

|  |
| --- |
| Ministry of Health |
| National eHealth Guidelines and Standards |
| [NeGS] |
|  |
| **V 2.4.5** |
| **1/1/2015** |

|  |
| --- |
| [Type the abstract of the document here. The abstract is typically a short summary of the contents of the document. Type the abstract of the document here. The abstract is typically a short summary of the contents of the document.] |

Table of Contents

[1. The Architectural Model of the National eHealth information System 2](#_Toc421717294)

[1.1 Architectural model 2](#_Toc421717295)

[2. Management of Computer Hardware and software for eHealth Services 4](#_Toc421717296)

[2.1. Computer Hardware 4](#_Toc421717297)

[2.2. Software 4](#_Toc421717298)

[3. Network and Connectivity 7](#_Toc421717299)

[3.1. Network Architecture 7](#_Toc421717300)

[3.2. Network Management 7](#_Toc421717301)

[4. Communication Interface 8](#_Toc421717302)

[4.1. Websites of the state healthcare sector 8](#_Toc421717303)

[4.2. Domains names for State Healthcare Sector Institutions 8](#_Toc421717304)

[4.3 Email 8](#_Toc421717305)

[5. Privacy, Confidentiality, Security and Medical Ethics 10](#_Toc421717306)

[5.1 Medical Ethics 10](#_Toc421717307)

[5.2 Privacy and Confidentiality 10](#_Toc421717308)

[5.3. Security 11](#_Toc421717309)

[6. eHealth Systems Interoperability standards 13](#_Toc421717310)

[6.1 Personal Health Number 13](#_Toc421717311)

[6.2 Healthcare Institution Registry 13](#_Toc421717312)

[6.3 Healthcare Provider Registry 14](#_Toc421717313)

[6.4 Data Interchange Standards 14](#_Toc421717314)

[6.5 Standardized Clinical Vocabulary 14](#_Toc421717315)

# 1. The Architectural Model of the National eHealth information System

## 1.1 Architectural model

1. The National eHealth Information System architecture consist of

Stakeholders connected through a communication network to the eHealth services

1. Categories of stakeholders identified in the national eHealth information

 system are as follows (Figure 02).

* + - Health service providers (State and Private)
		- Health service consumers
		- Allied Services (e.g registrar General Dept)
1. Communication layer will consist of a dedicated State Health Network,

 Internet and the Mobile.

1. All eHealth services handling Personally Identifiable Data should only be

connected through the State Health Network (SHN). It is recommended to connect through a secure VPN until such time a State Health Network is established.

1. eHealth services will closely follow the Health Service domain categories

 listed below

* + - Curative Health Services (CHS)
		- Public Health Services(PHS)
		- Health Supportive Services (HSS)
		- Administrative Services (AS)



 Figure 1.The detail architectural model of the National Electronic Health Information System

# 2. Management of Computer Hardware and software for eHealth Services

## 2.1. Computer Hardware

1. The current applicable National Procurement Guidelines should be followed

 when purchasing computer hardware. “*Procurement Guidelines of 2006 for*

  *Goods and Work by National Procurement Agency*”

1. Any such procurement procedure should essentially be accompanied with

 appropriate maintenance and service agreements.

1. While ensuring the minimum requirement of the composition of a TEC, an

 expert on Health Informatics shall be included whenever possible.

 Procurement of electronic medical equipment should be accompanied by a

 compatible necessary workstation and / or software, where applicable

1. When procuring ICT hardware, it is recommended that the cost of

 consumables and maintenance are considered.

1. A hardware inventory must be maintained at institutional level with detailed

 specifications of any hardware following the treasury guidelines of Sri Lanka.

 “Treasury Circular IAI/2002/02”

1. It is recommended that service agreement/s should be reached for

 maintenance of equipment that are not covered under warranty conditions.

1. Service agreement/s for maintenance of equipment should be reached as a

 service following relevant guidelines. “Procurement Guidelines of 2006 for

 Goods and Work by National Procurement Agency

## 2.2. Software

1. **State Healthcare Sector eHealth Software list:**All eHealth systems that are

 developed, tested, piloted or implemented in all State sector Healthcare

 Institutions should be enlisted in the eHealth software List maintained at the

 HIU of MoH.

1. **Piloting of software systems:**Decision to implement a software system or

 component(s) of software shall be done after a piloting, and shall be done at

 selected institutions/units followed by a proper evaluation. If pilot involves a

third party, the evaluation may be done independent of the third party.

1. ***Acquisition of software*** Government healthcare organizations should only

 use appropriate licensed software. Such licensing is applicable for both

 proprietary as well as free and open source software.

1. Acquisition of software including software donated free of charge should

 always be accompanied by contractual agreements with relevant parties for

 developing, customizing or piloting of software.

1. Acquisition of software including software donated free of charge should

 always be accompanied by an appropriate software maintenance agreement

1. When a software is Built From Scratch, the total ownership of the intellectual

 property rights of such software should be transferred to the healthcare

 organization/ Ministry of Health.

1. When accruing Built from Scratch or Customized software solutions where

 third party components have been used, appropriate licenses for such

 components should also be provided along with the software

1. Agreements/contracts should cover important issues including the

 following:

* + - Software Requirement Specifications
		- Source code availability
		- If the software is a unique solution meant for the healthcare institution
			* Milestones of development process and percentage of payments (partial payments) to be made at reaching each milestone
			* Provisions for flexibility in the specifications during the development process
		- Software documentation including installation and user manual
		- Provision for modifications and updates to the software
		- Declaration of the developer/s stating that the software complies with existing legislations (of the country).
		- Handling of critical and non-critical failures.
		- Clauses handling dispute situations. This should include preventing remotely disabling features.
		- Third party licences
1. Clauses which are detrimental to the acquiring entity similar to but not

 limited to the following should not be included in the agreement/ contracts:

* + - Clauses preventing smooth transition of the healthcare institution to a different software from another vendor in future (i.e. Vender Lock)
		- Broad exculpatory clauses which limits or exclude vendor’s liability
		- Clauses that prevent or limit the inheritance of the software in an event of a change of ownership of the healthcare institution (e.g. taking over a hospital from PDoHS to MoH)

# 3. Network and Connectivity

## 3.1. Network Architecture

1. It is recommended to follow the latest and/or widely accepted versions on networking (including mobile devices) and cabling standards by IEEE (Institute of Electrical and Electronics Engineers), ISO (International Organization for Standardization), EIA (Electronic Industries Alliance) and TIA (Telecommunications Industry Association)
2. All institutions under the Ministry of Health and the provincial departments of health should be able to exchange health related data through a dedicated State Health Network when available.
3. Health Institutions are recommended to maintain their own Private Local Area Network (P-LAN) interconnecting all the devices within the institution.
4. Open network protocols are recommended to ensure freedom of hardware selection.
5. Wired communication is preferred over wireless communication.

## 3.2. Network Management

1. Whenever planning new buildings for healthcare institutions, it should be designed to support the network infrastructure.
2. Physical topology, physical cable layout and upgrades, access methods, protocols, communication devices, operating systems, applications, and configurations should be adequately documented.

# 4. Communication Interface

## 4.1. Websites of the state healthcare sector

1. Contents to be available in Sinhala, Tamil and English for documents relevant

 to the public.

1. Any complaints or concerns on healthcare related content in a web site may

 be submitted to Health Information Unit of the Ministry of Health.

1. Websites created must comply with the “Guidelines for Development of

 Websites for Government Organizations Guidelines for Development and

 maintenance of Websites of Government Organizations” set by the ICTA

## 4.2. Domains names for State Healthcare Sector Institutions

1. Line Ministry Institutions and Institutions under the Provincial Department

 should contact the HIU of the MoH with regard to obtaining the official

 domain address.

1. The domain names under “healh.gov.lk” and

 “healthdept.<prov\_code>.gov.lk” will be allocated according to “**General**

  **Circular Letter No. 02-lB7/2012**” and owned by the Ministry of Health

 and the relevant Provincial Ministry of Health.

1. Domain names that include health related generic words under the .lk

 domain should obtain a clearance from the Ministry of Health. This includes

 English generic words and Sinhala or Tamil Generic words in native script or

 transliterated to Latin script.

## 4.3 Email

1. Email addresses should be assigned in accordance with the “**General**

  **Circular Letter No. 02-lB7/2012**”

1. Email accounts on the organization’s domain shall be used for official

purposes only.

1. All official electronic communications should only be carried out using the

 official Email address under the organization’s domain.

1. All email should follow the proper channel of communication as per existing

 guidelines and norms of paper based document communication.

1. Paper based archiving regulations should also be applied to all email

 communications.

1. The relevant officer shall ensure that his/her email account is checked for and

 responded according to the guidelines applicable to postal mail.

# 5. Privacy, Confidentiality, Security and Medical Ethics

## 5.1 Medical Ethics

1. Ensuring privacy and confidentiality of care recipient is a fundamental Ethical

 concept in Medical Practice and should be considered in eHealth solutions.

1. eHealth systems that handle personally identifiable data of patients, clients

 or general public for research purposes should get ethical approval from an

 accepted ethics review committee coming under the *Forum for Ethics Review*

 *Committees in Sri Lanka* (FERCSL).

## 5.2 Privacy and Confidentiality

1. Ensure confidentiality of personally identifiable data and information at all

 stages of HIS cycle

1. Personally identifiable data and information shall be used only for the

 intended purpose of collecting the data. If such data is to be used for any

 other purpose, a proper de-identification procedure shall be followed.

 Annexure - Manjula

1. Unless the disclosure is enforced by law, personally identifiable information

 should not be disclosed without informed written consent of the individual

 concerned for other than the intended purpose.

1. Employees’ access to healthcare related information should be strictly on a

 *need to know* basis and such access should be revoked when the job role

 changes or terminates.

1. Role based access control profiles should be clearly defined and documented.
2. It is the duty of the Healthcare institutions to ensure information of an

 individual is accessible only by employee/s who have signed an information

 confidentiality agreement (Non-Disclosure Agreement).

1. Healthcare institutions shall ensure that employees who left the organization

 are bound to maintain the confidentiality of information which belongs to

 the institution.

1. Healthcare institutions shall ensure that third party personnel involved with

 health information systems including maintenance should sign non-

 disclosure agreement.

1. An individual has the right to appeal for amendments of personal

 information in an event of any discrepancy.

## 5.3. Security

1. Electronic documents should be maintained following the existing guidelines

 governing the paper based document and the prevailing legislation in the

 country.

1. eHealth systems must ensure that every Creation, Reading and Update

 actions on data should be recorded in an event log with the original data

 being preserved and visible.

1. A No-Deletion approach should be adopted in relation to Clinical Data.
2. During decommissioning of a system removal of data should be done using

 media sanitation tools. ????? Or the Storage devices should be removed and

 physically destroyed.

1. Institutions should ensure security of all ICT hardware and relevant

 documentations.

1. Institutions shall maintain access restricted rooms to keep critical computer

 equipment such as servers and networking equipment. Such access should

 be revoked when the job role changes or terminates.

1. Institutions shall ensure employee/s who are leaving the institution/unit have

 surrendered Identification cards, access cards, keys, and other means of access and dispose (destroy or deactivate) them appropriately.

1. Maintenance of internal or external data storage devices should be

 performed on-site whenever possible and it should only be done by

 authorized personnel.

1. Computerised eHealth systems shall be designed with an events (security) log

 that allows tracing of successful and failed Log-in attempts.

1. Personally Identifiable and Login Data must be encrypted using the

 appropriate algorithm.

1. Institutions shall ensure an appropriate procedure is followed for secure

 backup of data.

1. Institutions should make sure that the retrievability of backed up

 data/information is regularly checked to ensure reliability of the backup

 process.

1. Information systems security audit must be performed at least twice a year.
2. Systems should be promoted to enforce the usage of strong passwords [A

 strong password should contain at least 8 characters, consisting of at least

 one uppercase character, one numeric character and one special character]

 or implement a two-step verification.

# 6. eHealth Systems Interoperability standards

## 6.1 Personal Health Number

1. Computerised systems in the State healthcare sector shall use the Personal

 Health Number (PHN) and healthcare recipients are linked to their

 appropriate health record.

1. PHN is a unique number assigned to a particular individual.
2. The PHN will be issued to the patient upon his first contact with the

 healthcare sector and it is strongly advised to continue it for his/her life.

1. It is recommended that all Healthcare Institution issuing the PHN should not

 Issue a new PHN for individuals already having a PHN, unless in instances

 where anonymity of the individual is requested.

1. There are three components to the number which are;

|  |  |  |
| --- | --- | --- |
| Point of Issue number | Serial Number | Check Digit |
| XXXX(4 digit alpha numeric number) | XXX XXX1. digit numeric )
 | C |

1. Any segregated unit (functionally or physically) of or within a healthcare

institution where PHN is issued shall be referred to as a Point of Issue.

1. “Point of Issue” number – Health Information Unit (HIU) of the Ministry of

Health will be issuing authority to assign a number for the point of issue,

which is the “*Point of Issue*” number.

1. Serial Number – will be a 6 digit serially generated number
2. Check Digit – shall be generated using the modified Luhn Algorithm used by

Regenstrief Institute Inc.

## 6.2 Healthcare Institution Registry

1. A registry of the healthcare institutions is maintained at the Health

 Information Unit of the Ministry of Health and should be referred when

 necessary.

1. The registry will hold a unique identification number for the Institution and

 another relevant attributes.

## 6.3 Healthcare Provider Registry

1. The Sri Lanka Medical Council maintains a registry of the medical

 practitioners (Category code to be decided)

## 6.4 Data Interchange Standards

1. It is recommended to adopt Version 3.0 of the Health Level Standard (HL 7,

 Version 3.0) by *Health Level Seven International* as the data exchange

 standard in the healthcare domain.

1. For the purpose of clinical Document Recording it is recommended to use

 HL7-CDA release 2.

1. For interchange of Laboratory data it is recommended to use Logical

 Observation Identifiers Names and codes (LOINC) by Regenstrief Institute

 Inc.

1. For transferring images between software programs in the medical domain

 DICOM (Digital Imaging and Communication in Medicine) standard by

 *National Electrical Manufacturers Association, USA* shall be used.

## 6.5 Standardized Clinical Vocabulary

1. For the purpose of coding clinical data, it is recommended to use SNOMED CT

 (Systematized Nomenclature of Medicine – Clinical Terms) by *International*

 *Health Terminology Standards Development Organisation* (IHTSDO).

1. For the purpose of statistical reporting of health related data it is

 recommended to use ICD 10 (International Classification Disease) by WHO.

1. Applications that record data in SNOMED CT should be able to cross map

 their data into ICD 10 for the purpose of reporting