**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.

SYSTEM ADMINISTRATOR

Patient

Doctors

Patient

**TOPOLOGY**

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

**NETWORK SECURITY POLICY**

* Firewall
* Passwords
* System Logs

**SECURITY MEASURE FOR LOGIN**

* Login Captcha Code

**DATA CLASSIFICATION**

|  |  |  |  |
| --- | --- | --- | --- |
| **TOP SECRET** | **SECRET** | **CONFIDENTIAL** | **PUBLIC** |
| Admin Account | Student Account | Student Profile | Books |
|  | Staff Account | Transaction Reports |  |
|  | History Log |  |  |

**Data Support Regulations**

|  |  |
| --- | --- |
| Systems Manager | Data Account |
|  | System Logs |
|  | Admin Account |
| Administrator | Admin logs / Reports |
|  | Borrowed and Return Books |
|  | Students Transaction |

* 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 transactions

**Encryption Policy**

The encryption policy in this system is only the librarian/admin can access the system if the student want to borrow and return a book only the school id should presented to the librarian to borrow and return the book.

**Data and Backup Policy**

* The important data should back up are the data from books, borrowed and return books, report, barcode.
* The librarian backup every end of the using manual export from Xamp and save.
* After the exportation is directly save to the flash that only the librarian can used.
* Only the librarian/admin can allowed to back up the database from xamp and the procedure to back up is manual.

**Responsibilities, rights, and duties of personnel**

In this system all responsibilities and duties is on the hand of the admin/librarian because all the transaction from adding of books, borrowing of books, returning of book, and generating report, etc. are the duties of the admin to protect and secured the data from the system.

* In the system the big responsibilities is the admin/librarian because he/she only can access all the function in the system.
* The student is only presented their id for them to borrow a book.

1. Strong Passwords

Enforce complex passwords: Require a mix of upper and lowercase letters, numbers, and symbols. Set a minimum length (e.g., at least 10 characters).

Discourage reuse: Prevent users from reusing old passwords or using the same password across different websites.

Consider password expiration: Though somewhat debated, requiring periodic password changes can reduce risks if a password is compromised.

2. Two-Factor Authentication (2FA)

Adds an extra layer: Besides a password, require users to enter a code sent to their phone via SMS or generated by an authenticator app.

Significantly harder to bypass: Even if a password is stolen, attackers would need the user's physical device as well.

3. Limited Login Attempts

Block brute-force attacks: Lock an account after a few failed login attempts (e.g., 3-5 tries). This slows down attackers trying to guess passwords.

Temporary lockouts: Unlock accounts automatically after a set time (e.g., 30 minutes) to avoid inconveniencing legitimate users.

4. Input Validation

Prevent malicious input: Sanitize all data entered by users on forms or search fields. This helps block common web attacks like SQL injection and cross-site scripting (XSS).

Reduces unexpected errors: Improves system stability by not allowing invalid data to be processed.

Why Simplicity Matters

Ease of Implementation: These features are relatively straightforward to set up and manage, even if you don't have extensive technical expertise.

User-friendliness: Simple security measures are less likely to frustrate users and create barriers to adoption.

Strong Baseline: While advanced security is always a goal, these simple features provide significant protection against many common threats.