Title: Standard Operating Procedures (SOP) for Routine Registry Operations- Implementation, Establishment and Maintenance of Mother & Child Health (MCH) Registry

Sub-title: Data security, privacy and confidentiality

Effective date: 15th January 2017

Review date: 1st May 2017

Content

Aim

The main aim of this SOP is:

- To document the procedures needed to secure MCH e Registry's Hardware and Software.
- To have safe environment for data exchange and storage.
- To protect computers, network and data center from the risk of being penetrated by unauthorized or external users.

Tools

1. Virtual Private Network (VPN)
2. Endpoint Software (Licensed Antivirus and central management system)
3. Cisco Firewall (Network security devices from Cisco that provide firewall, intrusion prevention (IPS) and virtual private network (VPN) capabilities).

MoH legal framework for the MCH registry

MoH legal framework for MCH e Registry which is a crucial step and legal backbone to ensure the confidentiality and privacy of the MCH e Registry implementation process and related data, was developed by the Palestinian National Institute of Public Health (PNIPH) and approved by related department at Ministry of Health (MOH) (**Appendix 1)**

Confidentiality agreement

A clear statement of Confidentiality agreement was developed by the MCH e registry team (PNIPH) and singed by registry staff who has an access to the registry data including staff at PNIPH, data extractors, database super users, field registry implementers, end users at clinics level (Nurse and doctors) to agree not to disclose and disseminate any information from the eRegistry to anybody for any reason. All signed confidentiality agreements were saved appropriately within the documentation/ filing system of the MCH Registry. Example of signed confidentiality agreement is attached **(Appendix 2)**.

A confidentiality statement was added into the main login screen of the MCH e Registry where any authorized user to access the registry read the message every time he/ she access the Registry. See **(Appendix 3)**

Security measures for Computers used in the Primary Health Care Centers (PHCs)

Security measures are adopted & implemented to covers the three main domains as following:

1. Internet and Network
2. Desk top computers (PCs)

3. Data Center and Server

Where set of specific activities and procedures for each domain are adopted and implemented by the MCH e Registry staff (Field Registry implementers, Registry Administrator at MOH) to ensure comprehensive security

Steps to ensure PCs security

1. Certain Steps implemented to install VPN tools Windows 7 **(Appendix 4)** and to Install Kaspersky Endpoint Security 10 Windows 7 **(Appendix 5)**
2. Blocking certain websites
3. Blocking Universal Serial Bus (USB) ports

Steps to prepare security Package for new PC s

The following steps are taken by the MCH e Registry staff at PNIPH & MOH to prepare Security package for the new PCs:

1. Copy the installation package that provided to you earlier to the PC.
2. Make sure Cisco VPN Client installed and running and connected the HRHR Network
3. Add the Kaspersky Security Center server name in the host file located in C:\Windows\System32\drivers\etc , the server name is: KSC , server IP: 172.16.10.25
4. Run the installation package and monitor the progress to make sure it complete successfully.
5. Restart the PC after the installation is finished.
6. After the PC restart turn on the VPN connection and make sure the KES is connected to the server and updated.

Steps to do to ensure security for Internet, Network and Data Center

The following steps are taken by the MCH e Registry staff (Registry Administrator at MOH) to ensure Security for the internet, network and data center:

1. Configure Cisco ASA Firewall with Firepower support to provide IPS and threat management protection
2. Install Cisco Firewall to provide IPsec VPN for the Clinics using Cisco VPN Client to encrypt and authorize the connections to the datacenter
3. Apply a good firewall policies to both datacenters firewalls to ensure secure environment
4. Run the virtual servers with up to date operating system with patches and hotfixes
5. Protect all servers by antivirus with Endpoint protection
6. Connect all clinics' computers to the datacenter through VPN secured by antivirus and security policies to prevent the unauthorized applications and sites

Steps to do for quality assurance for the implemented security measures

The following steps are assured by the MCH e Registry staff ((Field Registry implementers, Registry Administrator at MOH)) to ensure quality assurance for the implemented security measures:

1. Connect to VPN by using user name and password
2. Open registry from the Google chrome (Google chrome is highly recommended)
3. Use the user name and password to access MCH eRegistry

Schedule of Clinic Visit for Installation of Security measures

Worthy to mention that specific Schedule have bent set to complete installation of security measures for computers, internet, data center and server without interfering with the work flow at clinics and hindering services provision at clinics, Template for clinic Visit Schedule as below

S.no.	District	Name of clinic	Date of visit	Status of installation
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				

Appendixes attached

- Appendix 1: MoH legal framework for the MCH registry
- Appendix 2: Example of signed confidentiality agreement.
- Appendix 3: Snapshot of a confidentiality statement appears on main login screen of the MCH e Registry when any authorized user accesses the Registry.
- Appendix 4: Steps implemented to install VPN tools Windows 7.
- Appendix 5: Steps implemented to Install Kaspersky Endpoint Security 10 Windows 7.