APPENDIX [C]

This document is part of the Data Processing Agreement (DPA) and needs to be submitted when requested.

TECHNICAL AND ORGANIZATIONAL MEASURES

The following technical and organizational measures must be implemented by the Data Processor in order to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or, or access to Personal Data transmitted, stored, or otherwise processed

S.No.	Category	Control Description	Implemented? (Yes/No/Partially)	Timeline for implementing (in case of Partially/No) in months
1		Assign access rights to the personal information processing system to the minimum extent necessary based on job roles.		
2		Cancel access rights immediately upon personnel changes (e.g., transfers, retirements).		
3		Record authorizations, alterations, or cancellations and retain records for at least 8 years.		
4	**Management of Authorization**	Issue unique user accounts for each personal information handler, prohibiting account sharing.		
5		Apply password creation rules: passwords must be at least 8 digits (3 combinations of uppercase/lowercase, numbers, special characters) or 10 digits (2+ combinations), changed every 3 months, and difficult to guess.		
6		Restrict system access after multiple incorrect passwords attempts to ensure only authorized handlers access the system.		

7	**Access Control**	Restrict system access to specific IP addresses to prevent unauthorized access.		
8		Analyze connected IP addresses to detect illegal personal information leakage.		
9		Use secure connection methods (e.g., VPN) or authentication when accessing the system via external networks (e.g., internet).		
10		Apply access controls to systems, business computers, and mobile devices to prevent unauthorized disclosure via internet, P2P, or sharing settings.		
11		Automatically stop system access after a period of inactivity by the handler.		
	Encryption of Personal Information			
12		Encrypt unique identification information (e.g., Aadhaar, PAN), passwords, bio information, credit card numbers, and bank account numbers during transmission or on auxiliary storage media.		
13		Encrypt unique identification information, passwords (one-way encryption), bio information, credit card numbers, and bank account numbers when stored in databases.		
14		Use secure encryption algorithms for all encrypted personal information.		
15		Establish and enforce procedures for secure cryptographic key creation, use, storage, distribution, and destruction.		
16		Encrypt unique identification information stored on business computers or mobile devices using commercial encryption software or secure algorithms.		
17		Log and regularly review system administrator and		

	Logging of System Administrator	operator activities, protecting logs from tampering and unauthorized access.		
	Prevention from Malicious Programs			
18		Install and maintain updated security programs (e.g., antivirus, PC vaccine software) to prevent and treat malicious programs.		
19		Immediately apply security updates or patches for applications and operating systems upon malware alerts or manufacturer notices.		
	Safety Measures for Management Workstation			
20		Prevent unauthorized access or arbitrary operations on management workstations.		
21		Use management workstations solely for their intended purpose.		
	Physical Security Measures			
22		Establish and operate access control procedures for physical storage areas (e.g., computer rooms, data storage rooms) holding personal information.		
23		Store documents and auxiliary storage media containing personal information in locked, secure locations.		
	Disaster Recovery Plan			
24		Prepare and periodically review a crisis response manual for protecting the personal information processing system during disasters (e.g., fire, flood, blackout).		
	Destruction of Personal Information			
25		Irreparably destroy personal information after the retention period or business purpose ends, issuing a Data Destruction Certificate to the Hospital.		
26		Destroy data using methods like database initialization, overwriting, complete destruction (e.g., incineration,		

		crushing), or dedicated device equipment.		
	Segregation Control			
27		Avoid using operational data with personally identifiable or confidential information for testing purposes.		
28		Protect sensitive details in testing data by removal or modification if such data is used.		
	Information Security Incident Management			
29		Report information security events to the Hospital as quickly as possible.		
30		Ensure all employees are aware of the procedure and contact point for reporting security events.		

These sections will be duly filled by Data Processors:

For data transferred to Data Sub-Processors, what specific technical and organizational measures are taken by the Data Sub-Processor to protect the data shared by Data Fiduciary:

Specific measures and/or guarantees applicable to the processing of Special Categories of Personal Data (where applicable):
