**Information Security Policy Plan**

TB Patient’s Appointment 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.

* **Unclassified** – Information that is publicly available and does not require protection. This includes general system information and non-sensitive data.
* **Patient Confidentiality** – 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.
* **Healthcare Staff Confidentiality -** 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 | Patient Confidential |
| Appointment History | Patient | Patient Confidential |
| Website Content | TPAS | Unclassified |
| System Logs | Admin | Healthcare Staff Confidentiality |
| Doctor-Patient Chat Transcripts | Patient/Doctor | Patient Confidentiality |
| Doctor Schedules | Patient/Doctor/Admin | Patient Confidentiality |

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.

System Administrator

Patient/User

Doctor

Patient/User

**TOPOLOGY**

* Client-Server Topology – In the Client-Server Topology adopted by TPAS, all user, including patients and other regular users, connect to a central server. This server serves as the focal point for managing and controlling exchange of information within the platform. The centralized nature of this architecture facilities efficient communication and coordination among various endpoints within the TPAS network.

**NETWORK SECURITY POLICY**

* Password Policy
* Role-Based Access Control
* 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**

* Passwords are encrypted irreversibly for heightened security.

**DATA CLASSIFICATION**

|  |  |  |  |
| --- | --- | --- | --- |
| **TOP SECRET** | **SECRET** | **CONFIDENTIAL** | **PUBLIC** |
| Driver Account | Patient/User Data | Patient Appointment History | Appointment Availability |
| Patient/Doctor Account | Doctor/User Data | Chat transcripts between patients and doctors |  |

**Data Support Regulations**

|  |  |
| --- | --- |
| Driver Account | Patient Appointment History |
|  | Chat transcripts between patients and doctors |
| Doctor Account | Doctor/User Data |
| Patient Account | Patient/User Data |
|  |  |
|  |  |

* **Password Policy -** The Password Policy in TPAS strengthens network security by mandating strong password practices, including complexity requirements and regular updates, to mitigate unauthorized access risks and safeguard patient information.
* **Role-Based Access Control -** Role-Based Access Control (RBAC) in TPAS restricts system access based on predefined roles, ensuring that users only have permissions relevant to their responsibilities. This minimizes the risk of unauthorized data access and enhances overall system security.
* **System Logs -** The System Logs policy in TPAS maintains detailed records of network activities for continuous monitoring and swift incident response. By tracking user actions and system events, it enables proactive threat detection, aids in compliance efforts, and enhances the overall security posture of the TPAS platform.

**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.

* **Administrator Responsibilities:** The admin runs the system and keeps everything organized. They make sure appointments are scheduled correctly and that patient information is kept safe. Only authorized admins can use all parts of the system.
* **Patient Responsibilities:** Patients need to give the right information to book appointments correctly. They should show their ID when needed. It's important to stick to appointment times and tell the doctor if plans change. Patients should follow the rules to keep their info safe.
* **Doctor Responsibilities:** Doctors manage appointments and give good care during visits. They keep accurate records of patient treatment. Working together with other healthcare pros helps give patients the best care.
* **Appointment Fulfillment:** Making appointments work well is a team effort. Admins keep things running smoothly, patients show up on time and share needed info, and doctors provide great care. Working together makes appointments go well and helps patients get better.