HIGHLY PRIVATE AND CONFIDENTIAL
Security Policy

Our system is designed with a multi-layered security approach to ensure the protection of sensitive medical data. The architecture consists of three distinct projects, each dedicated to enhancing security and operational efficiency.

1. System Architecture and Data Handling

To maintain a high level of security and compliance with data privacy regulations, our system is divided into three separate components:

- **Web Application**: The web interface provides access to the OCR portal but does not store any sensitive data. Even though file names may be visible in the progress table, the actual files are not retained on our servers. Only metadata such as filenames are temporarily referenced for process tracking.
- **Backend Scanner**: This component handles all communication with **Microsoft Azure for Optical Character Recognition (OCR) and AI processing**. It is hosted on a **high-security server** that performs only the necessary logical operations, ensuring that sensitive data is not stored or exposed beyond its required usage.
- **Clinic Software**: The downloadable clinic-side application is strictly limited to **scanning and transmitting medical files**. It has no access to any additional data or system resources beyond its intended function.

2. Data Encryption and Transmission Security

To safeguard the confidentiality of medical reports, we implement **AES-256 encryption**, the most advanced encryption standard widely adopted by government and military institutions. This encryption is applied to all files during transmission between the clinic software and our backend scanner, ensuring end-to-end security.

- Encryption keys are dynamically rotated and updated over time to strengthen security against potential vulnerabilities.
- Data transmission is secured using **TLS 1.3** encryption (The highest Encryption exists) to prevent interception and unauthorized access.

3. Data Retention and Storage Policy

We adhere to strict data retention policies to ensure compliance with regulatory requirements:

- **Temporary Storage of patient files**: All uploaded files are **automatically deleted from the memory** upon completion of the OCR process for every file. We do not retain or store any medical files beyond the necessary processing duration.
- **Log Data Management for billing purposes**: Only document filenames are kept for billing purposes and the document name logs are **automatically purged every 30 days** to eliminate unnecessary data storage.
- **No Persistent Data Storage**: Our system does not store any patient reports or confidential medical data, ensuring that patient privacy remains uncompromised.

4. AI Processing and Data Privacy Protection

To maintain patient confidentiality, our AI processing is designed with stringent data limitations:

- The AI is restricted to reading only a **minimal subset of data**, referred to as the "informative section," which includes **basic patient and doctor details**.
- **No diagnostic information or report content is processed by the AI**, ensuring that patient conditions and medical findings remain private and inaccessible to any external system.
- This approach guarantees that even within our secure environment, sensitive medical data remains confidential and protected against unauthorized exposure.

5. Secure Communication Between Clinic and the Server

To further reinforce security, we employ an **advanced authentication algorithm** for secure communication between clinic devices and our servers:

- A unique **key-based challenge-response authentication** mechanism verifies every transaction between the clinic software and the backend.
- The system dynamically generates authentication keys that must be returned in a specific sequence and structure.
- If an incorrect or out-of-order key is received, the communication session is automatically terminated, and access is temporarily disabled until re-authentication is successfully completed.
- This ensures that any potential security threats or unauthorized attempts to intercept communication are immediately detected and mitigated.

6. Compliance and Security Best Practices

In addition to the measures outlined above, our system adheres to industry best practices in cybersecurity:

- Regular **penetration testing and vulnerability assessments** are conducted to proactively identify and address potential security threats.

- System components operate on **hardened and continuously updated servers** to prevent unauthorized access and mitigate known security risks.
- Compliance with **HIPAA, GDPR, and other applicable data protection regulations** ensures that our security framework aligns with international healthcare standards.

Conclusion

Our security measures are designed to **ensure the confidentiality, integrity, and availability** of medical data while providing a seamless experience for clinics using our OCR portal. By implementing **strict encryption standards, data retention policies, AI limitations, and secure communication protocols**, we reinforce our commitment to protecting patient information and maintaining a **highly secure** processing environment.

IMC Pty Ltd
www.toolii.com.au
ABN: 39 663 004 386
Ground Floor, 470 St Kilda Rd
Melbourne 3004
Tel:1800934046