LOGO

CENTRE NAME

CENTRE ADDRESS

DOCUMENT NAME	POLICY MANUAL- IMS(Information Management System)
DOCUMENT NUMBER	IMS/JSL/10
DATE OF CREATION	22/05/2021-6 MONTH AGO TODAY
DATE OF IMPLEMENTATION	25/05/2021- AFTER 2 DAYS OF CREATION DATE
DATE OF REVIEW	21/05/2022- AFTER ONE YEAR OF CREATION DATE
PREPARED BY	Name & Designation: DOCTOR NAME DESIGNATION OF DOCTOR Signature:
REVIEWED BY	Name & Designation: DOCTOR NAME DESIGNATION OF DOCTOR Signature:
APPROVED BY	Name & Designation: DOCTOR NAME DESIGNATION OF DOCTOR Signature:
ISSUED BY	Quality Department

AMENDMENT SHEET

Sl.No.	Section No & Page No	Details of amendment	Reasons	Signature of preparatory authority	Signature of approval authority
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					

1. Purpose

To outline the process by which data and information is acquired, maintained, stored and utilized in a manner that protects the confidentiality, maintains the security and verifies the integrity of patient or employee related information.

TITLE	Policy on Information Confidentiality, Security and Integrity of
SUMMARY	This document provides instruction and guidance to Hospital staff on various issues pertaining to the management of data in the hospital both of clinical and administrative nature. The policy discusses the systems and processes established for ensuring confidentiality, security and integrity of clinical and administrative information of the hospital at various levels.
DISTRIBUTION	To all concerned departments

2. Definitions

a) **S ecurity**: The protection of information from unauthorized alteration, addition, change, destruction, or disclosure, whether intentional or accidental.

b) **Confidentiality:** The safekeeping of data and information is restricted to individuals who have authorization, need and reason for access to such data and information.

c) **Confidential (Sensitive) Information**: Information that requires special safeguards due to its private nature. Confidential information includes, but is not limited to, patient care (all information regarding a patient’s identity, treatment and diagnosis), personnel, financial and some business records.

mation Resources: Includes, but is not limited to, computers, faxes, telecommunication hardware, software, storage media, computer sign on codes, medical records documentation, and information stored, printed and/or processed by a computer system.

e) **Storage Media:** Includes, but is not limited to, paper, magnetic media, optical disk, film and other methods of retaining information.

f) **Integrity of Data**: The protection of data or information to insure that it can be identified by its author. Unauthorized alteration is prohibited to insure that data and or information is verifiable.

g) **CENTRE NAME Confidentiality Statement**: A signed statement that verifies the individual understands of confidentiality standards and the implications for inappropriate access or disclosure of confidential information.

3. Policy

a) Awareness and Responsibility

i. CENTRE NAME employees and junior doctors shall receive information regarding the facilities standards for appropriate handling of patient and other information in Orientation. The employee signature on the Orientation document and CENTRE NAME Confidentiality Statement signifies that the employee acknowledges the standards and any potential penalties for breach of these standards. Original orientation documents are maintained in the Human Resource Management's employee files.

ii. All employees shall receive orientation on the principles of appropriately processing information relative to their job function and role. Ongoing review of these standards shall be conducted for all personnel.

iiii. The -compensated observers, students, vendors, or other persons conducting business with CENTRE NAME shall receive specific instructions on the principles of appropriately processing information received or observed within the institution. Departments whose staff facilitate or mentor persons not associated with affiliation agreements shall maintain a signed CENTRE NAME Confidentiality statement.

iv. Affiliations agreements shall require that all persons associated with the agreement be informed, understand, and comply with the standards of confidentiality prior to entry into the facility. The affiliation is responsible for awareness and signed acknowledgment from all participants.

v. The system access should be deleted for the employees who separate from the facility.

vi. Department/Area supervisors shall notify the IT department when access rights of individuals are to be terminated following involuntary separation or reassignment. This notification shall be made as soon as possible, but no later than three working days from last date of service.

b) Access to Information

i. CENTRE NAME Management shall identify and approve the retrieval systems and information that shall be accessible to staff, volunteers and other third party business associates.

ii. Access to confidential information is given by written authorization and approval. Access to information or systems without the consent of appropriate CENTRE NAME authorities, constitutes illegal activity and the person(s) involved are subject to enforceable penalties.

iii. Access methods to CENTRE NAME information or communication systems are confidential. Sign on codes, when applicable, are individually assigned and shall not be shared with anyone. Penalties may be invoked if access methods are revealed or made available to anyone without the permission of appropriate CENTRE NAME authorities.

iv. All information systems shall have defined mechanisms to insure security and integrity of confidential or sensitive information. Individual departments who acquire and are responsible for maintenance of any related information systems shall be required to establish policies to secure the information contained in these systems. Department policies shall be consistent with existing Hospital policies.

v. Storage media and other methods that are utilized to access, retrieve, and communicate confidential or sensitive information shall be governed by the same uniform policies and procedures of CENTRE NAME to insure that confidentiality, integrity and security is optimally maintained.

vi. Access to information from CENTRE NAME systems is limited to defined personnel classifications, as appropriate.

vii. Individuals who have access rights to any confidential patient or employee data must secure the information through appropriate means.

Appropriate sign off procedures must be utilized with computerized systems.

viii. Information systems that contain sensitive or confidential data shall automatically display a screen saver or log the user out of the system when a specified period of inactivity occurs.

c) Securing Data

Manual Systems

i. Requests for health record information shall be made available only to those employees, medical staff members, support staff, etc. Displaying their identification badges.

ii. The medical record folder contains two warnings to staff members as a continuous reminder of their confidentiality obligation - “Confidential Health Information” and “This folder may not be removed from the hospital premises”.

iii. The medical record scare stored in areas directly controlled and monitored by the Medical Records Department.

iv. All requisitions for the retrieval of medical records shall contain the patient’s name, medical record number, current date/time and requesting party’s name.

Medical records are transported to patient care areas and administrative offices via duty nurses or pharmacy staff. All staff transporting medical records must ensure the privacy of patient- identifiable information during the transport process. Medical records shall not be left unattended during the transport process.

v. Records are maintained in the patient care areas in locked cabinets/designated areas in nurses station or Duty medical officers room that are not accessible by unauthorized individuals.

vi. Telephone request for patient-identifiable information are discouraged and limited to emergency situations. Emergency requests are usually generated by physicians or other ‘key’ hospital/physician office staff. Telephone request shall be handled using a ‘call-back’ procedure to verify the identity of the requesting party.

vii. Extra copies of printed reports containing confidential information (including but not limited to patient’s name, medical records number, etc.) shall be disposed of by shredding when the reports are no longer needed.

viii. The original medical record shall not be removed from the hospital premises except upon receipt of court order.

Automated systems

i. Personnel who are granted authorization to access mainframe applications must maintain an approved anti-virus software package. Failure to do so may result in termination of access rights.

Appropriate safeguards shall be defined when remote access is granted to the authorized parties. These connections to CENTRE NAME computer systems shall be routed through devices that require password verification. Personnel granted access shall sign a statement acknowledging they are responsible for all activity attributed to their user ID and shall only perform authorized activities.

ii. Data control and production areas shall be accessible only through a secured entrance by authorized personnel. Unauthorized personnel must be accompanied by authorized personnel.

iii. Storage media that is identified as confidential or sensitive information shall be labeled as “CONFIDENTIAL” and stored in areas that are restricted only to authorized personnel. Prior to discarding any CONFIDENTIAL storage media, the information shall be rendered unusable.

iv. Confidential information which has been downloaded must be maintained under the same confidentiality and security standards as the original data.

d) Integrity of Data

All persons entering and/or accessing data from information resources or storage media must be identified. Additions, corrections or amendments to data must identify the individuals performing the changes.

e)Violations of Confidentiality of Information

i.Violations will be reported to and investigated promptly by management to determine if the cause was due to an individual's negligence, an accidental mistake, improper training, or misunderstanding the information resource and or policy.
ii. Security violations are defined as follows:

- Failure to sign off from the access terminal prior to leaving the terminal.

- Utilizing another user's sign on or password.
- Accessing confidential information without a legitimate reason.
- Attempting to and/or circumventing security systems.
- Disclosure of confidential information.
- Disclosure of user password or sign on.
- Unauthorized entry, correction, amendments or change to existing data.

iii. An individual's access rights may be suspended immediately upon the discovery of a possible violation of this policy.

iv. Violation of this policy may result in disciplinary action up to and including termination.

f) Changes in Access Rights

i. Access rights shall be reassigned upon transfer to another budgetary unit when there is a change in job duties which requires a different access level.

ii. Access rights may be suspended if an individual is under investigation for cause.

a) Disposal of Written Documents

- When disposal is appropriate, all written or printed documents that contain confidential or restricted information must be disposed of in a ensuring that they are properly shredded or destroyed.

- Outdated computer equipment, other electronic devices, and electronic media must not be discarded in dumpsters or regular trash containers.

- IT Team are responsible for taking the appropriate steps so that any confidential or restricted information contained on outdated CENTRE NAME computer equipment or electronic devices is erased and not recoverable, including laptops and Personal Digital Assistants (PDA's) provided by CENTRE NAME. Outsourced IT Team if any must also follow these same procedures when there is a transition in who will be using the computer equipment or electronic devices.

- IT Team are responsible for taking the appropriate steps so that any confidential or restricted information contained in electronic media, such as tapes, hard drives, and diskettes, is erased and not recoverable. Appropriate methods for disposal include: overwriting or partition deletion for hard disks and overwriting, physical destruction, or magnetic erasure (degaussing) for tapes, diskettes, and other media.

○ Questions regarding the proper disposal of electronic devices or media containing confidential or restricted information should be directed to the IT Team.

Questions regarding the proper disposal of written or printed documents that contain confidential or restricted information may be directed to the Privacy Office.

b) Disposal of Film

Films, microfilm must be cut into pieces or chemically destroyed.

c) Disposal of Electronic Devices and Media

d) Vendors and Contractors

- All vendors and contractors that have responsibility for disposal of printed documents, films, or electronic information must adhere to CENTRE NAME Security and Confidentiality Policies.

Administrator and Purchasing are responsible for applying the CENTRE NAME security, confidentiality, and business associates.

Reference:

Standard - IMS 5 – All elements

Manuals – …………………, MRD Manual,

Annexure-I

CONFIDENTIALITY AGREEMENT

CENTRE NAME, has a legal and ethical responsibility to safeguard the privacy of all patients and protect information that is defined as confidential. Confidential information includes information contained in manual documentation as well as information stored in the Hospital's computer systems. Patient, personnel, financial and other business records contain confidential information.

I understand that information regarded as confidential must be maintained in the strictest of confidence. As a condition of my affiliation with CENTRE NAME, I hereby agree that I will not at any time during or after my affiliation CENTRE NAME, disclose any confidential information to any person, other than as necessary in the course of my affiliation with CENTRE NAME, and when accompanied by the appropriate, authorized personnel.

Information in the Hospital's storage media may be accessed only by authorization from the Administration; computer system access is granted only to persons who have been issued user identification codes. Using another employee's user identification code/password or giving your user identification code/password to another person may result in disciplinary action.

I understand that all user identification codes and passwords are confidential, and may not be shared or disclosed to any other person. I understand that I am directly responsible for the accuracy and completeness of data entries, which are entered into the facilities' storage media.

I understand that it constitutes a security violations to fail to sign off when leaving the computer unattended; accessing any medical or employment record without appropriate need and approval; requesting another employee to access my employment or medical record; allowing another employee to utilize my password; accessing medical or employment records without having a legitimate reason; using another employee's access code, revealing confidential information of patients, employees or business/financial details, etc. All security violations will be reported to and investigated by the appropriate authorities.

My signature below indicates I have read the Security, Confidentiality and Integrity of Information Policy and have been given the opportunity to have any questions regarding this statement explained to me, and the failure to abide by this agreement may result in disciplinary action, including dismissal from employment.

_________________________ ____________________

Name

SIGNATURE Date

Purpose:

To provide appropriate documentation of inpatient and outpatient medical care in such a way that it facilitates communication, coordination and continuity of care and promotes efficiency and effectiveness of treatment.

All entries shall be:

- Unique identifier of the patient on every document page.
- Written in black / blue indelible ink for handwritten documentation. No pencil entries.
- Dated and signed (include day, month, and year).
- Timing of entries is required on Medication Administration
- Legible and include clear, concise and pertinent patient information with authenticated Signature
- Chronological.

All forms in the record must have been previously approved and numbered.

1. No part of the medical record is ever to be removed after entry.
2. The patient's name and identification number must appear in the front page of the case sheet
3. Written Signatures validate written orders and written notes.
4. Inpatient Care is documented in the Medical Record and includes:

    - Reason for admission, diagnosis, and plan of care must be included in the documents.

Evidence of the initial patient assessment and all subsequent re-assessments.

- Documentation of interventions based on physician orders.
- Documentation of nursing care provided.
- Any operation /Procedure performed in detail. Name, signature, date, time on every entry made in the record.
- The records should be legible.
- The records should be in a chronological order demonstrating the continuity of care.
- Transfer notes should be in accordance to the policy of transfer and should include- Date, reason for discharge and name of the receiving hospital.
- Medication administration is recorded on the Medical Orders and Administration Chart.
- Aspects of patient care during operative or other invasive procedures, documented on forms specific to each specialized area.
- Patient discharge instructions
- Discharge summary should be prepared and signed by the Treating Doctors.
- Death summary should include – cause of death, date, time and should bear the signature of the clinician in charge.

Order of Filing of medical record:

SL. No	Patient file arrangement
1	Patient profile & Education form
2	Consent form
3	Initial Assessment form
4	Progress Note/Procedural notes
5	Pre Existing medication sheet
6	Medication sheet
7	Pain Assessment & Management
8	Treatment plan
9	Treatment sheet
10	Nutritional Assessment
11	Diet Slip
12	Nurses Assessment
13	Vulnerability assessment sheet
14	Referral Forms
15	Assessment sheets –
16	Discharge summary

16 Details of documents provided

Policy for making changes in the medical

Record Purpose:

Standardize the process of making changes in the medical record according to the requirement of the law.

Policy:

1. The changes made in the demographics of the patient only after submission of an application with identification proof (for name and age).
2. The application is approved by the Medical Director and is then filed in the medical records department.

Reference:

IMS 3 –

Amendment Record

ACCESSING MEDICAL RECORDS

1. Purpose

Medical Records Department (MRD) is the custodian of all the discharged/ expired medical records. It follows a set of rules & regulations while allowing access to the records to the care providers within the Hospital.

2. Scope

Hospital wide

3. Policy

a) Access of Information to Internal Staff of Hospital:

i. Access of information is allowed to the following internal staff.

a) Medical Director

b) Consultants

c) Duty Doctors

d) Nurses

e) Data entry staff

ii. The treating consultants and the other clinical doctors are authorized to have access to the discharged inpatient's medical records. When a patient is re-admitted, the treating doctor can request for previous admission file.

iii. The non-clinical and other administrative staff can access the patient medical records with the written approval of the Medical Director.

A form named "Requisition for disclosure of Medical Records" is filled by the concerned to request for the patient medical records. It is submitted to the Medical Records Department (MRD) and is filed in the patient records when the patients file is returned.

Reference: Standard - IMS 3g

AMENDMENT RECORD

AMENDMENT		DETAILS OF AMENDMENT	ISSUE STATUS	REV. STATUS
NO	DATE			

POLICY FOR SAFEGUARDING DATA/ RECORD AGAINST LOSS, DESTRUCTION AND TAMPERING

1. **Purpose**

   Protect and safeguard data/ records against loss, destruction and tampering.

2. **Scope**

Hospital wide

3. **Policy**

   All the employees should follow the laid down procedure for safeguarding data/ record against loss, destruction and tampering.

4. **Procedure**

   a) The death records are kept in separate cabinets under lock and key in the medical records department to protect them from any loss or theft.

   b) The records for the OP (outpatient) and IP (in patient) patients are kept in the racks.

   c) No unauthorized person (without I-Card) is permitted to enter the Medical Records department.

   d) The records are given only to the authorized person with their due signature on the requisition slip.

   e) A proper handing and taking over of records is done with the help of a written requisition, which is attached to the patient file. The file is manually checked before taking back the records.

5. Adequate pest and rodent control measures are taken for safeguarding records.

6. All due fire prevention measures and fire protection devices are in place for protecting the records from destruction or damage while in store.

7. All old IPD/OPD files are periodically made as inactive as per policy of retention of medical records.

Reference:
IMS 5c

Amendment Record

1. Retention and Destruction of Medical Records

Purpose

Establish policy and procedure for retention and destruction of medical records.

2. Scope

Hospital wide

3. Policy

As per hospital policy

a) For In Patients, if the patient does not visit the hospital for 7 continuous years the records are made inactive.
b) For Out Patients if the patient does not visit the hospital for 5 continuous years the records are made inactive.
c) The medical records department keeps a record of all the files, which are destroyed.
d) Files of death cases will be kept for 10 years
e) Medico legal case sheets are maintained forever

Electronic Records retention and destruction

a) Regular backup’s of the electronic data is taken on daily/ monthly/ yearly basis.

The retention period for daily backup is one week and the retention period of weekly backup is one month. The monthly backup’s is retained for two years while the yearly backup’s are retained for ten years

LOGO	CENTRE NAME CENTRE ADDRESS	Doc No	IMS/JSL/10
		Issue No	10
		Rev No.	00
		Date	22/05/2021
		Page	

Policy on Information Needs of Hospital

0.0 PURPOSE:

To maintain the information related to patient care and hospital administration well across the hospital and to provide guidance to designated staff or individual to manage all the information properly.

1.0 SCOPE: Hospital Wide

All data available in hospital.

2.0 DEFINITION: Nil

3.0 RESPONSIBILITY:

- Medical Director
- Chief Administrative Officer
- Operations head
- IT Administrator
- MRD In charge

4.0 POLICY:

All information pertinent to patient care and hospital administration must be well maintained both electronically and manually.

Following laws that are applicable for information management shall be abided

1. IT Act 2010
2. AERB Rules
3. RTI Act 2015

5.0 PROCEDURE:

A. <u>Guidelines or effective management of information and data.</u>

- The Hospital Software shall be able to incorporate, modify, add or delete the existing information in the System
- There shall be a provision in the Software to update and retrieve the information as and when the need demands
- The electronic information shall be stored such that only authorized personnel can gain access to it.
- The Staff and other hospital personnel in general shall have access to the online information on HIMS after written/confirmed approval from their respective Departmental /Unit Heads.
- The electronic system shall be subject to change as per the requirements of the personnel if the need arises
- The information shall be kept appropriately secured by using passwords and online security systems effectively
- The confidential information (esp., online policy documents, hospital statistics etc) shall be kept under strict security of limited personnel and on limited systems to prevent its misuse.
- In case of power failure/system failure, there shall be provision of back up such that there is no risk of data loss from the electronic data storage system
- Special cases, like patients and/or their relatives, third parties shall be allowed to see records (e.g.; medical records) only after a documented procedure has been adhered to
- In case of breakdown of software system, keeping records in registers shall use manual system. These data shall be updated in software as soon as software starts functioning.
- The departmental head shall mention corrective actions during faulty use by unauthorized personnel and the same shall be documented.

B. Information Needs of the Hospital

The information needs of the hospital both internal and external are summarized as given below.

Type	Agency / Authority	Information Requirements
Internal	Hospital Administration	- Service Utilization - Billing Details - Patient Information - Employee / HR Information - Utilities and Other Consumption Reports - Incidents and Risk Related Information
External		- Budgets - Service Utilization - Revenue
External- Statutory	- IT Dept - Sales Tax Dept - PCB - AERB - Municipality - Police - Health Department	- Reportable information on revenue, sales, utilization etc - Birth and Deaths - MLC / RTA cases - Notifiable Disease
External – Regulatory Body		- Service Utilization - Patient Information - Employee / HR Information
External – Others	- Insurance - Corporate / Employers	- Billing Details - Patient Information

All information and data that are required to be contributed to external databases shall be maintained and communicated to appropriate authorities. This includes, sending birth and death statistics and notifiable diseases.

Policy on Information Needs of Hospital

Procedures for Information Management

- MRD and IT Manuals are established
- Hospital manual covers relevant policies
- IT Dept maintains a HMS user manual provided by the vendor

Reporting to Health Authorities

This is the responsibility of the department to submit the following Diagnostic Reports to Health Agencies like D.H.S, CMO and other departments under the ambit of Health & Family welfare department, Government of Delhi.

- Intimation of Malaria and Dengue Fever cases to the DMO.
- All Communicable Diseases to the D.H.S
- Notifiable diseases are reported immediately to control room to Chief Medical Officer

Policy on Information Needs of Hospital

S No	Process	Details
1	Statistics	a) Compiling daily hospital census and reporting to authorized personnel. b) Updating statistics of all OP and IP census to monthly statistics
2	Discharge Summary	a) Collecting discharge files from all the wings. b) Discharge summary prints provided as requested by Doctors / Nurses.
3	Maintenance of medical records	a) Systematic maintenance of records. b) Check deficiencies in the records and ensure proper assembling and filing according to MRN. c) Coding as per ICD norms / Indexing in the system. d) Scanning all the IP files, MLC forms, outside lab reports, etc into the patient record. e) Modification of personal particulars.
4	Birth and certificates death	a) Sending Birth and Death reports to the corporation. b) Birth and Death Register Updating
5	MLC	a) Maintaining hospital copy of all MLC intimations. b) Handing over wound certificate to the Police.
6	Retention of records	a) Retention of records as per hospital policy.
7	Training	a) EMRD training for New doctors and new employees
8	Others	a) Issue medical records to authorized personnel for audits/ research purposes. b) Issue certificates to external agencies / authorities as required.

PROCESS SUMMARY

Policy on Information Needs of Hospital

Reference:

IMS 1

AMENDMENT RECORD

AMENDMENT		DETAILS OF AMENDMENT	ISSUE STATUS	REV. STATUS
NO	DATE			