**Information Security Policy Plan**

TB Patient’s Appointnment System

**Prepared by:**

Keyan Andy Delgado

**Introduction**

The TB Patient Appointment System (TPAS) is a web-based system for clinics that helps you managing your TB treatment. It allows you to schedule appointments, view medical records, and communicate with your healthcare team. However, this system also stores sensitive health information about you, such as your name, contact details, medications, and treatment progress.

We understand the importance of protecting your privacy. By using TPAS, you'll be entering into an agreement with your healthcare provider. This agreement outlines how both parties will work together to safeguard your confidential health information.

Here's what the agreement protects:

Your personal information: This includes your name, address, phone number, and email address.

Your medical history: This encompasses details about your TB diagnosis, medications, and treatment progress.

Your communication with your healthcare team: This includes messages exchanged through TPAS between you and your doctor, nurse, or other healthcare professionals.

We take data security seriously and implement strong measures to secure your information. This includes encryption techniques, access controls that limit who can see your data, and regular backups to ensure data availability.

**Responsibilities**

These are the following roles of each users of the system:

* **Patients** – The one who schedules clinic appointments correctly and on time, follows their treatment plan diligently, communicates actively with their healthcare team through the system, and keeps their personal and medical information secure.
* **Doctors** – The one who manages clinic appointments, monitors patient progress, communicates promptly with patients for inquiries and advice, and ensures the security of patient data within the system.
* **System Administrator** - the one who maintains the system's operation, provides technical support to users, safeguards patient data, and conducts training sessions to help users understand the system and protect data effectively. Additionally, the System Administrator is the only one who can create accounts for doctors within the system.

**Information Classification**

Classifying information is a must on our system. However, we will only classify information which allows us to finish the tasks given to us. Accessing personal data will only be allowed when it is needed for processing. We classify information into different categories so that the information will be protected, and will only be usable whenever it is needed.

* **Public Information (Unclassified)** – Information that is publicly available and does not require protection. This includes general system information and non-sensitive data.
* **Patient Confidentiality (Sensitive)** – Information related to patients' personal health information, medical history, diagnoses, treatments, and communications with healthcare providers. Access to this information is restricted to authorized healthcare personnel for patient care purposes.
* **Level 3: Healthcare Staff Confidentiality (Restricted) -** Information concerning healthcare professionals, their roles, responsibilities, and ethical obligations regarding patient confidentiality and data security. This category includes staff schedules, contact details, and internal communications. Access is limited to authorized staff members for operational purposes.

We have categorized the information we keep as follows:

|  |  |  |
| --- | --- | --- |
| **Type of Information** | **System Involved** | **Classification Level** |
| Patient Data | Patient | Sensitive |
| Appointment History | Patient | Sensitive |
| Website Content | TPAS | Unclassified |
| System Logs | Admin | Restricted |
| Doctor-Patient Chat Transcripts | Patient/Doctor | Sensitive |
| Doctor Schedules | Patient/Doctor/Admin | Unclassified or Sensitive |

Accidental dissemination of confidential information could cause great harm to patients and the organization, leading to privacy violations, legal repercussions, and loss of trust.. The main purpose of this policy is to reduce, or if possible, avoid those incidents.

**Patient Data** - related to a patient's health, treatment, and medical history.

**Appointment History** – Records of past and upcoming appointments for a patient.

**Website Content** – Information available on a website.

**System Logs** – Records of system activities and events.

**Doctor-Patient Chat Transcripts** – Conversations between a patient and a doctor, containing medical discussions.

**Doctor Schedules** - Timetables detailing a doctor's availability for appointments and consultations.

Central Server

Patient

Admin

Doctor

**TOPOLOGY**

* Star – A system require a network to centralize all the transaction.

**NETWORK SECURITY POLICY**

* Firewall
* Passwords
* System Logs

**SECURITY MEASURE FOR LOGIN**

* Strong Password
* Limited Login Attempts

**ROLE-BASED ACCESS CONTROL (RBAC)**

* Distinct User Roles
* Granular Access Controls

**TWO-FACTOR AUTHENTICATION (2FA)**

* Additional Verification

**PASSWORD HASHING**

* Irreversible Encryption of Passwords

**DATA CLASSIFICATION**

|  |  |  |  |
| --- | --- | --- | --- |
| **TOP SECRET** | **SECRET** | **CONFIDENTIAL** | **PUBLIC** |
| Admin Account | Patient Account | Patient Appointment History | Appointment Availability |
|  | Doctor Account | Chat transcripts between patients and doctors |  |
|  | History Log |  |  |

**Data Support Regulations**

|  |  |
| --- | --- |
| Systems Manager | Data Account |
|  | System Logs |
|  | Admin Account |
| Administrator | Admin logs / Reports |
|  | Appointment History |
|  |  |

* Firewall – Firewall with secure port locking for block unwanted access
* Passwords – account password recording using MD5 decoding or hash tables
* System logs – Monitoring employee logins, out and transsactions

**Encryption Policy**

The Encryption Policy for the TB Patients Appointment System establishes guidelines to secure system access and outlines procedures for interactions between healthcare providers and patients within the system.

**Data and Backup Policy**

* Essential data to be backed up includes patient appointment records, medical histories, treatment plans, and communications.
* Healthcare providers (admin) perform regular manual backups at specified intervals, ensuring data integrity and availability.
* Backup data is securely stored and accessible only to authorized healthcare providers.

The Responsibilities, Rights, and Duties of Personnel section delineates the roles and responsibilities of healthcare providers (admin) and patients within the TB Patients Appointment System.

* Healthcare providers (admin) are responsible for managing patient appointments, maintaining accurate medical records, and ensuring data security within the system.
* Only authorized healthcare providers (admin) have access to all system functions.
* Patients are required to provide accurate identification credentials to healthcare providers for appointment scheduling and management.