**Information Security Policy Plan**

TB Patient’s Appointment System

**Prepared by:**

Keyan Andy Delgado

**Introduction**

An efficient TB patient appointment system is essential for ensuring timely and consistent access to diagnosis and treatment services. By incorporating automated reminders, streamlined scheduling processes, and seamless integration with electronic health records, such a system can significantly enhance patient adherence, reduce missed appointments, and ultimately improve treatment outcomes for tuberculosis. Research has explored the potential of mobile health technologies and digital platforms to optimize TB appointment management, highlighting the importance of ongoing innovation and evaluation to tailor these systems to the diverse needs of healthcare settings and TB control programs. Patel, A.V., Brust, J.C.M., Loveday, M. et al. Patient-centered mobile tuberculosis treatment support tools (TB-TSTs) to improve adherence: a mixed-methods feasibility study. BMC Infect Dis 22, 522 (2022). <https://doi.org/10.1186/s12879-022-07508-4>.

The TB Patients Appointment System streamlines tuberculosis care with several efficient features. Patients can register and manage their profiles, allowing them to easily schedule, view, and modify appointments through a user-friendly interface. Automatic email reminders are sent as soon as appointments are booked, ensuring patients are reminded of their schedules. Additionally, the system includes robust security measures such as strong password policies, limited login attempts, system logs, access control, and session management with automatic logout to maintain security and privacy.

The TB Patients Appointment System is a perfect tool that helps in the management of tuberculosis treatment and care. Reminders, user-friendly scheduling, and rigorous security measures not only enable a patient to adhere to various appointments but help protect sensitive information. It has features to cater to the practical needs of both patients and healthcare providers. The system may be a very valuable commodity in the fight against tuberculosis. The continually evolving health technology landscape will necessitate the continual refinement and adaptation of such systems to result in healthier outcomes and more efficient care delivery across different healthcare settings.

**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 creates schedules, manages clinic appointments, manages user accounts, and monitors system logs, while also monitoring patient progress and responding promptly to inquiries and providing medical advice.
* **Assistant** – The one who supports administrative functions by helping with the scheduling and rescheduling of appointments, maintaining accurate patient records, facilitating communication between patients and healthcare providers, and assisting in the overall management of patient data to ensure its integrity and security.

**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 |
| System Logs | Admin | Healthcare Staff Confidentiality |
| Doctor Schedules | Patient/Doctor/Admin | Patient Confidentiality |

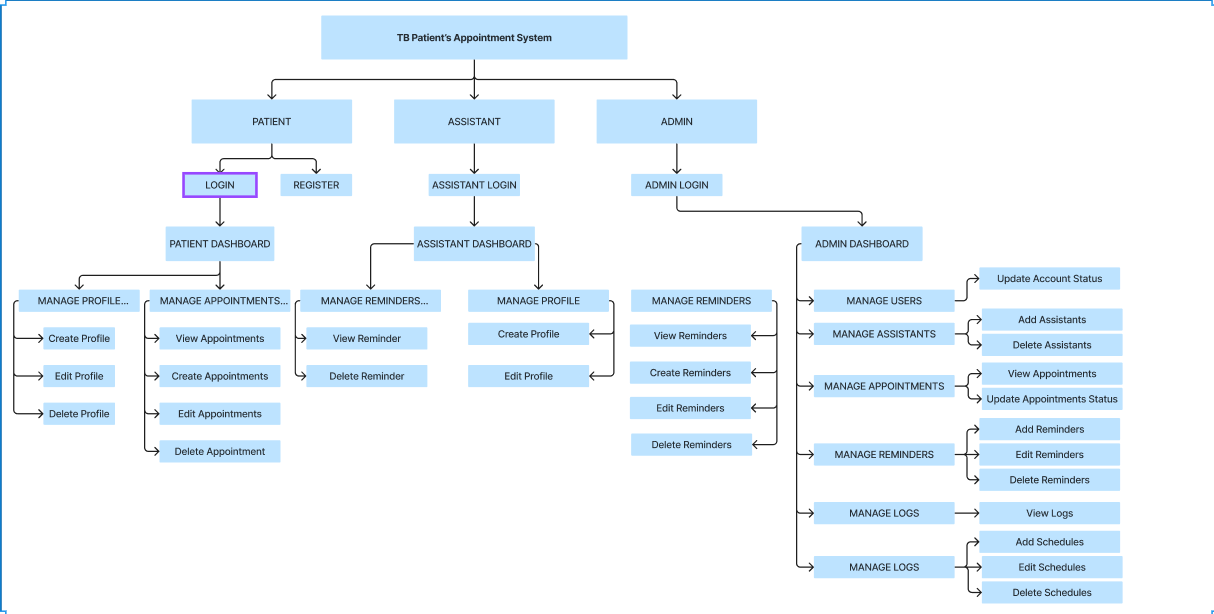
Accidental dissemination of confidential information could cause great harm to patients and the organization, leading to privacy violations, legal repercussions, and loss of trust.. The main purpose of this policy is to reduce, or if possible, avoid those incidents.

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

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

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

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



**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.

**SECURITY MEASURE FOR LOGIN**

* Password Validator
* Limited Login Attempts
* Anti-SQL Injection

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

* Admin Approval
* Logs

**SESSION MANAGEMENT**

* Auto-Logout

**Data Encryption**

* AES-256 Encryption

**DATA CLASSIFICATION**

|  |  |  |  |
| --- | --- | --- | --- |
| **TOP SECRET** | **SECRET** | **CONFIDENTIAL** | **PUBLIC** |
| Driver Account | Patient/User Data | Patient Appointment History | Appointment Availability |

**Data Support Regulations**

|  |  |
| --- | --- |
| Driver Account | Patient Appointment History |
| Doctor Account | Doctor/User Data |
| Patient Account | Patient/User Data |
|  |  |
|  |  |

* **Password Policy -** The Password Policy in the TPAS (TB Patients Appointment System) plays a crucial role in strengthening network security. This policy mandates the use of strong passwords that meet specific complexity requirements, including a mix of uppercase letters, lowercase letters, numbers, and special characters. Furthermore, it requires users to regularly update their passwords. These measures are designed to mitigate the risks of unauthorized access and help safeguard sensitive patient information.
* **Access Control Management:** Access control management policies are fundamental to regulating who can access certain data within an organization. Admin approval within this context acts as a gatekeeping mechanism that ensures all access to sensitive systems and data is granted based on strict necessity and through a controlled process. This type of policy is critical for preventing unauthorized access and ensuring that access rights are granted according to predefined roles and responsibilities.
* **Logging and Monitoring Policy:** The Logging and Monitoring Policy in the TPAS is essential for maintaining a secure and compliant healthcare environment. This policy requires the continuous logging and real-time monitoring of all system activities, including access events, system changes, and transactions. The logs capture detailed information, which aids in identifying, responding to, and mitigating security incidents promptly. Furthermore, these logs are used for forensic analysis, helping to trace how a security incident happened and determining the extent of any potential damage. Regular reviews and audits of the logs are mandated to ensure compliance with healthcare regulations and to safeguard against data tampering or unauthorized alterations.
* **Session Management Policy:** The Session Management Policy in TPAS enhances security by automatically logging out users after a predetermined period of inactivity and requiring re-authentication after set intervals. It ensures that all session data transmitted over the network is encrypted, and cookies are secured with HttpOnly and Secure attributes. These measures prevent unauthorized access and protect session integrity, maintaining the confidentiality and security of user interactions within the system.

**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 of the TB Patients Appointment System clearly outlines the roles and responsibilities of various stakeholders including healthcare providers doctors, patients, and assistants. This delineation ensures clarity in the functions and expectations attached to each role within the system.

* **Doctor Responsibilities:** Doctors are tasked with managing the schedule of appointments efficiently to ensure that each patient receives the necessary time for care. They provide high-quality medical care during visits and are responsible for maintaining accurate and comprehensive records of patient treatments. Collaborating with other healthcare professionals is essential for delivering the best possible care. Doctors also manage the overall operation of the appointment system, ensuring that it functions smoothly and that all patient information is kept secure. Access to all components of the system is limited to authorized admins to safeguard patient confidentiality.
* **Patient Responsibilities:** Patients are required to provide accurate and complete information necessary for the effective booking and management of appointments. They must present a valid ID when required for verification purposes. Adherence to scheduled appointment times is crucial, and patients are expected to inform the healthcare provider in advance if they are unable to attend. Patients must follow all guidelines and procedures designed to protect the security and privacy of their personal information.
* **Assistant Responsibilities:** Assistants support the healthcare providers by preparing for appointments, managing logistics, and ensuring that patient flow is handled efficiently. They facilitate effective communication between patients and healthcare providers and manage administrative tasks such as scheduling, record keeping, and responding to inquiries. Their role is pivotal in maintaining the efficiency of the healthcare service delivery.