manipalhospitals
LIFE'S ON

MANIPAL HEALTH ENTERPRISES LTD

DPDP - Do' s and Don'ts Guideline Document

DPDP Do's and Don'ts Guidelines

Obligations of the vendor w.r.t Digital Personal Data Protection Act (DPDPA), 2023

The guidelines mentioned below outline the basic data protection practices that all vendors must follow while handling or accessing patient information. They are designed to ensure compliance with the Digital Personal Data Protection Act (DPDPA), 2023, and to safeguard the confidentiality, integrity, and security of patient data. All vendors are expected to adhere strictly to these Do's and Don'ts throughout their engagement with Manipal Hospitals Enterprise Limited (Manipal Hospitals')

Do's: Actions to Protect Personal Data of Data Principal

a. Process Personal Data strictly in accordance with Manipal Hospitals' instructions, ensuring only the minimum necessary information (e.g., name, ID) is collected
b. Ensure the security of invoice data during both storage (e.g., on computers, cloud platforms) and transmission (e.g., via email).
c. Use strong passwords with a minimum of 11 characters, incorporating uppercase and lowercase letters, numbers, and special characters.
d. Use only licensed software (e.g., Tally, Windows) and licensed antivirus programs (e.g., Norton), ensuring they are regularly updated
e. Conduct annual staff training on DPDPA compliance, cybersecurity, and licensed software usage, and maintain proper documentation of all training sessions.
f. Obtain prior written approval from Manipal Hospitals before engaging any sub-processors, ensuring their full compliance with DPDPA requirements.
g. Respond to any requests for modification, deletion, or erasure of personal data within 30 days, and confirm compliance to Manipal Hospitals in writing, by maintaining records of such actions, and provide reports upon request.
h. In the event of a Data Breach, notify Manipal Hospitals within 48 hours, implement necessary corrective actions, assist with any required notifications, and maintain documentation of all measures taken.
i. Retain Personal Data only for the legally required duration (e.g., 7 years for tax or applicable medical laws), and securely dispose of it (e.g., shredding paper records, overwriting digital files) once no longer needed, maintaining appropriate logs of deletion activities.

Don’ts: Actions to Avoid Privacy and Security Risks

a. Don’t use Personal Data for unauthorized purposes (e.g., marketing) or sharing with third parties.
b. Don’t process Personal Data without confirming Manipal Hospitals consent.
c. Don’t withhold processing details or ignore patient requests forwarded by Manipal Hospitals.
d. Don’t retain Personal Data longer than required or in unsecured systems (e.g., unencrypted drives).
e. Don’t store or transmit Personal Data without encryption or use unsecured Wi-Fi.
f. Don’t use unlicensed software/antivirus, pirated tools, or unverified apps.
g. Don’t allow untrained staff to handle Personal Data or skip training on DPDPA, security, or software licensing.
h. Don’t delay reporting Data Breaches or attempt to resolve them independently.
i. Don’t use unapproved tools (e.g., personal cloud accounts) or unsecured personal devices.
j. Don’t leave invoices or devices unsecured or dispose of them without shredding.