Ministry of Health

Information Security Guideline for Healthcare Institutions

V 1.0

Mar 2023

Contents

1. Introduction

Digital health initiatives lead to a significant improvement in healthcare. However, the introduction of information systems also increases the risk of exposing the information to unauthorized parties as health information systems carry sensitive and personal information. Therefore, the issue of maintaining the privacy and security of health information has become a major challenge that needs to be addressed if the digitization of the health sector is to move forward.

At present, most public health facilities and some hospitals use health IT systems to establish a reliable system of patient care for the citizens of Sri Lanka. In order to regulate and govern such systems, the absence of a National Health Information security policy or legislation on the protection of privacy is presently considered a major drawback which hinders further health IT expansions.

In addition, it has also been noted that most health staff, including health administrators, have a minimal understanding and interest in information security and data privacy.

1.1. Objectives Of This Guidelines

These guidelines are intended to provide a compact and easily understandable overview of the most relevant security safeguards. The focus is on organisational safeguards and on illustrating threats through practical examples.

. Higher technical details have deliberately been avoided.

Advanced security considerations pertaining to information systems design development and change management are not covered with this guideline. Information systems audit and related controls are also omitted here. For areas not covered in this guideline, refer to existing legislation and the information and cyber security policy for government organizations.

In short, anyone who consequently implements the recommendations made in these guidelines or who uses them to draw up service contracts with IT service providers is benefited with a reliable level of IT security.

1.2. Application Of Guidelines

This guideline shall be applied to

- All healthcare personnel who are in contact with healthcare data and information, irrespective of their nature of work or location.
- All state sector and private institutions that deal with health data and information
- Any event that generates or consumes health data and information

This guideline line should be used as supplement to the National Digital Health Guidelines and Standards (NDHGS V2.0) and other relevant national guidelines , policies and acts on ICT equipment and information management. This should **not be** used as a substitute to the above guidelines and documents.

1.3. Definitions

Anonymise: To remove personal identifiers from personally identifiable data to make it unidentifiable to a person.

Controller: A person or authority that decides what to do with personally identifiable data and how to process them.

Hacking: Sites that provide content about breaking or subverting computer security controls.

Health Data and Information: This constitutes all data or information that are generated, captured, transmitted, stored, processed, analysed, and disseminated in either on paper or on electronic format, pertaining to health or healthcare service.

Information sharing: Exchange of information between various organizations, people, and technologies.

Internet Filtering: Using technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules.

IP Address: Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.

Malware: software designed to infiltrate or damage a computer system, without the owner's consent. Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware.

Peer to Peer File Sharing: Services or protocols such as BitTorrent and Kazaa that allow Internet-connected hosts to make files available to or download files from other hosts.

Personnel Information: If the information contains uniquely identifying data, such as email addresses, names, social security numbers, IP addresses, etc.

Phishing: attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

Personally Identifiable Information (PII): Any form of information that can be used to identify, contact or locate a person alone or combined with another easily accessible source is considered as Personally Identifiable Information.

Privacy: An individual right to control the acquisition, uses or disclosure of his or her information

Processing: Any action done on personally identifiable data from collection to erasure.

Protected health information: any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment

Removable media: Devices which are used for data storage, backup or transportation and can be removed from a computer without shutting down the computer.

Security: Processes and methodologies which designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption

Social Networking Services: Internet sites such as Facebook and MySpace that allow users to post content, chat, and interact in online communities.

Spam: Unsolicited Internet Email, SPAM sites are websites linked to unsolicited Internet mail messages.

Spyware:Software which takes control of user's computer, modifies computer settings, collects, or reports personal information, or misrepresents itself by tricking users to install, download, or enter personal information.

User ID: User Name or other identifier used when an associate log into the corporate network.

1.4. Important Concepts Relating to Information Security

Availability: services, IT system functions, data and information must be available to users as required.

Authentication: When a person logs in to a system, the system runs a check in an authentication process to verify the identity of the person.

Authorisation: Authorisation is the process of checking whether a person, an IT component or an application is authorised to perform a specific action.

Confidentiality: Information that is confidential must be protected against unauthorized disclosure.

Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Data protection: Data protection refers to the protection of personal data against misuse by third parties

Data backup: Data backup involves making copies of existing data to prevent its loss.

Integrity: data must be complete and unaltered. The loss of integrity of information can therefore mean that this data has been altered without authorisation, that information relating to the author has been falsified or the date of creation has been tampered with.

Nonrepudiation: Nonrepudiation is the assurance that someone cannot deny something.

Remote access: Any connection made to an organization's internal network and systems from an external source by a device or host.

2. Information Security on Human Resources

2.1. Appoint An Information Security Officer

.

It is very important to assign a responsible officer for information security who could take the initiative and responsibilities regarding the security of health information in the particular institution and further he/she would be accountable to the administration regarding decisions related to information security programmes, implementation of security controls, risk and incident management and conducting the awareness programmes as directed by the Health Information Unit at Ministry of Health.

As currently there is no cadre for Information Security Officer, the following personnel responsible for the information security of the institution should fulfil such duties. Health Informatician (Consultant in Health Informatics / Medical officer in Health Informatics) is the responsible officer for the information security of the institute. In such situations where Health Informatician is unavailable, the head of the institution can appoint a suitable officer for information security.

If necessary, it is advisable to establish an information security management team with appropriate staff members to coordinate information security practices.

Head of the institution shall provide all necessary logistics and authorization to the information security officer to conduct duties of information security management.

3. Information Assets Management

3.1. Information Management

Healthcare providers frequently handle very sensitive personal data of patients, and it is very important to take rigorous measures to protect the confidentiality of such information in order to safeguard their privacy. Health information is considered a Critical National Infrastructure. Therefore, health information shall be classified and handled accordingly. The classification is based on the impact or consequence of unauthorized disclosure of information.

If opting for cloud storage, t is advised to host all data and information in the Cloud servers in Sri Lanka. If planning to use an overseas server, it is advised to seek the consultation of the Health Information Unit, Ministry of Health.

According to the **Sri Lanka Government Information Classification Framework (SLGICF)** published in 2015, the information classification model adapted for Sri Lanka has the following elements:

This section will be updated with the latest version of the SLGICF accordingly
*Url:*https://www.gov.lk/elaws/wordpress/wp-content/uploads/2015/08/Information_Classification_FW_Report-v3-1.pdf

A. Classification Levels (Confidentiality Rating)
   a. **Unclassified:** Any unclassified information should be treated similarly or higher to information classified as 'Limited sharing.'
   b. **Public:** Any information which is easily available to the public. This type of information requires minimal or no protection from disclosure. This information should be specifically classified as public before its release and should at all times be approved as such by the information owner

      Ex:
      - Health Policies/ Guidelines
      - Advertisements
      - Organization Contact details.

c. **Limited sharing:** Disclosure of such information may lead to a minor probability of causing limited damage to the Sri Lankan Government, commercial entities, or members of the public. Ex. Personal information of citizens, Minutes of meetings and file notes of Organizations, Inventory data.
d. **Confidential:** Information may lead to a high probability of causing damage to national security, internal stability, national infrastructure, forces, commercial entities or members of the public.
e. **Secret:** Information may cause serious damage to national security, Government, and nationally important economic and commercial interests or threaten life.

B. **Dissemination Limiting Markers (DLM)** - Information where disclosure of information may be limited or prohibited by legislation or where it may otherwise require special handling.

a. **Sensitive:** It may be used with both classified and unclassified information.
b. **Sensitive: Legal** - May be used for any information that may be subject to legal professional privilege
c. **Sensitive: Personal** - Information which is personal and sensitive in nature. Example of such information may be protected health information, health records, salary, political beliefs of a person.
d. **Sensitive: Government** – Information used in clinical setting

The DLM "Sensitive" is intended to be modified by inclusion of the subject matter in order to ensure correct handling and an easy appreciation of the _need to know' requirement

Clinical-sensitive:

Clinical records that contain data or information relating to an individual patient/client (or groups of patients/clients) created to evidence the delivery of a clinical service.

Staff-sensitive:

Includes all official staff records where access would be Limited sharing to human resource personnel and nominated authorised staff. For example, personal files, recruitment information, grievance, or disciplinary records.

Executive-sensitive:

Information associated with executive management of the entity that would normally

be Limited sharing to the executive and nominated authorised staff. For example, sensitive financial reports, strategic plans, government matters and Staff issues.

Commercial-sensitive:

Procurement/contract or other commercial information such as sensitive intellectual property. For example, draft request for offer information, tender responses, tender evaluation records, designs and government owned research.

Audit-sensitive:

Information related to audit activities where access would be Limited sharing to officers of the Audit organization or nominated authorised staff. For example, audit and risk reports which identify security and control weaknesses.

Client-sensitive:

Personal information about clients or held on behalf of clients which needs to be treated confidentially.

So there should be a defined procedure to provide access to Restricted and Confidential information with an access control mechanism.

Least privileges for users

Users should be given the minimum required privileges to perform the authorized task and should not be assigned any unauthorized or higher-level privileges with the account access.

User Accounts

- Each should be given a unique user account to access the information with a user and a strong password for access to each information system.
- Institutions should maintain a user account registry under the head of the institution or assigned officer.
- If a staff member is transferred to another institution, retired, or no longer working with the assigned task user account should be deactivated immediately.
- The user activity log should be maintained in the information system log.

Passwords

- Each user should be provided with an unique user account and password to access the information system.
- Password should not be shared within the institution or outside the institution
- Should not use personal account password or any other password used in a separate system
- Password should not contain common terms or numbers (eg: Name, Telephone

3.2. ICT Equipment Management

All the ICT-related equipment including computers, UPS, Servers, Printers, Scanners Network switches, and Routers should be maintained in an inventory register.

Register should include

- Equipment name, Brand and Model
- Unique identifier (ex: Serial No / IMEI)
- Manufactured year
- Operating System (if relevant)
- Warranty period
- Purchased agent detail
- Maintenance agent's contact details

.

ICT Equipment Repairs and Decommissioning

- All the information including user accounts, passwords, images etc. should be properly backed up and removed/deleted before being handed over to the repair team.
- If the repair and maintenance are offered to a 3rd party organization, a Non-Disclosure agreement should signed at the time of awarding the maintenance contract.
- During the decommissioning of equipment, the identity of the equipment should be clearly documented.

- Separate inventory shall be maintained when ICT equipment components (ex-Hard drives, monitors, RAM, UPS Battery etc)

- Inventory Register should include asset owners, custodians, and users.
- All ICT assets such as hardware shall be checked to ensure that all confidential data and licensed software have been removed and secured prior to reuse or release outside of organizational control.
- All ICT assets being permanently taken out shall also be removed from the ICT asset inventory
- All ICT assets (hardware or software) which are decided to decommission ***according to the government procedures*** shall be destroyed either by an authorized third party vendor or by using secure discarding methods such as drilling, crushing or other demolition methods. This is to ensure that retrieval of any confidential data on the information asset are non-retrievable by any means.

3.3. Software Management

- It is observed that many new information systems are being built in the health domain to improve the delivery of health care, but there are duplications of such systems which meet the same requirements.
- In the event of a new requirement for an information system, the organization should contact the Health Information Unit of the Ministry of Health and obtain its concurrence, as indicated in the following circulars, in order to avoid duplication.

- *Circular No : 02-136/2015: Obtaining approval for implementation of eHealth Solutions*
- *Circular No : 01-58/2017: Central coordination of software development and deployment.*

- Vulnerability assessment should be encouraged on a regular basis and following a major version update deployment.
- In case of new software development, piloting, testing or implementation, institution shall follow instruction mentioned in National Digital Health standards and Guideline section (NDHGS V2.0 :3.1. Management of Digital Health Software)
- Security audits shall be performed by the competent authority prior to the piloting or implementation of a digital health software solution.

Other Software uses.

- Use only license software within an institution and should not be permitted to use cracked or pirated copies.
- If licensed version of the proprietary software are unable to purchase its advise to use free and open source software as an alternative
    - Ex: Operating systems – Ubuntu Operating System
    - Office package – Libre Office, Open Office
- User authentication should be in practice on all computers and protected with sufficient malware and virus security methods.
- Software should only be downloaded from approved and verified websites, and third-party applications should not be allowed to be downloaded from individual client PCs without proper administrative approval.
- All software, including the operating system, should be updated on a regular basis including the latest versions and patches, unless otherwise specified.

3.4. Network Management

Network Infrastructure and Administration

- Adequate physical protection should be provided to network devices, especially those in public areas, to prevent an adversary physically damaging a network device with the intention of interrupting services.
- Physical access to network devices can be restricted through methods such as physical enclosures that prevent access to console ports and factory reset buttons, mounting devices on ceilings or behind walls, or placing devices in locked rooms or cabinets.
- Power and telecommunications cabling need to be appropriately protected at all termination points
- Set clear administrator privileges , managing who has authorization to install software and change system configuration settings.

Monitor the Network

- Health institutions should implement network logging and monitoring strategies. These allow institutions to monitor unauthorized data transfers and unauthorized attempts to access institution private network.
- Detection systems should provide responsible parties with appropriate alerts and scheduled reports.

Maintain Firewalls VPN and Proxy Servers

- Institutions should install a firewall and do proper configuration to protect the network and limit outsider access by allowing only appropriate traffic to enter and leave the private computer network.
- Further this can be used to segment the network into unique security domains supporting enhanced layers of defence.

Isolate Guest Wireless Local Area Network (WLAN)

If the institution provides wireless access to the guest and visitors (WLAN) it is important that it is kept separate from the institution's main network.

3.5. Removable Media Management

- Includes and not limited to
    - Smart Phones
    - USB drives
    - External Hard Drives
    - Memory cards
    - Optical discs - CD/ DVD
    - Digital Camera
- Should not connect any unknown devices to a computer.
- Deactivate the autorun function for all removable media or devices.
- When removable media is connected, use an anti- virus / malware checking software to scan the device before opening the device.
- If any health data is stored in these devices, all such data stored in devices shall be encrypted when possible. If not, all personal identification data must be encrypted.
- If any health data is stored in these devices, all such data stored in devices shall be protected with a password.
- If any health data is stored in these devices, if possible, have remote wiping and/or remote disabling.
- If devices are used for new data storage or data transferring tasks, old data must be removed completely before handing over to another person.
- Report immediately if data breach is suspected or loss of device (refer incident management)

- For further information on using your own private device to access the health information system, refer to Section 5.6 Bring Your Own Device Policy

3.6 Legacy software and hardware management

Legacy software and hardware refer to outdated technology that is no longer supported or updated by the manufacturer. They can pose a significant security risk as they may contain vulnerabilities that can be exploited by attackers. To prevent such attacks following steps are to be followed:

- While legacy systems may no longer receive updates from the manufacturer, it's essential to keep them updated with the latest security patches and updates. This may require third-party vendors who specialize in providing support for legacy systems.

- Limit access to legacy systems to only those who require it. Additionally, restrict access to the Internet and other network resources to prevent unauthorized access or exploitation.

- Use strong passwords and multi-factor authentication to secure access to legacy systems.

- Use firewalls and encryption to protect legacy systems from external attacks. Firewalls can be used to restrict access to legacy systems while encryption can be used to protect data stored on them.

- Develop a disaster recovery plan that outlines how to recover from a security breach or other disaster. The plan should include regular backups, offsite storage, and procedures for restoring systems.

- When legacy systems reach the end of their life cycle, it's essential to decommission them properly. This may involve securely deleting data, disposing of hardware safely, and ensuring that all licenses and agreements are cancelled.

4. Physical and Environment Security

Information is susceptible to physical threats such as theft, physical damage, flood, fire, temperature fluctuations and other environmental changes. Therefore, a highly secure physical environment must be maintained within all health care institutions.

4.1 General Access & Protection

- Access to sites and buildings which contain sensitive and confidential areas should be restricted to authorized personnel only
- Access by authorized personnel on a “need to access” basis only.
- Physical keys or equivalent access mechanisms to server rooms, communications rooms and security containers should be handed over to authorized personnel and it should be documented.
- If a visitor needs to access those areas, they should be given a proper approval from the institution head and details should be log including date, time, name ,contact details and the reason for the access. In the event of visitor access it should be continuously supervised by the relevant person of the institution.
- Caring materials and equipment which are not essential for the tasks should be strictly prohibited when entering the restricted areas (ex: chemical, explosives, cameras etc.)
- All sensitive and confidential information storage areas should be located in stable , properly built premises and avoiding general public access areas. Lockable commercial cabinets or security containers should be used when necessary.
- Safety measures should be established to protect the assets from natural disasters (eg: Fire alarms , Thermal sensors , Lightning protectors etc).
- Steps need to be taken to provide backup power supply in case of power failure (generator , UPS). In case of prolonged power failure equipment must be properly shut down.

Clear Desk and Clear Screen

- Computers and terminals should not be kept unattended at any time. All devices shall keep logged off, screen locked or shut down when leaving the location.

- Keep all removable media, printouts, photocopies, or manual records containing confidential information in secure closed enclosures.
- Unauthorised people should be prevented from observing systems, in particular, workstation displays and keyboards.
- Avoid security cameras to be focused screens with sensitive information

4.2 Server Room Management

- Servers should be placed in a locked room where physical access shall be controlled and monitored.
- Server room must be accessible only via controlled doors and should not have external windows.
- Limit access to the server room to a small number of individuals whose duties require them to have access.
- Monitor who accesses the server room with log book / Video Surveillance / Biometric identification etc.
- Steps need to be taken to provide 24/7 uninterrupted power supply with backup power if possible
- As servers generate a great deal of heat, special attention may need to control the temperature of the room. May need to install 24 hour AC facility and maintain the temperature within desired range (Ex: Temperature alarm, dual synchronized AC supply)

4.3 Secure Disposal of Information

Information and data that are no longer required under existing practices (administratively or legally) shall be disposed securely

- Deletion of Data/ Information
    - Simple deletion of data or formatting of data devices is not a safe data disposal method, as there is a possibility of recovery
    - Permanent removal of data using overwriting or erasing method shall be ensured using a media sanitation tool . (DoD 5220.22-M is a software-based data sanitization method used in various file shredder and data destruction programs to overwrite existing information on a hard drive or other storage device)
        - Ex: Eraser (freeware)
          DBAN "Darik's Boot and Nuke" (open source, free)

- Deletion of Data/ Information shall be done under the authority of the controller preferably in their presence.

5. Access Control

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the organization. User shall be given access to the information on the principles of “Need to know” and “Need to do” basis which provides the least privileges for the required task .. Access should be granted after considering the sensitivity of the information and security clearance needed.

5.1 Physical Access Control

- Define and document the people / staff members who have physical access to all the ICT assets like servers, computers and other data collection devices.
- Restrict free access by implementing mechanical measures such as locks and key or technical measures such as passwords and access controls

5.2 Logical Access Control

Logical access control protects IT systems and data by verifying and validating authorized users

- Account Management
- Password Management
- Remote Access Management

5.3 Account Management

Account management is to support the appropriate rules, controls, and access rights. With the account management process, access should be provided only to the authorized users and should be able to prevent unauthorized access to the system and data.

- Each user should be given a unique user account to access the information with username and complex password for the information system
- Institution should maintain a user account registry under the head of the institution or an assigned officer.
- Limit user account privileges based on job role. The least amount of privileges to perform the intended task should be given.
- If provided, default passwords shall be changed following the installation of systems or at the first login to the system/software.

- User accounts should be locked out after using the wrong password or username for predefined times. Reactivation of the account shall be done only after identifying the user properly.
- If staff member is transferred to another institution, retired or no longer working with assigned task, such user accounts shall be deactivated immediately
- User account activity log shall be maintained in the information system log record.
- It is advised to use two-factor authentication to authenticate the user when even possible.

All user access rights and records should be reviewed periodically. User accounts must be checked for duplications, unused accounts or incorrect access level for the accounts. Duplicated and unused accounts shall be deactivated.

5.4 Password Management

- Each user shall be given a unique password to access an information system.
- Password shall not be shared within institution or outside the institution
- Personal account password or any other password used in separate system shall not be used
- Password shall not contain common terms or numbers (eg: Name , Telephone number, etc.)
- User should have unique criteria to work out password from passphrase to create a strong and complex password. A strong password must be at least 8 characters long and must consists of both upper- and lower-case characters, digits, and special characters.
- In case of a forgotten password, the system should facilitate the password recovery through a secured channel.
- Password shall not be communicated through any media like, fax, email or SMS
- The users shall be required to change their password periodically. The frequency should be determined based on the sensitivity of the information

5.5 Remote Access Management

Allowing access through the physical walls and firewall protections may lead to several security challenges.

- Provision of remote access to a system must be strictly controlled and monitored.
- When a remote system is accessed, make sure that the second device is not connected with third party applications or networks.
- User devices connected with a system should be in par with the BYOD policy mentioned in 5.6
- VPN should be used for remote access whenever possible

5.6 Bring Your Own Device Policy (BYOD Policy)

When the users are using their personal devices to access the information system of the institution, the following requirements need to be adhered.

- The devices should be updated with the latest security updates.
- There needs to be a virus guard that is updated.
- Other software from a non-trusted party should not be installed in the same device.
- The device shall be able to make a secure connection with proper encryption.
- In the event the user suspects of having a malware installed in the device, it should be brought to the attention of the system administrator in writing, immediately. This should be manged based on the guidelines mentioned in section 7.1 below.
- In the event the device is lost or stolen, it should be informed in writing to the system administrator immediately. This should be manged based on the guidelines mentioned in section 7.1 below.
- Before the user disposes the device, the user needs to consult the system administrator and make sure there is no data relating to the system remaining in the device. (Refer section 4.3 above)

6. Third-Party Security Management

When there is a requirement to provide access of ICT assets to a 3rd party (for maintenance / developments etc.), a Non-Disclosure Agreement (NDA) shall be signed beforehand.

NDA shall include

- Clear description of supplier's rights
- Access control levels and restrictions
- Protection of confidential information & legal obligations
- Prevention of information misuse such as unauthorized copying, sharing or saving.

If subcontracts are involved they also should comply with the conditions of the primary agreement.

Further, if a third party is given a physical / hardware access, following additional guidelines should be followed.

- A registry should be maintained to record all routine maintenance services and specific breakdown repairs with the details of the technician involved.
- If hardware devices need to be removed from the institution premises, all personal identifiable data should be removed / deleted (when possible) with a backup.
- Proper disposal of the removed hardware parts
- Remove the established connection like user accounts with 3rd party software after the completion of their service.

7. Information Management

A security incident is a single event or series of events that violate or threat of violation of computer security policies, guidelines or standards security practises.

Data breach is a type of security incident that expose confidential, sensitive, or protected information to an unauthorized person.

Few examples for security incidents

- Computer system intrusion
- Unauthorized access to, or use of, systems, software, or data
- Unauthorized changes to systems, software, or data
- Loss or theft of equipment used to store or work with sensitive university data.
- Denial of service attack
- Compromised user accounts.
- Malware infection
- Distributed denial of service attacks
- Unauthorized access
- Insider breaches
- Destructive attacks
- Unauthorized privilege escalation
- Loss or theft of equipment.

7.1 Breach Notification & Incident Management

- All security incidents and data breaches reported to the institution shall be documented in the institution register/ book
- Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk
- All security incidents and data breaches should be investigated by the Security Institution head within 24 hours of the incident.
- If preliminary investigations revealed a health data is compromised (unwanted exposure, effect the integrity or permanent loss of data), it should be notified to the Health Information Unit at the Ministry of Health. Provincial institutions should report the incidents to the relevant RDHS office too.

- Incident notification should include.
    - Nature of the breech (Date /Time/location / Causative factor)
    - Likely consequence of the breech
    - Measures taken to prevent further damage due to the breach.

- Suggestions to prevent future similar events
- Contact details of the reporting person

- Following an investigation into an incident, a detailed investigation of vulnerabilities needs to be done. Steps shall be taken at all levels to mitigate such vulnerabilities identified.

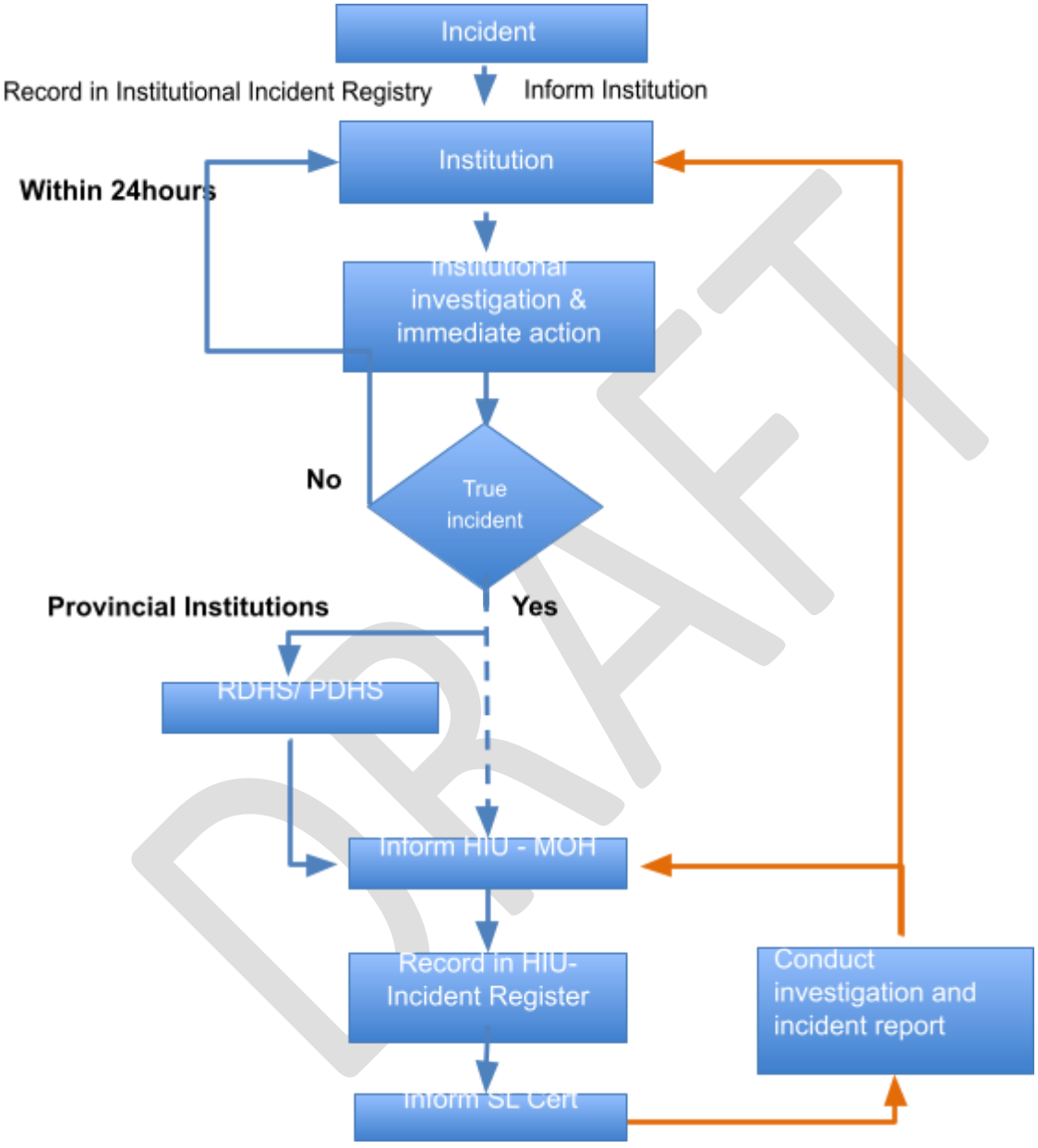

Figure 01: Incident management workflow

7.2 Disaster Recovery and Business Continuation

Disaster recovery implies placement of procedures and measures to ICT related equipment, Networks and information systems to recover from major disaster and plan in place to provide continued services and care of the routine practice.

Business continuity planning (BCP) is the process involved in creating a system of prevention and recovery from potential threats to an institution.

General guidelines

- All institutions need to identify and critically analyse their workflows and business process to identify the high risk and critical process.
- Risk level is based on the likelihood of the unwanted event or disaster to occur and level of the impact it cause on the institution
- As this guideline only addresses the disaster recovery related to the ICT event, this shall be supplemented to the institutional disaster recovery plan.
- Document the complete process to follow in a case of probable disaster (Ex : Flood , Power failure)
- Roles and responsibilities shall be assigned, tested and documented.
- All the staff of the institution shall be aware about the recovery plan . Conduct awareness programme time to time and these processes should be tested regularly (quarterly) and updated when necessary.
- Document the recovery procedures of ICT assets and equipment in case of disaster (ex : Where to store computers and how to store in case of floods)
- Make aware of all related staff about provisions of urgent procurement of related equipment or services in case of emergency.
- Maintain a registry of all related contact persons, services providers within the institution and outside the institution for an emergency contact.
- Identify and maintain buffer stock to essential ICT assists to replace in emergency event
    - Telephones
    - Computers
    - Network equipment's backups for replaces in disaster
- Planning /Architecture
    - Try to avoid install/ place all essential equipment in one place/building
    - Keep network diagram for easy accessible place
- Backup and recovery controls
    - Backup and recovery procedures shall be documented and followed
    - Backup procedure should include
        - 2 automatic backup on 2 separate location on daily basis
        - 1 offline backup weekly (Optical disc / External Hard Drive/ Tape drive)

    - Backup and recovery procedures should periodically tested
    - Regular validation and testing the backup by restore the systems on separate server/ machine
- Power Failures
    - Protect equipment from power failures and other disruptions caused by supporting utilities
    - Provide an uninterruptible power supply (UPS) to all key equipment
- Telecommunication Asset Management
    - Identify each telecommunication Asset, and maintain an inventory of all important assets
- Software Management

  Refer software management section (3.2)

8. Information Sharing

Timely information sharing is a key component of robust clinical governance. These principles are designed to promote the implementation of standard practice across the health care system where the shared information protects the privacy of patient data, empowers decision-making, and also increases the public trust.

8.1 Internet & Email

- All the employees should be responsible for using internet / email in an ethical and lawful manner and it should be adhered to work related activities during duty hours.
- When an official or government domain email address has been provided, always use it for official communication. Refer to National E Health Guidelines and Standards V.2.0 for acquisition of official email addresses.
- Never transmit patient information that contains identifying information through email as there is risk of exposing the information
    - Most email services have not implemented end to end encryption.
    - High probability to send an email to a wrong recipient.
    - Emails can be forwarded easily to third parties without consent from the original sender.
- When sending information regarding an employee, ensure you do not share confidential / personal health / medical information.
- Never use reply all when responding to an email regarding employee issues – reply to the sender and cc the appropriate additional individuals if there are any.
- If there is an email from an unknown sender , be vigilant about email. Should not download attachment without verification of the sender. Should not click any links included in the email. If you need to visit a site mentioned in the email you should type the URL in a browse if you know if not search for the website using search engine and follow the link there.
- Email addresses should be verified before sending an email.

8.2 Internet Usage and Monitoring

- Health staff should use internet relevant services legitimately needed for their work.
- The Health Information & Research Unit/Planning unit or any other relevant unit shall monitor Internet use of all inbound and out bound internet traffic in the organization should be monitored with source IP Address, date, time, the protocol, and the destination site or server and it should be clearly informed to all users.
- Internet Use records should be preserved for 180 days.
- In case of an incident, Investigating officers may access all reports and data. Further, activity reports will be made available to any employee as needed upon request.
- the following categories of websites and protocols should be blocked:
    - Anti-Social and Illegal

- Hacking
- Illegal Software
- Violence
- Racism, Hate & Intolerance
- Compromised
- Botnets
- Spyware/ Malware Sources
- Spam Sites
- Weapons
- Criminal Activity
- Illegal Drug
- Phishing & Fraud
- Adult Material and Abusive
- Child Abuse Images
- Nudity
- Pornography/ Sexually Explicit
- Gaming and Gambling
- Gambling
- Games
- Commerce
- Advertisements & Pop-Ups
- Shopping
- E Auctions
- Anonymizers
- Download Sites
- Image Sharing
- Peer-to-Peer
- Streaming Media & Downloads
- Chat / Instant Messaging
- Dating & Personals
- Social Networking
- Others
  - Alcohol & Tobacco
  - Cults
  - Unwanted Software

- The Health Information & Research Unit/ Planning Unit shall periodically review and recommend changes to web and protocol filtering rules.
- If a website or protocol is miscategorised, employees may request the website or protocol to be blocked or un-blocked by submitting a request to the relevant unit.
- If an employee needs access to a website or protocol that is blocked and appropriately categorized, they must submit a request to the Internet monitoring Unit. The Internet monitoring Unit will unblock that website or protocol following a thorough appraisal of the request, for that employee only.

The Internet monitoring Unit will track and record approved exceptions throughout.

- Any employee found to have violated this guideline may be subjected to disciplinary action.

8.3 Social Media Usage

- Health care institutions are encouraged to use social media to improve health education and awareness with verified health information.
- Any health institution that maintains an official social media profile shall notify the Health Information Unit along with the account administrators details.
- The organization is totally responsible for the material published on the social media sites. Special attention shall be taken when uploading content to the websites, in particular when publishing the personal identifiable data of health care recipients or providers.
- Under no circumstances these content should be posted without their consent.
- Under no circumstances can such content be made public without their consent.
- Social media comments should be monitored and should not allow any foul language or "hate speech" (racial-, ethnic- or gender-bashing language) and personal attacks.
- Visitors who repeatedly submit inappropriate content should be banned from the social networking sites

Editorial Board

Dr Lasantha Ranwala
Dr Sumaiya Mubarak
Dr Wikum Sudasinghe

Contributors

Dr Anil Samaranayayake
Dr Palitha Karunapema
Dr Ravi Wickramarathna
Dr Ravindra Premasiri
Dr Kusal Wijayaweera
Dr Chaminda Weerabaddana
Dr Muditha Hapudeniya
Dr Neranga Liyanarachchi
Dr Subodha Manoj
Dr Prasad Ranathunga
Dr Jayathri Wijayarathne
Dr Dhanushi Jayathilake
Mr. Priyankara Perera and SL Cert Team

Annexure 01:

Health Institutions Security Assessment – Scorecard

This scorecard is used to assess the present information security status of the health institutions in Sri Lanka. A responsible officer for information security management shall mark the scorecard quarterly and send to the HIU- MOH before end of the 1st week of next quarter. Please refer "Health institution Security guideline for further clarifications.

Points Scale
0:No implementation -no action has been taken in this regard
1:Initiated : *Actions have been initiated very recently or few people in the institution are involved yet.*
2: Sensitized: *More than 50% of work has been done including awareness of the staff.*
3: Completed: *Task is completed*
4: Integrated : *Activity has been established as a routine within the institution and a periodic reviewing mechanism is in place*

Information Security Officer/Responsible officers Details

Name **Designation** **Phone:** **Email:**	**Institution:** **Date:** **Year:** **Quarter:** **Total Score:**

Use of Information Systems (Please mark X)

Stand-alone Systems		**Cloud Systems**			
HIMS		DNMS- District Nutrition Monitoring System		LeIS - Leprosy Health Information System	
HHIMS		eIMMR-Electronic Indoor Morbidity and Mortality Registry System		Medical Supplies Management Information System	
OPD and clinic appointment management system		EIMS- Electronic Information Management System		National Human Resource Information System	
PACS system		Electronic Mental Health Management Information System		NBTSIS - National Blood Transfusion Service	
Letter Management		eMSRS- electronic Monthly Statistics Reporting System		QHRMS - Quarantine Health Record Management and Surveillance System	
CIGAS		eRHMIS (Electronic Reproductive Health		e-NIP	

Payroll	
URL of Institute Website	
Official email: (Please write)	

Management Information System)	
eRHMIS School Health Programme	
Health Facility Survey Management (HFSM) System	
HIMS-Anti Malaria campaign	
HRMIS-Human Resource Management Information System	

Others:	

Inservice Training Programmes on Data Privacy and Information Security during this Quarter

Total Number of Staff	
Number of Training programmes conducted/ Attended	
Number of staff trained	

Information Assets Management			
Information Management (*3.1)*	User Accounts	Information are managed according to their sensitivity level	
		Users are given the minimum required privileges to perform the authorized task	
		Each User is given a unique user account	
		Institution is maintaining a user account registry	
		Default passwords are not allowed to use after the full implementation of a new system/device	
		If a staff member is transferred to another institution, retired or no longer working with assign task user account is deactivated immediately	
	Passwords	User adherence to strong passwords usage	
		Passwords are not allowed to be communicated through any media like, fax, email or SMS	
		Passwords are not allowed to be shared within or outside the institution	

ICT Equipment *(3.2)*	An up to date inventory for all ICT devices is maintained	
	NDAs are signed with all 3rd party ICT service providers	
	Steps have been taken to delete/remove all information stored in devices before handing over to the repairs/disposal when applicable	
	All computers /devices are protected with Administrative user account and Password	
Software Management *(3.3)*	Concurrences from Health Information Unit of the Ministry of Health have already been taken for the implementation of new software as mentioned in the circular no:02-136/2015	
	Using only the license software within the institution and not allowed to use cracked or pirated copies	
	Software download/ installation is restricted on individuals devices and allowed only when the administrative approval granted	
Network Management *(3.4)*	All network devices including power and telecommunications cablings are adequately physically protected	
	Network logging and monitoring strategies are implemented to monitor unauthorized data transfers and unauthorized attempts to access institution private network	
	A firewall has been implemented and configured properly to protect the network by filtering outsider access	
	Public wireless access (if provided) is kept separate from the institution's main network.	
Removable Media *(3.5)*	Implementation of best practices for removable media usage	
Physical and Environment Security		
General Access *(4.1)*	Access to sites and buildings which contain sensitive and confidential information is restricted only to authorized personnel as “need to access” basis.	
	Physical keys or equivalent access mechanisms to server rooms, communication rooms and security containers are documented and handed over only to authorized personnel	
	Visitors are allowed to access those areas only following proper approval from the institution head and their details are logged	
	Adequate measures have been taken to protect the assets from natural disasters (eg: Fire alarms, Thermal sensors, Lightning protectors etc).	
	Steps have been taken to provide backup power supply in case of power failure	
	All users are educated about Clear desk / Clear screen practices	
Server	Servers are placed in a locked room where physical access is controlled and monitored	

Room Management *(4.2)*	Monitoring the accesses to the server room with logbook / Video Surveillance / Biometric identification etc.	
	Steps have been taken to control the temperature of the room ex: 24 hour AC supply /Temperature alarm	
Secure Disposal of Information *(4.3)*	Follow up secure deletion methods of information and maintaining records	
	Permanently deletion of data using overwriting or erasing method when those data are no longer required or before decommissioning of hardware	
	All condemned hardware are physically destroyed or handed over to an authorized third party for safe destruction under the permissible by government regulations of the destruction of equipment	
Access Control		
Remote Access *(5.5)*	Provisions of remote access to a system are strictly controlled and monitored.	
	User devices connected via remote access are kept updated with the latest versions of antivirus software.	
	VPN is used for remote access whenever possible	
Third-Party Security Management		
6.0	When there is a requirement to provide access to ICT assets for a 3rd party (for maintenance/developments etc.), Non-Disclosure Agreements (NDAs) are signed beforehand.	
Information Security Incident Management		
Breach Notifications *(7.1)*	All security incidents and data breaches are documented in the institution “security incident” register and investigated by the head of the institution	
	Institution adheres to “Data Breach Notification Workflow”	
Information Sharing		
Internet &	All the employees are educated about responsible use of internet /email in an ethical and lawful manner	
	Internet usage of the institution is monitored and regulated	

Email *(8.1)*	Unrelated/ Harmful websites are blocked	
Social media (*8.3)*	A mechanism to monitor and regulate contents uploads and user feedbacks in social media	

The security measures implemented in the information systems which beyond your control may be ignored in the above assessment. Ex. End user of a system which is implemented by another institution