KRM Ayurveda Pvt. Ltd.

77 Tarun Enclave, Parwana Road, Pitam Pura, Delhi, Delhi 110034

SERVICE NAME :	**SOP OF MRD**
DATE CREATED :	**17/11/2022**
APPROVED BY :	**Dr. Jyoti Sadasivan**
REVIEWED BY :	**Dr. Monika Yadav**

1. Definitions

a) **Security**: 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.

d) **Information 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) **KRM Ayurveda Pvt. Ltd. Confidentiality Statement**: A signed statement that verifies the individual understands of confidentiality standards and the implications for inappropriate access or disclosure of confidential information.

2. Policy

a) **Awareness and Responsibility**

i. KRM Ayurveda Pvt. Ltd. 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 KRM Ayurveda Pvt. Ltd. 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.

iii. All non-compensated observers, students, vendors, or other persons conducting business with KRM Ayurveda Pvt. Ltd. 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 KRM Ayurveda Pvt. Ltd. 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. KRM Ayurveda Pvt. Ltd. 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 KRM Ayurveda Pvt. Ltd. Authorities, constitutes illegal activity and the person(s) involved are subject to enforceable penalties.

iii. Access methods to KRM Ayurveda Pvt. Ltd. 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 KRM Ayurveda Pvt. Ltd. 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 KRM Ayurveda Pvt. Ltd. To insure that confidentiality, integrity and security is optimally maintained.

vi. Access to information from KRM Ayurveda Pvt. Ltd. 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.

viii. Appropriate sign off procedures must be utilized with computerized systems.

ix. 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

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.

ix. Opd File retention -3yrs

x. Ipd File retention -7yrs

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 KRM Ayurveda Pvt. Ltd. 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.

v. After a certain time period when we have to discard our records, they will be discarded by whatever employees we have who are our trusted employees. Paper seeder machine will be used to get discarded and that employee will make a complete check list of whatever records he discards and provide us.

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.

d) 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.

e) 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.

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 KRM Ayurveda Pvt. Ltd. computer equipment or electronic devices is erased and not recoverable, including laptops and Personal Digital Assistants (PDA's) provided by KRM Ayurveda Pvt. Ltd. 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.