# Yatharth Hospital & Trauma Care Services Limited

## Data Privacy and Security Policy

### 1. Purpose

This policy aims to ensure the protection of sensitive patient and healthcare data in compliance with Indian laws, such as the Information Technology Act, 2000 (IT Act) and any applicable sectoral regulations.

### 2. Scope

This policy applies to:

• All the employees, contractors, and third-party vendors.

• All patient-related data, including electronic medical records (EMRs), diagnostic results, and personal identifiable information.

• All systems and platforms used to store, process, or transmit healthcare data.(Including – Hospital Management System HMS)

### 3. Definitions

- Sensitive Personal Data (SPD): As defined by the IT Act, includes health records, financial data, and biometric data.
- Data Principal: The individual whose data is being collected (e.g., patient).
- Data Breach: Unauthorized access, loss, or misuse of sensitive personal data.

### 4. Principles of Data Privacy

4.1 Data Collection and Consent

- Patient data must only be collected for lawful purposes, such as diagnosis, treatment, or research.
- Patients must be informed of the purpose of data collection and provide explicit consent.
- Consent must be documented in a verifiable manner.

4.2 Data Minimization

- Only collect data necessary for the intended purpose.
- Avoid over-collection or unnecessary retention of data.

4.3 Patient Rights: Patients have the right to:

- Access to their medical records.
- Request corrections or deletions of inaccurate or outdated data.
- Withdraw consent for non-essential data processing.

## 5. Data Security Measures

### 5.1 Access Controls

- ❖ Implement role-based access to healthcare data.
- ❖ Require unique user IDs for access.

### 5.2 Encryption

- ❖ Encrypt sensitive data at rest and in transit using secure encryption protocols.

### 5.3 Network and System Security

- ❖ Use firewalls, intrusion detection systems (IDS), and regular security patches.
- ❖ Restrict access to systems through Virtual Private Networks (VPNs) or secure channels.

### 5.4 Device Security

- ❖ Only approved devices may access HMS systems.
- ❖ Implement remote wipe capabilities for lost or stolen devices.

## 6. Data Retention and Disposal

- Retain medical records as per the Clinical Establishments (Central Government) Rules, 2012, or other applicable guidelines.
- Securely destroy data when it is no longer required using shredding or electronic data wiping.

## 7. Breach Management and Reporting

### 7.1 Incident Response

- Report data breaches within 72 hours to the designated officer and regulatory authorities.
- Notify affected individuals if their data is compromised.

### 7.2 Investigation and Remediation

- Conduct a root-cause analysis of breaches.
- Implement corrective measures to prevent recurrence.

## 8. Third-Party Data Processors

- Ensure all third-party vendors comply with this policy and execute Data Processing Agreements.
- Perform regular audits of vendors' data security practices.

9. Legal and Regulatory Compliance

- Adhere to applicable Indian laws and standards, including:
- Information Technology Act, 2000 and its amendments.
- Personal Data Protection Bill (PDP), 2019.
- Guidelines from the Ministry of Health & Family Welfare (MoHFW).

10. Training and Awareness

- Conduct regular employee training on data privacy and security policies.
- Provide updates on new regulations and emerging threats.

11. Policy Enforcement

- Non-compliance with this policy will result in disciplinary action, which may include termination or legal consequences.

12. Policy Review

# This policy will be reviewed annually or as necessary to reflect changes in regulations or operational requirements.