PROTECTION AND PROCESSING OF PATIENT'S PERSONAL DATA

PERSONAL DATA PROTECTION PROCEDURE FOR PRODUCT OR SERVICE RECIPIENT ACCORDING TO THE LAW ON THE PROTECTION OF PERSONAL DATA NOVA DENTAL AND MEDICAL SERVICES LIMITED COMPANY

1 - PURPOSE:
To ensure the protection of customers' personal data and sensitive personal data during the provision of services.

2 - SCOPE:
This procedure covers all customers who apply to our company or receive products or services from our company.

3 - DEFINITIONS:

3.1 Data Subject: The real person whose personal data is processed.
3.2 Personal Data: Any information relating to an identified or identifiable natural person.
3.3 Sensitive Personal Data: Data relating to individuals' race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and clothing, membership of associations, foundations or trade unions, health data, sexual life, criminal conviction and security measures, as well as biometric and genetic data.
3.4 Data Processor: The real or legal person who processes personal data on behalf of the data controller based on the authority given by the data controller.
3.5 Product or Service Recipient: Customer/Patient

4 - RESPONSIBILITY:
All personnel working within the company are responsible.

5 - ACTIVITY FLOW:

5.1 It is essential to protect the security of personal data during storage and internal sharing. The customer may explicitly request the secure storage of their personal data.

5.2 The internal sharing of personal data among individuals or departments within the institution for purposes other than intended use is not permitted.

5.3 Customers’ personal data must not be stored on employees' personal phones, computers, or other electronic devices. Such data must not be shared or disclosed via personal devices, external email addresses, or social media platforms.

5.4 Unless the customer explicitly consents, personal data must not be shared with any of the customer's relatives. In cases where legal obligations apply, such data may only be shared with the approval of the department manager.

5.5 During information transfer between personnel, care must be taken to protect the confidentiality of the customer's personal data.

5.6 Printed forms, files, folders, and notebooks containing personal data must not be left in public view on desks, cabinets, etc. These materials must be stored in a way that only relevant personnel have access.

5.7 Customer registration areas and desks where forms containing personal data are filled must be arranged so that no one other than the customer can hear or see the information being shared.

5.8 All personnel using automation systems, software, portals, and websites are assigned personal access credentials. These usernames and passwords approved by the unit supervisor must not be shared with others. Personnel must not request the credentials of another employee.

5.9 Customers' personal data must not be taken out of the institution unless required by legal obligations.

5.10 In the event of a breach of personal data, the institution will initiate the necessary legal proceedings.