Islamic Republic of Afghanistan

Ministry of Public Health

ICT Infrastructure Strategic Plan

2012-17

General Directorate of Administration and Finance

Document Version: 1.0

Authors

This document was prepared by:

Arif Aslam Kundi
IT Advisor
Development Assistance Facility for Afghanistan (DAFA)–II (an AusAID Initiative)
GRM International
House No. 589, Street No. 10, District 6, Kart-e- Se, Kabul, Afghanistan
Telephone: +93 (0) 752 044 789
Mobile phone: +93 (0) 791 923 662
+92 (0) 300 555 4793
e-mail:
info.afghanistan@grminternational.com
arif.kundi@grm.com.af
arifkundi@hotmail.com
Web-site: http://www.ausaid.gov.au/
http://www.grminternational.com/

Wahidullah Wafie
ICT Manager/CIO
Ministry of Public Health, Wazir Akbar Khan, Great Masoud Square,
Kabul, Afghanistan
Telephone: +93 (0) 20 922 500
Mobile phone: +93 (0) 775 056 156
e-mail: wwafie@moph.gov.af
wwafie@gmail.com
Web-site:
http://www.moph.gov.af/

Hessamuddin Hamrah
General Director
General Directorate of Administration and Finance
Ministry of Public Health, Wazir Akbar Khan, Great Masoud Square,
Kabul, Afghanistan
Telephone: +93 (0) 20 230 1353 (3-lines)
Mobile phone: +93 (0) 770 276 152
e-mail:
hessamuddin.hamrah@moph.gov.af
hamrahd@gmail.com
Web-site: http://www.moph.gov.af/

Version History

Date	Document Version	Document Revision History	Document Author(s)/Reviser(s)
February 2012	1.0	Initial draft	Arif Aslam Kundi Wahidullah Wafie Dr. Hessamuddin Hamrah

Approvals

Date	Document Version	Approver's Name and Title	Approver's Signature
February 2012	1.0	Dr. Suraya Dalil Minister of MoPH	

Table of Contents

1 Abbreviations/Acronyms

AFMC	National Medical Council for Afghanistan
ANDC	Afghanistan National Data Centre
ANDS	Afghanistan National Development Strategy
ASM	Automatic Storage Management
ATRA	Afghan Telecom Regulatory Authority
BPHS	Basic Package of Health Services
CHW	Community Health Workers
CISSP	Certified Information Systems Security Professional
CMDB	Configuration Management Database
CRM	Customer Relationship Management
DAFA	Development Assistance Facility for Afghanistan
DSS	Decision Support Systems
e-	Electronic
EHR	Electronic Health Record
EIS	Executive Information System
EIS	Executive Information System
EMR	Electronic Medical Records
EPHS	Essential Package of Hospital Services
FOSS	Free Open Source Software
Gbps	Giga bits per second
GIROA	Government of Islamic Republic of Afghanistan
GIS	Geographic Information System

GoA	Government of Afghanistan
HCC	Health Contact Centre
HCS	Health Care Service
HF	High Frequency
HIS	Health Information System
HMIS	Health Management Information System
HNS	Health and Nutrition Sector
HNSS	Health and Nutrition Sector Strategy
HRMIS	Human Resource Management Information System
HSS	Hospital Sector Strategy
ICT	Information and Communication Technologies
IOPS	Input/Output (I/O) per second
IP	Internet Protocol
IT	Information Technology
ITIL	IT Infrastructure Library
LAN	Local Area Network
m-	Mobile
M&E	Monitoring and Evaluation
MCIT	Ministry of Communications and Information Technology
MDGs	Millennium Development Goals
MIS	Management Information System
MoF	Ministry of Finance
MoPH	Ministry of Public Health
NAC	Network Access Control
NEHR	National Electronic Health Record

NEHTA	National E-Health Transition Authority
NHIN	National Health Information Network
NHMIS	National Health Management Information System
OLAP	On-Line Analytical Processing
OLTP	Online Transactional Processing
PGA	Program Global Area
PH	Primary Health
PHCS	Primary Health Care Services
PKI	Public Key Infrastructure
PMI	Project Management Institute
PND	Public Nutrition Department
POP	Points of Presence
PPHDs	Provincial Public Health Directorates
SDL	Security Development Lifecycle
SGA	System Global Area
SMS	Short Messaging Service
SWAp	Sector Wide approach
TDF	Telecom Development Fund
T-M	Telemedicine
ToRs	Terms of Reference
TRM	Technical Reference Manual
VHF	Very High Frequency
VLDB	Very Large Database
VPN	Virtual Private Network
WAN	Wide Area Network

2 Executive Summary

Afghanistan has a timely opportunity and an urgent need to build a 21st-century health support system — a comprehensive, knowledge-based system capable of providing information to all who need it to make sound decisions about health. Such a system can help realize the public interest related to disease prevention, health promotion, and population health[i]. Various policies, strategies and plans such as Afghanistan National Development Strategy (ANDS) 2008–2013, Health and Nutrition Sector Strategy (HNSS) 2007-2013, Strategic Plan for the Ministry of Public Health (2011-2015), Information and Communication Technologies (ICT) Policy November, 2003, and Afghanistan Comprehensive Health Information System Strategic Plan 2009-2013 play a very supportive role.

The IT functions carry the responsibility of servicing the gap between where the public sector organisations are currently and where they want to be in the decades to come. Over the years this servicing has been evolving from streamlining the Information Technology (IT) cost model, to working with the different segments of the business to utilise IT to help increase the IT foot print and introduce seamless citizen services given the budgetary constraints enforced by the global financial meltdown and recessionary forces. But this gap has been growing increasingly to include innovation, specifically determining what future technologies and capabilities will accelerate the ministry's mission. Many IT function owners are overseeing a mix of technologies, and in many cases, disparate IT organizations stemming from organic technology growth, downsizing, and reorganizations. The IT function faces a multitude of concerns such as improving business processes, minimising costs, optimising scarce resources while servicing citizens and providing the backbone for organizational innovation.

This document serves as a guide and provides a road map to address the challenges and benefits of implementing an IT governance solution given these often competing forces and details a pragmatic approach to enterprise governance. Using a governance approach, even across a diverse technology landscape, can help ensure that only the projects that provide the highest IT portfolio or program value to the ministry actually get implemented. The strategy will follow the Sector Wide approach[ii] (SWAp) for the health and nutrition sector.

The mission[iii] of the Ministry of Public Health (MoPH) is to improve the health and nutritional status of the people of Afghanistan in an equitable and sustainable manner through quality Health Care Services (HCSs) provision, advocating for the development of healthy environments and living conditions; and the promotion of healthy lifestyles.

3 Introduction

Australian AID's Development Assistance Facility for Afghanistan's (DAFA) Goal is to strengthen government institutions at the central and sub-national levels to achieve measurable improvements in the delivery of services and the protection of rights of all Afghans.

DAFA'S IT Strengthening Activity contributes to the ANDS strategic objective of improving the health and nutrition of the people of Afghanistan through quality health care and the promotion of healthy life styles. It also contributes to the long term policy and strategic framework to improve health and nutrition through conducting monitoring and evaluation of health care services and the efficiency of the system, coordinating with other agencies and decentralising responsibility and managerial autonomy to the provincial level. The Activity is specifically contributing to the Health and Nutrition Sector - Administration Program Strategy 9.3 Communications and Information Technology to establish, maintain and further develop a functioning communications network using modern information and technology systems at national and provincial level.

Health is not merely the absence of illness. Nor is health achieved solely by combating disease. Rather, as the World Health Organization puts it, health is a "state of complete physical, mental, and social well-being". The goal of using and disseminating ICT is to bring benefits in all aspects of our daily life, and that ICTs are enormously important in facilitating citizens' access to these applications. The importance of an effective, comprehensive health information infrastructure that links all health decision makers, including the public cannot be over emphasised. Through the use of integrated information technologies, it is hoped that different segments of the medical care system will be able to "talk" to one another better and faster and, in the process, dramatically increase diagnostic accuracy and spot potential errors before they injure patients. The Health ICT has the potential to also improve community health by taking seemingly isolated events, identifying patterns and trends, and suggesting public health actions to safeguard populations.

Technology is not a major barrier to making this future a reality. Most of the barriers to an effective and beneficial national health information infrastructure are legal, societal, organizational, and cultural in nature. The Ministry of Public Health (MoPH) lacks a modern IT enabled environment, however under another activity DAFA is providing IT based tools and structures for the General Directorate of Human Resources which would dovetail in the overall IT Infrastructure activity. A Ministry wide network is available which can be used for provision of basic services such as email, file sharing, etc. at the Ministry level while all the Provincial Public Health Directorates (PPHDs) and other remote offices would be connected with the Ministry using available communication media in the country over the medium term.

The following two objectives of the Information and Communication Technologies (ICT) Policy[iv] of Afghanistan support the mission of MoPH:

1. Wide adoption of ICTs in order to improve all aspects of Afghan life, including education, health, employment and access to information;
2. Use of ICTs to increase Government efficiency and to effectively deliver improved social services.

With the policy objectives supporting the mission of the Ministry of Public Health it is required that MoPH picks up the pace towards becoming digital by enabling wide-deployment of IT based e-Government systems in the Ministry and IT based Health Care and Services systems for benefiting the populace.

In the long run the ministry's vision is that all data, both quantitative and descriptive, should be captured at source. All paper forms for collecting data will be changed to intranet based web forms. Electronic work flow will be the prime vehicle for transmission of data. The target is to create a reduced paper environment within the Ministry. Matching funds, grant and budgets would be required to see the initiative to fruition.

The Ministry of Communications and Information Technology (MCIT) is setting up a Public Key Infrastructure (PKI) at the Afghanistan National Data Centre (ANDC) to fulfil the following requirements:

- Confidentiality: Information security by encryption of transaction data.
- Integrity: Prevent forgery and alteration of transaction data.
- Authentication: User identification for data transaction.
- Non-repudiation: Reliability enhancement for Transaction by using electronic signature.
- Access Control: Permit to access information only for selected receiver.

This arrangement would enable authenticated data transmission within the whole of the Government.

The Ministry should plan for continuous enhancement of computers provision to staff, install non-stop servers and networks and provide fast access to the Intranet and Internet, to enable successful deployment of IT based Services delivery. The re-engineering of the administrative processes and office procedures, the recognition of digital signatures which requires authentication, the secure transmission of integral documents and the provision of complete audit trails for data recovery are a few of the critical developments that will facilitate the fulfilment of IT enablement of important services.

Health and Nutrition has been identified as the 5th Pillar[v] in the Afghanistan National Development Strategy - 2008 – 2013 (ANDS) oversight structure with the following cross-cutting issues:

1. Regional Cooperation
2. Counter Narcotics
3. Anti-Corruption
4. Gender Equity
5. Capacity Building
6. Environment

This document will form the basis of a long term ICT Strategic and Investment Plan for the Ministry. The Ministry should plan for continuous enhancement of computers provision to staff, install non-stop servers and networks and provide fast access to the Intranet and Internet, to enable successful deployment of Electronic (e)-Services. The re-engineering of the administrative processes and office procedures, the

recognition of digital signatures which requires authentication, the secure transmission of integral documents and the provision of complete audit trails for data recovery are a few of the critical developments that will facilitate the fulfilment of IT enablement of important health services.

This document will form the basis of a medium term ICT strategic and investment plan for the Ministry (2012-2017). The IT Steering Committee is the body that will guide all work under his strategy and measure its progress.

4 Afghanistan National Development Strategy

As an Afghan-owned blueprint for the development of Afghanistan in all spheres of human endeavour, the Afghanistan National Development Strategy (ANDS) serves as Afghanistan's Poverty Reduction Strategy Paper. ANDS will help in achieving the Afghanistan Compact benchmarks and Millennium Development Goals (MDGs). Moreover this document gives a roadmap for the long-desired objective of Afghanization, as the country endeavours to transition towards less reliance on aid and an increase in self-sustaining economic growth[vi].

4.1 ANDS for ICT

ANDS envisaged that by end of 2010 and implementation of e-Government, e-Commerce, and telemedicine Afghan citizens will be able to more fully participate in the information age.

4.2 ANDS for Health and Nutrition

The ANDS strategic objective for this sector is to improve the health and nutrition of the people of Afghanistan through quality HCS provision and the promotion of healthy life styles. ICTs will help MoPH achieve these strategy objectives quickly and successfully. Healthcare IT has greatly evolved in the past decade to enable MoPH reach beyond these objectives as well. It is imperative that IT is included in Expansion of Primary Health Care Services (PHCS), Basic Package of Health Services (BPHS) and Essential Package of Hospital Services (EPHS).

4.3 Gaps and Barriers

Main health issues relative to the health priority - include both population/public health issues (cause) plus consequence of health issue (effect/condition) for Afghanistan. ANDS has identified "variable levels of service quality"[vii] as one of the challenges and constraints facing Health and Nutrition sector. Internationally limitations in leadership, resources, standards, privacy and confidentiality protections, and consensus about appropriate information sharing have been recognised as major impediments to the development of the Health ICT. There is unanimity in identification of chief barriers which are human and institutional, not technological.

MoPH faces a number of problems and constraints in taking a leading role:

- No sustained financing for information technology investment or IT based health services delivery.
- Availability and attraction of trained and capable HR.
- Visibility as a higher level service provider in the Ministry.
- Technical Constraints.
- Resource allocation and constraint.

- Limited skill set.
- Lack of Standard Operating Procedures.
- Lack of appreciation in the ministry.
- Motivation issues.
- Inadequate financing for many of the key programs.
- Difficulty in keeping abreast of all ICT development efforts and projects in the health sector.
- The MoPH has very limited equipment, space and human resources for managing the development of and maintaining expanded ICT across the health system.

This potentially highly beneficial technology deserves continuous monitoring and periodic evaluation including cost-benefit and effectiveness analysis. Continuing innovation and improvement is needed with support of international expertise, in line with the MoPH priorities. Criteria and pre-requisites for effective ICT application are needed in line with the MoPH plans.

5 Health and Nutrition Sector Strategy

The goal of the Health and Nutrition Sector (HNS) is to work effectively with communities and development partners to improve the health and nutritional status of the people of Afghanistan, with a greater focus on women and children and under-served areas of the country. In order to develop the HNS to the point that it can realize this mission and goal, the MoPH will continue to develop and implement nine broad Programs that will add strength to its ability to create a favourable policy environment and to manage and deliver a wide array of Health Care Services at all levels of the National Health Care System (NHCS), from the remotest rural communities through to tertiary care hospitals in the major urban areas[viii].

ICTs can play an effective role in achieving the objectives of the approved Health and Nutrition Sector Strategy (HNSS).

5.1 HNSS Policy framework: sector strategy

It has been recognized in the HNSS that lack of Communications and Information Technology, proper database and absence of Management Information System (MIS) within the administration, notably for procurement, finance and stock management (data provided are incomplete and unreliable) impedes enforcing Public Health and Private Sector Law and Regulation[ix].

5.2 Implication of MCIT/ATRA Policies

MCIT and Afghan Telecom Regulatory Authority (ATRA) are working on a number of initiatives which are relevant to the success of this strategy such as mobile platform, software standards, national data warehouse, ***.gov*** email domains, and Fibre Optics network. All these elements can be utilised in the IT enablement drive of the Ministry.

ATRA has financial resource available under the Telecom Development Fund (TDF) which can be utilised in expanding IT Infrastructure and developing ICT applications for the Ministry.

6 IT Operations

The ICT Unit, under the ICT Manager, is responsible for providing all ICT services in the Ministry which are currently restricted to networking services, internet, browsing and emails. An organogram showing the reporting levels of the ICT Unit is available at Annex-I. Details of the IT operations that are in vogue and its short comings may be reviewed in Annex-II. Some of the major constraints faced by the ICT Unit are explained below:

- Lack of appropriate ICT Infrastructure
- Lack of appropriate support structure such as Help desk etc.
- Shortage of Human Resource

6.1 Organisation of the ICT Unit

The ICT Unit is divided into 3 sections, which are explained in detail below:

6.1.1 Information Technology (IT) Section

IT Section is headed by Mr. Ajab Gul, he is assisted by 2 technical resources in managing the operations of the section. The section is responsible for the IT Infrastructure including hardware, basic software, networking etc., plus the daily operation of the infrastructure. The section is responsible for the IT Infrastructure including hardware, basic software, networking etc., plus the daily operation of the infrastructure. The section will be responsible for administration of users IDs, passwords and authorities, monitoring of log files etc. in the future when systems get procured and implemented.

6.1.2 PABX and Telephone Section

This section is headed by an officer, Mr. Saifuddin who maintains the telephony communication system with the help of a technician. Mr. Saifuddin is constrained by the location of his office and an old computer which does not work properly. He is assisted by 1 person. Mr. Saifuddin was interviewed to determine how his section works.

6.1.3 HF Radio Section

Mr. Wesal Muhib, the head of the section is responsible for the smooth operation and maintenance of the HF Codan and Barrette systems. In addition he is responsible for other VHF systems. He is assisted by one technical resource in the daily activities. Mr. Muhib was interviewed to determine how his section works.

7 MoPH's IT Strategy

MoPH is aiming to prepare to adopt the E-Government principles set out in the ICT Strategy of MCIT. E-Government requires that a majority of business processes and services are automated and available on-line in real-time. It also requires that information systems (databases) architecture is integrated so that single-purpose databases are interfaced and able to be networked in a data-warehousing approach. This requires a sophisticated and reliable ICT infrastructure platform. The Government of Afghanistan (GoA) has identified the importance of IT development for the continued competitiveness and sustainable growth of the economy. In the two policy addresses of the President, he has indicated the GoA's desire and decisive actions to enable Afghanistan to remain as one of the few key players in the knowledge-based economy of the future world through wide deployment of IT.

MoPH will have to make a considerable investment in its ICT infrastructure and corresponding investment in its IT human resources in order to achieve the foundation-level infrastructure required. A proposal for five projects was prepared by the ICT Unit in December 2010 for the consideration of the Ministry of Finance, which were not provided funding due to budgetary constraints. The non-funding is related more to competing (and higher priorities) for ICT funds across the Government for Afghanistan, particularly from the security sector.

MoPH's Information Technology Road Map serves the MoPH's mission as it frames itself through activities linked to that. The MoPH's technology Road Mapping process also focuses on the viability of emerging technologies, track records of off-the-shelf technical solutions and takes MoPH's financial constraints into account. The aim of the IT strategy is to enhance and promote MoPH's information technology infrastructure and service so as to make it a leading digital ministry in the country. The strategy is based on four main enabling factors which can be broadly summarized as follows:

(1) to develop a high-capacity communications infrastructure to place the Ministry as a leading and information hub for health;
(2) to establish an open and secure common interface for electronic transactions, through which individuals, business and Government can interact easily and securely using their own systems;
(3) to empower staff and users with the know-how to use IT; and
(4) to nurture a culture which stimulates creativity and welcomes advances in the use of IT

7.1 How the Strategy Will Contribute to Addressing Health Problem

The strategy will tie all elements of the health care systems into an IT platform. Various health related data repositories will be integrated or linked together using Web-services. New databases such as patient information systems will be deployed in hospital which will form the core of the larger Health Information System. This will result in bringing efficiency and effectiveness in health care over the long-term. The strategy will assist tremendously in driving the automation effort of the Health Management Information

System[x] (HMIS) and Health Information System (HIS). Provision of fiscal support is of utmost importance for the success of the strategy.

7.2 ICT Steering Committee

For the success of Healthcare ICT or Health Informatics, it is necessary to garner top-level sponsorship, which will be obtained from the ICT Steering Committee. The committee is the penultimate forum responsible to approve all major ICT initiatives and investments in the Ministry. Since the strategy covers the whole of the Ministry, its departments, its hospitals etc., in Kabul and the provinces, therefore, involving appropriate stakeholders in the life cycle of large projects and initiatives will ensure the success of the IT program which will follow the approval of this strategy. Steering committee is the body that will guide this work and watch & measure progress of the IT initiatives.

The Steering Committee will also consider the set of priorities and their ranking in terms of phasing and levels of investment. The MoPH leadership, through the Steering Committee will be asked to dedicate a budget allocation from both core and development budget to IT services for which the ICT Unit would be responsible and accountable, however, all major and decisions for IT maintenance and ongoing initiatives will lie with the Committee.

7.3 Strategic goal

The strategic goal to achieve under this strategy is to leverage IT so that the ministry can have an automated workflow and provide automated services to the population.

7.4 Objectives

The following are the main objectives of the ICT Strategy:

- IT Enablement of the Ministry and attached departments
- Capacity Development[xi] of the IT staff. Train key IT Unit's personnel in certified courses that will enable them to properly design and implement network infrastructure for the future and liaise with key directorates, such as the Health Management Information System (HMIS) Directorate, about the required information systems platform. Building skills of MoPH staff in basic computer skills for which different levels of training courses suited to the Afghan situation are required to be designed and implemented under a program.
- Improvement of Hardware and software platform in phases with the high priority elements taking precedence over others.

- Implement whole of the Ministry integrated databases and application software, including workflow based Hospital Management Information databases and applications.

- Creating patients' Electronic Medical Records (EMR)

- Improve the technical structure of the National Health Management Information System (NHMIS) and integrate it with the Ministry specific databases such as Human Resource Management Information System (HRMIS), Financial Management Systems etc.

- Pilot implementation of Management Information Systems and applications at all levels of all sample facilities to create EMRs and effectively provide data to drive NHMIS at the central level. This would help meet the working principles of revising HMIS "Any data to be recorded at a service level must be able to be used by both the staff and the community to analyze and improve the provision of health services within their community" and "Efforts should be made to make better use of existing data at all levels through practical analysis and improved presentation of data" and "Improvement in health data generation and use at the various service levels should be undertaken in support of efforts to improve service task performance and should be seen as a by-product of such performance improvement. Care should be taken to share information in a non-threatening be used.

- Leverage mobile application deployment for providing citizen health services.

- Deployment of E-Learning and creating an E-Library.

- Implement a Configuration Management Database (CMDB).

- Train IT Unit staff to achieve certification in IT Infrastructure Library (ITIL), Project Management Institute's (PMI) Project Management Professional, Oracle/MS SQL certification, Security (CISSP) certification, etc.

- With the rapid expansion of optical Fibre Cable network connecting major metropolitan areas and creating of Fibre Points of Presence (POP) MoPH can plan for establishing seamless connectivity with all levels of nation-wide institutions under the Ministry. As an interim measure Internet Service Providers' can be contracted to create a Virtual Private Network (VPN) based Wide Area Network (WAN).

The long term ICT strategic plan and investment plan will be the avenue through which MoPH can consult with Ministry of Finance and Ministry of Communications and Information Technology about future budgeting and investments. Improved ICT Unit work performance and improved IT platform planning, budgeting and implementation. It will also serve as a document to guide and channel the investment of donors into the Ministry support services for management information systems. It will ensure that there is some tangible improvement in IT services. It will cover the provincial IT development needs and provide an implementation path to e-government applications and m-applications.

7.5 Organisational Structure

The current ICT organisation structure as explained in Section 5 is very weak and rudimentary. It cannot be expected of it to play an effective role in implementing the ICT Strategy unless it is strengthened.

The ICT Unit is not responsible to maintain databases and any software applications in the Ministry. This responsibility rests with the HMIS Department which falls under the General Directorate of Policy and Planning. Both the ICT Unit and the HMIS Department being technical arms of the IT domain require to be under one technical General Directorate.

To bring efficiency and effectiveness in the ICT operations of the Ministry, which will consequently benefit the IT enablement of the Ministry, the strategy requires forming a new Technical Directorate – ICT Directorate, which should be at-par with the other Directorates. HMIS Department and ICT Unit - upgraded to ICT Department – be given under the charge of the ICT Directorate. Additionally a new Information Security department needs to be created under this new Directorate. The ICT Directorate and its three departments should be housed together in single premises. The General Director of the ICT Directorate will be an IT Specialist with at least 12 years of technical experience and 3 years of administrative experience. A separate budget line should be provided to the directorate so that it can embark on high priority projects immediately.

An organogram of the new proposed Directorate is given in Annex-III.

7.6 Human Resource

The ICT Unit is severely short of staff to effectively contribute to the IT enablement of the Ministry. Similar is the case with the PPHDs which would need to be improved. The ICT Unit has already moved a request to the Minister of Public Health to create a Help Desk in The ICT Unit for providing a point where the users can go IT support services and for removing the ICT Manager from managing the help desk so that he can work on priority areas such as ICT strategy, trainings, capacity building and thinking in terms of applications for the ministry.

The ICT Unit is under staffed and some of the available staff requires training to improve their skills. Induction of a least two staff qualified and trained in managing database systems that are being inducted in the Ministry and the administration responsibilities lie with the ICT Unit. People with required knowledge, skills and abilities are required for ICT Unit and Provincial Directorates.

7.7 Training

Ongoing Staff Development will be a permanent feature of the strategy since technology is changing at an accelerating rate, unless we continuously develop the skills of both ICT staff and other MoPH staff, we will never realise the potential of advances in technology. Additionally the IT technical qualification of MoPH IT professional staff in MoPH central and provincial offices will be improved. Moreover, HF/VHF radio training courses for MoPH staff, especially in provincial and central health centres.

7.8 Defining the IT Governance Process from a Project Perspective

Governments have been placing a great deal of emphasis on project management practices as a means of instituting IT project governance. However, perfect project execution does not ensure that the project will deliver real value. The planning function together with the IT function will demonstrate value for every project and balance generating this value against portfolios or programs of projects competing for resources. For the success of Strategic IT governance the ministry will establish a value management framework and define the process for applying it. Using a defined process that is visible to all stakeholders will ensure buy-in and strengthen accountability.

Portfolio management has gained increased acceptance as an approach in managing projects, and by extension the programs they support, as investments. Portfolio management employs a consistent process to propose, select, and manage IT investments and the projects that support them – not just to completion, but through to benefits realization. The Ministry shall use Portfolio management approach incorporating objective criteria to evaluate both existing projects and new project proposals, and it shall apply these criteria in a consistent way so that everyone in the ministry can trust the process as fair and objective. The process shall be collaborative for ensuring buy-in.

Portfolio management actively manages proposed IT investments as well as existing ones, always driving towards the maximum value returned for the money being spent. Using objective criteria, top-down portfolio management ensures that:

- Projects are aligned with strategic objectives (a key executive concern);
- Spending is balanced across those objectives;
- Risk and value are balanced appropriately; and
- Projects underway remain healthy.

Under the strategy a heightened portfolio visibility will be achieved using specialized automated software

tools, enabling stakeholders to gain a greater understanding of what projects are over or under budget so proactive action can be taken.

7.8.1 Best Practices for implementing an IT governance process

Some best practices that can be followed to implement IT are given below:

- Focus should be on the value to be derived from the projects, and programs they support. Value shall be measured by establishing appropriate evaluation criteria.
- Rationalize existing projects by applying the evaluation criteria as if new projects were being approved.
- Terminate the programs or projects that do not make sense. Whether it is because they are not performing well or because they exhibit low value.
- Emphasize what will be realistically adopted and used consistently.
- Establish a comprehensive Management function to manage, monitor and follow-up on the network design activities.
- Ensure appropriate KPIs are established to measure the performance of work of the design and engineering section.

7.8.2 e-Services

The Government of Afghanistan has set its target to promote and provide e-Services to its citizens by leveraging ICTs. With the legal framework for electronic transactions under development, it will ensure legal recognition of electronic records and digital signatures, confidentiality and integrity of electronic transmissions, and authenticity and non-repudiation of electronic transactions. MoPH should be well positioned to adopt this new paradigm of e-Services.

Successful e-Services implementation in the Ministry will rely on the following provisions:

a) A framework that would provide the reliability and security in conducting electronic transactions within the Ministry and with the outside agencies;

b) A robust and dependable network environment;

c) Reliable and scalable hardware and software that support the IT environment at all times (365 days in a year); and

d) Software that would work seamlessly with existing applications.

e-Services require implementation of Very Large Databases (VLDB).

8 Strategic Plan for MoPH

This strategic plan follows the priorities articulated for the Health and Nutrition Sector in ANDS[xii], which are:

1. CDC and Non-CDC Program
2. Primary Health Care Program
3. Hospital Care Program
4. Reproductive Health and MCH Program
5. Policy and Planning Support Program
6. Human Resource Development and Research
7. Pharmaceutical Management Support Program

The approved Strategic Plan for the Ministry of Public Health (2011-2015) articulates a number of areas that require ICT deployment or usage to achieve the relevant strategic objective. The Strategic Plan has ten strategic directions[xiii] and each of the strategic direction proposes ICT intervention in one or many of the strategic objectives under each directive.

8.1 Purpose statement

The purpose of the IT strategy is to use IT tools and technology to further the mission and vision of the Ministry of Public Health.

8.2 Systems and applications

Clinical and public health information systems are the chief engines of Health ICT. They capture, store, organize, and present data about medical care and population health status that are crucial for routine work, problem solving, planning, and emergency response. Applications enabling these systems to perform and communicate need to be quite robust. A fully developed HIS would improve cross-system data exchange and enhance multimedia and geospatial capacities. Essential non-data applications include interpersonal communications (text, voice, and video), remote monitoring and reporting, transactional services such as scheduling appointments and purchasing items, and interactive educational and decision-support tools for professionals and the public. The requirement is to develop and deploy ICT Infrastructure and applications for information management, decision-support tools, communication, and transactional programs.

The ICT Unit and HMIS Department which currently have separate reporting lines and hierarchies will be responsible for the administrative and technical parts of the database system and software applications respectively. It is required that these two entities be under one common structure.

The Ministry has a few software applications running and it will get new application software systems from a number of donor funded projects and the ministry will develop new application software systems to meet its business needs. The new software applications would be dynamic web-based applications that combine multiple data sources in real-time for increased awareness and improved decision-making while meeting the stringent governance and data security requirements of enterprises. There are number of systems already developed and in varying levels of use within MoPH, Annex-IV provides a brief on such systems.

All applications that will either be developed for MoPH or implemented at MoPH will have integration points to all other applications that either will take input from such new applications or will provide inputs to these applications.

8.3 Databases and Application Software Systems development

Development and implementation of the following databases and application software have been recommended in various approved policies, strategies and plans of the MoPH. Important features of the systems have been briefly mentioned under each heading.

8.3.1 Procurement System

An effective procurement system for the whole of the Ministry will streamline and simplify the procurement process and make it more transparent. A stated requirement is that the system should be capable of harmonizing system of procurement of essential medicine for health facilities. Moreover the system should meet enable in international bidding and contracting[xiv]. This system will be tightly integrated with the Supply Chain system.

The Ministry has system that has been developed in MS-Access and does not meet the complete requirements of the ministry.

Commented [MM1]: As the procurement process is owned by MoF, so the strategy should have a statement that the system will be developed in close collaboration with MoF.

8.3.2 Pharmaceutical Management System

Implement an MIS for data and information sharing and reporting on all pharmaceuticals by all active parties. The MIS will also help in pharmaceutical Regulatory System and implement a Drug registration system as well.

There is inadequate tracking of procured and distributed health system commodities including pharmaceuticals[xv]. The system will streamline the process and provide dash boards for various information related to tracking of such commodities.

Amongst others the system would enable the Ministry and stakeholders develop standardized plans, mechanisms, Standard Operating Procedures, and tools to implement Management Information System for data and information sharing and reporting on all pharmaceuticals by all active parties[xvi].

8.3.3 Supply Chain System

Develop a Supply Chain (logistic[xvii]) system for Public Nutrition Department (PND) and with a linkage to the Central Warehouse Operations to attain optimal stock performance. The system will be extendable to all other Directorates etc. It will maintain complete inventory of PND and others.

Many facilities report frequent drug stock-outs that go without any response from higher levels. The system will have inbuilt features to escalate the stock-outs to appropriate officers of the Ministry or hospitals.

8.3.4 Geographic Information System

Globally Public health officials are using geographic information systems to enhance surveillance capabilities. As envisaged[xviii] mapping of Health Facilities in the country using Geographic Information System (GIS) will help achieve identifying gaps in coverage of HCSs and identifying locations for investments in health care. This will help overcome challenges in allocating funds for program planning and service delivery. It will create information which will help evidence based decisions that result in efficient and effective distribution of development resources. For success of this initiative population profile of the country showing population centers, population of the area (giving breakup for the province, district and village), demographics, gender ratio and age group identification will be required at the minimum. Annex-V provides an over view of GIS.

8.3.5 Monitoring and Evaluation System

A Monitoring and Evaluation (M&E) system is already working in the Ministry however, it needs to be extended to the nutrition programs so that M&E of the implementation of HCSs can be done in order to ensure quality, equity and efficiency of the health system[xix/xx]. The system will later be extended to all General Directorates, Provincial Public Health Departments, Hospitals etc.

8.3.6 Additional Databases and software application software systems required

The following application software, which are not mentioned in any MoPH approved document, are required to meet the vision and mission of MoPH:

8.3.7 Financial Information and Management Systems

To improve health financing a Financial Information and Management Systems are required. This will help in proper reporting of expenditure and drive budgetary reporting. Spend analysis will be a useful tool to determine the areas where more resources can be diverted.

8.3.8 Registration System and Web based portal for National Medical Council for Afghanistan

Commented [MM2]: This can be established easily as MCIT has the CMS for the web sites already deployed.

National Medical Council for Afghanistan (AFMC) is under the process of establishment, its main goal is to regulate the medical profession and it has been envisaged that the council will be an independent body with its own board- the National Medical Council Board.

AFMC Database will provide information regarding the composition of Health sector HR and build relationships with key stakeholders to improve the flow of information within the health sector relating to HR requirements, availability, shortages and losses due to attrition.

8.3.9 Telemedicine System

In Telemedicine (T-M) – doctors in provinces refer to and discuss and consult with expert/specialist doctors in urban areas. Any Telemedicine application development needs to fit within the MoPH strategy for developing central-level tertiary hospitals. The Ministry, based on provincial needs, will develop a T-M program, together with MCIT - since it is an action item in MCIT's IT Policy, extending the reach of specialist care to the un-served and under-served areas.

8.3.10 e-Learning System

For on the job training of various categories of health workers web-based delivery of course materials over the Intranet can play a great role. This new paradigm is called Electronic (e)-Learning. It is a huge innovation of the teaching and learning environment. The system would exploit the advantage of IT and electronic service delivery to assist the development of problem-based teaching and learning models. One of the requirements is that the Ministry's ICT would require supporting high-quality video-broadcasting of on-line lectures and video-conferencing for distance learning. Furthermore it will be necessary to provide 24-hour non-stop support for the system.

Initially self-paced learning modules can be developed by the respective General Directorates for the various categories of in-service staff in the Ministry, Provincial Directorates, Hospitals and other care giving institutions, for e.g. learning module on case management for Community Health Workers (CHWs). New inductees can also benefit from e-Learning where they can be given initial training on the rules and regulations etc.

Some of the benefits of e-Learning are that e-Learning can increase retention and application. Short, targeted learning experiences offer participants an opportunity to apply the concepts, principles and procedures before the next class. Participants who travel to a training session don't always have time to practice and apply concepts between classes. E-Learning provides a diverse setting for e.g. participants from many geographical locations can bring different ideas and backgrounds to the learning activities. Some of the important e-learning best practices[xxi] that need to be considered before designing any e-Learning program are as follows:

- Visualize how learners will experience the learning environment and anticipate and answer their unspoken questions.

- Don't waste learners' brain power on how to access online learning. Use programs that are clear and easy to use.
- Balance audio, text, visual media and interactivity to meet different users' needs.
- Cater to the younger, sophisticated workforce with top-quality graphics. Clip art just doesn't cut it anymore.

A concept note developed for E-Learning can be perused at Annex-VI.

8.4 e-Health

e-health is defined as the use of ICTs, locally and at a distance, to strengthen health systems and address public health priorities. E-health has the potential to increase the efficiency of health systems, and to improve access, especially in remote areas, or for marginalised or excluded populations, or people with disabilities and the elderly. Within the health system strengthening approach, e-health could be used to improve service delivery, improve the quality and quantity of the health workforce, expand health information systems, improve logistics management for and access to medical products and commodities, and increase the efficiency with which health sector resources are used.

Under this strategy a nationwide e-Health system would be developed and deployed that will enable connectivity between all tiers of medical support systems, seamless interchange of medical records of populace and statistical analysis. e-Health System will enable physicians at the Primary Health (PH) Care to capture and provide background information on patients along with referrals to other institutions for consultations in advance. It enables health care giving institutes capture the necessary history and diagnostics of patients.

It is recommended to establish a National Electronic Health Record (NEHR) program based on international accepted standards by health systems operators (and hence suppliers) and ensure the exchange of vital health information between health care providers.

e-Health requires developing IDs for individuals and providers; agreed clinical terminologies and compliance to internationally agreed standards for future government procurements of e-Health systems. e-health alone is not successful without considering information management requirements of stakeholders, such as:

- Statistical information and management
- Health data Standards
- National health performance
- Population health information development

Internationally the medical fraternity advocates spending on:

- More effective General and Specialist Practitioner Computerization

- Automation of Acute and Long Term Hospitals
- Computer support for pharmacies, radiology and laboratory practice
- Common interoperable forms of secure health messaging.

The strategy outlines four detailed work streams:

- Governance
- Change & Adoption
- e-Health Solutions – Information Flows, Service delivery Tools and Information Sources
- Foundations

For further details on e-Health please refer to Annex-VII.

8.4.1 Deployment of e-Health Solutions

The use of healthcare IT has increased significantly as more providers use electronic health records (EHRs) to support direct patient care. A major trend is the emergence of specialized or general health-information portals. Web-based health-information services offer a great potential to 'health care customers' that is every one of us.

Typically e-Health systems are interlinked and work on the following three levels:

i. Hospital and Health Unit Management Systems
ii. Electronic Medical Record System (EMR) System
iii. Electronic Health Record (EHR) System

In the short-term the following e-Health Systems (for details please see Annex-VIII) will be deployed and implemented:

i. Hospital and Health Unit Management System
ii. Electronic Medical Record System (EMR) System
iii. E-Prescription

In the medium-term the following systems (for details please see Annex-IX) will be implemented:

i. Establish Health Contact Centre
ii. m-Health

In the long-term an Afghanistan wide Electronic Health Record (EHR) (for details please see Annex-X) would be created. The pre-requisite for which is the availability of EMRs.

8.5 MoPH Web Portal

A major trend is the emergence of specialized or general health-information portals, which are user-friendly and strongly integrated with organizational databases for content availability. Web-based health-information services offer a great potential to 'health care customers' that is every one of us. Information on health and messages on nutrition, healthy eating, healthy living, and food hygiene & food safety in the home will be hosted for the benefit of the population will be hosted on MoPH portal. Promotional messages and easy to understand topics pertaining to infant and young child feeding shall also be posted on the portal. The web portal can also be effectively used to improve public awareness regarding hospital services (availability, cost and quality). Moreover the portal will play a central role in promoting public awareness related to the Health Service Ombudsmen, increase awareness of gender and health and rights, and raising women's decision-making role in relation to health seeking practices[xxii].

Seasonal health advice can be communicated to the population through the MoPH portal and other means such as SMS messaging service. The portal will be the point of access for internal and external stake holders into the ministry's various systems and service offerings. Some of the Guide-lines for portal application design and development can be viewed at http://www.redbooks.ibm.com/abstracts/redp3829.html.

8.6 Towards a Paperless Environment

It will be a strategic move for the MoPH to initiate as soon as possible wide deployment of e-Services in all its activities. E-Services promises convenience, reliability and an easy means of data delivery within the MoPH. It also provides an efficient way to maintain control of the MoPH data, a continuous audit trail to verify delivery and status, and a streamlined interface to MoPH's administrative systems.

We can also envision the deployment of e-Services as a move towards a paperless environment. It will help to cut the paper chain, provide a user-friendly environment for our staff to communicate effectively, shorten the processing cycle and improve the quality of information. Using less paper and cost savings are only part of the whole picture. The real leverage lies in the opportunity to re-engineer the MoPH's business processes and to re-think the flow of information.

Working under the e-Services framework and with wide deployment of electronic/web based forms and a good workflow management system, MoPH will be moving closer to a paperless office environment. All memos and notices will be delivered by email, all messages will be authenticated and all archived material can be searched and retrieved efficiently. It will probably still take some years before we can do away with paper, but it is crucial that the MoPH should take a strategic move towards this direction without delay.

An effective document management system will be essential for managing the vast amount of archive documents, with suitable security protection measures built in.

8.6.1 Web-based Electronic Forms

A number of paper forms exist throughout the MoPH. With the increasing use of the web, many offices have already resorted to the storage of the forms in the Intranet so that users can print out the forms themselves, thus reducing the need to ask for the delivery of a form.

With the establishment of an e-Services infrastructure firmly in place, this scenario can be largely altered. The electronic forms can be completed on the web, the data gathered can be directly stored in the database and the forms can be routed for processing by the approving authorities via the Intranet. The successful implementation of electronic forms will help to largely improve our overall efficiency and productivity of the work done in the Ministry. The aim is to convert all paper forms into web-based electronic forms, with a target of completion within three years.

The directorates will need to recognise that process re-engineering is a must in order to have an overall gain in productivity and efficiency. A successful e-Services implementation will provide them with a greater and better control on their resources, and will also help them to shorten decision cycles and improve efficiency.

8.6.2 Electronic Workflow Management System

Electronic documents will need to be transmitted electronically from one place to another to get electronic approval by the appropriate authority before it gets sent to a higher level. An electronic work flow management system will have to be developed to keep track of the status of all the administrative applications. Audit trails will provide the necessary tracking in case any dispute should arise. The work flow management system will also need to provide the capabilities to handle attached documents, which could be in electronic form or scanned documents.

8.6.3 Management Information

An effective Executive Information System (EIS) will form an integral part of the digital environment. The EIS will provide department heads with easy access to internal as well as external management information relating to their critical success factors. It will be particularly useful to the MoPH senior management for strategic planning and to integrate development plans of the Ministry.

Both current and historical data will be stored in a central data-warehouse. Under the e-Services framework, all data will be collected from source and updated directly into the database and extracted to the data warehouse. Timely and accurate data will be available to help management to make decisions. Web access to the management information in the EIS will be controlled by different security levels and governed by digital certificate authentication. The creation of the central data-warehouse will depend on the successful implementation and operation of the EIS.

8.6.4 Digital Library

A digital library or an e-Library is a library in which collections are stored in digital formats (as opposed to print, microform, or other media) and accessible by computers. The digital content may be stored locally, or accessed remotely via computer networks. A digital library is a type of information retrieval system.

It is important because it is not constrained by physical boundary; it is available round the clock; it permits multiple access etc. Digital information requires very little physical space, provides added value and easy access.

Internationally large scale digitization projects are underway at Google, the Million Book Project, and Internet Archive. With continued improvements in book handling and presentation technologies such as optical character recognition and eBooks, and development of alternative depositories and business models, digital libraries are rapidly growing in popularity as demonstrated by Google, Yahoo!, and MSN's efforts. Just as libraries have ventured into audio and video collections, so have digital libraries such as the Internet Archive.

With the upgrade of the MoPH's Network infrastructure it is possible to make wider use of the network for information search and retrieval through the use of state-of-the-art digital library technology. Information that can be digitized into electronic form includes text, graphics, audio and video images. It would be vital that with wide deployment of electronic service delivery in the MoPH, the aim should be to provide all library materials in digital full-text form. An education portal for the Ministry will provide the gateway to the stock of library material in the MoPH.

Easily and rapidly accessing books, archives and images of various types are now widely recognized by commercial interests and public bodies alike. In the health care domain MoPH will develop an e-Library system to provide an enabling environment to the medical practitioners and other paramedical, auxiliary and administrative staff to enhanced knowledge and obtain certifications.

8.7 ICT Infrastructure Development

Continuous investments in the ICT infrastructure in MoPH, PPHDs, Hospitals, Health Units etc. needs to be ensured. In the immediate term the infrastructure of Food and Drugs Control Laboratory and HIS needs to be enhanced and developed respectively.

Over the last many years the Ministry has invested in building up an ICT infrastructure of sorts that has not followed any deliberate strategy rather it has followed point requirements raised by various domains within the Ministry. The requirement is to have a modern, fast and efficient campus network infrastructure.

The need is to develop a ubiquitous network - wherein any user on any of the Ministry facility can be digitally connected. In addition to enabling access to internet, administrative and other applications the network shall facilitate web-based teaching and learning and the use of electronic newsgroups as an academic forum. All data, both quantitative and qualitative, should be captured at source. Electronic work flow will be the prime vehicle for transmission of data in the Ministry. This will help achieve the aim of building a quality electronic Ministry environment which will serve to radically improve overall efficiency. Paper use will be reduced over time and appropriate information will be made available efficiently and timely to the right person in the Ministry.

It is deemed necessary that the Ministry should plan for continuous enhancement of IT provisions, to provide for non-stop servers and network, and most important of all, fast access to the Intranet and Internet. The re-engineering of our administrative processes and office procedures, the recognition of digital signatures, the secure transmission of integral documents and the provision of complete audit trails for data recovery are a few of the critical developments that will facilitate the fulfilment of the ministry's vision.

Funding will be required to implement this strategy as follows:

(1) Strengthen technological infrastructure;
(2) Develop databases and application software;
(3) Build up human capital meeting the needs of the IT deployment in the Ministry;

To develop reliable, secure, high performance computing services that meet MoPH's daily needs and support the realisation of the vision of a 21st century institution, MoPH's IT Strategy calls for acquiring state-of-the-art equipment and developing robust ICT software applications and Databases. For details please see Annex-XI.

8.7.1 Data Centre

Under the strategy a Data Center will be developed in the Ministry, which will be a Computing Facility capable of providing 24 x 7 operations. The following services will be provided from the Data Centre:

- Internet Services
- Directory Services (Includes Authentication and File Server Services)
- Backup/Restore/Data Security Services
- E-Office Services
- Hosting various Databases etc.
- Helpdesk Services

For provision of smooth services mentioned above development of the Data Center is required in the following domains:

- Hardware Infrastructure
- Software Infrastructure
- Physical Layout and Security
- Air-conditioning Requirements
- Electricity/Power Requirements
- Cabling Infrastructure

The loss of computing environment at the Ministry of Public Health is unaffordable because all the deployed systems are heavily used. Moreover the computing environment at the Ministry is not equipped with Electric Power Generator facility. For 24 x 7 operations no service can be stopped for any time period exceeding the permitted down time, which needs to be separately defined for each service. This can lead to the loss of productivity. Hence a state of the art Data Center at the MoPH is a necessary requirement that can provide 24x7 services. The Minimum interventions required on an immediate basis in creating a Data Center may be perused at Annex-XII.

8.7.2 Nationwide Health Information Network

The HNS is committed to establishing, maintaining and further developing an affordable, useful and functioning communications network using modern information technology systems at both national and provincial levels. This effort should improve the decision making process[xxiii].

The National Health Information Network (NHIN) will integrate patient records from hospitals, Doctors' clinics, medical centres and pharmacies. This can be achieved by:

- Developing ICT infrastructure in the Ministry of Public Health premises and all other related directorates and departments including all hospitals and other health facilities in Kabul.
- Establish standard & secure network and ICT infrastructure for all 34 Provincial Public Health Directorates; including provincial Hospitals and all other Health Facilities.
- Establishing of Audio & Video Conferencing facilities.
- Creating 3 Digit Hotline number for assistance on health related issues all over the country.
- Developing current HF Radio System Network in all provinces.
- Establishing of Telemedicine Centers in Provinces.
- Arranging series of training courses and workshops in ICT for all 34 provincial public health directorates' staff ICT Assistants (current HF Radio Officer).

Under this strategy a project to establish a Cyberport would be initiated to inject into the Ministry, its directorates & departments and the 34 provincial health departments broadband multimedia applications, e-Government applications, communication, and access to information. In addition, it will be a facility designed to foster the development of telemedicine services and to enhance the Ministry's position as the top rated citizens' health services provider in the country – competing with the private sector on quality parameters. The Cyberport will attract, nurture and retain the relevant innovative talent necessary to build a cyber culture critical mass, with an aim to develop, within the Ministry, leading edge applications of information technology to generate new information for successful long-term planning. With this reporting would be quicker and consolidation can happen a lot faster.

8.7.2.1 Network Development

MoPH will implement a very efficient and high-bandwidth network at the Ministry's compound. Every ministry activity, whether it is related to administration, finance, projects, learning, research, will be dependent on the network. We need to ensure that the network remains healthy all the time and we need to ensure that the network bandwidth is sufficient for everyone in the Ministry. It is envisaged that broadband multimedia capability is required everywhere.

While the current network provides network connections to the desktops, it is necessary to ensure we should continue to monitor the fast-developing network technology and to further enhance our network to make best use of those new technologies at the most opportune time. To fully exploit our network infrastructure, the ICT Unit Centre will strive to provide a better and more user-friendly environment for the use of video and multimedia contents to support effective multimedia communications. The ICT Unit shall strive to introduce resilience in the buildings network to ensure high availability of the network infrastructure.

8.7.2.2 Core of the Network:

The core now commonly uses 10Gbps interconnections between switches, and large data centres are anticipating the delivery of 40G and 100G Ethernet standards. This is the direction in which the Ministry's infrastructure should expand.

Core Switch – to have better control on the network usage a Core Switch is required. This switch will provide numerous management and latest technical features for a robust HO Network.

For the access layer, investment in 10Gbps switches is desirable since it will give investment protection for 10 years at least. 1000Mbps (1Gbps) edge switches with Power over Ethernet (PoE) would suffice for most of the Ministry's user population, or can look to vendors with significant value propositions for 10/100/1,000 options.

On the security front, Network Access Control (NAC) will be implemented in the Data Centre. With NAC embedded security will expand to provide more-complete protection, including wireless connectivity, and will include technologies such as post admission control, threat containment and content security.

8.7.2.3 Internet

Internet will be the main communication media for creating NHIN and connecting remote offices and hospitals etc. Various implementation strategies can be used for e.g. Virtual Private Network etc.

Annex-XIII provides some details on the internet pipe available at MoPH. The situation in the provinces and remote offices and hospitals in Kabul seems to be quite different. Afghan Telecom can conduct an assessment and provide details on the locations which can be connected through the Fibre Optic cable or other media.

PPHDs continue to access the internet with Satellite services in spite of proximity of the Fibre Optic Network in some areas. HMIS reports are sometimes sent by memory stick because of low bandwidth connections.

Initially remote offices and Hospitals in Kabul and other cities that have Fibre point or presence will be connected by high speed connections. We should ensure there will be continuous improvement in the network bandwidth in the major remote sites as the data traffic builds up. We should also aim to connect other smaller remote sites with sufficiently- high bandwidth network connectivity. To ensure security of the

Intranet, suitable deployment of fire-walls and other security measures will be necessary to prevent unauthorized access to the network.

8.7.2.4 Wireless Network

High-bandwidth wireless networking technology will enable deployment in open space areas in the campus, or inside offices. This technology is not a replacement of the wired Local Area Network (LAN).

8.7.2.5 Telecommunication

Those facilities which lack access to mobile telephone communications may be provided such facilities with HF radios.

8.7.2.6 Intranet

Internet access – requires very secure internet connectivity. This can be achieved by leveraging Secure Socket Layer (SSL) encryption (minimum 128-bit) and the services of a Certification Authority for trust relationship between the MoPH and its customers. The use of Fibre Optic network, wherever available, in place of more expensive alternatives would be opted to an Intranet.

The Ministry will embark on the Digital Ministry Initiative and build up a strong foundation of IT infrastructure and applications in the Ministry. A state-of-the-art ministry wide network backbone, as explained above, is a requirement which will facilitate the deployment of advance applications, over the distributed environment of the Ministry. Staff will have convenient and speedy access to the Ministry's Intranet, subject to rigorous security assurance, whether they are in the office or at home.

Web-based applications shall be widely deployed to provide more acceptable and user-friendly interface to the users. Other initiatives include creation of e-Library, web-based teaching and learning, introduction of video-conferencing throughout the ministry's IT fabric. The aim shall be not to simply reduce the use of paper, but to achieve the objective of improving the quality of the ministry's work environment to bring about improvement in productivity and efficiency.

9 Technology

The tangible technical aspects of the NHIN include network backbones such as the Internet in its present and future versions; the World Wide Web; wireless connections; hardware such as computers, Internet appliances, and handheld devices; and applications for information management, decision-support tools, communication, and transactional programs. Also involved are technical capabilities in areas such as bandwidth and latency. A critical part of the strategy will be proactive efforts to ensure that technologies and standards that enable these technologies evolve specifically to meet the Ministry's needs.

The technology stack must be kept the same across various HMIS and other implementations to ensure compatibility and ease of re-use. In fact if detailed technical requirement document is available, it is even easier to extend the system in the future. Obviously this would necessitate that the detailed Technical Reference Manuals (TRMs) as well as logical and physical database design all are available. If all this is in place then the existing code base can be enhanced in the future more complex work flows. If built intelligently the business processes could be tuned with the help of configuration parameters. This is exactly the methodology that Oracle and SAP use to build their Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) system where individual modules can be tailored to behave differently and follow different workflows based on how the module is configured. A consistent set of tools and technologies also ensures that MoPH will be properly equipped to keep the systems operational on a long term. In case some of the personnel leave, others in the team will be able to help maintain the system while new talent is recruited. This is not possible with silos that get created with a diverse set of tools and technologies, a hotchpotch of different technology stacks, each one of them requiring specialised expertise and knowledge.

9.1 Free Open Source Software

Free Open Source Software (FOSS) and tools have been on the maturity curve for over a decade and the World is seeing increasing deployments of IT based on FOSS. Open source software and open source content are challenging existing software and content developers. One the major advantages of FOSS is that it can give the same functionality as any proprietary system at a much lower cost. Another advantage of Open Source is availability of community support which is a great asset in resolving issues and problems that are faced during deployment of IT systems using FOSS. The use of proprietary software tools invites recurring expenditure in terms of license renewals and version updates, which requires additional expenditure. When MoPH will use community-supported versions of FOSS there will be no direct cost component involved.

As Government of Islamic Republic of Afghanistan (GIRoA) continues to strive for greater transparency, the movement to expand access to public databases will spread and evolve since open tools empower pro-poor innovation by broadening access to government data. Further details on FOSS can be found in Annex-XIV.

9.2 Source Code

Source code for all bespoke application software that will be developed for MoPH will be the property of MoPH. An appropriate repository will be created for version control of the Source Code.

9.3 Database Management System

A Relational database management system will be deployed at MoPH and other entities under its domain for information systems development and usage. Salient features of the Database system are given in Annex-XV.

Sizing a Database solution requires careful analysis and usually will involve the cooperation of the General Directorates. The requirements of each area must be understood to achieve an optimal database solution design. A typical analysis comprises:

- Capacity planning (capacity to be supported by solution infrastructure).
- Business requirements – (includes continuity, availability, and security features)
- Technology selection – (server, storage, backup, and switch technologies)
- Software requirements (front-end applications)

The creation of a solution stack requires collection of input based on known business requirements such as database size, number of users, Input/Output per second (IOPS), and throughput expectations. This knowledge is used to develop a Database configuration. The recommended solution covers a comprehensive set of components, including servers, storage arrays, switches, and software. Some of the items that require to be determined in order to size a database are Hardware Capacity Planning and Sizing, Workload/Application Type, Business Continuity. Further details are available at Annex-XVa.

A system which can be securely configured to protect it from unauthorised access will be deployed. This helps eliminate as many security risks as possible. System hardening is done by removing all nonessential elements from the system and by selecting configuration options that limit access and reduce risk. Further details on system hardening can be seen at Annex-XVb.

9.4 Interoperability Framework

All databases and application software will comply to industry standards so that interoperability can be assured with other systems. With an interoperability framework in place, it becomes easier to integrate systems and solutions from multiple vendors, thus avoiding vendor lock-in.

MoPH should look to vendors that are able to deliver integration technologies to bridge different development platforms. Application integration and platform interoperability will continue to be critical elements of MoPH's strategy. MCIT's E-Gov Interoperability framework enables the government to adopt the best standards for the development of the e-Services applications. Under this strategy MoPH

adopts this framework. Annex-XVI Some level of detail on importance of interoperability systems.

9.5 Security

The information stored in computer files on our desktop computers and on the local area network is one of the most valuable assets of the Ministry, which needs to be protected and safeguarded. ICT Security is a continuously evolving field. Security breaches can be avoided up to the maximum possible extent by employing a two-tier strategy. First, is to shore up the weak links in the systems and procedures with either technology or eliminate them completely. Second, penalties for the various levels of security breaches needs to be introduced, documented and enforced in the Ministry. Access control implementation throughout the organization coupled with biometric identification of the employees can ensure physical security of the various areas.

Studies show that 60% or more of "impact events" where critical missions have been compromised are associated with human activity. This activity includes routine switching and reconfiguration of critical systems, maintenance tasks and, of course, human error. ICT systems and applications security concerns have to be understood and identified. For this An ICT Security Section needs to be created within the Ministry, which will be responsible for the over-all ICT security of the MoPH, PPHDs, Hospitals and other health units.

Some of the important aspects that would need to be considered are as follows:

- Designing the best security topology for firewalls
- Making a password policy part of the security plan
- Developing a software installation policy

MoPH will implement assessment and mitigation processes and technologies, in combination with shielding technologies, to defend against targeted attacks, but also needs to proceed under the assumption that defences will sometimes fail. Therefore, it becomes important in the context of ICT security to read system, firewall and database logs for potential breaches. Similarly, under the strategy, vulnerability testing of all software code whether written in-house or by a third party will be performed before going live.

For effective vulnerability mitigation the ICT Security Section works with IT operations to develop and implement operational processes. ICT Security Section shall work with IT operations to define security configuration standards, and drive implementation of security configuration standards in desktop, network and server provisioning processes. Furthermore, security monitoring shall be used to augment assessment shielding and mitigation efforts.

Annex-XVII provides details on this subject whereas a list of some threats and vulnerabilities can be viewed at Annex-XVIIa.

9.5.1 Defence in Depth

Break downs happen within networks due to human error, malicious behaviour, or hardware/software failure. The Ministry's operations plan must be sufficient to cope with these threats; to do so, it must meet five basic criteria: The plan must be comprehensively documented, widely supported, and it must reflect the current operations while allowing for both growth and the possibility of disaster.

The Defence in Depth model will conclude with policies for operating the Ministry's network. It mandates that every element of the network operation should be written and defined. The policy shall not be limited to daily operations. Although daily operations are important, a truly effective policy defines what actions should take place when the network is under stress from a systems attack or failure. Defining how the Ministry's network should operate and what actions should occur during critical events is the difference between hoping that the network is secured and knowing it's secured. Operating the network without a policy is an open target to disaster. Security operations should be fluid and should cover seven basic procedural areas, which can be seen at Annex-XVIIb.

Since the automation effort will heavily rely on internet for access and updates therefore internet facing serves will be in a Demilitarised Zone for ensuring security of the database servers.

9.5.2 Cyber Security

Contemporary attacks on ICT systems are happening over the Web; attackers usually develop malware to defeat anti-malware defences to compromise ICT systems. It is necessary to address cyber security concerns at the outset in order to ensure safety and reliability of networks for providing secure and accessible e-service applications. Another area where many organizations have a process gap that needs to be filled is incident response. The Ministry shall be developing comprehensive incident response plans in case of any security breach.

Since MoPH will be deploying internet server(s) for the various applications that will be developed for its internal use and for provision of eServices to the population, therefore Cyber security will be of paramount importance. We are aware that cyber attacks against states are on the rise and current Internet server hacks primarily concentrate on unpatched bugs and application errors. To protect against this risk developers will be required write their code using Security Development Lifecycle (SDL) techniques.

At a minimum the following will be done:

- Implement Intrusion Detection and Prevention– this will provide system administrators the ability to manage and apply security policies at a level of detail that protects against attack while providing legitimate users access to required computing resources. This feature can be implemented by using an appliance.

- Implement Workstation Endpoint Security – This will allow IT staff to ensure that individual PCs' can be "locked down", thereby decreasing their vulnerability.

- Commit to ongoing security training for IT staff – this will ensure that staff maintain an awareness

of emerging security threats and learn to implement the strategies required to defend against those threats.

- MoPH shall filter and monitor staff's Internet usage to ward off low productivity and the security of the network. Internet is notorious for hosting malware and many web-sites contain content that attracts numerous visitors and this attribute makes them the ideal medium for spreading malware.

Annex-XVIII provides details on Cyber security.

9.5.3 Data protection

Man made or natural disasters can take their toll on MoPH's systems. Therefore deploying the right resources, processes and technology to protect key information and minimize downtime is important. Having adequate resources and technology in place for protecting invaluable data is very important and critical. For MoPH as an IT enabled and IT driven Ministry it becomes very important to take regular backups of all the information on all IT systems. Further details can be seen in Annex-XIX.

10 Hospitals Automation

The Ministry has an approved Hospital Sector Strategy (HSS), April 2011. Under HSS hospital autonomy will be established in National and Specialty Hospitals, first. All other hospitals followed suit upon success of the strategy in the National and Speciality Hospitals. ICT can be very effectively leveraged in achieving the over-arching objective.

Some of the problem areas that HSS mentions can be addressed quite effectively by implementing IT Application Systems in the hospitals. These areas are highlighted as follows:

- HSS terms "Poor coordination, un clarity on rules and responsibilities, un transparent financial and procurement system and low knowledge of data and information are the common problems at the hospitals" as an Implementation Risk in moving towards hospital autonomy.

- Information Gathering and Utilization is one of the larger Strategy components as well as a component of the Implementation of the Strategy that can be IT based. The components states "Information Gathering and Utilization will be used in the management of all hospitals, the control of all finances, and the improvement of clinical practices. Data collection and utilization will be started on a limited basis with the initial system being within the capacity of existing hospital staff and resources. As success is gained in information use, increasingly complex indicators will be introduced. The eventual goal is the implementation of a comprehensive Hospital Information System (HIS) at all facilities" and "Regular utilization data collection is implemented in National and Specialty Hospitals by Jul of 2011. Utilization data is collected on a regular basis in all hospitals under the control of the MoPH by January of 2012" respectively.

- A high priority objective of the Hospital Sector Strategy is Budget Based Management, which states "Hospitals will be managed on the basis of full financial knowledge. In the immediate term, all financial information such as actual budget allocation, the MoPH and the Ministry of Finance (MoF) will provide budget utilization and complete historical expenditure records to hospitals".

- Under Monitoring and Evaluation heading IT systems can help in Information Gathering and Utilization by automating the process through which utilization data reports summary data reports are created for the Hospital Management Team and for the meetings of Community Boards/Boards of Directors respectively.

To achieve the above and many more automation of the hospitals will be initiated under a programme, which will provide interfaces to MoPH and MoF systems for seamless connectivity. For details on hospital ERP System please see Annex-XX.

11 Funding

High-level funding details for two programs, summarised below, can be seen in Annex-XXI.

Summary of Investment for ICT Program of MoPH

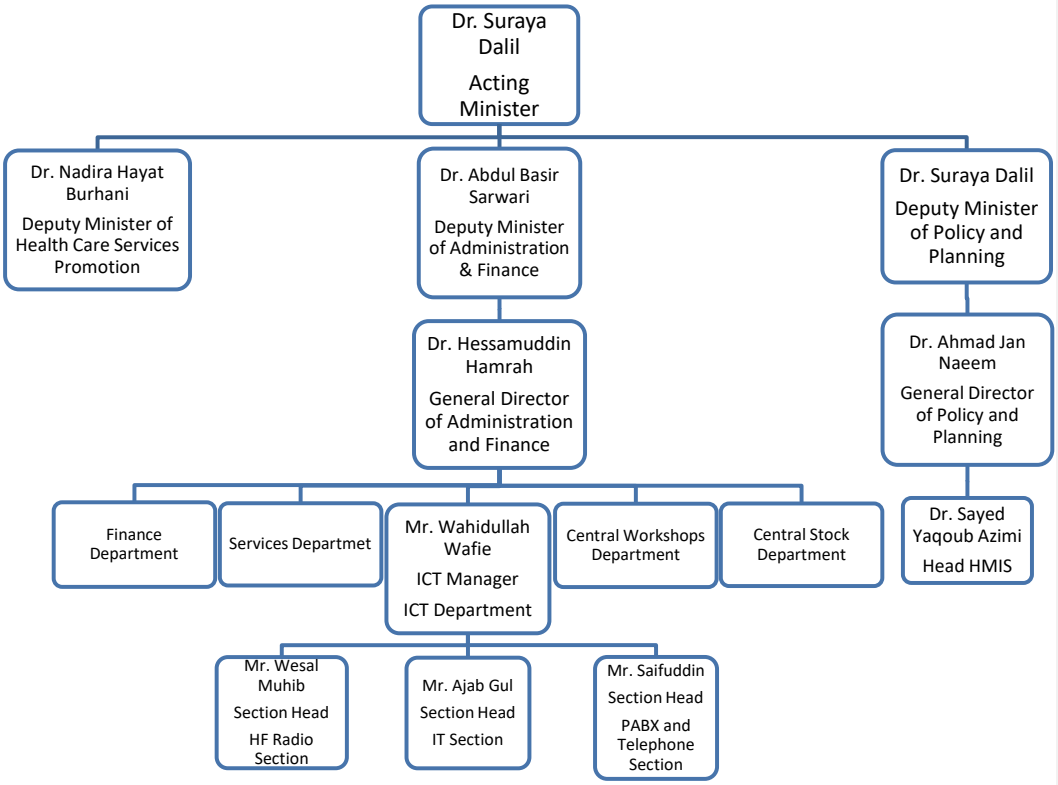
Values in US Dollars

Description	Budget year					Grand Total
	2012-13 (1391)	2013-14 (1392)	2014-15 (1393)	2015-16 (1394)	2016-17 (1395)	
Ministry of Public Health and Provincial Public Health Directorates Automation Program	1,318,000.00	3,391,000.00	2,272,600.00	1,906,860.00	1,902,546.00	10,791,006.00
Hospitals Automation Program	240,000.00	495,000.00	630,000.00	1,205,000.00	1,860,000.00	4,430,000.00
Grand Total	**1,558,000.00**	**3,886,000.00**	**2,902,600.00**	**3,111,860.00**	**3,762,546.00**	**15,221,006.00**

The ICT initiative will spawn a number of short and medium term projects under this strategy. It is recommended to hire an International ICT Consultant for this purpose. Telecommunications Development Fund can be approached for using funds under their control for financing this initiative.

Annex-I

Organogram of the ICT Unit of MoPH is shown below:



Annex-II

Details of the IT operations that are in vogue and its short comings

Procedure for implementing and maintaining IT Systems

The responsibility of the IT Section under the ICT Unit presently is the supervision of the daily operation of Internet, Local Areas Network, DHCP Server, and ISA Server. Human Resource Management Information System (HRMIS) server has been moved in January 2012 to the Server Room, which needs to be managed by the IT Section.

The IT Section is currently overwhelmed with providing help desk support to the user base which is around 1000 Laptops and PCs. People usually walk in the IT Section with their malfunctioning machines and want the issue resolved in quick time. The IT Section is mostly busy in installing hardware and software and troubleshooting problems. Little time is left for planning activities to improve the infrastructure and think in terms of modernization and implementing new application software. More IT staff is required to create a separate help desk section within the ICT Unit. This would save the IT Manager's time and allow him to strategise more.

The unit does not have run books/procedures/manuals for maintenance and operations of the various Servers and Software installed and running in the Server room. Such manuals usually describe the procedure to be followed when changes need to be implemented. The IT Unit does not have any responsibility to manage or maintain any Database systems or any application software. This responsibility lies with the HMIS department.

Daily Operation of the IT Systems

The daily operation of the system in the Ministry includes supervision of the operation of the hardware and basic windows software, assistance to the users in case of hardware problems, minor repairs like swapping of screens, and keyboards etc.

These daily operations are based on "Job streams" where the ICT Unit has no possibilities of interfering. Data backup is lacking and it needs to be instituted.

.Systems Architecture / IT Policies

The Ministry has not established formal overall policies in relation to the systems architecture but is following the de facto standards of the IT market concerning IT hardware and basic software. Currently Ministry bases its IT-architecture on the following standards:

Component Standard / Supplier

Servers Intel / Microsoft

Workstations Intel / Microsoft

LAN UTP Category 5/6

Network architecture/Equipment Cisco

Office Automation Microsoft Office

The Ministry should for cost and performance reasons needs to start looking at the freeware Linux Operating System and Open Source horizontal applications as potential replacements for Microsoft Windows and Microsoft Office. The Ministry at the moment does not have a Business Continuity Plan or Disaster Recovery Plan.

Specific Implementation of the Systems Architecture

Hardware and Basic Software

The hardware architecture implemented in the Ministry is based on client server architecture with a central server configuration installed in Server Room of the ICT Unit to which the clients (workstations) are directly connected. Presently directory services have not been implemented.

The only application that is hosted in the Server room is the HRMIS and it utilizes three tier architecture.

Central Servers

The central servers are installed in the Server room. The central servers comprise of network-, database-, application-, and ISA-, servers installed in a common rack. The network server controls the LAN network of the Ministry.

The database server has MS SQL Server Standard Edition, Crystal ……., HRMIS database, Internet Information Server (IIS). The servers are all running under Microsoft Windows 2008 Server operating system. The database system is Microsoft SQL Server. The Server Room is equipped with two UPSes of 10KVA each. The Ministry has at the moment no spare servers, DAFA will soon provide the Ministry with more servers.

Network Implementation

LAN networks have been installed in the ministry; the network is based on UTP type 5 cables. The LAN networks are all running at 100Mbps. The majority of the network components (switches) are based on Cisco equipment.

Client Configurations at Head Office

All client workstations at HO are PC's based on Intel processors. In general the capacity of the PC must correspond to the tasks the employee is performing. Almost all PC's and notebook computers that connect to the LAN are running under MS Windows operating systems.

.

Security Systems

The Ministry has not established and implemented formal procedures for allocating User ID's, passwords for network access and email addresses. A form needs to be designed and approved for filling in for each user that needs temporary or permanent access to the network. The request should be approved by the respective General Director and In charge of the IT. Based on this the network administrator of the IT Department will set up the user in the system.

All control of network, user ID's and passwords will take place via the Ministry where the Master Domain Controller will be configured and it shall allow the network administrator to access the equipment in the PPHD. In case that a user exceeds the maximum number of attempts to enter password he will be locked out of the system and the manager of this person has to start a procedure to have the system reopened for him/her. The network administrator, together with the Manager IT, will have the authority to access the operating systems and other pieces of basic software and undertake the administration of the users as described above.

Procedures manuals

The Ministry has today no formal written procedures for the operation of the central server configurations, backup- and restore procedures etc. This means that the Ministry is dependent of individual members of the staff when the activities have to be performed. In case that these individuals are not available it might cause serious delays if other members of the staff or the suppliers have to take over.

A minimum of these procedures should be present.

Software Application

User Security, Access Control, Authorization

Each user of the IT systems will be allocated a user id and a password, which will give her/him access to the network of the Ministry including the email system and other systems. To get access to the application software systems a new password must be allocated to the user as well as authority to use specific functions within the system. The Ministry will prepare and implement a procedure where the general director of the user signs a form where the relevant information about the user plus the authority levels wanted is specified. This form will be signed by the Head of IT and the Manager of the Information Security Department. Following this the officer of the Information Security Sector keys in the data and the user will have access to the system. The system will allow for automatic request for

changing of passwords at specified interval, certain format of passwords not allowed etc., but these functions are not implemented at the moment.

Audit Trails

All application software systems in the Ministry will include an audit trail function. This will assist in tracing certain incidents. In addition these selected reports might also be used for audit purposes including export of data for further analysis. The Information Security Department will be responsible for ensuring compliance.

Users Manuals

Manuals for allocating user ID's, passwords and authorities need to be developed and implemented.

Manuals for back up restore of systems need to be development and implemented.

Manuals for operating the central servers need to be developed.

Production Volumes and Performance

Reports on the operation of the IT systems are missing and need to be are prepared on a daily basis. Based on this the IT Department will be able to maintain an overview of the operation and also prepare some statistics and management reports.

Supply Systems and Physical Security

UPSses are available in the Server room which give uninterruptible clean power to the Servers and Network equipment installed in the Server room. However for nonstop operation a redundant and alternate power source is needed to support all equipment and air conditioning in the Server room(s)/Data Center.

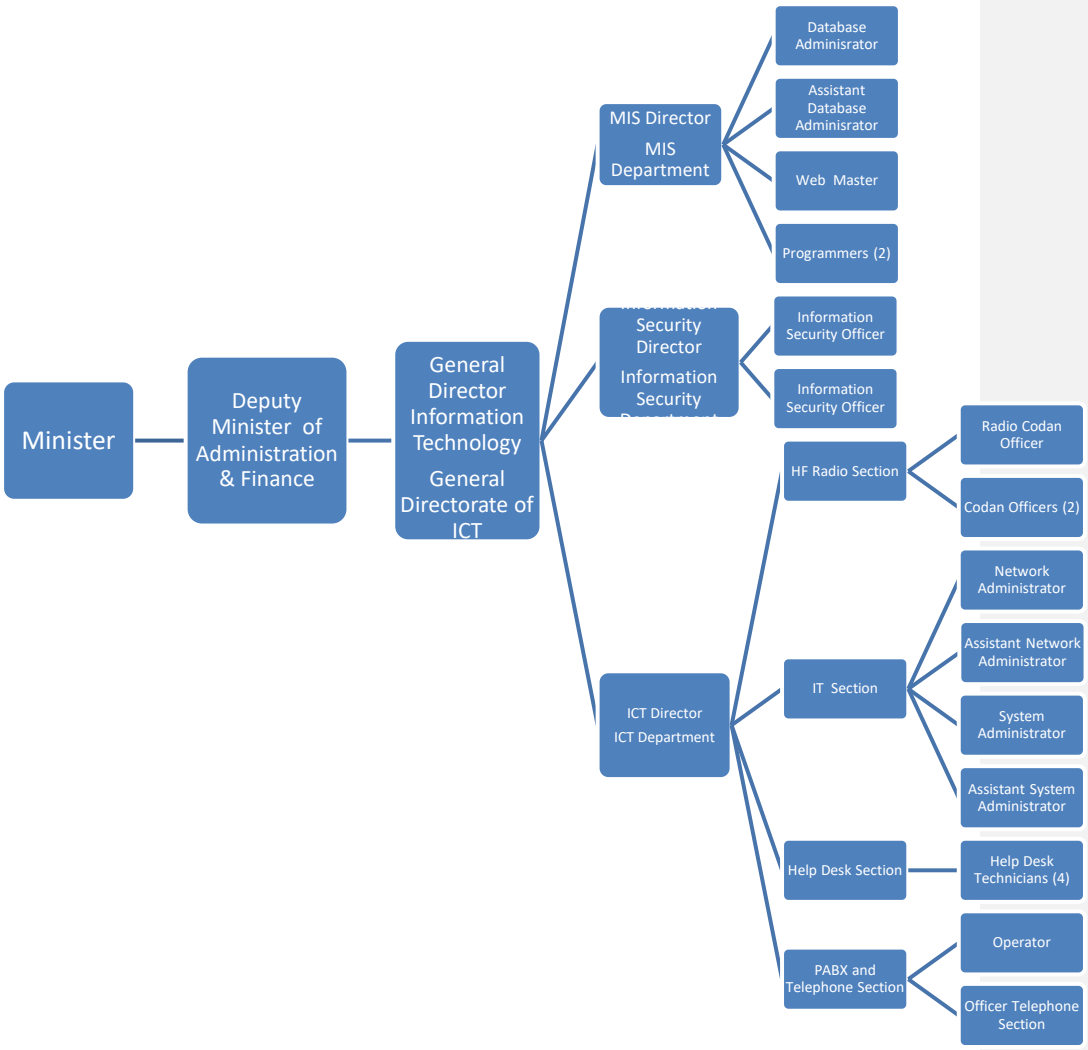
Maintenance

The Ministry utilises the warranty period of the equipment and is setting up maintenance agreements when the warranty expires. The Ministry needs onsite maintenance on all pieces of equipment. In connection with the procurement of the new servers the Ministry needs to sign a maintenance agreement according to which the supplier is obliged to set up spare servers if IT cannot repair a server within a given period of time.

Backup, Fall Back and Disaster Recovery

The Information Security Department, which is a function proposed under this strategy will be responsible for the allocation of user ID and passwords. In addition to this the department should also become responsible for the operational risks in relation to the IT systems of the Ministry.

Annex-III


Minister
Deputy Minister of Administration & Finance
General Director Information Technology
General Directorate of ICT
MIS Director
MIS Department
Database Adminisrator
Assistant Database Adminisrator
Web Master
Programmers (2)
Security Director
Information Security
Information Security Officer
Information Security Officer
ICT Director
ICT Department
HF Radio Section
Radio Codan Officer
Codan Officers (2)
IT Section
Network Administrator
Assistant Network Administrator
System Administrator
Assistant System Administrator
Help Desk Section
Help Desk Technicians (4)
PABX and Telephone Section
Operator
Officer Telephone Section

Annex-IV

Databases being used in the Ministry are: M&E database, HMIS, DEWS, EPI database, HR database, Procurement database, and Payroll system. These need to be integrated, wherever feasible technically and required operationally, and brought under one data centre control. The databases also need to be improved to be used effectively in evidence based decision making:

1. Health Management Information System

HMIS is a database developed in Micro Soft Access and in use in the Ministry and all Provincial Public Health Directorates developed with USAID assistance under Tech Serve project contract to Medicine Science for Health (MSH). It is an off-line, stand alone system which is constantly evolving with the aid of MSH. HMIS department is responsible for this database and all databases in the Ministry.

2. Human Resource Management Information System:

Human Resource Management Information Systemxxiv (HRMIS) - a bespoke software application - has been developed by a local Software House to provide database capability to General Directorate of Human Resource (GDHR). The application has been developed with the cooperation of Australian AID's Development Assistance Facility for Afghanistan (DAFA). The application is expected to go live very soon. The domain owner of the subject is General Directorate of Human Resource (GDHR) in the Ministry.

The direction is to improve information availability regarding the composition of health sector human resources and build relationships with key stake holders to improve the flow of information within the health sector relating to HR requirements, availability, shortages and losses due to attrition (key stake holders here would be Hospitals, Health Care Institutions, Medical Schools, Health technician training schools, Afghan Medical Council, Nursing Council etc.).

3. HR database

It is a MicroSoft Access based database in control of GDHR which will be replaced by the new HRMIS. HRMIS is currently undergoing testing in GDHR.

4. Procurement database

It is a MicroSoft Access based database in control of General Directorate of Administration and Finance (GDA&F). It is a very limited database and does not fully meet the requirement of the Procurement Department.

5. Health Care Workers (HCW) Registration System[xxv]

A system of HCW registration and the early maintenance of a HR database, a preliminary national testing and certification examination process (in collaboration with MoHE) to identify training needs and an upgraded pre-service curriculum for nurses and midwives, are already in place. Standards for

accreditation of training institutes and programs as well as for medical doctors registration are also being put in place.

Annex-V

Geography plays a major role in understanding the dynamics of health, and the causes and spread of disease[xxvi]. The classic public health triad composed of man, agent/vehicle and environment emphasises the importance of geographic location (environment or space where we live) in health and disease. Interactions within this triad can also change with time. Today's health planners aim at developing health policy and services that address geographical and social inequalities in health, and therefore should benefit from evidence-based approaches that can be used to investigate spatial aspects of health policy and practice, and evaluate geographical equity (or inequity) in health service provision[xxvii].

One widely agreed upon definition of Geographic Information System (GIS) comes from Star and Estes (1990) who state that a GIS "is an information system designed to work with data referenced by spatial or geographic co-ordinates. In other words a GIS is both a database system with specific capabilities for spatially referenced data as well as a set of operations for (analysis) with the data" (quoted in Wheatley and Gillings 2002: 9).

A GIS is able to provide:

1. Quick and easy access to large volumes of data
2. The ability to; link one data set with another; analyse spatial characteristics of data; update data quickly and model data and access alternatives.
3. Output capabilities (maps, graphs, address lists and summary statistics) tailored to meet particular needs.

Annex-VI

PAPER ON MoPH E-LEARNING PROGRAM

Introduction & Background

Information and Communication Technology (ICT) is a powerful enabler of positive and sustainable development in countries around the globe. Globalization and the shift to a 'knowledge-based economy' require that educational institutions develop individuals who have the ability to transform information into knowledge and to apply that knowledge in dynamic, cross-cultural contexts. Information Communication Technologies (ICTs) are a means for meeting these twin challenges.

This paper aims to explain that how ICT can be used in providing learning opportunities to MoPH staff and how it can better benefit current and future users. It also highlights the ways in which ICTs can be leveraged to support and improve the delivery of learning at Provincial and National levels.

Concept

Learning and Education in the future will exist in a different format and technology will transform and dictate that format. The effectiveness of these new tools and formats are always being associated with learning styles, pedagogy, equity, access and many other variables. This shift of paradigm is necessary to utilize the technology in gaining and disseminating knowledge to the society.

For initiating this concept Ministry of Public Health (MoPH) will require to develop a cross-cutting E-Learning Program targeting all levels of the employed technical staff and staff that will be inducted in the future. E-learning also includes digital content, experienced through a technology interface, and is net-enabled. However the following need to be ensured before we can embark on any e-Learning program:

a. Develop a detailed concept.
b. Clearly delineate roles and responsibilities of MoPH Directorates.
c. Institute indicators to measure success.
d. Develop a model for sustaining the initiative.
e. Develop an E-Learning program

E-Learning Enterprise Portal (ELEP) can be created to establish close relationships with Directorates and occupying strategic ground in the growing trend toward Web-based, learning-centered MoPH system.

Successful implementation of this concept can improve access to and promote learning in MoPH by providing opportunities to a greater number of staff on a pace and time of their own choosing. This can

also improve management of professional leanings through more efficient administrative processes, including human resource management, monitoring and evaluation, and resource sharing.

This initiative shall be owned and implemented by the General Directorate of Human Resources. The ideas presented here respond to the educational priorities including:

- Increasing Educational Access in remote offices, hospitals and provinces.
- Increasing and Improving Skills Development of the staff and doctors within the domain of MoPH.

Action-Plan

The development of **E-Learning Program** will be based upon the following Terms of Reference:-

- To consult General Directorates and gather information and recommendations for developing the E-Learning program.
- To prepare a Project Plan that will cover all elements needed to launch a successful and sustainable program.

Guidelines that will help in implementing the action plan are:

- Formulate and assess ICT-enhanced programs.
- Plan for physical and human requirements.
- Plan for ICT-enhanced contents.
- Generate program costs.
- Create a master plan and monitor implementation, effectiveness, and impact.

Estimated Project Cost

The financial cost of ICT acquisition is usually a major focus of attention in policymaking and project planning. But the cost of acquisition is only one aspect, and policymakers and administrators need to budget for the recurring costs that form part of the Total Cost of Ownership (TCO). Thus, even if computers may be acquired for free, as in the case of donated computers, they require a substantial financial investment for maintenance and support. The costs are given in the Financials in Annex-XXI.

The development of content for ICT-supported teaching and learning is another key policy area. Development of content software that is integral to the teaching/learning process is a must. We need to make a choice between acquiring or creating new ICT-enhanced educational content and software. Suitability (including curriculum relevance), availability, and cost are key considerations in making this choice. And the selection of appropriate content and software has to be made not once but many times, since different learning contexts will have different requirements, for example in terms of age and learning abilities, subject-specific demands, and culture and language.

Annex-VII

The aim of e-Health is to eventually have an integrated system for the country. A number of Health Information Standards have been developed internationally to have a uniform and interoperable e-Health System such as HL-7 etc. A standards based deployment ensures an agreed and repeatable way of describing something to achieve a common understanding. Standards in health information have come about as a result of changing technologies and changes in the way healthcare is delivered. Health information standards support the increasing need to safely and securely exchange a wide variety of patient information between various healthcare providers. Adopting a standardised approach to health information across the health and disability sector will assist the Ministry to achieve their vision of high quality health care and improved patient safety.

The eHealth IMPACT study[xxviii] provides empirical evidence on the benefits of eHealth systems and services. It demonstrates the potential of eHealth as enabling tool for meeting the 'grand challenges' of European health delivery systems. Policy makers, industry, and healthcare providers alike must be aware that the realisation of this potential depends on six key factors:

i. Commitment and involvement of all stakeholders: All phases of eHealth development, implementation and deployment have to be supported by citizens/patients, health providers, industry, authorities, and third party payers.

ii. Strong health policy and clinical leadership that guides a flexible and regularly reviewed eHealth strategy: While the strategy should be directed by a long term vision of a citizen-centered health delivery system, it must address concrete needs of actors in the system. The strategy should include achievable, shorter term goals that create an eHealth investment dynamic. A big-bang approach with ambitious goals to be achieved over a short period of time is not recommended.

iii. Regular assessment of costs, incentives and benefits for all stakeholders: Considering purely financial return on investment at an institutional level, or potential benefits for only one of the stakeholders, may lead to suboptimal decisions. Particular attention should be paid to include all users, some of whom are often neglected in such assessments.

iv. Organisational changes in clinical and working practices: This is indispensable in order to optimise the use of ICT-enabled solutions and realise the benefits. Such changes should be facilitated by greater legal certainty in using eHealth solutions.

v. Strong clinical leadership, good organizational change management, multi-disciplinary teams with a well-grounded experience in ICT and clear incentives: The combination of skills of the people involved will make the difference between success and failure, not the specific eHealth solution. Skills development through continuous education and training is essential.

vi. Long term perspective, endurance and patience: Beneficial eHealth investment is like a good wine. It takes a considerable amount of time (about 5 years) to mature and develop its potential fully.

Data dictionary containing metadata for a range of health services is important to develop for Afghanistan. Some of the Health care IT Standards are given in the following table:

Data Standards	
Examples of Standards Development Organizations, Data Content Committees & Designated Standard Maintenance Organizations	**Domains**
ASC X12	Financial/Business Transactions Terminology
CDISC	Clinical Trial Terminology
AMA – CPT Editorial Board	Clinical Procedure Terminology
DICOM	Digital Images
HL7	Healthcare, Public Health
NCHS/CMS – ICD-9-CM Coordination and Maintenance Committee	Healthcare, Epidemiology, Health Statistics
ISO	Medicinal Products, Pharmaceutical Doses, Units, Common Terminology Services
LOINC	Laboratory, Clinical Observations
NCPDP	Pharmacy Terminology
NUBC	Hospital Billing Form
NUCC	Professional Claims
OASIS	Bed Availability
ANA	Nursing Terminology
PHDSC	Payer Typology

IHTSDO	Clinical Terminology (SNOMED-CT)
NLM - UMLS	Biomedicine, Healthcare, Drugs (RxNorm)
UCUM	Units of Measures in Science, Engineering, Business

Landscape of e-Health Applications

e-Health Applications	Type of e-health application	Short summary description
Integrated Healthcare Environment IHE Pathway for the Patients: "Patient Treatment Lifecycle Management (PTLM)"	IHE's application is high resolution patient image and data storage and the availability of the same patient data at any authorised point of presence, within and outside UBHT. Integrated with audio-video-data conferencing, it enables real time consultation as in eMDTs or eMDMs between medical staff across the region and in the presence of the patient when necessary Regional Network / Electronic Health Record; Virtual, region wide multi disciplinary clinical teams (eMDTs) in real time consultation with an expert centre. United Bristol Hospitals NHS Trust. UBHT is a teaching hospital with some 1,200 beds. The IHE network extends across South West England and serves seven specialist	The IHE initiative is operated and driven by the Directorate of Clinical Radiology. It applies the ICARAS* standards-based implementation strategy to develop and deploy medical images and health records across the South West region. The facility is available to an expert in any part of the World. It uses high speed fixed and mobile-wireless data links. The Directorate is the expert centre for acute care in the South West, and connects to all trusts and hospitals that refer patients to UBHT. Clinical services in the IHE framework currently include: cancer, paediatrics, obstetrics, cardiac catheter laboratory, pathology, GI, ENT and radiology. The organisational core that underpins the IHE initiative are the numerous, virtual, region wide multi disciplinary clinical teams (eMDTs) that exchange and share real time clinical images and data. It uses the expert contributions of the specialists located at other hospitals without them travelling to these meetings at any one site. IHE relies on clinical patient data acquisition systems as from "direct digital and digital click-stream data" which include ultrasound US, CT, MRI, DR, CR, PACS, HIS, RIS, Intranet, and the Internet through broadband communication networks such as ISDN6, NHSnet, xDSL and Cable. Within the next few months, satellite based facilities will be in place as well. They will facilitate extending the current activities to remote areas in order to enhance the eHealth & eLearning services.

	hospitals and GP practices. It is also available to the rest of the UK and accessible globally.	Integrated audio-video-data conferencing facilities are used for some activities in the provision of eMDT support for patient care Nationally and Internationally. The medical "image and report" viewing facilities ("GUIs") are work-station, thin client and Web based to allow for standards based vendor-neutral, multi-modal image data acquisition and viewing platforms at any secure, authorised Point-of-Presence "PoP". * **I**nteroperability, **C**ompatibility, **A**ccessibility, **R**eliability, **A**ffordability, **S**calability
PCDOM PimaCare	An integrated Electronic Health Record (EHR) and Clinic Management System (CMS) developed by GPs for GPs	Third party applications do not meet needs of GPs – Inability of MOH to collect data from GPs despite regulatory provisions – Current available data not useful for planning purposes – No attempt at standardized approach – Timely access to information resources – Delivery systems that support clinical decision-making – Best available evidence of efficacy and risk for a shared understanding of appropriate practice – Research and evaluation

e-Prescription

e-Prescription is understood as the process of the electronic transfer of a prescription by a healthcare provider to a pharmacy for retrieval of the drug by the patient. e-Prescription is seen as a set of at least three types of application, namely: electronic medication records, decision support systems, electronic transmission of prescriptions. Till now, computerised procedures for prescriptions (e.g. transmission of prescriptions) have been used mainly in hospitals, between physicians and internal pharmacies, but mainly for administrative purposes (e.g. consumption, stock management) and not, let us say, for recording medication to control incompatibilities (however it is possible to have some such local IT applications, but they were not rolled out). 1The prescriptions need to be signed, dated and stamped by the prescribing physician for which an implementation of digital signatures would be required. Afghan National ID number can be used as unique identifier for patients in addition to biometrics such a thumb and index fingers prints.

Electronic Medical Records

An electronic medical record (EMR) is a computerized medical record created in an organization that delivers care, such as a hospital or physician's office. Electronic medical records tend to be a part of a local stand-alone health information system that allows storage, retrieval and modification of records[xxix].

Benefits of Using an EMR or EHR over Paper Charts

Legibility of Notes – No more dealing with various handwriting styles since notes are typed. **Accessibility of Charts** – Indexed and easily searchable by multiple identifiers. No more searching the entire clinic for a lost paper chart.

Transcription Costs Savings – Many users have been able to save on transcription costs by implementing an EMR.

Space Savings – Many people are able to save space where they'd normally be storing shelves and shelves of paper charts.

Eliminate Staff – This almost never happens immediately. Usually this happens through natural turnover of employees and usually occurs with your front desk or medical records staff.

Eligibility for Pay-for-performance – It could take two years or more for you to implement an EHR and implement a meaningful quality improvement mechanism that would lead to your receiving payments from these programs.

New Physician Recruitment – Many new physicians are looking for practices that use an EHR and will only work for an organization that uses an EHR.

Multiple Users Use a Chart Simultaneously – Most EMR programs support multiple users accessing a chart at the same time. Many even allow multiple people to chart notes at the same time also.

Lab Results Returned Automatically – This depends on a lab interface, but is more reliable and integrated with the care given.

X-Ray Results Returned Automatically – This also depends on a X-ray interface, but has the same possible benefits of a lab interface.

Save a Tree and the Environment – You won't eliminate your use of paper, but you can significantly reduce the amount of paper/charts you use in your practice.

Electronic Prescriptions – Scripts sent electronically or printed out avoid problems of legibility by the pharmacy receiving the script.

Spell check – Many EMR software includes a spell check and often even include a medical dictionary.

Disaster Recovery – Depending on your EMR backup schedule, you can store a copy of your data in multiple locations for better disaster recovery. Plus, in an emergency you could carry a backup of your data with you. Think about how you'd carry a room full of charts with you in an emergency.

Drug to Drug Interaction Checking – Most EMR provide a database of Drug to Drug interactions when writing a prescription.

Drug to Allergy Interaction Checking – Most EMR provide a database of Drug to Allergy Interaction checking when writing a prescription.

Patient Safety – Better information access, reduced gaps in communication between providers and reduction in duplicate testing.

Annex-VIII

e-Health Systems including Hospital and Health Unit Management Systems

This would cover all administrative and financial requirements of the facilities form a large hospital to a small health unit. List of major modules is as follows:

- Patient Registration
- Appointment
- Admission Discharge Transfer
- Wards & Bed Management
- Operation Theatre
- Clinic Specialties
- Laboratory Information System
- Radiology Information System
- Management Information System
- Pharmacy
- Blood Ministry
- Patient Billing
- General Store
- Inventory System
- Hospital Administration
- Payroll System
- Financial Accounting

Annex-IX

Establish Health Contact Centre

The Health Contact Centre (HCC) would be a multi channel Contact center. It is envisaged that the contact center will provide the following services:

b. Act as a client (Citizen) complaint system[xxx] and facilitate provision of remedial measures
c. Communicate health advisories and emergencies and provide information on transportation to the health facilities
d. The HCC is also responsible for the development and integration of existing or future health care services which can be delivered through contact centre management practices. Contact centre environment, and involves the provision of clinical human resources.
e. Provide counseling services to Citizens.
f. Provide Physicians answering service
g. Deploy 24 hour staffed health advisory center based on a rigorously defined health "decision tree" for bi-directional dialogue between the BPHS and CHS levels of service delivery, and the MoPH Knowledge Base (KB) of practitioners.

Contact Center Strategy

One of MoPH's role is to facilitate the public in getting health care services. Therefore it is also important to assist the public to an extent where it can comfortably obtain information on the many dimensions of health and related services. A high quality CRM application system will be required to assist the contact center staff the managers to provide a good service. An exercise to evaluate the feasibility of such a center would be required.

For a successful contact center use of Key Performance Indicators (KPIs) to evaluate operational efficiency on metrics that are important to both the MoPH and the public play a key part. KPIs may include average speed of answer, average handle time (how long it takes to complete a transaction), abandonment rate (percentage of calls that don't get answered), or first call resolution rates (percentage of customers satisfied when the call is closed) etc. Other KPIs can be used to measure effectiveness, such as public satisfaction surveys etc. Collectively, these KPIs would help in creating a large array of measures that ensure there is a balance between efficiency and effectiveness. By monitoring the right metrics, an efficient and effective contact environment can be run that would satisfy the requirements of the MoPH and the public at large.

m-Health

Mobile health or m-health or Mobile IT in health, has the potential to empower health workers (midwives, CHWs, community nurses) especially female health workers with ICT Tools to increase effectiveness of the support they provide in the community. It is expected that by the year by 2020 most

of the World's population will have basic mobile voice communications, and more than half will have access to a smart phone or inexpensive tablet computer[xxxi]. Asia Pacific region has also started to see this growth in such mobile devices from 2011. Conservative estimates state that the number of smart phone devices sold is expected to reach almost 500 million by 2015[xxxii]. These devices will be capable of voice and text communications, high speed Internet, high-resolution interactive video, location sensing, and considerable computing power and data storage. Manufacturing economies of scale will drive down costs, as hundreds of millions of devices are produced annually. Sophisticated personal devices will become important sources of sensory data about their owners and their urban surroundings.

It can reasonably be expected that following global trends the proliferation of Smart phones and tablet computers would increase in Afghanistan as well. These devices can be used by the care givers and citizens for rendering or obtain health related services. Mobile technologies can be used to broadcast health related public service messages through multiple channels such as Short Messaging Service (SMS).

Annex-X

Electronic Health Record

A commonly used definition describes EHR as "digitally stored healthcare information about an individual's lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times". In other terms, EHRs are repositories of electronically maintained information about individuals' lifetime health status and healthcare, stored such that they can serve the multiple legitimate users of the record. According to Institute of Medicine, there are eight core functionalities that constitutes EHR system i.e. i) Health information and data ii) Result Management iii) Order / Entry Management iv) Reporting and population health management v) Electronic communication and connectivity vi) Patient support vii) Administrative processes viii) Decision Support.

EHR should include information such as observations, laboratory tests, diagnostic imaging reports, treatments, therapies, drugs administered, patient identifying information, legal permissions, and allergies. This information is stored in various proprietary formats through a multitude of medical information systems available in the market. (This information always established beyond an institutional framework (regional, national, global), web-based, includes participation of citizen in creating the record). Quite obviously, this is a rather idealistic definition and concept, probably not yet brought to real life anywhere worldwide. Systems consistent with this definition can be found only in rather confined local or regional contexts, and for persons born only recently so that indeed complete lifetime data are available. Furthermore, to meet this challenging definition, usually an interoperable system connecting partial EHRs stored at various healthcare providers and other actors will be necessary.

EHR Standards

EHR is complex system comprises information related to observations, laboratory tests, therapies, treatments, diagnostic imaging reports, patient demographic and identification information, allergies, legal permissions and drugs[xxxiii/xxxiv]. The implementation of huge system with scattered modules is challenging and the information is needed to be stored and communicated in standardized way. Three parameters[xxxv] are followed to make information useful and standardized in EHR;

- Healthcare message exchange
- EHR Object Model (contents and structure)
- Healthcare terminology / vocabulary

The first parameter indicates that EHR should have capability of exchanging standard based information. In simple words, EHR should be interoperable and support exchanges messages of healthcare domains. The second parameter represent requirement of having common reference object model for information encompassing the healthcare arena. All the domain specific information should be derived from these reference object model. Third parameter stressed on binding the attributes of reference object model to standardized vocabulary. This will enable two different EHR applications to share information as both based on consuming standardized vocabulary from standard coding systems.

National E-Health Transition Authority (NEHTA) of Australia provided feasibility and recommendation of Shared EHR for Australian healthcare domain with using existing standards of EHR. In reports, two types of standards are mentioned to be used in Shared EHR for effective sharing of information[xxxvi];

- Shared EHR Architecture Standards for specifying contents of logical structure of the information and concepts in clinical domain. This part relates to last two parameters mentioned above.
- E-Health Information Interchange Standards for providing syntax and structure of the contents exchanged between Shared EHR systems. It maps to first parameters mentioned in above.

According to survey[xxxvii] three organizations are responsible for creating standard for EHR, HL7, CEN TC 215 and ASTM E31. openEHR is also providing standards specification and reference implementation for EHR[xxxviii/xxxix]. In this section, only leading standards including HL7, EN13606 from CEN and openEHR are discussed.

openEHR as EHR Standard

openEHR is detailed open specification for comprehensive and interoperable healthcare computational platform incorporated for EHR. The standard is based on real world experiences and provides full proof reference implementation of the specification[xl]. The main strength of openEHR is its comprehensive leading edge architecture and reference model in the form archetypes[xli]. The specification development follows the coherent design philosophy and mainly extracting artefacts from real implementation experiences. Moreover, it distinctly separates information; services and enterprise view points and provide orthodox object oriented extension for additive semantic provision in object models[xlii]. openEHR is not focusing on messaging paradigm; however it interoperates with messages and can be aligned with some particular messaging standard specification like using HL7 specification (e.g. units; UCUM specs).

openEHR have some principal drawbacks that makes hurdle in its deployment. First; there is no widely accepted SDO on the back of the specification of openEHR. Second; lack of individuals having proficient skills in openEHR technology that leads to deployment by fulfilling the actual intent of the technology. Third, stakeholder resisted on deployment of openEHR components as a ground of cost, disruption and risk. Finally, lot of research is needed for improvements and it subjects to change in specification.

Healthcare Information & Management Systems Society

The Healthcare Information and Management Systems Society (HIMSS) is the organization exclusively focused on providing global leadership for the optimal use of healthcare information technology (IT) and management systems for the betterment of healthcare. HIMSS was founded in 1961. Currently it is spread across different parts of the globe. Currently it has nearly 25000 individual members and about 400 corporate members. These members collectively represent organizations employing millions of people. HIMSS frames and leads healthcare public policy and industry practices through its advocacy,

educational and professional development initiatives designed to promote information and management systems' contributions to ensuring quality patient care[xliii].

HIMSS Electronic Health Records Association

The HIMSS EHR Association is a trade association of EHR companies. It addresses the national efforts to create interoperable EHRs in different care units like hospitals, ambulatory care centres etc. It operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system[xliv].

It contains industry experts in the field of healthcare IT with a broad scope of expertise and experts who not only represent the EHR software industry but also interact and represent the entire healthcare community.

Annex-XI

IT infrastructure includes planning and implementation of all facilities, equipment etc. on which IT automated applications can function. It also deals with power, cooling and security issues that can put MoPH's IT systems at risk. Moreover, under infrastructure optimized strategies are developed that increases IT reliability and longevity.

Planning for reliable Infrastructure is important because according to Price Waterhouse research, after a power outage disrupts IT systems:

- 33+ percent of companies take more than a day to recover.
- 10 percent of companies take more than a week.
- It can take up to 48 hours to reconfigure a network.
- It can take days or weeks to re-enter lost data.
- 90 percent of companies that experience a computer disaster and don't have a survival plan go out of business within 18 months.

MoPH infrastructure requirements at the base-level include:

- Servers
- Desktop/laptop
- Storage
- Networking
- Security
- Servers
- Power Management

At an advanced level it includes:

- Virtualization – Server, Storage and Desktop
  (A key benefit of virtualising storage is the ability to retain older gear, rather than doing the replacements typically required of storage upgrades)
- Private Cloud implementation
  (By 2012, Gartner predicts that private clouds will account for at least 14% of the infrastructure at Fortune 1000 companies, which will benefit from service-oriented, scalable and elastic IT resources.)
- Security systems and Disaster recovery

A successful IT infrastructure requires addressing many elements, some are them are listed below:

- Document IT infrastructure.
- Diagram a server farm.
- Track network changes.
- Design a firewall topology.
- Implement a password policy.
- Infrastructure Design and Documentation

- Track server changes (change control form)

Annex-XII

Data center design considerations

ICT departments face a variety of data centre challenges – from power and cooling limitations to continuous operations and maintenance difficulties. To combat this issue the MoPH needs to know and then implement best practices for data centre design and maintenance. High availability for critical facilities typically necessitates complex redundancy schemes to provide sufficient redundancy available to support uninterrupted operations. The requirements for sustaining critical operations needs to be included in the design and construction of the Data Center before operations begin. A design rule for a data center is that the mechanical/electrical support space being at least another 50% (and probably closer to 100%) of the technology room space. In other words, whatever space is predicted for cabinets and other technical hardware, double it.

Servers Virtualisation

Servers will be virtualised so that business continuity can be achieved should one or more servers fail due to any reason. Additionally agreed Service Levels for all applications should be maintained at all costs. Core software applications will get preference over all other applications. More than 4 million virtual machines will be installed on x86 servers this year (2009) and the number of virtualized desktops could grow from less than 5 million in 2007 to 660 million by 2011, according to Gartner.

With virtualization, even those anti-social applications could be made to share servers. The virtualization product isolates each instance of an application, so the application doesn't necessarily need its own hardware.

According to an IDG Research study of IT decision makers[xlv], more than 83 percent of respondents indicated that virtualization is a priority for their organizations and 80 percent are currently using or have invested in virtualization technology.

Hosted virtual images deliver a near-identical result to blade-based PCs. But, instead of the motherboard function being located in the data centre as hardware, it is located there as a virtual machine bubble. However, despite ambitious deployment plans from many organizations, deployments of hosted virtual desktop capabilities will be adopted by fewer than 40 percent of target users by 2010.

Virtualisation will disrupt old models and help companies cut costs or improve productivity and efficiency. allowing organisations to deploy and fix applications quickly and ultimately reduce support costs and improve application reliability.

Virtualisation to eliminate duplicate copies of data on the real storage devices while maintaining the illusion to the accessing systems that the files are as originally stored (data de-duplication) can significantly decrease the cost of storage devices and media to hold information.

Virtualisation helps in consolidating IT assets while simultaneously expanding pool of applications, workloads, and users – not an easy task otherwise.

Virtualization gives cost-efficient redundancy as "virtualized" primary servers can be backups, too. By encapsulating a specific virtual machine (an application and its operating system needs), any application can be nearly instantly ported to any available server.

Clustering

With Clustering of servers, data centre servers also can fail over to one another while offering guaranteed performance even for demanding e-mail and database applications. They also scale easily; however clustering requires a storage-area network.

Storage Area Network

In the enterprise, IDC reports, structured, transactional data will grow at a 27.3% compounded annual rate over the next three to five years.

Combined disk space of the branches database servers and the servers installed in the Data Centre approaches 2.0TB (1TB = 1000GB). By deploying an iSCSI Storage Area Network (SAN) with a capacity of 3.0TB Storage will be optimized and readily available to all servers. Creating an iSCSI SAN is a pre-requisite to centralizing the branches databases.

Local Area Network

For LAN traffic Server should communicate on 10Gbps Ethernet segments while clients (Desktop computers and laptops) use 1000Mbps links.

Annex-XIII

MoPH has an optical fibre based 6Mbps bandwidth internet connection with capacity to service on average 700 clients. This connection would be adequate to meet the current needs if other issues were resolved. This bandwidth costs Afg. 270,000 per month out of the total MoPH allocation of US $10,000 per month informally assigned each month by senior management to IT. When the internet is down MoPH has no other backup to keep clients online. The internet has been working reasonably well for the past three months, however the Ministry needs to either have Customer Premises Equipment (CPE) in back up if the ones installed fail or altogether terminate the internet in an appropriate router.

Annex-XIV

Open Source

Open Source Software – by using open source software (Linux, Send mail, Apache, Squid etc.) and certain proprietary / closed software we will be able to create powerful, easy to use MoPH and collaboration environments as well as automate business processes.

By using open source software (Linux, Send mail, Apache, Squid etc.) and certain proprietary / closed software we will be able to create powerful, easy to use applications and collaboration environments as well as automate business processes.

Open Source offers flexibility since open source products are customizable and can involve third parties. Moreover it offers continuous improvement since extensive collaboration ensures that software products keep improving.

Linus Torvalds, the founder of Linux Operating System, has released the next version of the Linux kernel, and with it come virtualization enhancements and support for the emerging OpenRISC processor architecture. Linux 3.1 also includes updates to graphics drivers that expand its range of 3D image rendering—and, for the first time, a driver to support use of the Nintendo Wii handheld motion-control device. As usual, the new version also includes many other additional drivers and bug fixes. Torvalds released the new version during the security session at the Kernel Summit that was held in Prague. This release is notable in that it is the first version to be hosted on distributed code hosting service GitHub, where it will reside while its usual home, Kernel.org, gets revamped after the damage caused by a security breach. In its new iteration, Linux has support for nested virtualization within the KVM (Kernel-based Virtual Machine) hypervisor. This feature, built from AMD's Nested VMX, allows a virtual machine to be run from inside another. Linux will also provide KVM with the ability to tap into the SMEP (Supervisory Mode Execute Protection) of Intel's next-generation Ivy Bridge processors, which should reduce some of the performance over-head typically associated with virtual clients. Users of the Xen hypervisor get some new features as well: Linux 3.1 will be the first to al-low Xen-based virtual machines to directly access devices on a PCI bus, a capability previously only available through a patch. It also folds in Xen's Balloon Driver, which can be used to adjust the amount of working memory required by a virtual machine during operation. In the realm of processors, Linux 3.1 is the first version that can be run on the 32- bit OpenRISC 1000 family of processors. OpenRISC is a volunteer-driven project to design an open source processor architecture. Linux 3.1 also supports the newest version of the Oracle Sparc processor, the SPARC-T3 series.

In the Health care domain Laika is an open source program developed by Certification Commission for Healthcare Information Technology (CCHIT) to check EHR software for compliance with CCHIT interoperability standards. The CCHIT described four different levels of data structuring at which health care data exchange can take place. The four levels are;

Level	Data Type	Example
1	Non-electronic data	Paper, mail, and phone call.

2	Machine transportable data	Fax, email, and unindexed documents.
3	Machine organizable data (structured messages, unstructured content)	HL7 messages and indexed (labeled) documents, images, and objects.
4	Machine interpretable data (structured messages, standardized content)	Automated transfer from an external lab of coded results into a provider's EHR. Data can be transmitted (or accessed without transmission) by HIT systems without need for further semantic interpretation or translation.

A number of open source projects in the medical domain exist. Some of the popular ones are:

Debian Med: Integrated Software Environment for All Medical Purposes Based on Debian GNU/Linux

- The Debian Med project started in 2002 with the objective to bring free medical software into the focus of users.
- In preparation of the Med-e-Tel 2011 conference the Debian Med team prepared an extensive paper in PDF format that covers the content of the talk to be hold at the conference. For the interested reader the paper which is made it available at:

  http://people.debian.org/~tille/papers/201012_debian-med.pdf
- Explains how Debian Med works, how the project is organized and how they try to serve medical practitioners and bio-medical researchers as best as possible by turning Debian GNU/Linux into the distribution of choice for any medical application. They are providing this collection of software in the hope that it will be useful for medical research as well as medical service providers who might base their business model on providing commercial support for Free Software in medical care.

Open Source Based IHE XDS.B Prototype for Regional Health Networks

- The goals of this research project are to set-up a multi institutional document registry and repository based on existing pure Open Source Software (OSS) components implementing PIXPDQ, XDS and ATNA. In detail the intentions are: - Education of students in standards based health networks - Creation of a test environment for the development of further software components - Proof of concept Methods: Based on previous research the Open Health Tools and the IPF of the Open eHealth Foundation were chosen to implement the core infrastructure of the PEHR concept.
- Linked Data in the Heterogeneous PONTE Environment

  Several international Open Source standards exist for Information Models which support SCT, including [Health Level 7 - Term info project (HL7 version 3)], [HL7 RIM (Reference

Information Model)], [HL7 HMD (Hierarchical Message Description)], [Clinical Document Architecture (CDA)], and [openEHR Templates] or [EN13606 Archetype] and [Logical Record Architecture (LRA)]. HL7 RIM and HL7 HMD are required to represent SCT data in an Information Model in order to share with those data based on HL7 V 3 Standard

Annex-XV

Database Features & Requirements

Salient Features of Database

- No Limit On Memory (RAM) Use
- AWE Support
- Compression
- Resource Governor
- Parallel Index Operations
- Indexed Views
- Enhanced Read Ahead And Scan
- Can Act As Consolidated In Sync
- Can Sync to Oracle
- Database Encryption
- Auditing
- View Matching
- Full Query Optimizer
- Profiling
- High Availability
- Concurrency and locking
- different levels of protection to isolate data
- Freedom to access the system from anywhere around the globe.
- User friendly interfaces (web pages) and output reports.
- Comprehensive security mechanism to allow access to only authorized users with their assigned rights for record entry, view, update and deletion.

- Access level of each user to be defined at the time of creating of the user.
- Security features will store history of changes in database by a particular user.
- Configurable list of Values for different standard information for ease of use (e.g. Provinces, Wulaswali, Villages, Project Categories etc.)
- Easy to use data input/access interfaces.
- Comprehensive Search Options with the combination of multiple attributes for data access
- Criterion-based filtration of the Data Reports (Summary, Detailed, Pivot and Graphical).
- Options to Exports Reports in variety of formats (PDF, Word, Excel etc.)
- Data Validations for the Data Inputs
- Un-approved schemes will be stored in database and will be reflected where required
- Database data-backup is required periodically to ensure safety of information

MoPH will deploy a database management system that is adequate for handling transactions. An adequate system has the following properties:

Atomicity
Results of a transaction's execution are either all committed or all rolled back. All changes take effect, or none do.

Consistency
The database is transformed from one valid state to another valid state. This defines a transaction as legal only if it obeys user-defined integrity constraints. Illegal transactions aren't allowed and, if an integrity constraint can't be satisfied then the transaction is rolled back.

Isolation
The results of a transaction are invisible to other transactions until the transaction is complete.

Durability
Once committed (completed), the results of a transaction are permanent and survive future system and media failures.

Annex-XVa

Hardware Capacity Planning and Sizing[xlvi]

Capacity planning is the process of determining the resources needed to meet the specifications of the current and future growth of a business. The required resources are estimated based on anticipated end-user demand statistics over a specific period of time.

Sizing is the process of estimating and tuning the individual components to meet the requirements based on the supporting capacity planned. Hardware resources such as memory, processor, number of hard disks, and storage arrays are all key components of this process. When performing the sizing activity, it is critical to perform various performance benchmarks and tests to minimize any single component from becoming a bottleneck either in the hardware sizing or application sizing portions of a solution.

There are two basic types of database workloads: Online Transactional Processing (OLTP) and Decision Support Systems (DSS). OLTP workloads often serve transaction-based applications, such as order processing and online banking. By contrast, the DSS workload is used to answer analytical queries such as budgeting, forecasting, and data mining. The Dell Oracle Database Advisor Tool provides the option to select between OLTP/ On-Line Analytical Processing (OLAP) application types, server form factors, entry-level and enterprise-level storage arrays, and various database parameters including database size, number of concurrent users, IOPs, and throughput requirements. Taking the workload requirements as the input it should be possible to recommend the appropriate solution stack based on various bench marks scores publicly available.

Workload/Application Type

The workload type is one of the key parameters in capacity planning that is used for sizing the solution stack to address the needs of a particular database application. It is useful in understanding the nature of the workload's read and write characteristics in order to quantify the appropriate components for the solution. OLTP application environments are characterized by small, random I/O requests where potentially tens of thousands of user requests have to be processed in a permissible time slice. OLAP applications on the other hand are identified by a small number of IO and CPU intensive queries that process huge amounts of data, which require high storage bandwidth. Since each workload is different, it is important to understand your application type in order to correctly meet your business specifications.

Database Size

Database size is a top priority when analyzing business requirements for critical data storage. The database size is a key input because it directly impacts the calculation of memory and storage requirements. When sizing a database, it is important to understand the size of the database and the amount of memory to allocate to their Program Global Area (PGA) and System Global Area (SGA) for each Oracle instance. The correlation between PGA and SGA size and the amount of memory to allocate to each area is directly influenced by the size of the database.

Business Continuity

Business continuity features are an essential aspect of any database environment. Its purpose is to minimize performance degradation, enhance security, and prevent unexpected application downtime. This is accomplished by implementing features that Oracle provides, such as backup and recovery, disaster recovery, Automatic Storage Management (ASM) partitioning, and encryption.

Sizing Methodology

Ask a series of questions and collect the information provided by the domain owners in the Ministry. Once the information is gathered, analyse the data, to generate a solution. When analyzing the data, the outcome consists of the best fit solution. It is important to note that the solution is intended to be a baseline and should be adjusted accordingly to meet the requirements. The following sections detail questions, the reasons why these questions.

Questionnaire and Reasoning

Following question 1 which captures application type, the questionnaire flow is as follows:

- General Questions ¢w Q1 to Q5
- OLTP workload specific questions ¢w Q6 to Q7
- OLAP workload-specific questions ¢w Q8
- Q9 are general questions applicable to both OLTP and OLAP workloads.

Question 1: Is this database designed for Online Transaction Processing (OLTP) or Online Analytical Processing (OLAP)?

As mentioned earlier, the workload plays a critical role in understanding database usage. Most database applications can be placed in one of the following two workload types, the Online Transaction Processing (OLTP) and the Online Analytical Processing (OLAP) workload. The OLTP workload consists of transaction oriented environments such as e-commerce and banking, while the OLAP workload is selected in environments when trying to solve or gather analytical data such as forecasting future sales, financial reporting, and data mining.

OLTP and OLAP databases are characterized by two different input/output (I/O) characteristics. The OLTP workload is measured by the amount of input/output per second (IOPS) and the OLAP database is measured by its megabytes per second (MB/s) throughput. Since both database workload types differ in I/O characterization, sizing considerations vary between the two types. By comprehending workload requirements, we can than adjust the hardware requirements accordingly to meet their environment specifications.

Question 2: Which of the following capabilities should be achieved?

One of the main focus points when sizing a database workload is an understanding of the type of performance and system utilization that the environment will require. The choice is between three options- functionality, price/performance, and performance.

The functionality option provides a low-end solution built on optimizing the system for high utilization with respect to CPU processing power (very high CPU utilization) and a 1:1 PGA:SGA memory tuning ratio. The price/performance option delivers a solution that is achieved by allowing a better balance between CPU utilization of and a 1:2 PGA:SGA memory tuning ratio. Finally, the performance option is built around achieving optimal performance for database environment. When selecting the performance option, the system should be optimized for memory intensive workloads providing a 1:4 PGA:SGA ratio for memory tuning and the most optimal CPU utilization.

The next set of questions provides the framework in the process of creating a solution. Once storage and database requirements are answered in the following questions, the solution will be tailored to increase the number of processors required as well as the memory required to meet the specification selected in order to attain the optimization requirement found in question 2.

Question 3: How would you characterize your storage requirements?

Entry level storage has benefits over internal server storage, such as high availability, increased manageability, backup/recovery and higher drive capacity utilization. Enterprise class storage has all of the benefits of entry level storage plus greater scalability, increased data protection capabilities, and better integration for disaster recovery solutions.

When deciding between an entry-level storage class or an enterprise-level storage class, the following should be considered:

- How much storage capacity will be required?
- What type of performance does the environment require?
- What feature sets will be needed?
- Does the maximum IOPs or MB/s still fall in the entry-level storage parameter or will enterprise-level storage be required?
- If entry-level storage is chosen, will we grow beyond the storage's capabilities?
- Is the storage class considered Tier 1, Tier 2, or Tier 3?

By answering the questions above, the Ministry will gain a better perspective on how to evaluate the various storage options for its environment.

Question 4: Which server form factor and processor type do you prefer?

Using CPU-intensive benchmarks a particular CPUs scalability and user-load are characterised.

Question 5: What is the maximum expected size of the database (include growth for the next three years)?

This question deals with understanding the importance of the database size and expectations for future growth. When selecting the appropriate database size, it is critical to take into account future growth of MoPH database needs. This will ensure that Oracle database solution not only will be optimized for today's growth but that it is ready to handle future growth and continues to deliver optimal performance. Once the database size is selected, the number of backend storage disks required to meet database capacity requirement is calculated. However, this will not be the final deciding factor of the spindle count since the throughput required (IOPs or MB/s) will directly affect the spindle count. A common misconception that occurs is that IT Departments do not take into account their IOPS or MB/s requirements. If these requirements are not directly tied to the spindle count formula, system performance may have limitations in providing the correct throughput. For example, if a 500GB database and one spindle was purchased to hold that 500GB database, the performance of the database may suffer since a single spindle would not be sufficient to drive the entire database. On the other hand, if we add to the spindle count to spread the database across multiple spindles, the performance and thus the overall throughput would greatly increase because multiple spindles are available to access the database simultaneously.

OLTP workload specific questions: Q6 - Q7

Question 6: What is the maximum number of concurrent application connections to the database?

In a typical multi-tier environment, the application tier utilizes a pool of connections to connect to the database server to serve incoming requests. A concurrent connection is an active connection that has access to the database. Users do not typically make a direct connection to the database but are served by an application layer that creates a request on behalf of the user. For instance, the most common scenario is an application layer that serves requests for multiple users as in Figure 1. However, some instances do have users directly querying the database which is depicted in Figure 2.

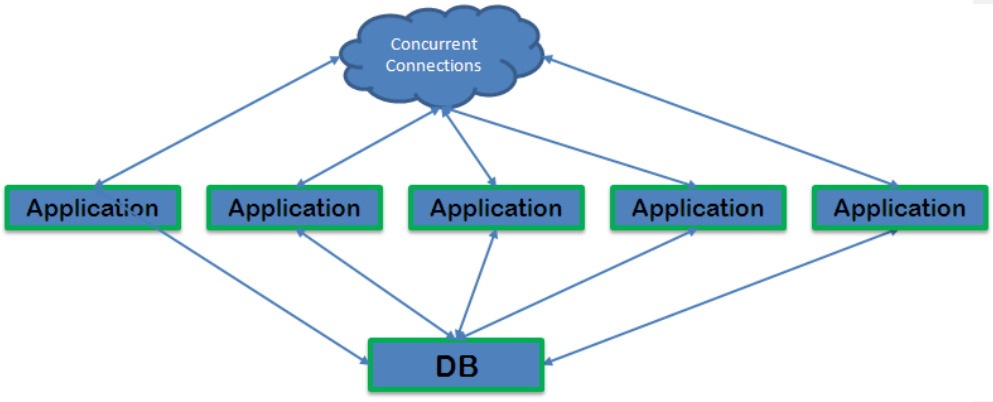


Figure 1

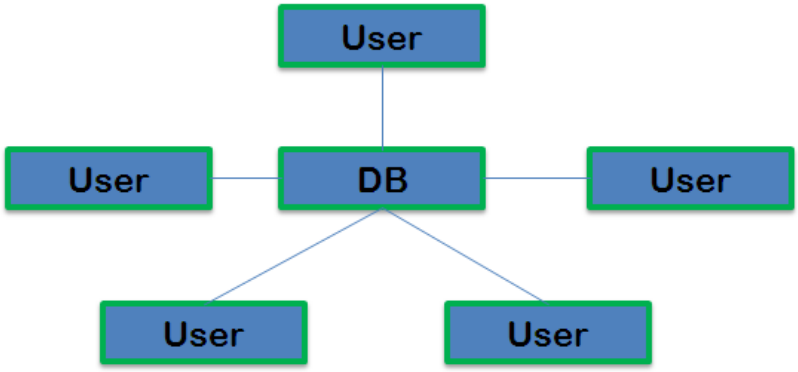


Figure 2.

Determining the correct scenario used in MoPH environment is vital to allocate the correct amount of CPU and memory resources required. Each connection made to the database consumes a small portion of CPU and memory resources in order to achieve this connection. As more concurrent user connections are established, more data will be retrieved from your database, taking up more of these to make these connections. The calculation done to correctly establish the correct number of CPUs and memory needed to meet MoPH requirement is directly impacted by how previous questions were answered. For example, in question 2 in which functionality, price/performance, or performance, get selected have different CPU and memory utilization ratios. Thus the resources are adjusted based upon the input requirements.

Question 7: Please enter your IOPs or MB/s throughput requirement (asked only if question 1 OLTP was selected).

Characterizing throughput is a critical aspect in understanding how to correctly size storage requirements. While every environment and workload is different, the IT Department should characterise both OLTP and OLAP workloads, using industry standard benchmarks such as TPC-C like and TPC-H like workloads to assess throughput requirements. Once these factors are known the factors essential to selecting the correct storage type and spindle count to achieve the required I/O throughput are determined. It is important to understand that each question adds key answers to correctly size an environment. An environment cannot simply be created based on a single question but the series of questions provided with answers to allow for the design of an optimal solution. Question 7 above specifically characterizes OLTP workload environments.

Question 8: Please enter your I/O Bandwidth requirement (asked only if question 1 OLAP was selected).

This question captures the MoPH's storage bandwidth requirements specific to the OLAP environment. OLAP workloads are characterized by complex queries demanding large amount of data retrieval from the database. Storage should be properly sized to enable the server to process the user requests by pulling the data.

Question 9: Please select any additional features that may apply.

Different editions of various databases sometimes provide additional feature sets which improve the application performance and availability. These cans be:

Backup and recovery solution: This feature allows the customer to capture data backups from the primary storage to the tape devices. The archival of data to tape devices will allow users to keep the most important critical data in the primary storage.

Business continuity: Business continuity creates an infrastructure that is highly available in order to reduce application downtime. The IT Department will recommend at least two nodes to ensure that if one of the Oracle nodes fails, the database instance can failover to another node within the cluster. Once the failed node is operational, the database instance will failback to its original node to load balance the workload.

Disaster recovery solution: The disaster recovery solution option will prompt the IT Department to recommend a replica configuration of your primary site for your secondary site. This creates the highest availability to ensure no downtime if the primary site was interrupted by a catastrophic event. To sustain consistency across both sites, the data from the primary site is copied to the secondary site at regular intervals, using either an asynchronous or a synchronous fashion to provide business continuity without degradation in performance.

Question 9a: Which application will be using the Oracle database?

Each application requires different parameters and settings to be set or changed to have an optimal solution. This question allows IT consultants to pinpoint and focus directly on optimization of the best practices of these applications based on the input provided.

Question 9c: How do you plan on backing up your database?

There are two options recommended for backing up a database - tape backup and disk backup. While each backup methodology has its advantages and disadvantages, the main differences between the two are cost, stability, power usage, and availability. When deciding between the two choices, MoPH needs to consider these factors and select which one best meets the needs of the environment. For instance, if it is required to restore data at a particular point in time and have a need for data to be accessed regularly by multiple users, a tape backup solution would not work since these solutions are sequence read-write systems; tape backup solutions allow only one operation at a time. However, a combination of both technologies could be used to create a balance between storing older data on tape and having a disk backup to access current data immediately.

Annex-XVb

How to choose a Hardening Guideline

Hardening of any complex system involves many little details. The more a system can be configured, the lengthier the list of tasks you need to perform (or validate) to create a hardened configured, the lengthier the list of tasks you need to perform (or validate) to create a hardened configuration. Database Security Technical Implementation Guide (STIG), developed by Defence Information Systems Agency (DISA) for the Department of Defence (DOD) - USA, is a document that provides very mature guidelines for implementing a secure RDBMS.

Database STIG

STIGs are documents published by the DISA to assist in improvement of the security of DOD information systems. There are numerous STIG documents – all of them are accessible at http://iase.disa.mil/stigs/index.html. The checklists can be downloaded from http://iase.disa.mil/stigs/app_security/database/general.html. The Database STIG focuses on relational databases. The Database STIG has a generic section which outlines guidelines relevant to any database management system (DBMS). The sections within the general document address Integrity, discretionary access control, database auditing, Network Access, Operating System, etc.

Annex-XVI

Interoperability is the ability of one system to communicate or work with another. This is achieved when different vendors follow the same technical standards in developing their products. Interoperability exists function by function. Two products may interoperate for some functions but not for others.

An Interoperability Framework can be defined as an overarching set of policies, standards and guidelines that describe the way in which organisations have agreed, or should agree, to do business with each other. The emergence of the information society over the last decade has triggered two related developments. On the one hand, administrations in various countries increasingly provide their services online. Citizens now demand integrated and interoperating electronic services that offer "one stop shops" and "no wrong doors", free of time constraints. In order to meet these demands, it is essential to ensure the interoperability of services at the National level.

There are three relevant aspects that any Interoperability Framework needs to tackle: technical, semantic and organisational interoperability. Technical interoperability covers the technical issues of linking up computer systems and services by agreeing on standards for presenting, collecting, exchanging, processing and transporting information. Semantic interoperability aims at ensuring that the meaning (semantics) of exchanged information is shared by the systems that participate in the exchange of data and allows a meaningful manner of processing information. Last, organisational interoperability is concerned with defining business goals and processes and bringing about the collaboration of administrations that wish to exchange information but may have different internal organisations and structures for their operations. In addition to the issues described above, the Interoperability Framework needs to meet high-level policy issues such as cultural, legislative and linguistic challenges.

Since Interoperability means, above all, the "collaboration" of systems, services and people in order to deliver results, the necessity for the different stakeholders to collaborate is key. The dynamic nature of government e-services makes it necessary for Interoperability Framework evolve on a regular basis and integrate changing developments in the field of organisational, semantic and technical interoperability.

Annex-XVII

Organizations often don't know for weeks, months, sometimes years after they've been breached. That study found that 86% of breached parties learned of their breach through notification from an external party, only 6% of breaches were uncovered through internal monitoring, such as reading security logs[xlvii].

It is known that passwords, despite the fact that they are known to be insecure, are the most common method used today to authenticate computer users. A hardware token, or smart card, used together with a personal identification number or biometrics, would provide much better security for the computer system. Using well-engineered systems for user authentication based on such hardware tokens, taking care to make sure they are more secure and convenient for users.

Use such software applications that make security application administration easier by allowing network managers to configure large numbers of devices from one computer. Rather than making changes to network security device by device.

For information exchange between servers and client browsers and server-to-server, deploy load balancing devices and SSL accelerators, Secure Server IDs-now recognized as the bottom line in security. Working with the Secure Sockets Layer (SSL) protocol for encryption, Secure Server IDs protect businesses against site spoofing and data corruption. They would assure MoPH and all stake holders that it is safe to submit personal information, and provide colleagues with the trust they need to share sensitive business information.

Database Security Key Recommendations

All firms can benefit from enterprise database auditing solutions that can improve data security and help meet compliance requirements in a cost-effective manner. Forrester's in-depth interviews with decision-makers and influencers for their firm's enterprise wide data security strategies and implementations yielded several important observations:

• **Native auditing has several gaps and limitations.** These range from lack of strong reporting, clear separation of duties, and enterprise wide scalability, to inability to deliver end-to-end security analysis. Look beyond native auditing to simplify auditing processes and improve data-level security.

• **Deeper insights are critical for compliance and security.** Simply collecting audit logs is not good enough; what is required is end-to-end analysis and correlation with detailed activity to understand access patterns and abuse. Enterprise database auditing solutions deliver deeper security insights out of the box with detailed "who, what, how and when" analysis.

• **Enterprise wide auditing requires a comprehensive solution.** Unlike native auditing, enterprise database auditing solutions can support hundreds and thousands of databases, offering a consistent auditing implementation across distributed heterogeneous enterprise environments.

• **Database auditing solutions can lower cost.** Firms can save money with enterprise database auditing solutions because of automation, improved manageability, simplified reporting, role separation, and lower system resource usage.

• **Centralize auditing and monitoring.** Standardizing, centralizing, and automating policies across data centers, applications and databases will ensure consistent and strong database security. Although different countries may have different compliance requirements, enforce local security policies only after global policies have been enforced.

Annex-XVIIa

The various types of threats & vulnerabilities[xlviii] that ICT systems face are listed below:

Read Attack

- Unauthorized disclosure of non-public information
  - client account information
  - employee personal data
  - credit history
- Learning Network Information
  - Unauthorized port scanning can lead to other attacks

–Prevent attacks such as Denial of Service

Manipulate Attack

- Customer Database and Functions
  - Change information on a worker's compensation claim
  - Change the amount of compensation on a claim
- Human Resources Database

–Change personnel information such as salary, addresses, social security numbers, etc.

Spoof Attack

- New dynamic web interface
- Identity Spoofing
- Attacker pretends to be a valid customer through log in
- False claims
- Wasted manpower and time

Flood Attack

- Denial of Service Mitigation
- High network availability crucial – single office location
- If external router is flooded, no claims can be filed online by customers
- If internal switch is flooded, no claims can be processed by employees

Viruses, Worms, Trojans

- Viruses and Worms introduce possibility of loss of customer data
- Trojans may be used to steal data
- Policies
  - Example: Email Policy provides guidelines when accessing emails

Physical Threats

- Hardware Failure
  - Loss of data possible
  - Network downtime
- Backups
  - All system backups in stored in same office building

Annex-XVIIb

System services policy

This policy demonstrates the purpose of the Ministry's network and the services it offers internally and externally. This will define traffic flow based on ports that run through the network. The policy shall be updated as the network architecture changes. Further, the policy has to be concise and clear to users, managers, and administrators.

Baseline policy

This policy provides clear guidelines for the deployment of any system or application. Before any software or hardware is applied to the network, a clear understanding of the network effect must be thoroughly tested and accepted.

Security posture policy

As new threats develop to the network, new solutions will emerge. This policy includes procedures for testing and applying patches and updates to the existing system baselines. It should also include a baseline and repository for all access lists and rules on security devices. These security rule sets will grow with the network and in response to specific threats.

Security assessment policy

The purpose of this policy is to obtain prior approval to monitor and aggressively probe the Ministry's network for weaknesses and noncompliance with established policies. This requires performing non-destructive penetration of accounts (to verify strong passwords) and of network services (to verify that security devices are functioning and reporting).

Monitor and Reaction Policy

This policy defines how, why, where, and when log files are read. For example, "Firewall logs will be monitored continuously, security event logs will be checked at a minimum of once per hour." This policy identifies exactly how security information will flow from machine to administrator. Specify the type of alert that should be received for different security events and who will be notified during those events. This policy is the building block for the criteria list of security devices that are acceptable for deployment on the network.

Response policy

Having clear procedures to follow during a crisis will greatly increase the Ministry's effectiveness during a security incident. In this policy, describe the response to events identified under the monitor and reaction policy. For instance, if MoPH's Web server is under attack, it is not required to disconnect the entire network from the Internet; the attack should be filtered attack at an upstream device.

Recovery policy

This policy defines how to rebuild and recover the network. It must include everything from rebuilding a server to restoring the entire network. In this policy, document the plan for backing up and restoring data. If the network requires 100 percent redundancy for specific hardware, define that requirement. Don't wait for a late night failure to discover that you don't have a vendor maintenance agreement or any spare hardware on hand.

Annex-XVIII

Cybercrime includes attacks on ICT infrastructure and services, for example hacking, denial of service threats and identity theft. It also includes more traditional criminal activities that have merely 'moved' on to the web, such as child pornography. Hence, organizations that use software code that accesses or protects critical data or infrastructure should conduct their own tests. The Web is brimming with both free and commercial testing tools for just that task. One of my long-time free tools for checking website security is Nikto. It searches for thousands of vulnerabilities across a very large range of Web server software. It's free and fairly easy to use, as long as you aren't scared by Linux or Linux subsystem emulation. You can run its tests as a plug-in to Tenable's Nessus vulnerability scanner, which runs on Windows. Along the way, you can scan for a bazillion other vulnerabilities. Also, don't forget to check your software with an application vulnerability fuzzer. Fuzzers specifically look for the type of vulnerability found in the recent Apache bug: They take a line of input requesting code and respond to it with hundreds, even thousands, of predefined malformed responses. The idea is to respond in many unexpected ways to see if it makes the application barf (a technical term). Fuzzing is how most of today's vulnerabilities are found. As with regular vulnerability testing tools, you can find free and commercial fuzzers. Among the freebies, there's iDefense's Filefuzz, which lets you mal-form many different Windows file formats. SPIKEfile does the same thing for Linux files. The HTML Manglizer fuzzes HTML parsers. Many fuzzers, such as Smudge, are written in scripting languages like Python. I heavily recommend that all your applications undergo SDL processes and review. Part of that review should include vulnerability testing and fuzzing. In today's world of expansive hacking, any-thing less is simply neglectful.

The malware that we need to be protected against is:

- Spyware
- Viruses (with behavioural-based scanning and ability to fights Zero-Day viruses)
- Spam (with text based scanning and image based scanning)
- Adware
- viruses,
- Trojans
- bots
- root kits

Advanced Malware Defined[xlix]

Malware innovations have been driven by attackers' quests to gain increasing control of compromised Computer systems and the networks in which they reside. Whether attackers use viruses, Trojans, bots or root kits, today's malware is designed for the long-term control of compromised machines. Often offensive tactics disrupt client-based security, like re-writing the Windows HOSTS file to disrupt antivirus

signature and patch updates, or resetting Microsoft security updates to manual. Advanced malware also establishes outbound communications across several different protocols to upload stolen data and to download instructions and further malware payloads for other reconnaissance and malicious purposes. Early cyber attackers compromised systems primarily for fame and bragging rights. As criminals became aware of the value of information being placed online, they quickly became involved in developing such malware for profit. Law enforcement, computer crime experts and the military are now playing catch up to the threat posed to consumers, businesses and national security as cyber criminals cash in on stolen identity data, fraudulent online transactions and cyber espionage. It is clear that criminals with profit motives or political agendas are the main cause for the explosion of malware as we know it. Web sites and applications now support user-contributed content, syndicated content, iFrames, third-party widgets (or applets) and convoluted advertising distribution networks into which malware can easily be injected. The malware that criminals have developed is dynamic and stealthy. It leverages unknown vulnerabilities across a range of applications and communications protocols. The specific characteristics of particular strains of malware differ depending on the purpose of the attackers, be it for cyber crime, cyber espionage or emerging cyber warfare scenarios.

Zero-day Targeted Attacks

Cyber criminals have developed ways to bypass outdated security techniques, such as signatures, leaving businesses and consumers vulnerable to attack. Signature-based technologies like IPS and antivirus software, both within perimeter and endpoint solutions, are increasingly ineffective against this rapidly evolving, blended threat, as is evidenced by the continued and successful intrusions into commercial, federal and educational networks. At the same time, more and more businesses and consumers are storing data on the network, "in the cloud," and conducting transactions through the Internet, making cyber crime more attractive than ever.

Understanding Next-Generation Threats

An advanced malware attack can no longer be seen as a single incident consisting of exploit, infection and remediation stages. Today's attacks are coordinated efforts to penetrate an organization's defences and establish a foothold for the purposes of reconnaissance, network asset exploitation, data exfiltration, data alteration, data destruction and ongoing surveillance.

The first step of an infection is the initial exploit or social engineering attack. It leads directly to a series of
follow-on malware infections that persist despite repeated attempts to scan and disable the attack. As malware has become more sophisticated, conventional client-based antivirus scans and network-based intrusion scans no longer are able to disrupt and stop these coordinated sets of infections and attacks. While some infections are detected and removed by scans, the criminal maintains control over the system. Other, often zero-day, malware components that were not removed allow the criminal to re-install malware and disrupt endpoint security to prevent future removal.

Advanced Malware in Action

Cyber Crime

When it comes to cyber crime, the criminal's main goal is to steal assets, services or financial information that can eventually be turned into hard currency. There are attackers who are making money by infecting and linking up thousands of computers, often referred to as "botnets." These are then monetized in a variety of ways. For example, some criminal organizations rent out the computing

power of these networks to send phishing spam. In other cases, criminals perpetrate extortion schemes by threatening to take a business's website down through distributed denial of service attacks. They have even jumped onto the Cloud Computing trend with "Malware-as-a-Service" offerings, where cyber criminals sell capacity and services on a subscription basis to each other[i].

Cyber Espionage

Cyber espionage uses advanced malware to covertly obtain data that is considered secret or confidential. As more information is moved online, we will only see a continued increase in the use and sophistication of cyber espionage. Given the relatively low barriers to entry, superior cyber espionage capabilities will not be the exclusive domain of traditional super powers. No doubt, the efforts of much of the global intelligence community are focused on cyber espionage. There have been a few public cases of advanced malware being used in corporate espionage. Malware that was stealthy and unknown to signature-based systems was highly effective in stealing sensitive information.

Cyber Warfare

Emerging cyber warfare scenarios would most likely involve using sophisticated and stealthy malware in reconnaissance activities, intelligence gathering, communications disruptions, and critical infrastructure attacks. Sophisticated technical capabilities, including hacking, have had limited usage within conventional
warfare scenarios thus far, not yet in a coordinated and targeted attack against a country's communication
and critical infrastructure. Known cyber reconnaissance infiltrations have taken place, and in part led to the
establishment of the US Cyber Command in September 2009. Other Cyber Command operations around the world have now also been established, so it is clear that cyber warfare is a distinct possibility with all sides considering their options and preparing defences.

Disrupting Next-Generation Threats

Given the serious consequences and ineffectiveness of current solutions, FireEye is publishing and sharing its five key principles to designing an effective network-based defence. Solutions should be held up to these criteria as part of any investment decision involving malware defences. The 5 key principles are:

1. Dynamic defences to stop targeted, zero-day attacks
2. Real-time protection to block data exfiltration attempts
3. Integrated inbound and outbound filtering across protocols
4. Accurate, low false positive rates
5. Global intelligence on advanced threats to protect the local network

Dynamic Defenses to Stop Targeted, Zero-day Attacks

To be effective, anti-malware solutions need to be intelligent enough to analyze network traffic and processes, rather than just comparing bits of code to signatures. Advanced malware has been developed with traditional defences and software architectures in mind to maximize its chance to exploit an end-user system.

Dynamic analysis, as opposed to static signature-based comparisons, is critical to enable a product to detect and stop polymorphic malware on the wire as well as malware hosted on dynamic, fast-changing domains. In order to address these advanced threats, real-time, dynamic, and accurate analysis is critical.

Rather than relying on signatures and lists, we must be able to dynamically recognize new attacks in real time, without requiring a priori knowledge of vulnerability, exploit or variant, and then prevent system compromise and data theft.

Real-time Protection to Stop Data Exfiltration Attempts

To protect the network, real-time analysis and blocking are essential to stopping data exfiltration that can take place within minutes, if not seconds, of the zero-day infection. It is important to be able to dynamically analyze network traffic to capture and detect zero-day malware, but equally important to provide real-time capabilities to stop the outbound call-back communications to disrupt the attack and halt the flow of data.

Integrated Inbound and Outbound Filtering Across Multiple Protocols

Advanced threats include attacks on multiple fronts, exploiting the inability of conventional network protection mechanisms to provide a unified defence. As soon as one vulnerability is defended, network attacks quickly shift to another.

It is now possible to have both inbound attack detection and outbound malware transmission filtering in a single appliance form factor. Administrators gain a clientless solution that is easy to deploy and maintain. This integrated solution allows coverage across the many vectors used in attacks and can keep pace with the dynamic nature of attacks. Defending corporate networks from the advanced malware in next-generation threats requires new protections that function across many protocols and throughout the protocol stack, including the network layer, operating systems, applications, browsers and plug-ins like Flash.

An integrated approach enables the most comprehensive threat protection against malware that attacks across multiple vectors to penetrate the network. The initial compromise of a system could be a social engineering attack like a spear phish email with a URL or malicious PDF. Once the dropper malware is installed, it calls back out to upload stolen data and download further malware payloads. With both inbound and outbound threat protection, it is possible to protect against next-generation threats and go beyond simple signature matching or rudimentary packet analysis.

Accurate, Low False Positive Rates

Other technologies, whether heuristic or behavioural analyses, are touted as an encouraging development, but in practice they are too inaccurate or compute intensive to function as standalone, real-time security mechanisms. This methodology often augments an anti-malware solution's signature protections, but at the
same time increases the likelihood of false positive alerts.

The sheer volume and escalating danger of advanced malware attacks are overwhelming limited IT resources
and outmaneuvering conventional defences. For most enterprises, traditional network connection-oriented and software-based defences are inadequate, because of the gaps they leave in security coverage. However, trying to integrate conventional defences from multiple vendors is far too complicated and costly an undertaking for an enterprise IT group.

Global Intelligence on Advanced Threats to Protect the Local Network

For pre-emptive protection against a dynamic cyber threat, it is important to have a global network to provide the latest intelligence on malware threats and zero-day attacks. Real-time malware intelligence can protect the local network against zero-day malware and advanced persistent threats. It can stop

outbound call-backs that threaten to exfiltrate sensitive data. By building an intelligence-sharing network with customers, technology partner networks, and service providers around the world it is possible to share and efficiently distribute malware security intelligence to essentially serve as an Internet cyber crime watch system and stop both inbound attacks and unauthorized outbound call-backs and prevent data exfiltration, alteration, and destruction.

Malware Protection Systems

Next-generation protection systems prevents data loss and intellectual property theft. Additionally it stops zero-day attacks and outbound call backs while inoculating networks from future attacks. They stand behind existing firewalls, IPS, AV and Web gateways to block attacks that have sneaked past. It eliminates the headache of false positives and tuning associated with traditional defences.

Next generation products capture details about the attack that allow to fingerprint confirmed malware and block outbound malware call-backs across multiple protocols, including HTTP, IRC, FTP and other protocols designed by cyber criminals. Deploying advance protection appliances within the network security layer complements existing network and endpoint security solutions by blocking unknown threats and their outbound communications and feeding critical and timely security intelligence to the IT organization. Endpoint security software, for example, still serves a critical role within IT security since it protects against legacy infections and provides cleanup services. Next-generation firewalls can overlay beneficial policies to manage user- and application-based use of the Internet.

The primary challenges today are zero-day threat and APT attack detection and outbound blocking of malware call-backs. IT needs protection tools in order to mitigate the risk of massive data losses, while providing critical attack insight to assist IT security analysis and response processes.

Annex-XIX

The major elements of the backup strategy are as follows:

- Planning
- Selection of devices
- Determination of backup schema
- Other logistical issues
- Factors to consider:
    - Staffing
    - Technical expertise
    - Budget

Mirroring data is not backup and neither is imaging on the same system. If the storage array has two copies of MoPH data does not mean that it is completely protected. A complete backup paradigm required backing up more than just the data such as configuration files, program patches and system state information for a lot of work if you need to do a full restore.

Automate Backup

Human error is listed as the second leading cause of backup failure after media problems. A lot of problems with media, such as improperly handling tapes, are actually caused by human error as well. To minimise errors/problems due to human errors automated backup systems help tremendously. Most backup softwares allow scheduling backups.

Duplicate backup

At two copies of backup should be maintained. By having more than one copy of data in backup, we increase our chances of being able to get all, or most, of the 1data back. 1One common scheme is to keep the last two full backups as well as the partial backups.

Store backup copies -- safely

At least one full copy of MoPH data should be stored securely away from MoPH, in a bank vault, for example. That way we can be sure of having our data even in the event of a disaster. This requires that at least one copy of our last full backup is stored offsite in a place where it is available 24-7.

Testing

MoPH will need to test its system by restoring all or part of the image from the backups at regular intervals. One good way to do this is to create a separate partition on your system and restore to it for testing. Another way is to restore it to another machine.

Annex-XX

List of major modules in a Hospital ERP system are:

- Patient Registration
- Appointment
- Admission Discharge Transfer
- Wards & Bed Management
- Operation Theatre
- Clinic Specialties
- Laboratory Information System
- Radiology Information System
- Management Information System
- Pharmacy
- Blood Ministry
- Patient Billing
- General Store
- Inventory System
- Hospital Administration
- Payroll System
- Financial Accounting

Annex-XXI

Ministry of Public Health and Provincial Public Health Directorates automation program									
Description	**Budget year (Amount in US Dollars)**								
	2012-13			**2013-14**			**2014-15**		
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**
IT Infrastructure									
Data Center	50,000.00	100,000.00	150,000.00	50,000.00	150,000.00	200,000.00	-	-	-
Security	-	-	-	50,000.00	-	50,000.00	25,000.00	50,000.00	75,000.00
Storage Area Network	-	-	-	65,000.00	-	65,000.00	-	-	-
Server Room (Active and Passive components complete with civil works etc.)	-	100,000.00	100,000.00	-	300,000.00	300,000.00	-	250,000.00	250,000.00
Servers, Computers, Laptops, Printers, UPSes etc.	50,000.00	100,000.00	50,000.00	100,000.00	100,000.00	200,000.00	25,000.00	200,000.00	225,000.00
Local Area Network (Active and Passive Components)	100,000.00	-	100,000.00	-	100,000.00	100,000.00	-	200,000.00	200,000.00
Wireless Network	15,000.00	-	15,000.00	-	15,000.00	15,000.00	-	30,000.00	30,000.00

Ministry of Public Health and Provincial Public Health Directorates automation program									
Description	**Budget year (Amount in US Dollars)**								
	2012-13			**2013-14**			**2014-15**		
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**
Virtual Private Network based WAN (Fiber Points of Presence)	-	-	-	50,000.00	-	50,000.00	50,000.00	-	50,000.00
Establishing of Audio & Video Conferencing facilities	-	-	-	50,000.00	50,000.00	100,000.00	-	100,000.00	100,000.00
Developing current HF Radio System Network in all provinces.	-	-	-	-	-	-	-	-	-
Total	100,000.00	300,000.00	415,000.00	365,000.00	715,000.00	1,080,000.00	100,000.00	830,000.00	930,000.00
Capacity Development									
IT Infrastructure Library Training	10,000.00	-	10,000.00	-	-	-	-	-	-
Project Management Professional Certification or Prince 2 Training	25,000.00	-	25,000.00	-	25,000.00	25,000.00	-	25,000.00	25,000.00

Ministry of Public Health and Provincial Public Health Directorates automation program									
Description	**Budget year (Amount in US Dollars)**								
	2012-13			**2013-14**			**2014-15**		
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**
Oracle/MS SQL/MySQL certification Training	15,000.00	-	15,000.00	-	-	-	-	-	-
Linux Training	15,000.00	-	15,000.00	-	-	-	-	-	-
CISSP (Security) certification Training	-	-	-	25,000.00	-	25,000.00	-	30,000.00	30,000.00
Radio Codan training	15,000.00	-	15,000.00	-	-	-	-	-	-
MCITP	-	-	-	15,000.00	-	15,000.00	-	-	-
CCNA	-	-	-	10,000.00	-	10,000.00	-	-	-
MCTS	-	20,000.00	20,000.00		20,000.00	20,000.00	-	-	-
Other training	-	10,000.00	10,000.00	10,000.00	40,000.00	50,000.00	-	50,000.00	50,000.00
Total	80,000.00	30,000.00	110,000.00	60,000.00	85,000.00	145,000.00	-	105,000.00	105,000.00
Enterprise Resource Planning (ERP) system for MoPH and PPHDs									

Ministry of Public Health and Provincial Public Health Directorates automation program									
Description	**Budget year (Amount in US Dollars)**								
	2012-13			**2013-14**			**2014-15**		
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**
Financial Information and Management Systems	50,000.00	-	50,000.00	100,000.00	100,000.00	200,000.00	150,000.00	150,000.00	300,000.00
MoPH Web Portal									
Stores and Inventory System									
Procurement System									
HRMIS (already developed will be integrated with the three new systems, MoPH has the source code)	-	-	-	-	-	-	-	-	-
Total	50,000.00	-	50,000.00	100,000.00	100,000.00	200,000.00	150,000.00	150,000.00	300,000.00
Databases and Application Software (New)									
Supply Chain System	30,000.00	-	30,000.00	-	-	-	-	-	-

Ministry of Public Health and Provincial Public Health Directorates automation program									
Description	**Budget year (Amount in US Dollars)**								
	2012-13			**2013-14**			**2014-15**		
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**
Customer Relationship Management (CRM) system (To be integrated with ERP)	-	-	-	-	-	-	150,000.00	-	150,000.00
E-Learning System	-	-	-	500,000.00	-	500,000.00	100,000.00	-	100,000.00
E-Library System	-	-	-	100,000.00	-	100,000.00	-	100,000.00	100,000.00
Pharmaceutical Management System	-	-	-	-	-	-	-	-	-
Geographic Information System	-	-	-	25,000.00	-	25,000.00	25,000.00	50,000.00	75,000.00
Registration System and Web based portal for National Medical Council for Afghanistan	100,000.00	-	100,000.00	500,000.00	-	500,000.00	-	-	-
Total	130,000.00	-	130,000.00	1,125,000.00	-	1,125,000.00	275,000.00	150,000.00	425,000.00
Databases and	-	-	-	-	-	-	-	-	-

Ministry of Public Health and Provincial Public Health Directorates automation program									
Description	**Budget year (Amount in US Dollars)**								
	2012-13			**2013-14**			**2014-15**		
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**
Application Software (Improved)									
National Health Management Information System	-	-	-	100,000.00	-	100,000.00	100,000.00	-	100,000.00
Monitoring and Evaluation System	-	-	-	25,000.00	-	25,000.00	-	-	-
Configuration Management Database	35,000.00	-	35,000.00	-	-	-	-	-	-
Total	35,000.00	-	35,000.00	125,000.00	-	125,000.00	100,000.00	-	100,000.00
Telemedicine System									
Telemedicine System (MCIT has a leading role in this one) and establishing of Telemedicine Centers in Provinces	-	-	-	100,000.00	100,000.00	200,000.00	50,000.00	200,000.00	250,000.00

Ministry of Public Health and Provincial Public Health Directorates automation program									
Description	**Budget year (Amount in US Dollars)**								
	2012-13			**2013-14**			**2014-15**		
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**
Total	70,000.00	-	70,000.00	225,000.00	100,000.00	200,000.00	50,000.00	200,000.00	250,000.00
Creating 3 Digit Hotline number for assistance on health related issues all over the country (In the year 2015-16 the hot line will be merged into the Health contact center)	-	-	-	30,000.00	-	30,000.00	40,000.00	-	40,000.00
Health Contact Centre	-	-	-	-	-	-	150,000.00	-	150,000.00
Total	-	-	-	30,000.00	-	30,000.00	190,000.00	-	190,000.00
ICT Directorate in MoPH (Human Resource induction)	-	-	-	-	-	-	-	-	-
General Director	36,000.00	-	36,000.00	39,600.00	-	39,600.00	43,560.00	-	43,560.00
Database	18,000.00	-	18,000.00	19,800.00	-	19,800.00	21,780.00	-	21,780.00

Ministry of Public Health and Provincial Public Health Directorates automation program									
Description	**Budget year (Amount in US Dollars)**								
	2012-13			**2013-14**			**2014-15**		
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**
Administrator									
Help Desk Technicians (Quantity: 02)	12,000.00	-	12,000.00	13,200.00	-	13,200.00	14,520.00	-	14,520.00
Asstt. DBA	-	-	-	12,000.00	-	12,000.00	13,200.00	-	13,200.00
System Admin	12,000.00	-	12,000.00	13,200.00	-	13,200.00	14,520.00	-	14,520.00
MIS Manager	-	-	-	21,600.00	-	21,600.00	23,760.00	-	23,760.00
Assistant Network Administrator	-	-	-	9,600.00	-	9,600.00	10,560.00	-	10,560.00
Help Desk Administrator	-	-	-	12,000.00	-	12,000.00	13,200.00	-	13,200.00
Help Desk Officer	-	-	-	9,000.00	-	9,000.00	9,900.00	-	9,900.00
IS Sec Manager	-	-	-	24,000.00	-	24,000.00	26,400.00	-	26,400.00
IS Sec officer	-	-	-	12,000.00	-	12,000.00	13,200.00	-	13,200.00
SAN Administrator	-	-	-	-	-	-	18,000.00	-	18,000.00
Assistant SAN Administrator	-	-	-	-	-	-	-	-	-
Total	78,000.00	-	78,000.00	186,000.00	-	186,000.00	222,600.00	-	222,600.00

Ministry of Public Health and Provincial Public Health Directorates automation program									
Description	**Budget year (Amount in US Dollars)**								
	2012-13			**2013-14**			**2014-15**		
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**
International ICT Advisor for charting our programs and project based on the ICT Strategy	500,000.00	-	500,000.00	500,000.00	-	500,000.00	-	-	-
Total	500,000.00	-	500,000.00	500,000.00	-	500,000.00	-	-	-
Grand Total (USD)	**973,000.00**	**330,000.00**	**1,318,000.00**	**2,491,000.00**	**900,000.00**	**3,391,000.00**	**1,037,600.00**	**1,235,000.00**	**2,272,600.00**

Ministry of Public Health and Provincial Public Health Directorates automation program							
Description							**Grand Total**
	2015-16			**2016-17**			
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	
IT Infrastructure							
Data Center	-	-	-	-	-	-	350,000.00
Security	-	75,000.00	75,000.00	-	50,000.00	50,000.00	250,000.00
Storage Area Network	-	-	-	-	-	-	65,000.00
Server Room (Active and Passive components complete with civil works etc.)	-	300,000.00	400,000.00	-	300,000.00	300,000.00	1,350,000.00
Servers, Computers,	25,000.00			50,000.00			1,050,000.00

Ministry of Public Health and Provincial Public Health Directorates automation program							
Description							**Grand Total**
	2015-16			**2016-17**			
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	
Laptops, Printers, UPSes etc.		200,000.00	225,000.00		300,000.00	350,000.00	
Local Area Network (Active and Passive Components)	-	250,000.00	250,000.00	-	300,000.00	300,000.00	950,000.00
Wireless Network	-	50,000.00	50,000.00	-	50,000.00	50,000.00	160,000.00
Virtual Private Network based WAN (Fiber Points of Presence)	25,000.00	-	25,000.00	100,000.00	-	100,000.00	225,000.00
Establishing of Audio & Video Conferencing facilities	-	100,000.00	100,000.00	-	200,000.00	200,000.00	500,000.00
Developing current HF Radio System Network in all provinces.	-	-	-	-	-	-	-
Total	50,000.00	975,000.00	1,125,000.00	150,000.00	1,200,000.00	1,350,000.00	4,900,000.00
							-
Capacity Development							-
IT Infrastructure Library Training	-	-	-	-	-	-	10,000.00
Project Management Professional Certification or Prince 2 Training	-	25,000.00	25,000.00	-	10,000.00	10,000.00	110,000.00
Oracle/MS SQL/MySQL certification Training	-	-	-	-	-	-	15,000.00
Linux Training	-	-	-	-	-	-	15,000.00
CISSP (Security) certification	-	-	-	15,000.00	-		70,000.00

Ministry of Public Health and Provincial Public Health Directorates automation program							
Description							**Grand Total**
	2015-16			**2016-17**			
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	
Training						15,000.00	
Radio Codan training	-	20,000.00	20,000.00	-	-	-	35,000.00
MCITP	-	30,000.00	30,000.00	-	-		45,000.00
CCNA	-	-	-	-	-		10,000.00
MCTS	-	-	-	-	-		40,000.00
Other training	-	50,000.00	50,000.00	-	70,000.00	70,000.00	230,000.00
Total	-	125,000.00	125,000.00	15,000.00	80,000.00	95,000.00	580,000.00
							-
Enterprise Resource Planning (ERP) system for MoPH and PPHDs							-
Financial Information and Management Systems	-	200,000.00	200,000.00	-	100,000.00	100,000.00	850,000.00
MoPH Web Portal							-
Stores and Inventory System							-
Procurement System							-
HRMIS (already developed will be integrated with the three new systems, MoPH has the source code)	-	-	-				-
Total	-	200,000.00	200,000.00	-	100,000.00	100,000.00	850,000.00

Ministry of Public Health and Provincial Public Health Directorates automation program							
Description							**Grand Total**
	2015-16			**2016-17**			
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	
							-
Databases and Application Software (New)							-
Supply Chain System	-	-	-	-	-	-	30,000.00
Customer Relationship Management (CRM) system (To be integrated with ERP)	-	-	-	-	-	-	150,000.00
E-Learning System	50,000.00	-	50,000.00	-	-	-	650,000.00
E-Library System	-	-	-	-	-	-	200,000.00
Pharmaceutical Management System	-	-	-	-	-	-	-
Geographic Information System	-	100,000.00	100,000.00	-	-	-	200,000.00
Registration System and Web based portal for National Medical Council for Afghanistan	-	-	-	-	-	-	600,000.00
Total	50,000.00	100,000.00	150,000.00	-	-	-	1,830,000.00
							-
Databases and Application Software (Improved)	-	-	-	-	-	-	-
National Health Management Information System	-	-	-	-	-	-	200,000.00
Monitoring and Evaluation System	-	-	-	-	-	-	25,000.00

Ministry of Public Health and Provincial Public Health Directorates automation program							
Description							**Grand Total**
	2015-16			**2016-17**			
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	
Configuration Management Database	-	-	-	-	-	-	35,000.00
Total	-	-	-	-	-	-	260,000.00
							-
Telemedicine System							-
Telemedicine System (MCIT has a leading role in this one) and establishing of Telemedicine Centers in Provinces	-	200,000.00	200,000.00	50,000.00	250,000.00	300,000.00	950,000.00
Total	-	200,000.00	200,000.00	50,000.00	250,000.00	300,000.00	1,020,000.00
							-
Creating 3 Digit Hotline number for assistance on health related issues all over the country (In the year 2015-16 the hot line will be merged into the Health contact center)	-	-	-	-	-	-	70,000.00
Health Contact Centre	50,000.00	-	50,000.00	75,000.00	-	75,000.00	275,000.00
Total	50,000.00	-	50,000.00	75,000.00	-	75,000.00	345,000.00
							-
ICT Directorate in MoPH (Human Resource induction)	-	-	-	-	-	-	-

Ministry of Public Health and Provincial Public Health Directorates automation program							
Description							**Grand Total**
	2015-16			**2016-17**			
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	
General Director	47,916.00	-	47,916.00	52,707.60	-	52,707.60	219,783.60
Database Administrator	23,958.00	-	23,958.00	26,353.80	-	26,353.80	109,891.80
Help Desk Technicians (Quantity: 02)	15,972.00	-	15,972.00	17,569.20	-	17,569.20	73,261.20
Asstt. DBA	14,520.00	-	14,520.00	15,972.00	-	15,972.00	55,692.00
System Admin	15,972.00	-	15,972.00	17,569.20	-	17,569.20	73,261.20
MIS Manager	26,136.00	-	26,136.00	28,749.60	-	28,749.60	100,245.60
Assistant Network Administrator	11,616.00	-	11,616.00	12,777.60	-	12,777.60	44,553.60
Help Desk Administrator	14,520.00	-	14,520.00	15,972.00	-	15,972.00	55,692.00
Help Desk Officer	10,890.00	-	10,890.00	11,979.00	-	11,979.00	41,769.00
IS Sec Manager	29,040.00	-	29,040.00	31,944.00	-	31,944.00	111,384.00
IS Sec officer	14,520.00	-	14,520.00	15,972.00	-	15,972.00	55,692.00
SAN Administrator	19,800.00	-	19,800.00	21,780.00	-	21,780.00	59,580.00
Assistant SAN Administrator	12,000.00	-	12,000.00	13,200.00	-	13,200.00	25,200.00
Total	256,860.00	-	256,860.00	282,546.00	-	282,546.00	1,026,006.00

Ministry of Public Health and Provincial Public Health Directorates automation program							
Description							**Grand Total**
	2015-16			**2016-17**			
	Ministry	**Provinces**	**Total**	**Ministry**	**Provinces**	**Total**	
							-
International ICT Advisor for charting our programs and project based on the ICT Strategy	-	-	-	-	-	-	1,000,000.00
Total	-	-	-	-	-	-	1,000,000.00
Grand Total (USD)	**406,860.00**	**1,400,000.00**	**1,906,860.00**	**522,546.00**	**1,380,000.00**	**1,902,546.00**	**10,791,006.00**

Hospital Automation Program						
Values in US Dollars						
Description	**Budget year**					**Grand Total**
	2012-13	**2013-14**	**2014-15**	**2015-16**	**2016-17**	
	One Hospital	**Two Hospitals**	**Two Health units**	**Four : (Hospitals:02, Health Units: 02)**	**Eight: (Hospitals:03, Health Units: 05)**	
IT Infrastructure						
Server Room development	10,000.00	25,000.00	25,000.00	60,000.00	150,000.00	270,000.00
Local Area Network (Active and Passive Components) and Wireless Network	40,000.00	80,000.00	50,000.00	135,000.00	180,000.00	485,000.00
Servers, Computers, Laptops, Printers, UPSes etc.	60,000.00	120,000.00	80,000.00	210,000.00	280,000.00	750,000.00
Electric and backup Power cabling	30,000.00	70,000.00	100,000.00	100,000.00	100,000.00	400,000.00
Total	140,000.00	295,000.00	255,000.00	505,000.00	710,000.00	1,905,000.00
Enterprise Resource Planning (ERP) system for Hospitals and other health care institutions	**One Hospital**	**Two Hospitals**	**Two Health units**	**Four : (Hospitals:02, Health Units: 02)**	**Eight: (Hospitals:03, Health Units: 05)**	
Hospital and Health Unit Management Information Systems	100,000.00	200,000.00	300,000.00	300,000.00	350,000.00	1,250,000.00
Total						

	100,000.00	200,000.00	300,000.00	300,000.00	350,000.00	1,250,000.00
E-Health			**One Hospital**	**Two Health units**	**Two Hospitals**	
Electronic Medical Record System (EMR) System	-	-	75,000.00	200,000.00	400,000.00	675,000.00
E-Prescription						
Electronic Health Record (EHR) System (Tying together the One Hospital and Two health units for which EMR would be created in the prior years)	-	-	-	-	300,000.00	300,000.00
Total	-	-	75,000.00	200,000.00	700,000.00	975,000.00
m-Health						
m-Health System	-	-		200,000.00	100,000.00	300,000.00
Total	-	-	-	200,000.00	100,000.00	300,000.00
Grand Total (USD)	240,000.00	495,000.00	630,000.00	1,205,000.00	1,860,000.00	4,430,000.00

12 References

[i] Adapted from Information for Health, a Strategy for Building the National Health Information Infrastructure, Report and Recommendations From the National Committee on Vital and Health Statistics Washington, D.C., November 15, 2001. http://www.himss.org/content/files/NHII_Fact_Sheet.pdf
[ii] Strategic Plan for the Ministry of Public Health (2011-2015) – Pages 2, 14 & 57
[iii] Strategic Plan for the Ministry of Public Health (2011-2015) – Pages 19
[iv] Information and Communication Technologies (ICT) Policy November, 2003 Objectives – Page 13
[v] Afghanistan National Development Strategy - 2008 – 2013, Figure 2.1. ANDS oversight structure, page # 18
[vi] Adapted from Afghanistan National Development Strategy - 2008 – 2013, Foreword page # v
[vii] Afghanistan National Development Strategy - 2008 – 2013, An Overview, page # 11
[viii] Health and Nutrition Sector Strategy 2007-2013, Page # 5
[ix] Health and Nutrition Sector Strategy 2007-2013, Page # 41
[x] Health and Nutrition Sector Strategy 2007-2013, Page # 9
[xi] Afghanistan National Development Strategy (2008-13), Table 13.0.1. Cross Cutting Issues in Social and Economic Development Pillar – Page 140
[xii] Afghanistan National Development Strategy (2008-13), Chapter 7, Economic and Social Development, Health and Nutrition, Policy Framework: Sector Strategy – Page 110
[xiii] Strategic Plan for the Ministry of Public Health (2011-2015) – Pages 21
[xiv] Health and Nutrition Sector Strategy 2007-2013, Page # 25, 40 and 41
[xv] Afghanistan Comprehensive Health Information System Strategic Plan 2009-13, Page # 8
[xvi] Health and Nutrition Sector Strategy 2007-2013, Page # 41
[xvii] Health and Nutrition Sector Strategy 2007-2013, Page # 40
[xviii] Strategic Plan for the Ministry of Public Health (2011-2015) – Page # 39
[xix] Health and Nutrition Sector Strategy 2007-2013, Page # 27
[xx] Afghanistan National Development Strategy (2008-13), Chapter 7, Economic and Social Development, Health and Nutrition, Policy Framework: Sector Strategy – Page 109
[xxi] http://learn.gotomeeting.com/?elqPURLPage=69&elq=99efa98e9cff4d6eb805bd13aadd958b
[xxii] Afghanistan National Development Strategy (2008-13), Table 13.0.1. Cross Cutting Issues in Social and Economic Development Pillar – Page # 140
[xxiii] Health and Nutrition Sector Strategy 2007-2013, Strategy 9.3 - Communications and Information Technology (CIT), Page # 41
[xxiv] Health and Nutrition Sector Strategy 2007-2013, Page # 40 and 53
[xxv] Health and Nutrition Sector Strategy 2007-2013, Page # 40
[xxvi] Davenhall, B. Building a Community Health Surveillance System. *ArcUser Online.* 2002. http://www.pubmedcentral.nih.gov/redirect3.cgi?&&auth=0ofsLnwxDjkf0U6h31uRoAOou97McQtxggSvA2k7p&reftype=extlink&artid=343292&iid=10204&jid=122&FROM=Article%7CCitationRef&TO=External%7CLink%7CURI&article-id=343292&journal-id=122&rendering-type=normal&&http://www.esri.com/news/arcuser/0102/comhealth1of2.html
[xxvii] Higgs G, Richards W. The use of geographical information systems in examining variations in socio demographic profiles of dental practice catchments: a case study of a Swansea practice. *Prim Dent Care.* 2002;**9**:63–9. doi: 10.1308/135576102322527829. [PubMed]
[xxviii] eHealth is Worth it - The economic benefits of implemented eHealth solutions at ten European sites by Karl A. Stroetmann, Tom Jones, Alexander Dobrev, Veli N. Stroetmann, ISBN 92-79-02762-X
[xxix] http://en.wikipedia.org/wiki/Electronic_medical_record

[xxx] Strategic Plan for the Ministry of Public Health (2011-2015) – Pages 30
[xxxi] A planet of civic laboratories, the future of Cities, Information, and Inclusion. http://iftf.me/public/SR-1352_Rockefeller_Map_reader.pdf
[xxxii] Mobile Devices a Hot Area for ICT in 2011, says Frost & Sullivan. http://www.frost.com/prod/servlet/press-release.pag?Src=RSS&docid=222097247

[xxxiii] M. Eichelberg, T. Aden, J. Riesmeier1, A. Dogac, G. B. Laleci, "Electronic Health Record Standards – A brief Overview". [Online]. Available: http://www.srdc.metu.edu.tr/webpage/projects/ride/publications/icict06_20060810.pdf

[xxxiv] S. Cohan, A. Shabo ; "Electronic Health Record (EHR) Standards Survey," August 2001. [Online]. Available: http://www.haifa.ibm.com/projects/software/imr/papers/EHRSurvey.pdf

[xxxv] S. Cohan, A. Shabo ; "Electronic Health Record (EHR) Standards Survey," August 2001. [Online]. Available: http://www.haifa.ibm.com/projects/software/imr/papers/EHRSurvey.pdf
[xxxvi] NEHTA Report, "Review of Shared Electronic Health Record Standards", NEHTA Report V 1.0, Feb 20, 2006
[xxxvii] S. Cohan, A. Shabo ; "Electronic Health Record (EHR) Standards Survey," August 2001. [Online]. Available: http://www.haifa.ibm.com/projects/software/imr/papers/EHRSurvey.pdf
[xxxviii] Gillogley Services, "EHR Standards", [Online], http://www.gillogley.com/ehr_standards.shtml, visited September 4, 2009
[xxxix] openEHR EHR Standard, "Homepage of openEHR". [Online]. Available: http://www.openehr.org/home.html
[xl] P. Schloeffel, T. Beale, G. Hayworth, S. Heard, H. Leslie;"The relationship between CEN 13606, HL7, and openEHR", Ocean Informatics Pty Ltd, Sydney Australia. [Online], http://www.oceaninformatics.com/Media/docs/Relationship-between-CEN-13606-HL7-CDA--openEHR-2ba3675f-2136-4069-ac5c-152139c70bd0.pdf
[xli] NEHTA Report, "Review of Shared Electronic Health Record Standards", NEHTA Report V 1.0, Feb 20, 2006
[xlii] Comparison report, "openEHR and HL7 V3" , Version 3.0, Apr. 13, 2008
[xliii] "HIMSS Electronic Health Record Association," [Online]. Available: http://www.himssehra.org/ASP/index.asp
[xliv] "Canada Health Infoway" 29 June 2009 at 18:47. [Online]. Available: http://en.wikipedia.org/wiki/Canada_Health_Infoway
[xlv] IDG Peer2Peer Triad Research Program: Virtualization, December 2007,

http://wenku.baidu.com/view/3c9f7f1cc5da50e2524d7fce.html?from=related

[xlvi] Adapted from DELL's Oracle Database Advisor Underlying Methodology - A Dell™ Technical White Paper
[xlvii] Verizon Data Breach Investigations Report – 2011

[xlviii] Adapted from A Forrester Consulting Thought Leadership Paper Commissioned By IBM
[xlix] Adapted from a FireEye whitepaper titled "5 Design Principles for Advanced Malware Protection - Winning the war against next-generation threats"
[l] Fest, Glen, "Malware-as-a-service Takes a Bow," Bank Technology News. http://www.americanbanker.com/btn_issues/2 21_5/-352304-1.html