side of any of these will result in poor service.
Key areas are:

- Event Management and Incident Management
- Service Desk (Request Management)
- Problem Management

Event and Incident Management

Definition – Event Management

Event Management is concerned with normal and exception condition events. Events have been defined into three categories:

- Informational events -- which are logged
- Warning events – also called alerts, a minor alarm or an event where a specified threshold value is exceeded
- Critical events -- which typically lead to the generation of Incidents

Many organizations find it helpful to consider the "operational health" of services. This identifies "vital signs" that are critical for execution of Vital Business Functions. If these are within normal ranges, the system or service is healthy. This leads to a reduction in the cost of monitoring and enables staff to focus on areas that will lead to service success.

Definition – Incident Management

Incident Management aims to minimize disruption to the business by restoring service operation to agreed levels as quickly as possible. Incident Management is often the first process instigated when introducing the ITIL quality framework to a Service Desk and offers the most immediate and highly visible cost reduction and quality gains. In Incident Management, interaction with customers is usually reactive, with the main objective being to find a workaround solution to restore normal services for the customer as quickly as possible.

Findings

Tools currently in place to provide incident management support are not being utilized properly. Incident management tools are a vital part of being able to provide prompt response to incidents under formal SLAs. A formalized incident management process will become even more critical for a data center supporting thousands of users.

Recommendations

Recommendations	Suggested Timeline
Evaluate incident management tools for all of the NHIS enterprise	3 – 6 months

5.5.14. SERVICE DESK (REQUEST MANAGEMENT)

Definition

In the ITIL framework the Service Desk provides a vital central point of contact between the customer and the IT organization. The Service Desk encompasses a range of services that reach beyond the typical Help Desk, including the ability to process incidents, problems, questions, change and service requests, and IT service management processes (e.g. Configuration Management).

The Service Desk is often seen as the 'front door' into an organization where quality service is delivered. Its purpose is to ensure that customers are able to resume their work as quickly as possible following a disruption to an IT Service, minimizing the adverse impact on business operation.

Findings

The Service Desk as it functions today for the NHIS is ineffective. Reports of ticket submission indicate that the reporter is never notified of the resolution. Unconfirmed reports of troubles not being resolved were noted.

Recommendations

Recommendations	Suggested Timeline
Determine the help desk functionality that will be provided by the NHIA and develop an implementation plan	2 – 4 months
Formalize the help desk process using applicable tools as needed	3 – 6 months

5.5.15. PROBLEM MANAGEMENT

Definition

Problem Management investigates the underlying cause of incidents, and aims to prevent incidents of a similar nature from recurring or permanently remove the causes from the IT infrastructure. By removing errors, which often requires a structural change to the IT infrastructure in an organization, the number of incidents can be reduced over time. In Problem Management, IT support staffs are more proactive as they dedicate resources to establishing the underlying causes of incidents. There is usually little or no interaction with the customers as this is left to the responsibility of the Service Desk.

Problem Management assists Incident Management by the following:

- Providing the next path to escalation and resolution (part of the Incident Lifecycle)
- Establishing root cause and Known Errors
- Supporting Incident Management in restoring services

- Providing management reporting on historical data and trend analysis

Findings

There seems to be limited Problem Management in place today within the NHIS network. Observed software problems at Schemes that have been occurring for an extended period of time, indicate poor Problem Management.

Recommendations

Recommendations	Suggested Timeline
Formalize the problem management process using applicable tools as needed	3 – 6 months

5.5.16. CONTINUAL SERVICE IMPROVEMENT

Definition

Continual Service Improvement focuses on the ability to deliver continual improvement to the quality of the services that the IT organization delivers to the business. Continual implies an activity that is undertaken on a phased, regular basis as part of a process.

Key areas are:

- Service Reporting
- Service Measurement
- Service Level Management

Findings

We were not able to identify any SLA agreements between the NHIA and the Schemes and Providers.

Recommendations

Recommendations	Suggested Timeline
SLAs should be established for all services to be provided by the NHIA data center	Ongoing

Backup
Definition

Although backup management is considered a service this area is highlighted in this section to demonstrate where Service Measurement and Service Level Management processes would generate problem tickets and force reprioritization of resources to address.

Findings

We were not able to identify any formal backup and restoral procedures.

Recommendations

Recommendations	Suggested Timeline
Standardize on a backup tool such as Symantec Backup Exec which includes Granular Restore Technology	2 – 3 months
Implement a standard password policy including password length, required characters (upper/lower case, symbols, numbers) and password expiration	1 – 2 months
Establish and publish to each computing or network device a login banner stating the acceptable/unacceptable use policy and privacy rights for anyone who logs into the device.	1 – 2 months

5.6. NHIA DATA CENTER SITE ISSUES

Data Center Build vs Co-location Options

The current situation where the NHIA DC is located at STL's offices is not a viable option for long term operations. As cited in the GAP Analysis Report, previously submitted, substantial risks exist. In order to mitigate those risks we recommend that immediately look to re-locate the existing DC systems to another location and that NHIA take over responsibility for the management of the DC.

It is our understanding that the NHIA is committed to relocating the DC within the next 12 months to a new location that is to be built. Other alternatives will soon exist as to where and under what model to house the NHIA systems. The Government has secured funding from the World Bank to construct and operate an e-Government Data Center. Should the e-Government Datacenter be ready in time, the need of a separate DC for the NHIA, could be eliminated and the systems could be hosted in the Government DC.

The Ghana ICT Directorate (GICTeD), an agency within the Ministry of Communication, is in the process of creating a Government-wide Data Center and Backup Data Center in Ghana. The costs for co-locating the NHIA infrastructure in this facility could not be determined at this time. Pricing for services under the DC have not yet been developed but should be available in the near future.

We are recommending that the NHIA remain in contact GICTeD to review their plans as to availability of co-location services at this facility. It is most likely that co-location will be far less expensive than the creation of a separate NHIA DC and provide the highest level of security and redundancy needed for the NHIS data.

Also part of the GICTeD mandates is the connection of all Government offices via GovNet. GovNet is also funded and under construction today. Additional discussion of this option can be found in the section *WAN Connectivity* below.

Backup Data Center

Due to the critical nature of the data the NHIA DC houses it is important that a full Disaster Recovery Plan be implemented. Part of that plan will need to define how the NHIA would resume operations in the case of a major event. In considering that plan it may be decided that the NHIA systems need to be duplicated in a backup facility.

Should it be decided that the NHIA needs to have a fully operational DC to serve as backup in case of a major disaster and the central DC, then both the building of a separate facility and the possibility of co-location need to be considered. The costs associated with the building of a mirror site can be as much as the central facility.

An alternative is to house the mirror site at the e-Government DC or a private facility. Costs for both of these alternatives need to be gathered and the cost/benefit analysis needs to be calculated.

This study has made no analysis of associated costs of a backup mirrored site but recommends that as part of the creation of a Security Plan these alternatives be considered.

5.7. SECURITY PLAN

It is important that a Security Policy be put into place immediately. The risks to the operation of the NHIS are high without a well defined and enforced security policy. The development of the Security Plan requires a detailed analysis of all system stakeholders, data center and NHIA office facilities.

There are numerous standards that can be used in this process. We would recommend a plan that uses the model developed by the SANS Institute, http://www.sans.org/resources/policies/. Special attention should be paid to the information on Health Information Portability and Accountability Act (HIPAA), a U.S. Government law dealing with patient identifiable data security.

HIPAA was put in place specifically to deal with data similar to what the NHIA is responsible for here in Ghana. Passed in 1996, HIPAA is designed to protect confidential healthcare information through improved security standards and privacy legislation. It defines requirements for storing patient information before, during and after electronic transmission. It also identifies compliance guidelines for critical business tasks such as risk analysis, awareness training, audit trail, disaster recovery plans and information access control and encryption. The regulations covered under HIPAA can be viewed at http://www.hhs.gov/ocr/privacy/index.html.

It is our recommendation that a professional security consultant be hired to assist in the development of a plan and the subsequent audit policies and procedures. The consultant should work closely with the NHIA personnel designated as responsible for security and mentor them during this process.

We did not survey the installed machines for applications that were not supplied by NHIA nor did we ascertain separate Administrator and User logins. This should be mandatory on all systems supplied.

The machines installed by NHIA personnel or contractors should contain Administrative passwords separate from the user's access to eliminate the installation of software other than that supplied by NHIA. In addition all CD, DVD and USB devices should be disabled on existing systems.

The use of Thin Clients in future deployment of any computers would eliminate the external introduction of virus infections. The Thin Clients would contain no CD or DVD drives and can have their USB ports disabled.

As part of a comprehensive Security Plan a policy on virus updates should be addressed. Even with the recommendations already mentioned it is still possible for machines to become infected through connection to the Internet. There is currently no method to prevent a user from connecting a cable from an Internet access point to a machine and potentially accessing unsafe sites. A strong policy prohibiting this practice along with current virus definitions will eliminate infections.

Recommended Immediate Steps

1. NHIA to take steps to take control and ownership of NOC.
2. Detailed audit to be conducted to identify all risks.
3. An independent VPN security platform/solution (e.g. a combination of SSL and IPSec) to be adopted for use to strengthen the prevention of unauthorized access.
4. Plan, develop and enforce a system-wide IP Security policy for the WAN.
5. System / Network audit must be carried out immediately.
6. A system / Network audit policy must be put in place to ensure regular half-yearly audit.

5.8. QUALITY ASSURANCE

A major requirement on the success of Phase 2 will be the quality of the delivered solutions. The quality of the HIS solutions will determine the success of their use at the health facilities. The success of the claims submission and member validation portion of these systems is however directly tied to the performance and reliability of the central NHIA systems.

During our study we identified instances where problems exist in the QA process leading to software errors and poor system performance. It was not a requirement of our study to identify existing issues in the Phase 1 system but to evaluate the readiness of the NHIA systems to support Phase 2.

Based on observed performance issues we believe that the WAN VSAT network currently in use does not have the reliability needed for the real-time verification of membership. As identified in the Gap Analysis report previously submitted, a through QA of the WAN is needed and identified issues need to be resolved prior to Phase 2 implementation.

We believe that a through QA process also needs to be performed on the Phase 1 system to identify areas requiring improvement. The TTI team has concerns in the performance of the existing NHIA system. Observed system delays at Providers and Schemes need to be tested and problems identified before Phase 2 systems are installed. At a minimum the system response times need to be evaluated against the original performance criteria.

Additional major concerns exist in the current performance capacity of the existing systems. While TTI did not perform any quantitative or qualitative tests on the existing systems we did identify potential problems based on other criteria.

Two issues that are of concern are based on off-hours batch processing. During discussions we became aware that reports are currently run off-hours so as not to impact system performance. An additional item gathered from the ICR Implementation Plan for the OCR readable claim forms processing where it states "The CSV files will be loaded into the application every night." leads us to question why this process is not performed in real-time.

These concerns are amplified by the fact that currently the system is lightly loaded based on a current usage statistics. When Phase 2 is fully implemented usage will be significantly increased. We believe a full performance audit should be conducted prior to Phase 2 implementation.

6. WAN CONNECTIVITY

One hundred and twenty (120) sites have been selected and considered for this report. These were selected based on the physical sizes of the facilities, size of operations and extent of use of the WAN. They are largely medium sized providers, mainly regional hospitals (GHS, CHAG, Police, Military and teaching hospitals).

The provider sites have been categorized into three i.e. Large, Medium and Small providers. This would provide for appropriate solution for the site. Typical examples are:

Large Provider – Korle Bu Teaching Hospital in Accra
Medium Provider - Effia Nkwanta Regional Hospital in Western Region
Small Provider – Sekyere Clinic in Ashanti

After the series of visits to sites, interviews with STL and consideration of existing technologies and solutions available in Ghana, a set of solutions have been recommended, with the following justification:

i. Widespread installations using VSAT must be changed with inclusions of other solutions like terrestrial Microwave (Radio) and ADSL for the following reasons:
    a. Quality of service is usually poor, especially during rain, cloudy and dusty conditions, resulting in low rates of network availability
    b. Round Trip Time (RTT) or latency, for any VSAT connection is in excess of 500ms. This is the extreme for any kind of communication, especially with Oracle server in the centre of the communications
    c. Other alternative technologies like terrestrial MW and ADSL exist for commercial access and could be adopted. These have been proven to be stable and more adaptable to local conditions.
    d. VSAT should only be considered as a last resort, especially note-worthy for harsh tropical conditions.

ii. Number of WAN connections to each provider site should be limited to one (1) as much as possible. Korle Bu, for instance, has twelve (12).
    a. Such implementation is inefficient as the provider's other departments can together share a common WAN connection
    b. The design is technically not cost effective as it introduces 1200% (for Korle Bu Teaching Hospital) Capex and Opex cost

iii. Introduce WAN / VPN Node in NHIA for monitoring and supervise for audit purposes
    a. It is important that NHIA monitors the network, activities and operations of the NOC and provider and scheme sites
    b. Monitoring offers good basis for audit of WAN and operations

iv. Steps must be taken to improve Security Implementation with a double firewall implementation. This is because

a. Current security implementation provided by via Cisco 6500 router is not enough. Network of such capacity would require dual firewall implementation with specialized equipment of very high processing power to assure secured but fast connectivity.
b. Personal and sensitive health records being managed over the WAN requires optimum security

v. The location of NOC must be in NHIA designated place and must be under the full control of NHIA, both physically and logically. This location must have good physical conditions, loading dock, clearances, amenities, good stable power, cooling capabilities, Disaster Recovery options, and accessibility. This will accord the NHIA full control and security of WAN infrastructure. NHIA could also outsource hosting of NOC as a service, paid for with SLAs.

vi. A Backup WAN should be considered. This could be a narrow band implementation with low bandwidth, but inexpensive solution. This could be deployed at areas requiring high availability to handle their high usage of the infrastructure, and satisfy the high availability requirement.

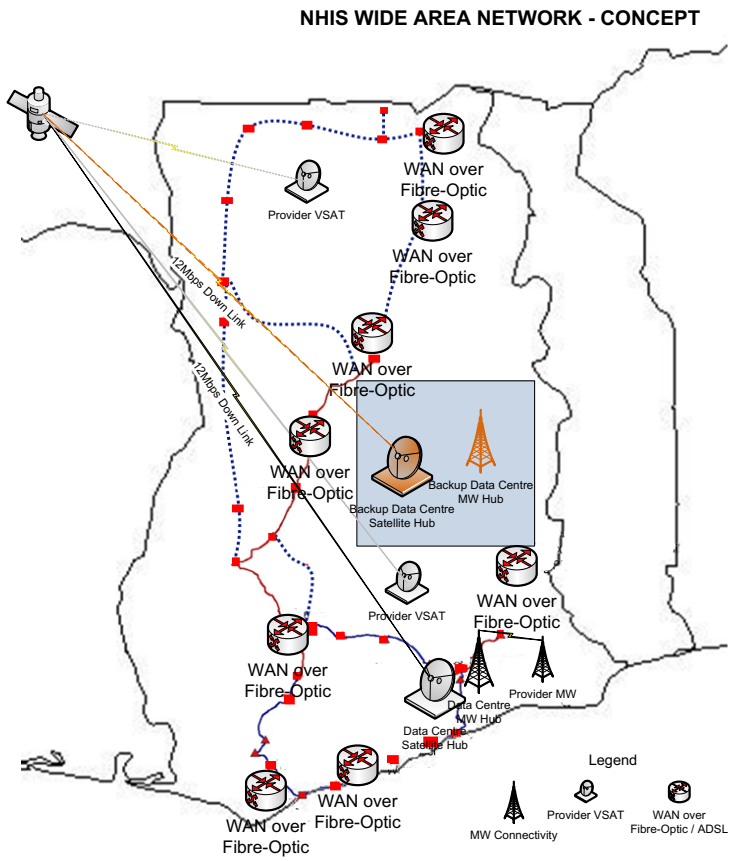
a. A backup network for critical provider sites and NOC would provide platform for Disaster Recovery readiness. This is required in a network of the scale of NHIS WAN used to transmit such sensitive data as customers' health and personal information

vii. It is our recommendation to deploy more efficient Network Monitoring tools.
a. This is required to ensure full bandwidth delivery and utilization
b. It is necessary for quick and easy troubleshooting, and uptime management

viii. Keep Spares Inventory. Industry standard estimate of volume of stock is 6% of installed network elements. This would help improve Mean Time To Recover (MTTR) from major faults causing prolonged downtimes.

ix. Periodic training must be provided for selected users and managers of the WAN to ensure capacity to manage the network with high efficiency.

Suggested typical designs include:



Assumptions and Considerations

1. Bandwidth distributed to each site would not exceed 128Kbps,scalable though, per site, and 10Mbps aggregate channel capacity to Data Centre.

2. Other terrestrial solutions that are more reliable and with higher availability than VSAT (e.g. fibre optic or regional Microwave (MW)) would be employed. These solutions are much less expensive than VSAT.

3. Other commercial solutions exist and could be deployed to provide connectivity, e.g. the national fibre-optic backbone, and e-govnet (Future 2010).

4. Sites that are difficult to connect with any terrestrial solution would be connected with VSAT and risk link quality

5. All links terminate at the Data Centre (proposed to be NHIA-designated location), and Backup data Centre.

6. Backup Data Centre is proposed to be at different physical location from primary.

7. All over 700 Sites, and any new sites would be connected

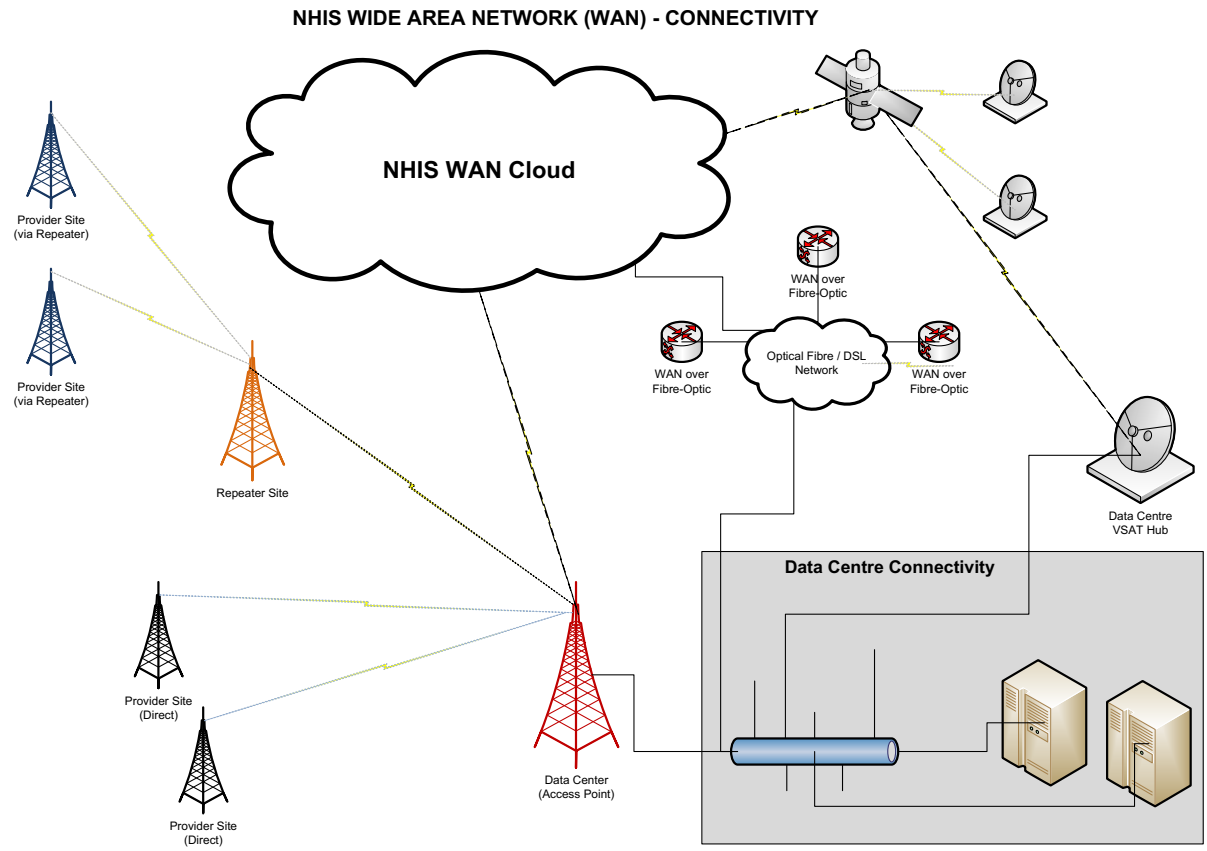
8. WAN Security is implemented using existing Firewall Cisco 6500 security and other specialised Firewalls

*9. A VPN link is provided at NHIA offices for Network monitoring and high-level view of WAN

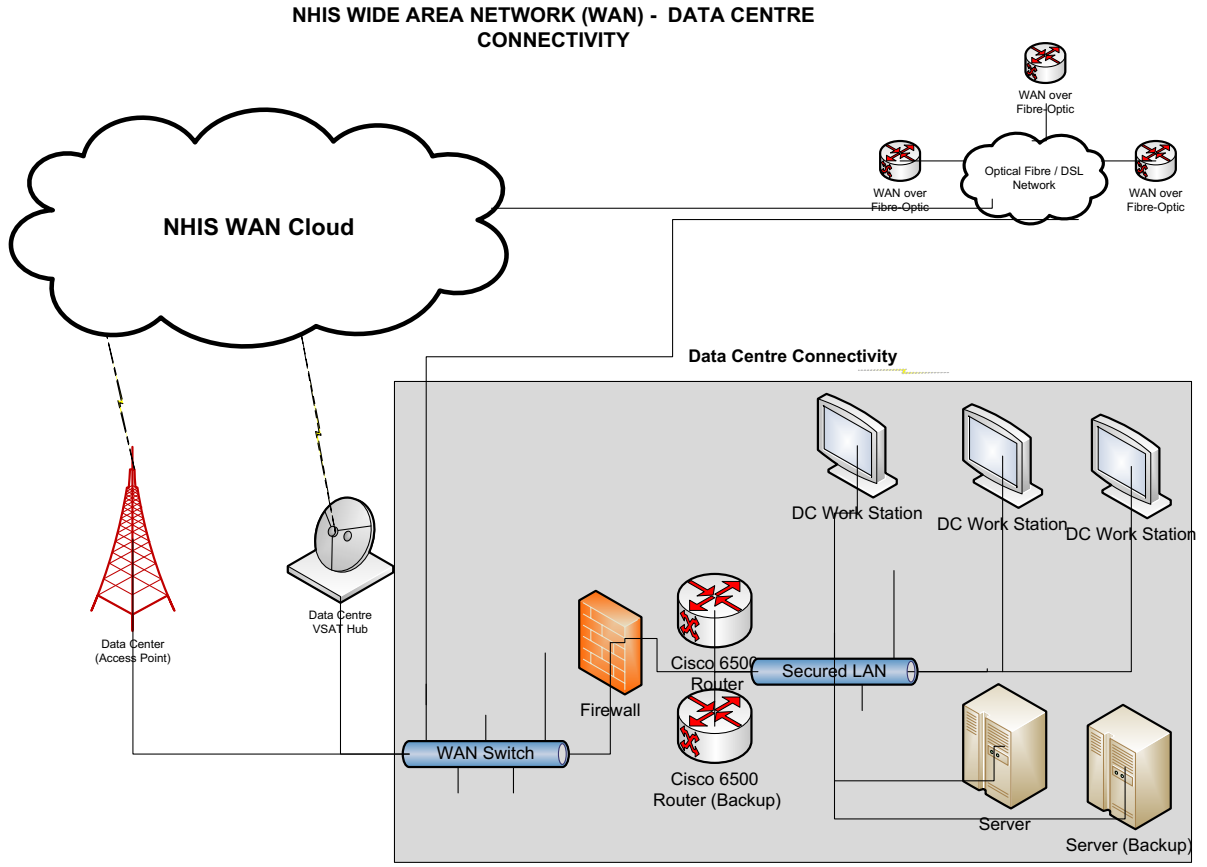
*10. WAN usage policy would be formulated to enhance WAN usage and improve connectivity and also optimise the use of WAN resources.

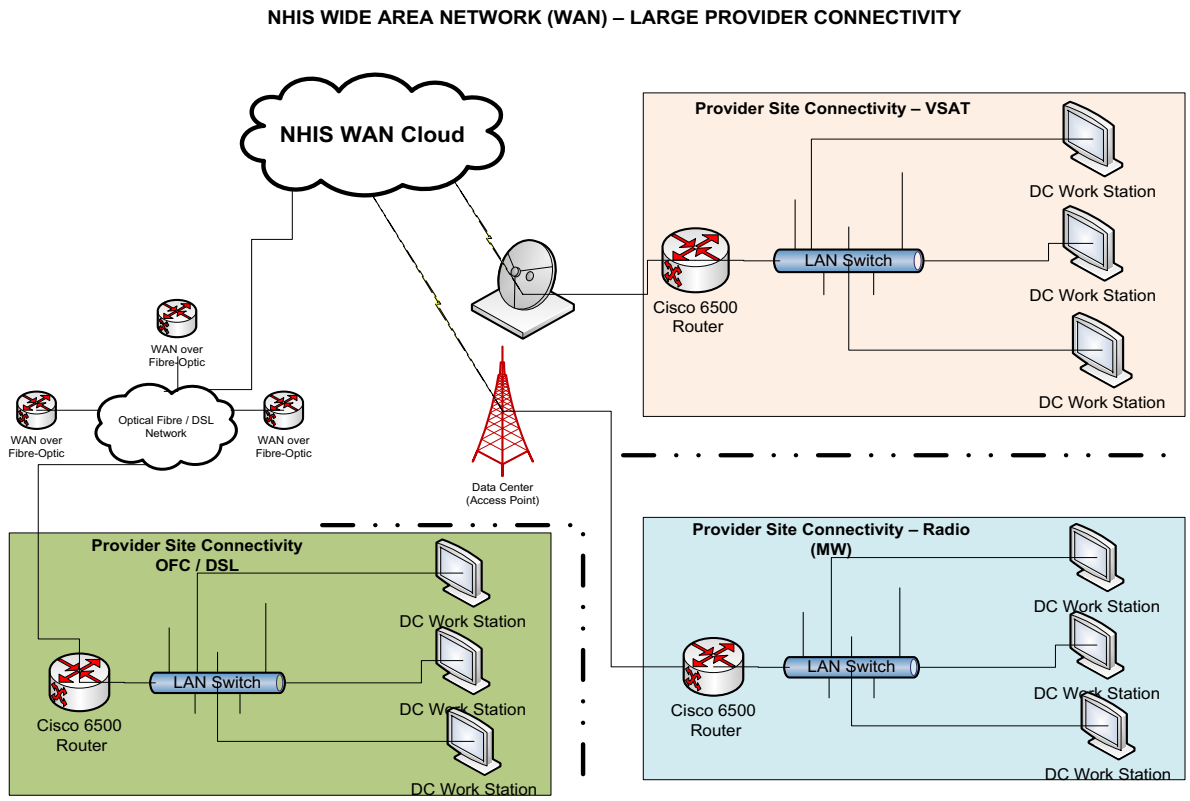
11. Backup Narrowband Network proposed for redundancy of network key sites

General Concept of NHIS WAN considering existing and possible connectivity options

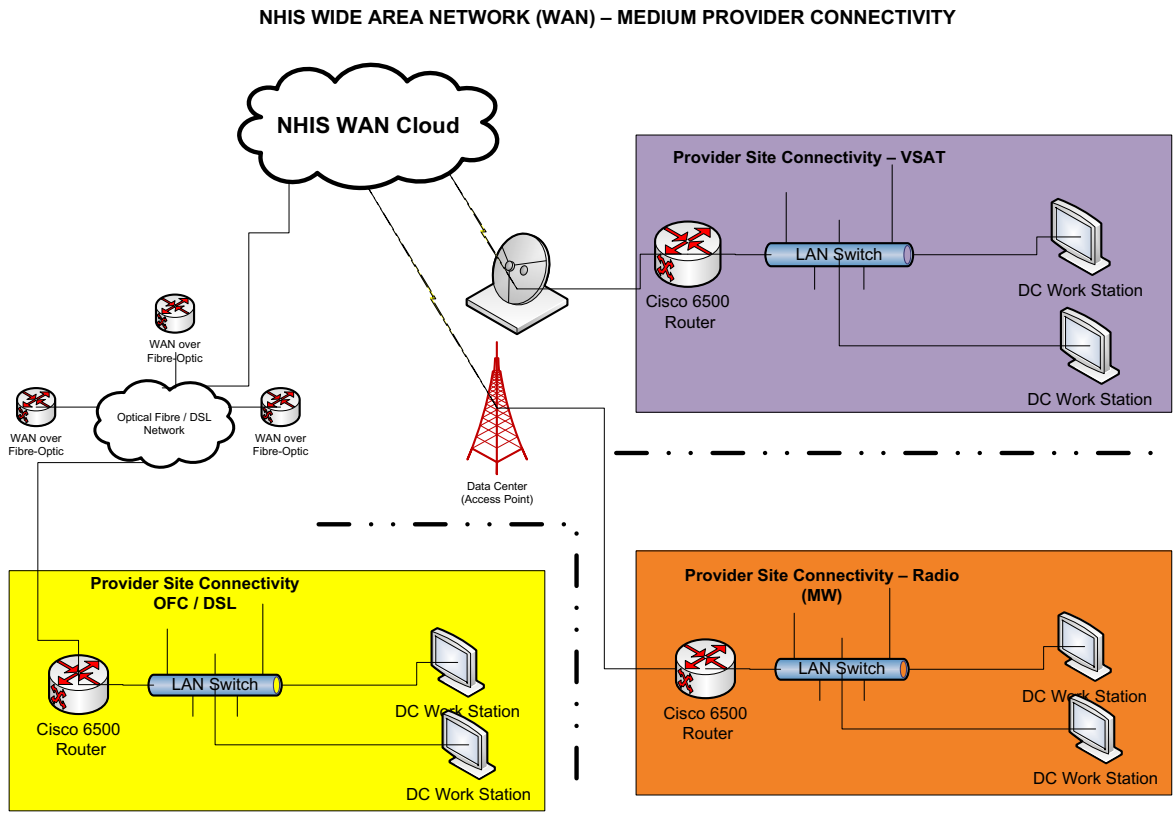


High-Level view of Proposed NHIS WAN

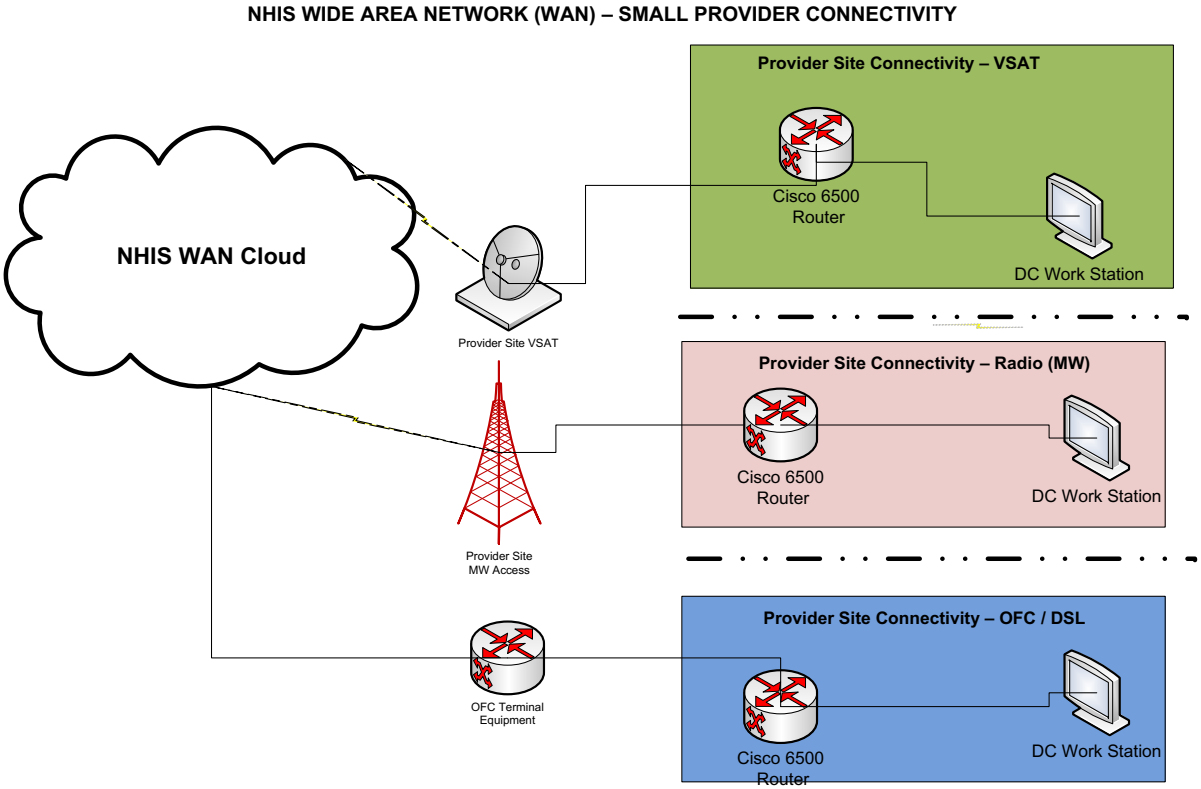




WAN Connectivity Design for Large Provider



WAN Connectivity Design for Medium Sized Provider



WAN Connectivity Design for Small Provider

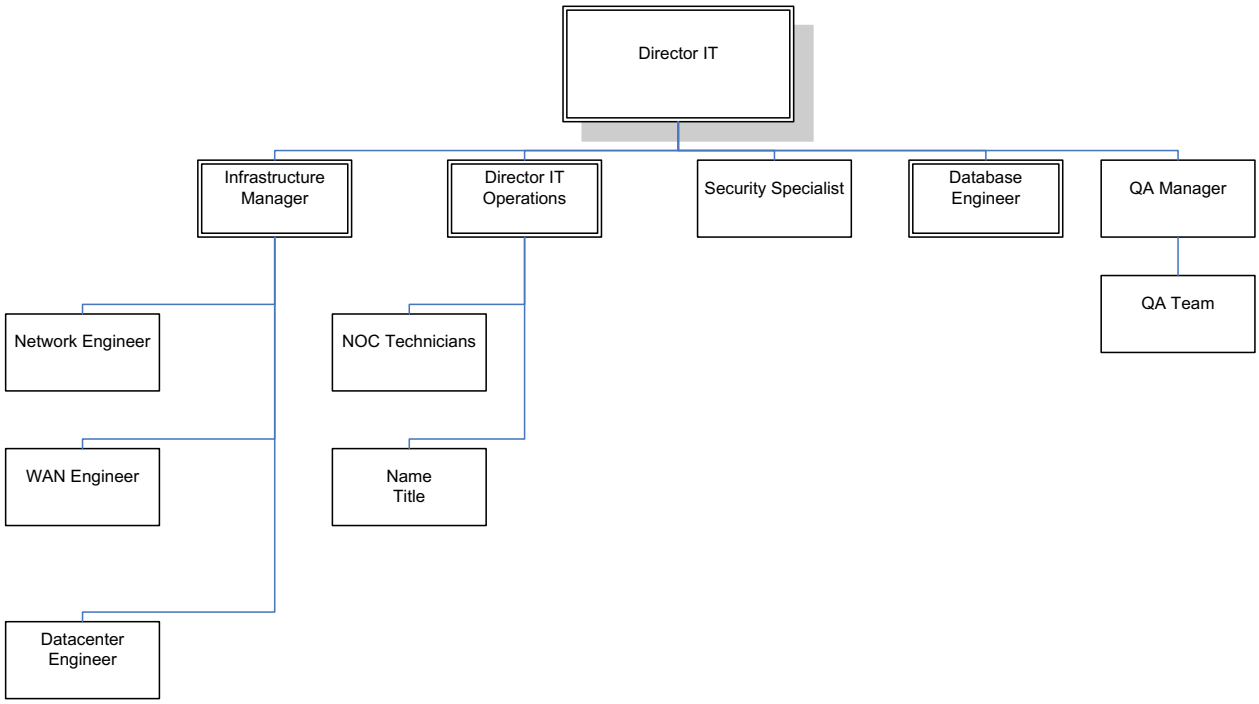
6.1. DATA CENTER OPERATIONS

6.1.1. SERVICE DELIVERY ARRANGEMENT

A datacenter will need to be constructed. Once a suitable building is identified all renovation will need to be done to provide a secure, environmentally adequate facility.

The data center will operate on a 24x7 basis since a prime objective of this project is that the Providers be able to access the NHIA central computers. The delivery of these services will need to meet the Output requirements defined Datacenter Construction and Datacenter Operation found in Section 2.4.1.

Staffing



6.1.2. NETWORK OPERATIONS CENTER (NOC)

NOC Technicians

The NOC is the core support for all technical operations. The NOC Technician serves as the point of contact on all technical issues regarding the NHIA Data Center operations. Their responsibilities include:

- Application and systems monitoring, administration, and daily operations of production infrastructure for server, storage, applications, facilities (including data center) and network infrastructure.
- Respond and diagnosis problems. Includes problem recognition, research isolation, escalation, and resolution steps.
- Manage SLA level escalations

- Identify critical issues through event correlation
- Initiate Critical Incident Response Team to critical events identified
- Documentation of issues related to outages, and reported problems with releases and configurations.
- Provide to end users training and guidance in the use of hosted applications
  Performs other duties as requested

Network Engineer

The primary responsibilities of the Network Engineer will be the diagnosis of network infrastructure and system configuration problems and their resolution. They will apply firmware updates after approval by the QA department and perform routine maintenance on network systems. They will work with the NOC Technicians in communicating with customers on the status of problem resolution.

Additional responsibilities will require running diagnostics and other key performance indicators on all network connected devices. They will mentor other Data Center and NOC personnel in advancing their skills on networks.

- Design and Install new LAN/WAN network infrastructure
- Level 2 support for Data Center and Customer network problems
- Analyze network statistics to identify potential future problems
- Work closely with the Security Specialist on policies and procedures to ensure the Data Center and Provider's networks
- Assist in coordination of data center tasks and resolving network repairs tickets
- Understand and debug network related issues on network hardware and OS
- Resolve technical challenges of managing networks in multiple geographical locations
- Develop and maintain network automation and installation tools
- Create documentation to streamline and improve upon data center best practices
- Identify opportunities for process improvement, plan, and implement changes.
- Performs other duties as requested

Data center Engineer

The primary responsibilities will be the diagnosis of server infrastructure and system OS problems and their resolution. They will apply OS patches after approval by the QA department and perform routine maintenance on systems. You will work with the NOC Technicians in communicating with customers on the status of problem resolution.

Additional responsibilities will require running diagnostics and other key performance indicators.

- Install new servers, switches, routers, and storage hardware
- Assist in coordination of data center tasks and resolving machine repairs tickets
- Understand and debug network related issues on network hardware and OS
- Resolve technical challenges of managing servers in multiple geographical locations
- Develop and maintain server automation and installation tools
- Create documentation to streamline and improve upon data center best practices

- Identify opportunities for process improvement, plan, and implement changes.
- Performs other duties as requested

Security Architect

The Security Architect leads the support, development and implementation of best practices for the secure operation of the data center, computer systems, servers and network connections. This person is responsible for providing a timely response and resolution for security breaches and vulnerability issues. This includes advanced analysis of server and firewall logs, scrutinizing network traffic, establishing and updating virus scans, troubleshooting and conducting user activity audits where required.

This position operates at a higher level than a Security Administrator due to specific and verifiable expertise in helping to create network and enterprise-wide security solutions.

Responsibilities

- Familiarity with multi-platform environments and their operational/security considerations
- Serves as lead technical expert in the overall analysis, design, implementation, monitoring and support of an enterprise-wide technical architecture focusing on information security
- Conducts analysis of critical information security systems, network architectures and infrastructures to detect information security deficiencies and provide resolution to complex problems
- Provide innovative solutions to automate other security administration and access control tasks
- Research, design, implement and support network security solutions
- Evaluates future security requirements and develops and recommends technical and operational solutions accordingly
- Administrator of TCP/IP, Load Balancers, network security & authentication protocols, network and security management tools and techniques
- Conforms to all change control procedures, and to Policies, Procedures, Guidelines, and Standards for all network security changes
- Research and maintains advanced level of knowledge on current and future IT security solutions
- Maintain enterprise network model and industry best practices
- Mentor less experienced personnel

Data Center Manager

Responsibilities

- Supervises, selects, develops, trains, and evaluates Database, Systems and Storage Area Network staff
- Mentors and coaches team members in order to retain and rapidly develop staff capacity
- Manages the development, deployment, monitoring, maintenance, upgrade, and support of all information technology systems, including servers, database, storage area network, operating systems, hardware, software, and peripherals

- Reviews, develops, documents, and implements policies, procedures, and best practices for the data center
- Ensures sound ITIL management practices for IT hardware, software, and equipment
- Performs research on potential technology solutions and writes requests for proposals in support of procurement efforts
- Plans employee training sessions on new and existing hardware and software components
- Maintains current knowledge and understanding of regulations, industry trends, current practices, new developments, and applicable laws regarding data center management
- Oversees negotiation and administration of vendor, outsourcer, and consultant contracts and service agreements
- Manages budgets, including the forecasting, allocating, and monitoring the human, physical, and financial resources for the assigned area
- Develops measures to analyze and improve departments overall efficiency
- Performs other duties as assigned.

Oracle Database Manager

Senior Oracle Database Administrator to manage, maintain and optimize the NHIA's database services. You will be responsible for all Oracle databases deployed for claims management, membership, accounting and H/R. This position requires the commitment to provide services as needed to maintain our 24x7 environment.

***Responsibilities Include**:*

- Daily administration of Oracle databases.
- Designing and administering Oracle RAC clusters for scale and fault tolerance.
- Designing, implementing and monitoring database functionality to ensure stable environments.
- Performing database administration and management activities in a safe, recoverable and professional manner that ensures the optimal operation of all database environments.
- Staying abreast of the most current release of Oracle, including compatibility issues with operating systems, third party software and utilities.
- Identifying and initiating resolutions to user problems/concerns associated with database server equipment, both hardware and software.
- Identifying potential service level problems before they occur and notifying appropriate parties.
- Maintaining up-to-date plans for disaster recovery and fail over capabilities and test as required.
- Performing capacity monitoring and short and long-term capacity planning in collaboration with development resources, system administrators and system architects.
- Proposing solutions, identifying tools, and generating procedures to ensure an efficient, consistent repeatable environment using and deploying RDBMS software, data management tools and utilities, data warehouse and replication tools.

- Maintaining security according to best practices and generating security solutions that balance auditor requirements with user requirements.
- Participating in 24x7 on call rotation.
- Support internal customer requests in an efficient and timely manner.

Requirements

- At least 5 years of advanced operational experience as a database administrator using Oracle.
- Advanced experience designing and implementing Oracle RAC clusters using OCFS2 and ASM.
- Advanced experience with Oracle Data Guard in a RAC environment required.
- Experience working with large scale, high transaction production database environments.
- Familiarity with complex RDBMS implementations (e.g. replication, high availability, clustering, disaster recovery, snapshots).
- Excellent knowledge of SQL, SQL tuning concepts, data modeling, and other Database Developer skills.
- Experience working on Linux and Windows.
- Excellent verbal and written communication skills.
- Familiarity with shell programming in both Unix and Windows environments.
- Commitment to deadlines and willingness to meet the needs of a 24x7 environment.

QA / Release Manager

QA / Release Manager will oversee a team of testers and will work closely with full project team. They will be responsible for all quality assurance aspects of the NHIA system hardware and software infrastructure. The QA / Release Manager will certify that all changes to the operational systems have been fully tested for compliance and will issue release notices to the responsible implementation personnel for installation. They will work closely with the Security Analyst to insure that any changes meet all security requirements.

Responsibilities:

- Must be able to communicate effectively with testers, developers, managers
- Understanding of Unit, Functional, System, Performance, Technical, Operational testing and the tools utilized
- Experience with design, creation, execution, reporting of both manual and automated test cases
- Experience designing and implementing test environments (client-server, web, hardware, software, networks, databases, etc.)
- Will work closely with full project team including project management
- Will interpret functional requirements and design documents to develop appropriate test plans, test cases, and test scripts
- Will perform functional and performance testing and evaluate results
- Will record software defects in defect tracking tool and provide feedback with development team
- Will work closely with testers and with developers
- Provide project status

Required Experience:

- At least 3 years Software Testing experience as QA Manager
- Must have solid documentation skills
- Familiar with system architecture and database analysis
- Understanding of full development and testing lifecycle
- Experience with defect tracking tools
- Experience with Source Control tools

Monitoring Tools

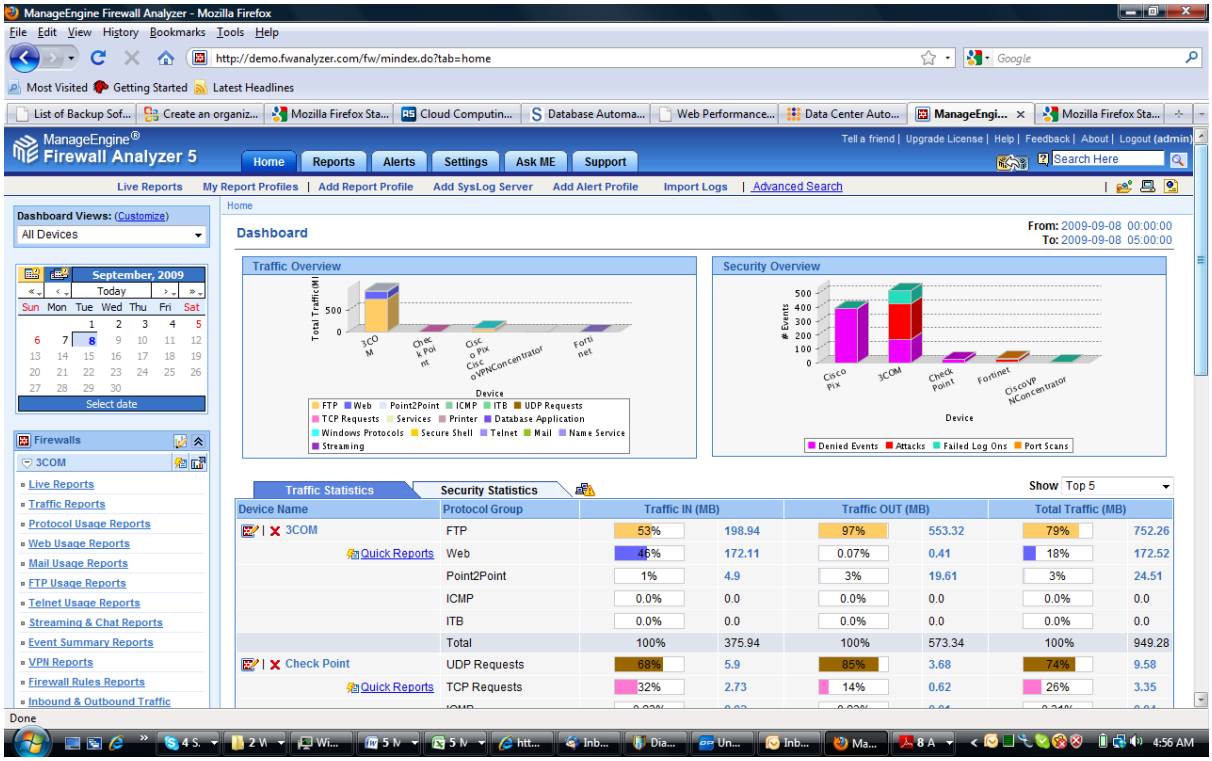
A prime need of any data center is tools to manage the infrastructure. NOC Technicians need to have efficient ways of monitoring all equipment, network performance and fault detection in order to meet SLA agreements for the center's clients.

Common concerns in Datacenter Management are:

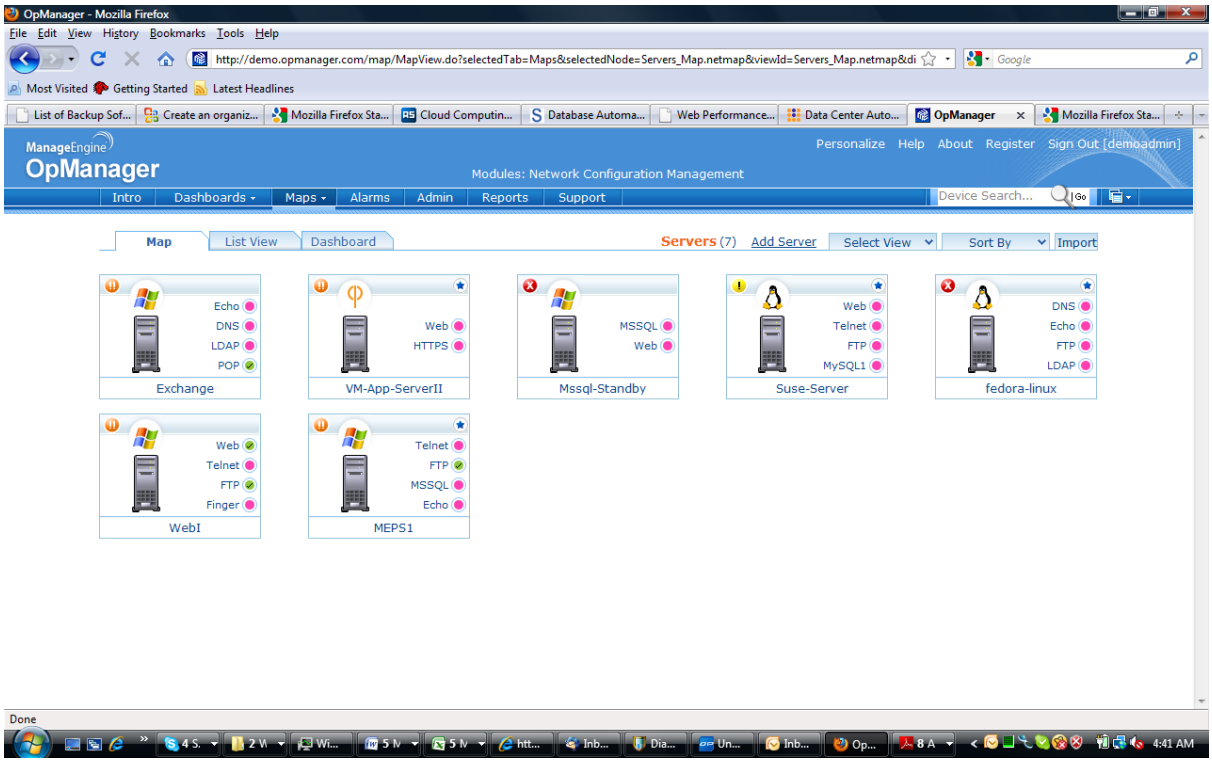
- Unavailability of Servers, Databases and Applications
- Application-level performance degradation
- Internal security breaches and unauthorized user access
- Malicious traffic, viruses and worms affecting servers
- Optimization of resource allocation

We are recommending a software suite of tools that is built around the practices identified in ITIL. The software is a complete package that allows for:

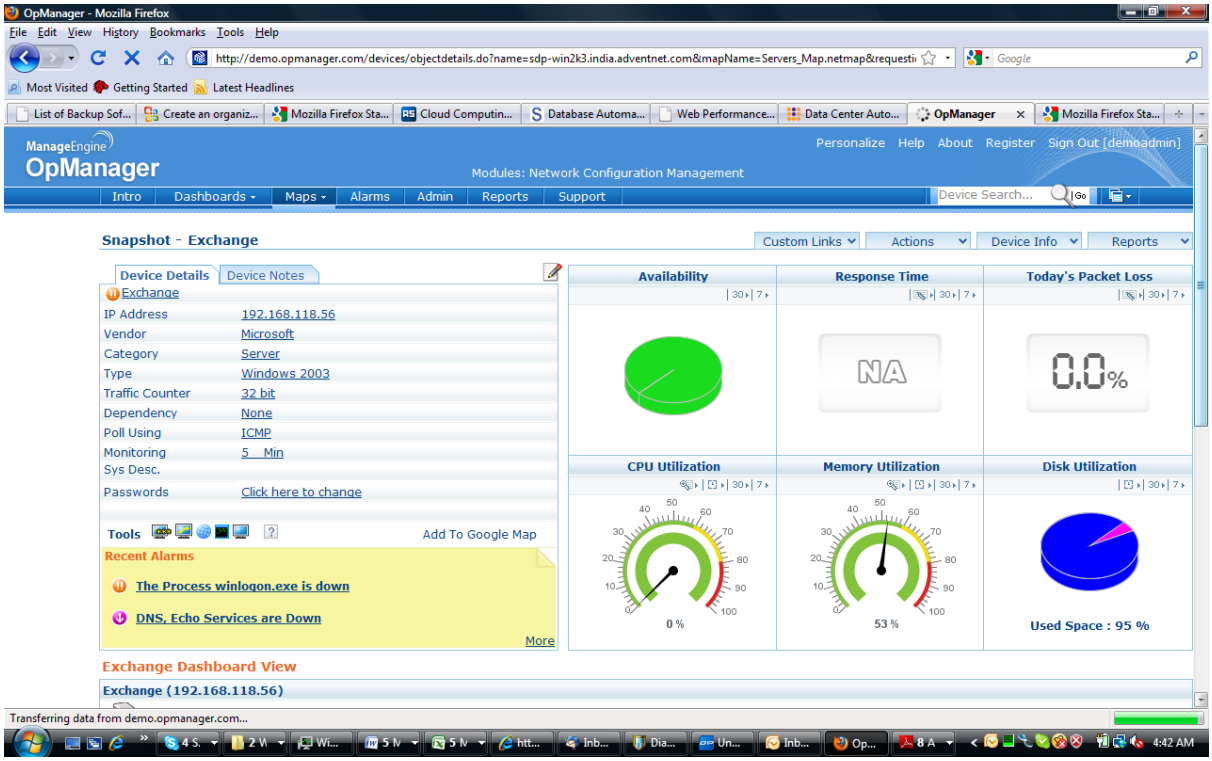
- Server CPU, Memory and Disk Utilization
- In-depth Application performance and availability management
- Management across heterogeneous databases
- Monitoring across websites and web transactions
- Service monitoring including Web Services
- Internal Security Management with Windows Eventlogs
- External traffic management with firewall analyzer
- Centralized password management including shared and service accounts , Specialized MS Exchange Server Monitoring



Firewall View



Server View

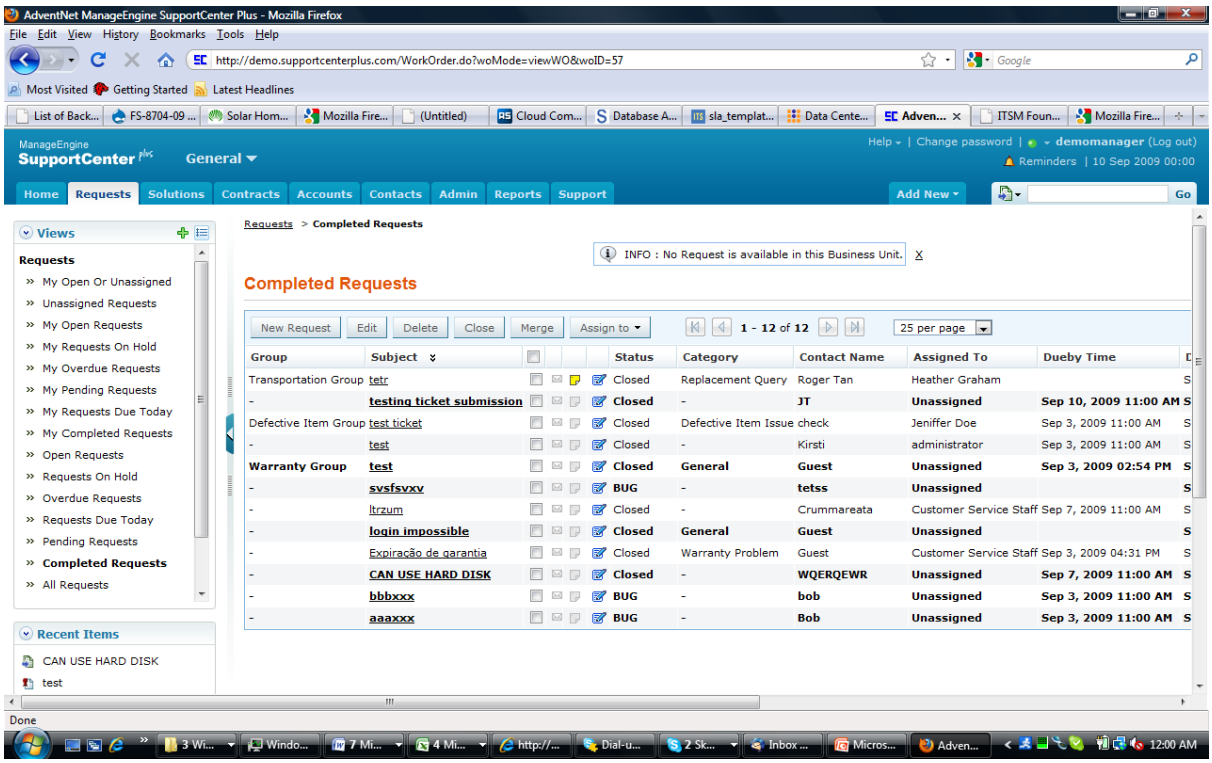


Exchange Server View

Trouble Ticketing

Critical to ITIL Service Delivery is Incident Management. The core management tool is trouble ticketing necessary to track, document and escalate issues related to SLA performance.

The ticketing product we are recommending is tightly linked with the automated monitoring functions. Detected alarms create trouble tickets which are then managed by the NOC Technicians.



SLAs with Clients

6.2. TRANSITION MANAGEMENT ISSUES

Since this project involves multiple stakeholders it will be necessary to have a joint management committee to liaison on ongoing issues once the project has gone live. This committee should be comprised of a senior representative from each of the Providers or their designated proxy. The committee should meet weekly during the first six (6) months post system activation and subsequent to that time on a monthly basis.

It is also recommended that a single source, with backup, be chosen to interact with the NHIA vendor on daily issues that may arise. This person and their backup should have the authority to act on behalf of each of the Providers on operational and maintenance issues. This liaison person shall also inform each of the management committee members on any issues that arise and should be responsible as the first escalation level of any operational problems that arise.

Change requests that arise from any of the Providers to their applications shall be brought to the joint management committee for discussion to assess the impact on the other Providers and the NHIA. A Change Request process will be defined that includes:

- Financial impact on Providers and NHIA
- Potential impact on business process changes to any of the Providers
- Priority of the change
- Impact on claims processing
- Detailed description of the changes requested
- Test plan for the changes
- Risk Mitigation Plan
- Name of the Provider representative who will serve as the Project Manager for the change

7. PROCUREMENT OPTIONS

7.1.1. POTENTIAL IMPLEMENTATION MODELS

For the purposes of this study we have looked at two models of funding for the Phase 2 implementation. These two options are:

- Build Option
    - NHIA to supply funding for application modification of Provider HIS systems.
    - Purchase and install LAN in identified Provider facilities
    - Supply WAN connectivity to the NHIA central facility from Provider locations.
    - Build primary data center and possible backup center
    - Provide continuing monitoring and training of Provider personnel
    - Hire network operations personnel
    - Create complete ICT management structure
    - Define all business processes required
    - Provide training of Provider personnel
- PPP Option
    - Procure a 5 year Build, Operate and Transfer (BOT) contract for
        - Software for HIS systems at Provider
        - Customization of HIS software to submit electronic claims and member validation
        - Install LAN at identified Provider facilities
        - Install and operate WAN connectivity to NHIA data center
        - Provide Business Process (BP) re-engineering at the Providers to improve the operations of ICT in the facility
        - Provide training of Provider personnel
        - Provide data center training and certification of NHIA personnel

7.1.2. BUILD OPTION

The financial impacts of this option are born mostly by the NHIA. The only cost transference is in the design and development of the Provider applications and the Provider side of the NHIA interface.

T/TI believes that this model could meet the goal of 60% of all claims being submitted electronically but bears significant risks as outlined below under Build Risks. These risks contain the fixed amount available under HIP of US$8,100,000. While this amount we believe sufficient to cover the needed capital costs on building out Provider locations with the needed ICT systems and the modification of the HIS application systems needed to be implemented at the Providers, we do not believe it sufficient to provide the ICT support for the Providers over a 5 year period.

7.1.2.1. FUNDING AND AFFORDABILITY

Under the Direct Funded option we believe it is possible to provide sufficient capital under the current World Bank HIP funding to install the needed ICT infrastructure and training to implement Providers systems to reach at least 60% of the claims being submitted electronically under Phase 2. There are significant risks under this option. These risks are discussed in the Build Risks section below.

In order to support the operational expense of this option the MoH will have to secure funding to allow for the budgeting of ICT staff not currently covered in their budget as well as WAN connectivity costs.

Upfront and short term capital items include:

- Office PCs and other peripherals for all of the included Providers
- PC Operating Systems (OS)
- PC Anti-virus software
- WAN development to connection for all included Providers
- Servers, routers, and firewalls for Providers
- Purchase costs of Provider HIS applications
- Customization costs of Provider HIS applications
- Provider employee training under private contract on using the claims portions of the HIS applications and PC use
- NHIA Application modification for NHIA to Provider Interface

Much of the CAPEX costs for significant implementation can be covered out of HIP funds. The funds however do not cover the continuing operation of installed Provider HIS systems. As mentioned at numerous areas of this report it is critical the MoH begin to include ICT budgeting in their overall budgets and those of their agencies. A Build option is not sustainable without this.

MoH funds will also be required for other capital expenditures dealing with business process improvement. Since the HIP funds cannot be expected to fund HIS systems for all of the Government medical facilities it will be the Ministry's responsibility to secure additional funding for future implementations.

For the purpose of this study we are assuming the following number of hospitals will be implemented over a 5 year period:

- Large Facilities 8
- Medium Facilities 149
- Small Facilities 50

These figures do not include Health Providers that already have HIS systems installed. These facilities will need to be considered on one-by-one basis to see what if any financial assistance will be required to modify the installed HIS software to submit electronic claims.

The following worksheet shows the capital and operating expenditures needed to implement this solution. We have included data center costs for MHIA reference only to compare to their already budgeted data center. The data center costs are also included to allow comparison between the Build vs PPP models. The estimated 5 year CAPEX cost is $11,608,360. The first year CAPEX primarily for large hospitals and interfaces is $2,216,755.

	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5	5-Year Total
TOTAL OPEX						
Small Hospital	$4,412	$29,781	$104,670	$229,111	$544,284	$912,258
Medium Hospital	$135,956	$721,230	$1,419,348	$2,095,716	$2,772,084	$7,144,334
Large Hospital	$523,800	$838,080	$838,080	$838,080	$838,080	$3,876,120
Regional ICT	$99,840	$199,680	$238,560	$238,560	$238,560	$1,015,200
SUB-TOTAL OPEX	$764,008	$1,788,771	$2,600,658	$3,401,467	$4,393,008	$12,947,912
TOTAL CAPEX						
Small Hospital	$29,885	$81,105	$162,210	$405,525	$675,875	$1,354,600
Medium Hospital	$1,030,540	$2,000,460	$2,000,460	$2,000,460	$2,000,460	$9,032,380
Large Hospital	$943,980	$0	$0	$0	$0	$943,980
Regional ICT	$47,350	$47,350	$16,200	$1,500	$0	$112,400
Interface Central System	$65,000	$0	$0	$0	$0	$65,000
Interface 5 HIS Systems	$100,000	$0	$0	$0	$0	$100,000
SUB-TOTAL CAPEX	$2,216,755	$2,128,915	$2,178,870	$2,407,485	$2,676,335	$11,608,360
TOTAL CONSOLIDATED EXPENSE	$2,980,763	$3,917,686	$4,779,528	$5,808,952	$7,069,343	$24,556,272
Datacenter OPEX	$478,968	$478,968	$478,968	$478,968	$478,968	$2,394,840
Datacenter CAPEX	$673,000	$0	$0	$0	$0	$673,000
Sub-total Data Center	$1,151,968	$478,968	$478,968	$478,968	$478,968	$3,067,840
TOTAL COST	**$4,132,731**	**$4,396,654**	**$5,258,496**	**$6,287,920**	**$7,548,311**	**$27,624,112**

Attached please find a full detailed Build XLS file

As mentioned, the largest financial risk of the Build Option is the continuing support of the operational costs over a 5 year period. We estimate that the operational costs over 5 years to be $12,947,912 with $764,008 needed for the first year of operation. This includes support for the proposed Regional Network Management proposed to service systems at regional and district hospitals. Currently the MoH does not have any item in their budgets to pay for ICT staff and equipment. Without the ability to employee the needed technical and ICT management staff any system installed under the Build Option will fail over time.

The operational costs over a 5 year period include staffing to meet what we believe to be a minimal support staffing requirement to make Phase 2 a success. The Operational costs include:

- 24x7 Network Operations Center (NOC) staffing or private party contract for Provider ICT. This is for all ICT related issues not directly related to the NHIA.
- Annual Provider application software maintenance
- Help Desk personnel
- GHS regional and district ICT personnel and their support costs
- Teaching, Military and Police Hospitals ICT staff
- Spare parts and cost of repairs
- Fuel for backup power generation at all facilities
- Communications costs

- Transportation costs
- Software renewal licenses
- Office supplies

7.1.2.2. BUILD RISKS

These risks include:

Risk ID	Risk	NHIA	Provider	Risk Level	Mitigation
1	**Change Management**			**H**	**Develop and implement a strong Change Management Plan**
1.a	Leadership does not demonstrate commitment in both word and action.	X	X		· Work with leaders to ensure a clear understanding of the goal.
					· Develop clear messages to be used by leadership to ensure consistency.
1.b	Change is treated as an option.	X	X	H	· Change must be mandated from the top down.
					· Clear guidelines regarding when and how the change will be implemented must be communicated.
1.c	Making changes unilaterally.	X	X	H	· Conduct outreach to ensure those affected provide insight and input on the proposed change.
1.d	Not providing incentives for change.	X	X	H	· Develop incentives for each population affected by the change. They can be positive or negative:
					o Paper bills get put at the back of the reimbursement pile.
					o Automated claims are processed within 30 days or you automatically receive 40% of the billed amount.
1.e	The project is implemented and there is no follow-up or assessment completed.	X	X	M	Once the project is implemented, follow-up should be conducted to make any modifications to the process and procedures that may be needed.

1.f	Contract Negotiation and Compliance Management	X		H	Past software purchasing projects, which the Government has done have proven to be problematic. In our opinion the Government does not have the expertise necessary to negotiate software development contracts and compliance.
1.g	Project Management	X		H	Projects of this size and scope require professional Project Management personnel. There are currently no visible HR resources, available on the full-time basis. Contract of hiring of a PM will be required.
2	**Business Process**	**X**	**X**	**H**	**Develop an end-to-end business process which includes:**
					· **Task**
					· **Responsibility**
					· **Output**
					· **Timeframe**
2.a	There are no clear business processes guiding people on how to do their jobs resulting in inconsistencies and misunderstandings.	X	X	H	Develop clearly defined and documented processes for each step within the overall process.
2.b	Processes are implemented without clearly defined roles, responsibilities and accountabilities.	X	X	M	Ensure that roles and responsibilities are documented and communicated.2
2.c	Leadership does not endorse and support the implementation of new processes.	X	X	H	Ensure management understands the changes being implemented and has the knowledge and tools to support the implementation.
3	**Organizational Structure**	**X**	**X**	**M**	**Develop and implement an organizational structure that supports the implementation of the new process including:**
					· **Reporting structure**
					· **Staffing**
3.a	The reporting structure does not support the new process.	X	X	M	Develop and implement a reporting structure that supports the process not the personal wants of individuals.

3.b	Staffing levels do not support the process.	X	X	M	Develop a staffing model which ensures sufficient levels of staffing and allows staff to become proficient in their responsibilities.
3.c	Roles and responsibilities are not clear.	X	X	H	Develop job descriptions for each position including: · Role · Responsibilities · Minimum skill set required
3.d	Employees do not have the skills necessary to perform their jobs.	X	X	H	Conduct a skills assessment of existing personnel and develop training and mentoring programs to bring skills up to minimum levels where possible. When hiring new employees ensure that they have the minimum skills identified in the job description.
4	**Training**	**X**	**X**	**H**	**Develop training program that ensure employees have the knowledge and skills required to perform their jobs.**
4.a	Training programs are not designed to support the various needs of the individuals and entities being trained.			H	Conduct a needs assessment of entities and individuals to determine the most effective way to develop and deliver training programs.
4.b	Training staff is not sufficiently prepared to conduct training.			M	Develop Train-the-Trainer materials and provide extensive training and support to the trainers.
4.c	Employees do not have the tools they need to help them as they begin using the new processes and procedures.			M	Develop quick reference tools and implement support to ensure employees have the tools they need to perform their jobs.
5	**Monitoring**			**M**	**Develop processes and procedures for ongoing monitoring of the new End-to-End process**
5.a	The process will be implemented and no one will follow up on what is working and what is not working.			M	Develop a comprehensive monitoring plan to evaluate processes and procedures on an ongoing basis, including review and approval of recommended changes and revisions, testing and implementation.
6	**Technical**			**H**	

6.a	Data Center Operations not under control of NHIA	X		H	Develop plan of action to move operations to control of NHIA. Second stage is to move the data center from STL's premises
6.b	Untested Disaster Recovery Plan	X		H	NHIA personnel install and test completely the current disaster recovery plan. Verify that plan documentation is complete. Verify backup logs on a regular basis.
6.c	No formal IT Enterprise Management	X		M	Develop ITIL based ICT management plan.
6.d	No Security Plan	X	X	H	Develop security plan and audit existing system
6.d.1	Lack of penetration testing	X	X	M	Immediate penetration testing of system from Scheme and current Provider sites
6.d.3	No Use Policies	X	X	M	Develop Acceptable Use Policies for all users
6.e	Poor Quality Assurance	X	X	M	Institute a formal Quality Assurance process under ITIL guidelines
6.f	Lack of an enforceable SLA Agreement	X	X	H	While Data Center is located on STL premises and under their operation modify penalties to be significant.
6.g	Acceptance Tests for WAN	X		H	Immediately perform professional acceptance testing of complete WAN network
6.h	No Design Requirements for WAN vs. NHIS Application	X		M	As part of WAN acceptance testing assure that the WAN capacity is adequate to perform NHIS applications
6.i	Quality of Installed Network	X		M	Perform professional review of quality and capacity of existing WAN and LAN networks
6.j	Unavailable System Documentation	X		M	Request formal documentation on system documents required for a ITIL operations model.
6.k	Proposed scan enabled forms	X		M	Validate and modify existing scanning implementation plan. See details below.
6.l	Provider based Hospital Information Systems (HIS)	X		M	Select a Hospital Information System to be used at providers. Work in conjunction with stakeholders to develop a complete project implementation plan.

6.m	System Requirements Definition	X	X	M	The expectation exists that the definition of required outputs for the Phase 2 project be more focused on the usability issues as well as completeness of the outputs expected.
6.n	Delivery	X	X	M	It is important that the any purchase contract contain penalty clauses that reflect the cost to Government due to any late delivery. The penalty should be substantial escalating based on the length of the delay.
6.o	Skilled ICT technical personnel H/R risk	X	X	H	Should the agency attempt to train existing personnel to raise their competency it is likely that they trained personnel will leave once the training is completed to join the private sector.
7	**Provider ICT Infrastructure**	**X**		**M**	**Implement a comprehensive ICT Infrastructure at the provider end**
7.a	Lack of a Local Area Network		X	H	Support the creation of a LAN for Hospitals to enable an effective use of the system.
7.b	Lack of Ownership of ICT Infrastructure at Provider site		X	H	Providers should own the local systems. They should have a budget for the maintenance of the systems in their facilities.
7.c	No Incentive to use the system		X	H	Integrate the NHIA systems to a Hospital Management System that is found useful for the facility.
7.d	Inadequate monitoring of WAN and LAN equipments	X	X	M	An effective monitoring mechanism should be established to facilitate the incident resolution process. An SMS base monitoring to assist local administrators to identify issues with the network.
7.e	Inadequate basic computer skills		X	H	A more effective ICT training may be necessary to ensure proper use of the system.
7.f	Continuous Link downtime affecting claims submission	X	X	M	The use of a SSL VPN should be considered instead of an IPSec VPN.

7.g	More hands required at the MIS dept		X	H	Providers should be encouraged to recruit more MIS personnel. All a third party IT Maintenance company should be engaged to provide additional help in solving basic problems.
8	**Provider HR and Training**	X	X	M	
8.a	Lack of basic computer skills		X	M	Provide on-site classes in basic skills
8.b	Sufficient training in application use		X	M	Provide on-site classes in each departments application use skills
8.c	Lack of trained ICT personnel		X	H	Develop a ICT technical management plan that includes all providers and schemes.
8.d	Lack of job requirements for claims personnel		X	M	Develop a job description including job requirements for each person involved at provider and scheme location in claims submission
8.e	Lack of job requirements for ICT personnel		X	M	Develop job descriptions for each defined ICT position at providers and schemes and validate existing personnel to those requirements. Develop plan to assist existing personnel in reaching those skill levels.
9	**Financial**	X	X	H	
9.a	Lack of ICT in budgets of GHS and other MoH reports		X	H	MoH must added line items for Provider ICT capital and operational costs
9.b	Lack of sufficient ICT operational budgets for CHAG facilities		X	M	Review with CHAG current ICT budgets and assist where possible in funding the budgets.
9.c	HIP funds insufficient to implement Provider systems	X	X	M	Find additional funding.

- Contract Negotiation and Compliance Management – Past software purchasing projects, which the Government has done have proven to be problematic. In our opinion the Government does not have the expertise necessary to negotiate software development contracts and compliance. Legal assistance from lawyers familiar with ICT contract law will need to be hired.

- Project Management – Projects of this size and scope require professional Project Management personnel. There are currently no visible HR resources, available on the full-time basis, which would be capable of managing a project of this size.

- System Requirements Definition – The Gap Analysis portion of this study identified shortfalls in the Phase 1 NHIS system that indicate that the requirements for the

system were not sufficient in their mitigation of the risks associated with the development of a systems of this size and scope. The concern exists that the definition of required outputs for the Phase 2 project be more focused on the usability issues as well as completeness of the outputs expected.

- Quality Assurance – Previous attempts to develop NHIS systems have suffered from a lack of through quality assurance. Part of this is due to the lack of specialized and trained QA engineers. The lack of knowledge of the QA process has led to systems that have been prone to failure, lacked required functionality and have performed below acceptable levels of responsiveness.

- Delivery – It is important that the any purchase contract contain penalty clauses that reflect the cost to Government due to any late delivery. The penalty should be substantial escalating based on the length of the delay.

- Skilled ICT technical personnel H/R risk based on pay scale differences between the Public and Private sectors in Ghana. Should the agency attempt to train existing personnel to raise their competency it is likely that they trained personnel will leave once the training is completed to join the private sector.

- Skilled data center staff – Currently there does not exist in the Government skills to operate and manage a data center. The center that will house all of the systems necessary to operate the applications will require, certified engineers to staff the Network Operation Center 24x7, a security specialist and a infrastructure management specialist at a minimum. Automated monitoring and trouble ticket systems will also be required.

- Funding - There does not appear that there is sufficient funding for this project within the MoH and NHIA at this time. It is possible we believe that there is sufficient funding to cover sufficient capital costs of the project but not the recurring operational costs. Any attempt to fund this project through existing budgets contains substantial risks.

Evaluation Summary

The following is a summary of the evaluation criteria for the Build Option:

- Technical Outputs - The Build Option meets all of the technical requirements
- Operation Outputs – This Option meets all of the operational requirements
- Time to delivery –The time to delivery assumes each of the HIS systems developers and STL will work full time on the interface integration and has been estimated at 6 months.
- Delivery Risk – The Delivery Risk rests with the Government and the vendor. The vendor will expect to be paid on an agreed to deliverables schedule. This means that at milestones in the project the Government will be expected to pay monies for work already completed. Since final acceptance and stress testing cannot be assured until the complete system is delivered it is possible that upon final delivery the system does not meet the performance requirements.
- Market or Government Funding Risk – Since this is a Build solution all costs for the

system are born by the Government. The total cost is low to medium and has the low risk that the Government lacks funds for the capital expenditure required. In addition this option requires continuing costs associated with software maintenance programmers and license fees, ICT infrastructure monitoring and maintenance.

- HR Risk – There is substantial HR risks involved in this option. The Government does not have today the technical and project management expertise necessary to have the project succeed. The Government also lacks the Quality Assurance and Change Management professionals needed to assure a reliable system. The Government pay scales prohibit the hiring of these professionals. Should the Government choose to try and train the required personnel there is considerable risk that once trained they will leave for jobs in the private sector.
- Political Risk – Political risks exist should the Phase 2 project fall behind schedule or not fulfill its objectives.
- Government Development and Infrastructure 5 Year Operational Costs $12,947.912.

7.1.3. PPP OPTION

An alternative to the traditional procurement model exists within the Phase 2 project to fund it out of a Public Private Partnership (PPP) model. There exists in Ghana the use of PPPs to develop total solutions for Government agencies which are paid for out of use fees or other repayment methods over an extended time.

We believe there that a PPP model could be used for the Phase 2 objectives and would transfer substantial risk from the NHIA/NHIS to the private partner. Initial capital investments as well as operational costs are paid by the private partner with compensation coming over a longer period of operation.

A well implemented Build, Operate and Transfer (BOT) model would work for the implementation of Phase 2. This model would be based on a percentage of each electronic claim being paid into a repayment fund for the Private Partner. The Private Partner would submit invoices to this special payment fund for all deliverables and maintenance items upon acceptance by the Government of the deliverable.

We believe that this type of PPP should be implemented by the MoH and not the NHIA directly. The reason behind this recommendation is that the proposed Phase 2 systems deliver more value to the MoH's facilities than just member validation and electronic claims submission. The ability for the MoH to bring full HIS capabilities to their facilities, that not only improves the operational aspects of the facility but provides timely statistical health information to the Ministry, adds significant value to MoH operations.

Having the project under the MoH removes the inter-agency issues between the NHIA/NHIS and the Ministry's other agencies. Given the reporting structure of the MoH, GHS hospitals, teaching hospitals, and other hospitals reporting directly to the MoH would be managed by the MoH with NHIA providing assistance with using the HIP funds as partial funding of the PPP repayment fund as a key element.

This option enhances the projects that GHS already has underway of installing HIS systems at it's facilities and assists them in the continuing support of these systems. The responsibility for the implementation of the systems would be under the oversight of the MoH and would mitigate the need for the NHIA to establish staffing required for the support of the Providers

infrastructure and applications.

Should it be decided that a PPP option is to be used; the MoH will need to secure the services of a Transaction Advisor to assist in the creation of a full PPP financial analysis, tender creation, bid evaluation assistance and contract negotiations. The complexity of such a financial analysis is beyond the scope of the current study. There exists precedence for this type of PPP arrangement in Ghana for the development of complete systems and their operation for MDAs.

7.1.3.1. FUNDING AND AFFORDABILITY

A recent single PPP arrangement for the revenue agencies MDAs and the Registrar General provide precedence for a PPP arrangement. Under the Revenue Agencies PPP the funding came in the form of increased revenues as the result of new systems and business process improvement in the agencies developed by the Private Partner. The repayment model was based on the Private Partner invoicing a special fund which contained increased revenue collections above the 5 year trend of each agency. The Private Partner will be compensated only for delivered services and not for any windfall revenues above their invoiced amounts.

Government financial risk under a PPP model is significantly reduced since the Private Partner is responsible for capital investment and operational costs over the Operational Period. In the case of this PPP, compensation to the Private Partner would be tied to the number of electronic claims submitted from HIS systems that they were responsible for implementing. Until there is are substantial number of electronic claims being submitted the Private Partner receives limited compensation. The success of the implementation is directly tied to the compensation thereby reducing the Government risks.

Of important note is the linkage between VAT and NHIL. Due to the Revenue Agencies PPP implementation it is expected that collections will be significantly increased. Because of the NHIL linkage it can also reasonably be expected that the NHIL will increase. This increase in revenues has the ability to fund a PPP with monies left over to support the NHIS. It is our preliminary estimate that a 1% increase in the NHIL receipts would cover the full operational costs of Phase 2 into the future. Without full access to NHIL revenues it was not possible to validate this premise. A complete analysis will need to be part of a Transaction Advisor tender to study a PPP implementation.

Further study of a PPP option is beyond the scope of this study. We recommend that if this model is to be evaluated it will be necessary to contract a Transaction Advisor familiar with PPPs for Government services and applications.

We would recommend that the current total HIP budget be allocated to the PPP model. These funds could be used as incentives to the Private Partner under such a plan. Again there exists precedence for the use of World Bank funds in this way in Ghana.

7.1.3.2. FINANCIAL IMPACTS

The financial impacts of the chosen PPP option are born mostly by the Private Partner. The Government costs are associated with the supplying of personnel in the system design stage,

evaluation of bids, contract negotiation, contract legal services and system acceptance. Upfront and short term capital items include:

- Contracted professional Project Manager
- Agency personnel available on an as needed basis during various phases
- Outside legal counsel experienced in IT contract law. Can be included in Transaction Advisor tender deliverables.
- Supplying needed datacenter infrastructure and operational staff once the transfer of ownership is made to the Government. This is post 5 year period and therefore not include in the 5 year cost to the Government.

The following worksheet shows the capital and 5 year operational expenditures need to implement this solution under a PPP:

	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5	5-Year Total
TOTAL OPEX						
Small Hospital	$2,340	$29,781	$104,670	$229,111	$544,284	$910,186
Medium Hospital	$68,470	$363,225	$693,885	$1,024,545	$1,355,205	$3,505,330
Large Hospital	$297,000	$475,200	$475,200	$475,200	$475,200	$2,197,800
Regional ICT	$6,000	$6,000	$224,640	$235,152	$235,584	$707,376
SUB-TOTAL OPEX	$373,810	$874,206	$1,498,395	$1,964,008	$2,610,273	$7,320,692
TOTAL CAPEX						
Small Hospital	$0	$0	$0	$0	$0	$0
Medium Hospital	$0	$0	$0	$0	$0	$0
Large Hospital	$0	$0	$0	$0	$0	$0
Regional ICT	$0	$0	$0	$0	$0	$0
Interface Central System	$65,000	$0	$0	$0	$0	$65,000
Interface 5 HIS Systems	$100,000	$0	$0	$0	$0	$100,000
SUB-TOTAL CAPEX	$165,000	$0	$0	$0	$0	$165,000
TOTAL CONSOLIDATED EXPENSE	$538,810	$874,206	$1,498,395	$1,964,008	$2,610,273	$7,485,692
Datacenter OPEX	$100,800	$100,800	$72,000	$72,000	$72,000	$417,600
Datacenter CAPEX	$673,000	$0	$0	$0	$0	$673,000
Sub-total Data Center	$773,800	$100,800	$72,000	$72,000	$72,000	$1,090,600
TOTAL COST	**$1,312,610**	**$975,006**	**$1,570,395**	**$2,036,008**	**$2,682,273**	**$8,576,292**

Attached please find a full detailed PPP XLS file

The Operational costs for the PPP option are:

- WAN Communications costs Project Manager
- Quality Assurance Team
- Help Desk Personnel
- Training of new employees
- Post Transfer costs:
    - Possible application software maintenance contracts
    - ICT Support personnel
    - Infrastructure management personnel capable of administering systems using ITIL based methods
    - Software renewal licenses
    - ICT equipment maintenance

For the purpose of this study we are assuming the following number of hospitals will be implemented over a 5 year period:

- Large Facilities 8
- Medium Facilities 149
- Small Facilities 50

These figures do not include Health Providers that already have HIS systems installed. These facilities will need to be considered on one-by-one basis to see what if any financial assistance will be required to modify the installed HIS software to submit electronic claims.

Based on a PPP model we estimate the capital costs over a 5 year period to be $165,000 used to fund the development of the HIS to NHIA interface. This would be eliminated should the NHIA decide to have the Private Partner perform these tasks.

5 year operational expenses to the Government are estimated at $7,320.692. It is possible to include the connectivity costs into a possible PPP solution there by reducing the Government's direct costs.

7.1.3.3. RISKS

These risks include:

Risk ID	Risk	NHIA	Provider	Risk Level	Mitigation
1	**Change Management**			**H**	**Develop and implement a strong Change Management Plan**
1.a	Leadership does not demonstrate commitment in both word and action.	X	X		· Work with leaders to ensure a clear understanding of the goal.
					· Develop clear messages to be used by leadership to ensure consistency.
1.b	Change is treated as an option.	X	X	H	· Change must be mandated from the top down.
					· Clear guidelines regarding when and how the change will be implemented must be communicated.
1.c	Making changes unilaterally.	X	X	H	· Conduct outreach to ensure those affected provide insight and input on the proposed change.
1.d	Not providing incentives for change.	X	X	H	· Develop incentives for each population affected by the change. They can be positive or negative:

					o Paper bills get put at the back of the reimbursement pile.
					o Automated claims are processed within 30 days or you automatically receive 40% of the billed amount.
1.e	The project is implemented and there is no follow-up or assessment completed.	X	X	M	Once the project is implemented, follow-up should be conducted to make any modifications to the process and procedures that may be needed.
1.f	Contract Negotiation and Compliance Management	X		H	Government will need professional Transaction Advisor for PPP bidding
1.g	Project Management	X		H	Projects of this size and scope require professional Project Management personnel. There are currently no visible HR resources, available on the full-time basis. Contract of hiring of a PM will be required.
2	**Business Process**	**X**	**X**	**H**	**Develop an end-to-end business process which includes:**
					· **Task**
					· **Responsibility**
					· **Output**
					· **Timeframe**
2.a	There are no clear business processes guiding people on how to do their jobs resulting in inconsistencies and misunderstandings.	X	X	H	Private Partner responsible for Business Process Re-engineering.
2.b	Processes are implemented without clearly defined roles, responsibilities and accountabilities.	X	X	M	Private Partner responsible for Business Process Re-engineering.
2.c	Leadership does not endorse and support the implementation of new processes.	X	X	H	Ensure management understands the changes being implemented and has the knowledge and tools to support the implementation.
3	**Organizational Structure**	**X**	**X**	**M**	**Develop and implement an organizational structure that supports the implementation of the new process including:**

					· **Reporting structure** · **Staffing**
3.a	The reporting structure does not support the new process.	X	X	M	Develop and implement a reporting structure that supports the process not the personal wants of individuals.
3.b	Staffing levels do not support the process.	X	X	M	Private Partner responsible for Business Process Re-engineering.
3.c	Roles and responsibilities are not clear.	X	X	H	Private Partner responsible for developing job descriptions for each position including: · Role · Responsibilities · Minimum skill set required
3.d	Employees do not have the skills necessary to perform their jobs.	X	X	H	Private Partner responsible for conducting a skills assessment of existing personnel and develop training and mentoring programs to bring skills up to minimum levels where possible. When hiring new employees ensure that they have the minimum skills identified in the job description.
4	**Training**	**X**	**X**	**H**	**Develop training program that ensure employees have the knowledge and skills required to perform their jobs.**
4.a	Training programs are not designed to support the various needs of the individuals and entities being trained.			H	Private Partner responsible for conducting a needs assessment of entities and individuals to determine the most effective way to develop and deliver training programs.
4.b	Training staff is not sufficiently prepared to conduct training.			M	Private Partner responsible for developing Train-the-Trainer materials and provide extensive training and support to the trainers.
4.c	Employees do not have the tools they need to help them as they begin using the new processes and procedures.			M	Private Partner responsible for developing quick reference tools and implements support to ensure employees have the tools they need to perform their jobs.
5	**Monitoring**			**M**	**Develop processes and procedures for ongoing monitoring of the new End-to-**

					End process
5.a	The process will be implemented and no one will follow up on what is working and what is not working.			M	Private Partner responsible for developing a comprehensive monitoring plan to evaluate processes and procedures on an ongoing basis, including review and approval of recommended changes and revisions, testing and implementation.
6	**Technical**			**H**	
6.a	Data Center Operations not under control of NHIA	X		H	Private Partner responsible for developing plan of action to move operations to control of NHIA data center.
6.b	Untested Disaster Recovery Plan	X		H	Private Partner responsible for to install and test completely the current disaster recover plan. Verify that plan documentation is complete. Verify backup logs on a regular basis. Manage DRP
6.c	No formal IT Enterprise Management	X		M	Private Partner responsible for developing ITIL based ICT management plan.
6.d	No Security Plan	X	X	H	Private Partner responsible for developing security plan and audit existing system
6.d.1	Lack of penetration testing	X	X	M	Private Partner responsible for immediate penetration testing of system from Scheme and current Provider sites
6.d.2	No Use Policies	X	X	M	Private Partner responsible for developing Acceptable Use Policies for all users
6.e	Poor Quality Assurance	X	X	M	Private Partner responsible for instituting a formal Quality Assurance process under ITIL guidelines
6.f	Lack of an enforceable SLA Agreement	X	X	H	Private Partner responsible for developing SLA agreements with customers (Providers & Schemes)
6.g	Acceptance Tests for WAN	X		H	Private Partner responsible for immediately performing professional acceptance testing of complete WAN network

6.j	No Design Requirements for WAN vs. NHIS Application	X		M	Private Partner responsible for to assure that the WAN capacity is adequate to perform NHIS applications
6.h	Quality of Installed Network	X		M	Private Partner responsible for performing professional review of quality and capacity of existing WAN and LAN networks
6.i	Unavailable System Documentation	X		M	Private Partner responsible for review of existing documentation on system and creation of missing documents required for a ITIL operations model.
6.j	Provider based Hospital Information Systems (HIS)	X		M	Private Partner responsible for assistance and certification of HIS system vendors
6.k	System Requirements Definition	X	X	M	Under PPP the Private Partner will define detail requirements in conjunction with all stakeholders.
6.l	Delivery	X	X	M	Under PPP the Private Partner will not be paid if claims are not submitted via electronic means.
6.m	Skilled ICT technical personnel H/R risk	X	X	H	Private Partner is responsible for all technical personnel and their training.
7	**Provider ICT Infrastructure**	**X**		**M**	**Implement a comprehensive ICT Infrastructure at the provider end**
7.a	Lack of a Local Area Network		X	H	Support the creation of a LAN for Hospitals to enable an effective use of the system.
7.b	Lack of Ownership of ICT Infrastructure at Provider site		X	H	Providers should own the local systems. They should have a budget for the maintenance of the systems in their facilities.
7.c	No Incentive to use the system		X	H	Integrate the NHIA systems to a Hospital Management System that is found useful for the facility.
7.d	Inadequate monitoring of WAN and LAN equipments	X	X	M	An effective monitoring mechanism should be established to facilitate the incident resolution process. An SMS base monitoring to assist local administrators to identify issues with the network.
7.e	Inadequate basic computer skills		X	H	A more effective ICT training may be necessary to ensure proper use of the system.

7.f	Continuous Link downtime affecting claims submission	X	X	M	The use of a SSL VPN should be considered instead of an IPSec VPN.
7.g	More hands required at the MIS dept		X	H	Providers should be encouraged to recruit more MIS personnel. All a third party IT Maintenance company should be engaged to provide additional help in solving basic problems.
8	**Provider HR and Training**	X	X	M	
8.a	Lack of basic computer skills		X	M	Provide on-site classes in basic skills
8.b	Sufficient training in application use		X	M	Provide on-site classes in each departments application use skills
8.c	Lack of trained ICT personnel		X	H	Develop a ICT technical management plan that includes all providers and schemes.
8.d	Lack of job requirements for claims personnel		X	M	Develop a job description including job requirements for each person involved at provider and scheme location in claims submission
8.e	Lack of job requirements for ICT personnel		X	M	Develop job descriptions for each defined ICT position at providers and schemes and validate existing personnel to those requirements. Develop plan to assist existing personnel in reaching those skill levels.
9	**Financial**	X	X	H	
9.a	Lack of ICT in budgets of GHS and other MoH reports		X	H	MoH must add line items for Provider ICT capital and operational costs. Contribute to PPP repayment fund
9.b	Lack of sufficient ICT operational budgets for CHAG facilities		X	M	Review with CHAG current ICT budgets and assist where possible in funding the budgets.
9.c	HIP funds insufficient to implement Provider systems	X	X	M	Implement under PPP
9.d	NHIL increase insufficient to fund continuing operations	X		H	Seek additional funding from MoH

- Contract Negotiation and Compliance Management – Past software purchasing projects, which the Government has done have proven to be problematic. In our opinion the Government does not have the expertise necessary to negotiate software development contracts and compliance. Legal assistance from lawyers familiar with ICT contract law will need to be hired.

- Project Management – Projects of this size and scope require professional Project Management personnel. There are currently no visible fulltime HR resources that would be capable of managing a project of this size.

- System Requirements Definition – As identified in the GAP Analysis report for Phase 2 there exists the risk of incomplete system requirements being defined. In order to clearly define upfront prior to tender the required Outputs of any system part of the PPP it is advisable to contract a Transaction Advisor for the process. Under a PPP the detailed system specifications are not defined only the required Output goals. This removes the need for the Government to have a System Architect to define system requirements since that responsibility falls on the Private Partner.

- Quality Assurance – Previous attempts to develop NHIS systems have suffered from a lack of through quality assurance. Part of this is due to the lack of specialized and trained engineers. The lack of knowledge of the QA process has led to systems that have been prone to failure, lacked required functionality and have performed well below acceptable levels of responsiveness.

- Delivery – It is important that the any PPP contract contain penalty clauses that reflect the cost to Government due to any late delivery or failure to meet SLA requirements. The penalty should be substantial escalating based on the length of the delay.

- Skilled ICT staff – Currently there does not exist in the Government skills to operate and manage a technical staff needed to manage a network of hospitals ICT needs. The MoH or other designated operating agency will need certified engineers to staff the Network Support group, a security specialist and a infrastructure management specialist at a minimum. Automated monitoring and trouble ticket system will also be required.

- Funding - There does not appear that there is sufficient funding for this project within the Government at this time. Any attempt to fund this project through normal MoH budgets contains substantial risks. Post Operational period the ability for staffing of the ICT staff is out of MoH budgets does not exist today.

7.1.3.4. EVALUATION SUMMARY

The following is a summary of the evaluation criteria:

- Operation Outputs – This Option meets all of the operational requirements
- Time to delivery –It is expected that the vendor would need 6 months to build a new data center and hire the required staff
- Delivery Risk is reduced since the Private Partner's compensation is based on electronic claims submitted
- Market or Government Funding Risk – There is the possibility that should a tender be issued that the private sector views the risk/profit model as being unfavorable.
- HR Risk – There is substantial HR risks involved in this option. The Government does not have today the technical and project management necessary to have the project succeed. The Government also lacks the Quality Assurance and Change Management professionals needed to assure a reliable system. The Government pay scales prohibit the hiring of these professionals.

  Should the Government choose to try and train the required personnel there is considerable risk that once trained they will leave for jobs in the private sector.
- Political Risk – Political risks exist should the Phase 2 project fall behind schedule or not fulfill its objectives.
- Government Development and Infrastructure Costs - $165,000
- 5 Year Operational Costs - $7,320,692

8. SUMMARY

Our study indicates that a Phase 2 implementation is possible that will result in a minimum of 60% of claims being filed electronically. The implementation of Phase 2 at the Health Providers will bring added value to the facilities and administration in the form of a complete Hospital Information System.

We believe that the World Bank supplied HIP funds are sufficient to fund the initial round of facilities capital expenditures for the needed ICT infrastructure. However, significant risk exists in the funding of the continuing operations of these systems without sufficient budgets within the Ministry of Health's agencies.

The use of a Public Private Partnership as a funding mechanism is a possible alternative. The payment mechanism exists in the use a small portion of the NHIL levy to be used for a special fund for the repayment to the Private Partner.

Before any implementation it is necessary to remediate the problems that exist today in the Phase 1 implementation. We feel the following are critical issues that require immediate attention:

1. Removal of the data center from STL's facilities
2. NHIA hire professional staff to manage the data center
3. NHIA institute ICT management under a standards model such as ITIL
4. Load testing of the existing Claims Applications to validate sufficient scalability for new Health Provider interfaces in Phase 2
5. NHIA take over database administration of the existing Oracle systems
6. Create vetting rule definitions for auto vetting of claims thereby allowing for more rapid reimbursement and post payment audits

A successful Phase 2 implementation will require true partnerships between health agencies. A successful implementation will be as much about the people as it will about the technology. Before any actions are taken on Phase 2 a detailed Implementation Plan needs to be developed. We have supplied a starting plan attached to this report. It encompasses both people and technology. Cooperation between stakeholders on the refining of this plan is step 1 for a successful implementation.

A core necessity of Phase 2 deployment is the technology needed at the Health Providers and Wide Area Network connectivity between them and the central NHIA data center that is both reliable and cost effective. Phase 1 connectivity problems show the need for higher reliability connections than the existing satellite systems. It is possible today to connect the 120 sites studied in this report via commercial terrestrial networks with higher reliability and lower costs.

At the center of Phase 2 is the application software interface between the Hospital Information Systems and the central NHIA claims system. As part of this report we have designed an interface that is not optimum but can be used as a starting design that working with STL and the HIS system providers can provide a mature interface. We believe that a

better implementation can be derived through cooperation with the existing Phase 1 system vendor, STL.

Phase 2 will have an extended implementation schedule due to the design and training at the facilities. We would estimate that the implantation of the larger facilities with the goal of 60% electronic claims may take as long as 3 years. Implementations at some large facilities could take 3 months with the hospitals business processes needing change and the physical installation of networks. Smaller facilities can be done within a 30 day period. Multiple implementation teams will accelerate the process.

The project team would like to thank all of the stakeholders in this project for their cooperation. We look forward to comments on this report so that we may incorporate those comments and concerns in our final report.

ATTACHMENTS

- Health Infrastructure Data
- Site Data Capacity
- Selected Site Financials
- Implementation Plan
- Build CAPEX OPEX Financial Analysis
- PPP CAPEX OPEX Financial Analysis