



## INODAYA Hospitals - Kakinada

Documentation code:  
INH/IMS.Doc.No:07

### Policy on Security, Confidentiality And Integrity of Information

Prepared date: 05/09/2023

Reference: IMS.5. a. NABH Standards – 5<sup>th</sup> Edition

Issue Date:05/09/2023

Issue no: 02

Review No: 1

Review date: 04/09/2024

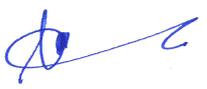
#### 1.0 Purpose:

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.

#### 2.0 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.

Page 1 of 13

Prepared by: 	Verified by: 	Approved by: 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director



## INODAYA Hospitals - Kakinada

Documentation code:  
INH/IMS.Doc.No:07

### Policy on Security, Confidentiality And Integrity of Information

Prepared date: 05/09/2023

Reference: IMS.5. a. NABH Standards – 5<sup>th</sup> Edition

Issue Date:05/09/2023

Issue no: 02

Review No: 1

Review date: 04/09/2024

- 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 ensure that it can be identified by its author. Unauthorized alteration is prohibited to ensure that data and or information is verifiable.

### 3.0 Policy:

#### A. Awareness and Responsibility:

1. Inodaya Hospitals, Kakinada employees shall receive information regarding the facilities standards for appropriate handling of patient and other information in Orientation.
2. 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.
3. All non-compensated observers, students, vendors, or other persons conducting business with Inodaya Hospitals, Kakinada shall receive specific instructions on the principles of appropriately processing information received or observed within the institution.

Page 2 of 13

Prepared by:	Verified by:	Approved by:
		
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director

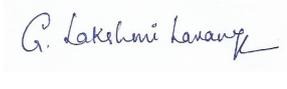
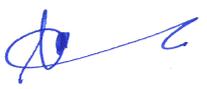
	<b>INODAYA Hospitals - Kakinada</b>		Documentation code: INH/IMS.Doc.No:07
	<b>Policy on Security, Confidentiality And Integrity of Information</b>		Prepared date: 05/09/2023
	Reference: IMS.5. a. NABH Standards – 5 <sup>th</sup> Edition		Issue Date:05/09/2023
	Issue no: 02	Review No: 1	Review date: 04/09/2024

4. 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.
5. Employees who leave the organization must obtain clearance from Information Technology Department who will delete system access.
6. Department/Area supervisors shall notify Information Technology Department when access rights of individuals are to be terminated following involuntary separation or reassignment.

**B. Access to Information:**

1. Inodaya Hospitals, Kakinada shall have a Communications Committee that shall determine and approve the retrieval systems and information that shall be accessible to authorized staff, and other third party business associates.
2. Access to confidential information is given by written authorization and approval. Access to information or systems without the consent of appropriate authorities, constitutes illegal activity and the person(s) involved are subject to enforceable penalties.
3. Passwords or access methods to view/retrieve 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

Page 3 of 13

Prepared by: 	Verified by: 	Approved by: 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director

	<b>INODAYA Hospitals - Kakinada</b>		Documentation code: INH/IMS.Doc.No:07
	<b>Policy on Security, Confidentiality And Integrity of Information</b>		Prepared date: 05/09/2023
	Reference: IMS.5. a. NABH Standards – 5 <sup>th</sup> Edition		Issue Date:05/09/2023
	Issue no: 02	Review No: 1	Review date: 04/09/2024

revealed or made available to anyone without the permission of appropriate authorities.

4. 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.
5. 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 Inodaya Hospitals, Kakinada to insure that confidentiality, integrity and security is optimally maintained.
6. Access to information from Inodaya Hospitals, Kakinada systems is limited to defined personnel classifications, as appropriate. Modifications to these defined levels must be obtained from the Communications Committee and submitted in writing to Information Technology Department.
7. 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.
8. 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.

Page 4 of 13

Prepared by: 	Verified by: 	Approved by: 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director

	<b>INODAYA Hospitals - Kakinada</b>		Documentation code: INH/IMS.Doc.No:07
	<b>Policy on Security, Confidentiality And Integrity of Information</b>		Prepared date: 05/09/2023
	Reference: IMS.5. a. NABH Standards – 5 <sup>th</sup> Edition		Issue Date:05/09/2023
	Issue no: 02	Review No: 1	Review date: 04/09/2024

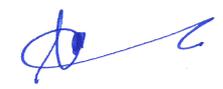
**C. Access to Medical Records**

- a) Access to Medical records within the Medical Records Department shall be restricted to certain staff identified by the In – Charge of the department.
- b) The physician, nurse, dietician, physiotherapist, medical social worker, executive, front office administrative staff, medical record personnel shall be the authorized members to make entries in the patient records.
- c) A copy of the Medical Record shall be provided to the patient/ Family Members/Insurance Companies only when an authorization letter is duly signed by the Deputy Medical superintendent

**D. Securing Data:**

**1. Manual Systems:**

- a) Requests for health record information shall be made available only to those employees, medical staff members, support staff, etc. displaying their identification badges.

Prepared by: 	Verified by: 	Approved by: 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director

	<b>INODAYA Hospitals - Kakinada</b>		Documentation code: INH/IMS.Doc.No:07
	<b>Policy on Security, Confidentiality And Integrity of Information</b>		Prepared date: 05/09/2023
	Reference: IMS.5. a. NABH Standards – 5 <sup>th</sup> Edition		Issue Date:05/09/2023
	Issue no: 02	Review No: 1	Review date: 04/09/2024

- b) The primary medical record and any secondary records (diagnosis and procedure cross indexes, etc) are stored in areas directly controlled and monitored by the Medical Records Department.
- c) 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
- d) Medical records are transported to patient care areas and administrative offices via the housekeeping staff. All staff transporting medical records must ensure the privacy of patient-identifiable information during the transport process. Medical records and/or carts loaded with medical records shall not be left unattended during the transport process.
- e) Records are maintained in the MRD in locked rooms that are not accessible by unauthorized individuals.
- f) Telephone request for patient-identifiable information are discouraged and limited to emergency situations.
- g) 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.

<b>Prepared by:</b> 	<b>Verified by:</b> 	<b>Approved by:</b> 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director

	<b>INODAYA Hospitals - Kakinada</b>		Documentation code: INH/IMS.Doc.No:07
	<b>Policy on Security, Confidentiality And Integrity of Information</b>		Prepared date: 05/09/2023
	Reference: IMS.5. a. NABH Standards – 5 <sup>th</sup> Edition		Issue Date:05/09/2023
	Issue no: 02	Review No: 1	Review date: 04/09/2024

h) The original medical record shall not be removed from the hospital premises except upon receipt of court order or state statute.

## 2. Automated systems:

- a) 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.
- b) Appropriate safeguards shall be defined when remote access is granted to authorize parties. These connections to authorized computer systems shall be routed through devices that require password verification.
- c) Data control and production areas shall be accessible only through a secured entrance by authorized personnel. Unauthorized personnel must be accompanied by authorized personnel.
- d) Storage media that is identified as confidential or sensitive information shall be labeled as “CONFIDENTIAL” and stored in areas that are restricted only authorized personnel. Prior to discarding any CONFIDENTIAL storage media, the information shall be rendered unusable.

Page 7 of 13

Prepared by: 	Verified by: 	Approved by: 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director

	<b>INODAYA Hospitals - Kakinada</b>		Documentation code: INH/IMS.Doc.No:07
	<b>Policy on Security, Confidentiality And Integrity of Information</b>		Prepared date: 05/09/2023
	Reference: IMS.5. a. NABH Standards – 5 <sup>th</sup> Edition		Issue Date:05/09/2023
	Issue no: 02	Review No: 1	Review date: 04/09/2024

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

**E. 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.

**F. Violations of Confidentiality of Information:**

1. 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.
2. Security violations are defined as follows:
  - a. Failure to sign off from the access terminal prior to leaving the terminal.
  - b. Accessing his/her own patient record.
  - c. Utilizing another user's sign on or password.
  - d. Accessing confidential information without a legitimate reason.

Prepared by: 	Verified by: 	Approved by: 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director



## INODAYA Hospitals - Kakinada

Documentation code:  
INH/IMS.Doc.No:07

### Policy on Security, Confidentiality And Integrity of Information

Prepared date: 05/09/2023

Reference: IMS.5. a. NABH Standards – 5<sup>th</sup> Edition

Issue Date:05/09/2023

Issue no: 02

Review No: 1

Review date: 04/09/2024

- e. Attempting to and/or circumventing security systems.
  - f. Disclosure of confidential information.
  - g. Disclosure of user password or sign on.
  - h. Unauthorized entry, correction, amendments or change to existing data.
3. An individual's access rights may be suspended immediately upon the discovery of a possible violation of this policy.
  4. Violation of this policy may result in disciplinary action up to and including termination.

#### G. Changes in Access Rights:

1. 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.
2. Access rights may be suspended if an individual is under investigation for cause.

#### H. Data Access Levels:

1. Each budget unit, department head, operational division, supervisor or designee shall be responsible for defining the levels within the guidelines established by their administrative head.

Page 9 of 13

Prepared by: 	Verified by: 	Approved by: 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director

	<b>INODAYA Hospitals - Kakinada</b>		Documentation code: INH/IMS.Doc.No:07
	<b>Policy on Security, Confidentiality And Integrity of Information</b>		Prepared date: 05/09/2023
	Reference: IMS.5. a. NABH Standards – 5 <sup>th</sup> Edition		Issue Date:05/09/2023
	Issue no: 02	Review No: 1	Review date: 04/09/2024

2. Each budget unit, department head, operational division, supervisor or designee within each defined area shall submit a formal request to the system management office for access for an individual.
3. The defined access levels of the clinical system are as follows:
  - a. Patient general information – information contained in the patient master index to include patient name, location, age, sex, address and telephone number, admitting complaint, attending physician, medical record number and account number.
  - b. Patient financial information – information relating to patient financial disclosure, patient insurance plans, and patient guarantor.
  - c. Physician order request – transcribing from a paper system to the electronic system and transmission of the request to the orderable service department.
  - d. Physician order view/status – view of the electronic or paper system physician orders limited to ancillary services, patient specific unit requesting services, utilization review, and medical Staff responsible for the care of the patient.
  - e. Technical charge data entry/view-data entry of procedural charge item codes and view of the entries made by the originating department.

<b>Prepared by:</b> 	<b>Verified by:</b> 	<b>Approved by:</b> 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director



## INODAYA Hospitals - Kakinada

Documentation code:  
INH/IMS.Doc.No:07

### Policy on Security, Confidentiality And Integrity of Information

Prepared date: 05/09/2023

Reference: IMS.5. a. NABH Standards – 5<sup>th</sup> Edition

Issue Date:05/09/2023

Issue no: 02

Review No: 1

Review date: 04/09/2024

- f. Patient Appointment System – Scheduling, viewing or amending the patient appointments within the computerized appointment system.
- g. Medical Records – information, data entry as related to medical record tracking, chart deficiency and transcription.
- f. Radiology and clinical laboratory results – view of results reporting of procedures performed as relevant to the systems.

#### TRANSMISSION OF INTERNAL AND EXTERNAL DATA/INFORMATION:

- The format and method for disseminating data/information are standardized to facilitate transmission of data/information in a timely and accurate manner, whenever possible.

#### AGGREGATED DATA:

- Monthly statistical report
- Fiscal year Analysis by Hospital Service
- Daily Collection report from In Patient and Out patient
- Comparative Report of Professional Performance
- Performance report

Page 11 of 13

Prepared by: 	Verified by: 	Approved by: 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director

	<b>INODAYA Hospitals - Kakinada</b>		Documentation code: INH/IMS.Doc.No:07
	<b>Policy on Security, Confidentiality And Integrity of Information</b>		Prepared date: 05/09/2023
	Reference: IMS.5. a. NABH Standards – 5 <sup>th</sup> Edition		Issue Date:05/09/2023
	Issue no: 02	Review No: 1	Review date: 04/09/2024

**COMPARATIVE DATA:**

**Performed Improvement**-Performance improvement is defined by the following

- Timeliness of products and services
- Commitment and dedication to continuous improvement.
- Reduction of costs and services
- Customer service.

**TRACER CARD:**

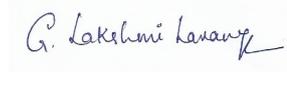
Tracer Card provides an important means of control over record usage. They are used to replace a folder that has been removed from the filing area. This card remains in the filing until the borrowed folder is returned and refilled. If there is a system failure, this card will be useful for finding out the location of the medical record. This card contains UHID No, Name of the consultant to whom the record issued, date of issue.

**RECORD RETENTION:**

Prepared by: 	Verified by: 	Approved by: 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director

	<b>INODAYA Hospitals - Kakinada</b>		Documentation code: INH/IMS.Doc.No:07
	<b>Policy on Security, Confidentiality And Integrity of Information</b>		Prepared date: 05/09/2023
	Reference: IMS.5. a. NABH Standards – 5 <sup>th</sup> Edition		Issue Date:05/09/2023
	Issue no: 02	Review No: 1	Review date: 04/09/2024

During the retention period Medical Records Department shall be custodian of Medical Records. The Medical Record shall be readily accessible for providing continuing patient care by medical and other staff, and permit retrieval of information for medical education, research, quality assurance activities, and statistical data.

Prepared by: 	Verified by: 	Approved by: 
Dr.D.N.S.Prakash	Ms.Lakshmi Lavanya	Dr.G.Rammohan
Medical Director	Accreditation Coordinator	Managing Director