TE MARAE ORA
COOK ISLANDS Ministry of Health

ManageMyHealth Application Usage and Management Policy

Effective: 6 June 2025

Policy Statement

This policy recognises that digital health application namely, ManageMyHealth (MMH), is a crucial tool for enhancing health care service delivery. Te Marae Ora Ministry of Health Cook Islands (TMO) understands the value of this application in improving patient communication, patient engagement, patient education, and decision support for self-management. By providing a platform for easy access to health records, appointment scheduling, and secure messaging with healthcare providers, MMH streamlines processes and fosters a collaborative environment between patients and clinicians, ultimately leading to better health outcomes.

Purpose

The purpose of this policy is to ensure the effective implementation, management of the MMH application and alignment to existing TMO digital systems. It aims to promote operational efficiency, patient safety and compliance to relevant regulations while fostering a secure and user-friendly environment for both patient and TMO personnel for better informed decision making.

Scope

This policy applies to all users of the MMH Application.

Principles

- **Confidentiality and privacy**
  Patient data must remain confidential and be accessed only to authorised personnel for legitimate purposes. Safeguarding patient privacy is paramount.
- **Transparency**
  Users should be informed about how their data is being used and the measures in place to protect their information.
- **Ethical Use**
  All users must adhere to high ethical standards in managing patient information. Responsible use of the application is crucial.
- **Accountability**
  Users are accountable for their actions within the application. Any breaches of confidentiality or unethical behaviour must be reported and appropriate action will be taken to mitigate risks.

Legislation and Regulations

- Ministry of Health Act 2013
- Official Information Act 2008
- Cook Islands Protective Security Policy Framework
- National Security Policy
- National ICT Policy 2023-2027

- Cook Islands Cyber Security 2024
- National Digital Strategy 2024-2030
- TMO HR Personnel Policies and Procedures 2024 (Sections 1.7 Code of Conduct & 2.3 Confidential Information).

Definitions

Account holders – refers to an individual that has created and maintains an active account within the MMH application.

Administrative functions – tasks related to patient management such as scheduling, updating records and communication.

Clinicians – refers to health professionals with direct patient contact such as doctors, Nurse Practitioners, Dentists, and psychologists.

ManageMyHealth (MMH) Application – A digital platform enabling patients to manage their health records, appointments, and communications with clinicians.

Patient – refers to any individual accessing the Patient Portal, including the vulnerable groups (i.e., children, elderlies and persons with disability).

Patient Portal – the interface provided by MMH for patients to access their health information.

Provider – refers to TMO clinicians and system administrators accessing the MMH application to manage patient records (e.g., update, register, modify, and suspension of patient records).

Provider Portal – the interface provided by MMH for providers to access and communicate with patients.

Subscription - the annual registration process for patients accessing MMH services.

Users – refers to individual who interact with the MMH application, which includes patients and providers such as clinicians and system administrators.

Usage and Management

I. MMH Application Interface

1. The MMH Application consists of two distinct interface which are restricted to registered patients and authorised TMO personnel:
   i. **Patient Portal**
   Designed for patients to access their personal health information, manage appointments, communicate with TMO, and utilise other health management features.

ii. **Provider Portal:**
Exclusively for TMO ICT Department and Clinicians, allowing access to patient records and facilitating communication with patients.

2. The various functionalities of this application are detailed in the Standard Operating Procedures (SOPs) attached to this Policy.

II. Access Management

1. Registration for the MMH patient portal is voluntary. TMO will encourage and inform patients about the benefits of enrolling to MMH.
2. Patients will have secure access to their personal health information through the MMH patient portal, enabling them to manage their health records and communication with TMO as their health provider. Access to the provider portal will be restricted to TMO, as outlined in the section I.1.ii above under Usage and Management section, with access levels granted upon approval. These levels will be determined based on the personnel's roles within the Patient Management Information System (PIMS) and their need to access specific information to fulfil job responsibilities.
3. Private clinics and approved non-governmental organisations will be granted access, as a provider, to the MMH **only** after successful implementation of the system. This access will be contingent upon ensuring that all necessary training and support are provided, and that the system has been thoroughly tested to ensure its reliability and effectiveness. Additionally, a clear protocol will be established for managing data security and patient privacy.
4. TMO ICT Department, as the system administrators of this application, reserves the right to modify access permissions and the functionality as necessary to enhance security and improve user experience.

III. Consent

1. By using the MMH application, patients give their consent to the collection, processing, storage, and use of their health information for the purposes of health management, clinical decision support, quality care and communication between TMO and patients.
2. Patients provide this consent upon registration and while using the MMH application.
3. Patient have the right to withdraw their consent at any time by submitting a request through the appropriate channels. Withdrawing consent restrict privileges on the use of MMH application.

IV. Subscription Management

1. Users can view and manage their subscription details through their account settings.
2. An annual subscription fee of $1 NZD will be charged to account holders to cover maintenance and management costs. This charge will be processed via the PIMS, with payment options using the normal process whether face-to-face or direct deposits to TMO bank account.

3. Patients may cancel their subscriptions any time; however, fee is non-refundable for the year in which the cancellation occurs. Re-subscribing to MMH will require the payment of the aforementioned fee.

V. Types of Data Collected

With the implementation of MMH, TMO may collect the following health information:

i. Patient personal information such as name, date of birth, gender, ethnicity, blood type, and medical conditions, contact details such as residential, personal or private email address.

ii. Patient medical records, including (but not limited) to sick leave, laboratory results, prescriptions, immunisations, clinical notes, and conditions.

iii. Information regarding lifestyle choices such as exercise habits, dietary preferences, and smoking or alcohol use, which may be relevant for health management.

iv. Details of individuals designated by the patient in case of emergencies.

VI. Data Sources

1. TMO's use and management of MMH will require access from various authorised data sources to ensure comprehensive and accurate patient health information. These sources may include, but not limited to:

   i. PIMS including supporting information system such as pharmacy, radiology, laboratory systems, cancer register, etc.

   ii. Immunisation Register

   iii. Jotforms for the Registration

   iv. ManageMyHealth Application

2. Data collected from these sources will be used solely for the purposes outlined in this policy.
3. Transparency regarding any data source partnerships and any third-party data sharing agreements will be ensured.

VII. Data Management

1. Collection
   - The data collected aims to enhance patient access to health records, verify identity and ensure consistency.
   - Crosschecking or referencing will be conducted to ensure accuracy of collected data (e.g. registration, PIMS records, prescription). Any discrepancies should be reported to the appropriate team with necessary steps taken to resolve the matter.
   - Privacy and security implications will be carefully evaluated when collecting and holding personal information.
   - Communication between patient and TMO clinicians will be facilitated, ensuring timely access to appointment bookings, prescription requests, and clinical results.
   - Data will be processed solely for the purposes intended by this Policy.

2. Storage and Data Migration
    - MMH registration data collected from *jotforms* will be saved on TMO file servers optimised with an encrypted firewall.
    - Data migration from registration to the PIMS and patient portal will employ a highly protected, systematic, and well-documented approach. Refer to relevant SOPs.
    - All data is stored in structured database implemented by TMO, with regular backups and encryption to ensure data integrity and availability.
    - Vulnerability testing, backup and disaster recovery measures will be in place.
    - Any documentation and data collected from the implementation of this policy will follow the government retention and disposal in accordance with government information management policies.

3. Quality Assurance
    - System Administrators will conduct site and audit checks on data sources to ensure accuracy and completeness. Procedures for addressing issues will be included in the relevant SOPs.
    - Ongoing training on MMH usage and cybersecurity will be provided to TMO to maintain high service levels. Regular training refreshers will be implemented to keep personnel updated on the latest cybersecurity practices and policy adherence.
    - High confidentiality and privacy standards will be maintained through Non-Disclosure Agreements (NDAs) signed by all providers.
    - Role-based access controls will be implemented to ensure that only authorised personnel can access patient information.
    - Patients will have access to their information (e.g., health summary, immunization records, prescriptions, appointments and laboratory results) via a secure patient portal. A summary or dashboard feature is also available for better visualization of personal health data trends.
    - MMH Application will meet security standards (e.g., firewalls, antivirus, two-factor authentication, spam filters) to enhance overall quality and security.
    - Patients will be encouraged to provide feedback through the TMO Helpdesk for continuous service improvements.

VIII. Data Ownership

1. All data collected through the MMH application remains the property of TMO. Patients retain access rights to their personal health information and may have the discretion to share data to relevant and appropriate third parties. Third parties are encouraged to verify with TMO the veracity of the shared data.
2. Upon suspension of access of account holder to MMH application, TMO will retain ownership of all data collected, while users will continue to have the right to request access to their personal health information using the normal process.

IX. Information Products

Patients can access various health records, including prescriptions, immunizations, lab results, and health indicators.

- Health records
    - Prescriptions
    - Allergies
    - Immunisations
    - Laboratory results
    - Conditions
- Appointments
- Repeat prescriptions
- Health indicators (e.g., readings on patient health level risk)

X. Dissemination and Use

1. Patients are responsible for providing accurate and complete information regarding their personal details, health history, medications, and any other relevant data.
2. Personal health information will be kept private and shared only with authorised individuals or health partners.
3. Patients should understand and consent to how their health information will be used, including potential sharing with third parties.
4. TMO must maintain patient confidentiality at all times, obtain patient consent, and adhere to this policy and relevant SOPs.
5. Clear communication will be provided to patients regarding how their data will be used and shared.
6. TMO reserves the right to use aggregated and anonymized data for research, analysis and quality improvement purposes, ensuring that individuals cannot be identified from such data.

XI. Data Security and Protection

1. No user —whether patient or provider—shall use, store, share or otherwise manage the other user's information except as required to perform services in accordance with this policy and relevant SOPs unless expressly authorised in writing by the relevant users.
2. TMO is responsible for ensuring that all necessary consents and authorisations required are obtained and maintained to enable MMH to process and store data in accordance with its terms.
3. Users must adhere to password terms and conditions of MMH application and report any security incidents immediately to the TMO ICT Department.
4. Regular audits will be conducted by the TMO ICT Department, in collaboration with the relevant clinicians, to ensure that data verification and security measures, including encryption and firewalls are in place.

5. A multi-layered security approach will be implemented including regular penetration testing including reviews of access levels to maintain appropriateness of management and access controls.

XII. Incident Management

This section addresses any breaches of this policy and the relevant SOPs.

1. The following activities may lead to a suspension of MMH account use by the patient or provider:
   i. Unauthorised sharing of passwords and disclosure of information in any form without prior consent from the user.
   ii. Fraudulent use of personal and health information to gain unauthorised access to MMH portals for personal gain.
2. Management of such incidents will follow the Code of Conduct outlined in HR Personnel Policies and Procedures for managing investigations.
3. Other types of suspension, such as death of a patient or transfer of healthcare centres, will follow relevant SOPs.

XIII. Feedback and Complaint Management

Users have the right to express concerns or complaints regarding their experience with the MMH application or any aspect of the services provided by TMO. The process to manage complaints follows the standard procedure through the Helpdesk at tmo.helpdesk@cookislands.gov.ck.

XIV. **Service Availability**

TMO strives to ensure the availability of the MMH application but does not guarantee uninterrupted access. Scheduled maintenance may occur, and users will be notified in advance when possible.

XV. **Liability Limitations**

TMO shall not be liable for any direct, indirect, incidental, or consequential damages arising from the use of the MMH application, including but not limited to loss of data or service interruptions.

Review and Update

This policy will be reviewed annually or as needed to ensure compliance with evolving regulations and technologies.

Monitoring and Reporting

1. Aligned with TMO's vision for a modern, patient-centred healthcare system, MMH aims to enhance patient engagement, access to health information, and care coordination. It supports seamless connections between patients and providers, fostering better health outcomes and accessibility. The policy's success will be measured by the following primary indicators:
   a) Number of patient registered for MMH (target of 5,000 subscribers within 3 years).

b) Utilisation rate of MMH as patient portal (e.g., primary healthcare: prescribing sick leave, prescription for long-term medication and appointment booking; oral health: appointment booking).

c) Incident management rate (less than 5% of the total subscribers in a given year)

d) Additional indicators for consideration:
   - appointment attendance rates
   - subscription cancellation rates
   - audit compliance rates

2. The TMO ICT Department, led by the Manager, will collaborate with the Policy Team to create a report annually, or as needed, to evaluate the effectiveness and compliance of this policy. This report will ensure that the overall objectives of the policy are being met.

Roles and Responsibilities

Patients

- Individuals who utilise the MMH application to access their personal health information, including medical records, prescriptions, lab results, and appointment details.
- Responsible for providing and sharing accurate and complete personal and health information and for managing their subscriptions and preferences within the application.

TMO ICT Department

- Responsible for maintaining the technical infrastructure of the MMH application.
- Ensures data security through regular audits, encryption, and vulnerability testing.
- Provides user support and training for users, addressing technical issues and inquiries.
- Acts as the system administrators to the MMH application.

Receptionist

- Manages patient inquiries regarding the MMH application, providing clear information about features and functionalities.
- Assists with user registration and helps patients navigate the registration process and subscription management.
- Facilitates communication between patients and clinicians as needed.

Clinicians

- Utilise the MMH application to manage patient information effectively, ensuring accuracy and confidentiality.
- Facilitate communication with patients through the application, including appointment scheduling, prescription requests and release of health records.
- Ensure compliance with privacy and data security policies when handling patient information.

Compliance and Enforcement

Compliance and enforcement to the terms and conditions outlined in this Policy is essential for maintaining the integrity and security of the MMH application. Non-compliance may result in disciplinary actions, including suspension or termination of access privileges.

Authorisation

The implementation of this policy is authorised by TMO Executive per approved Resolution No. 2025-06-02 and will be effective from 6 June 2025.

Other Provisions (if any)

All printed records related to this policy must be retained for at least seven (7) years and are accessible only to authorised personnel. Unauthorised access or tampering will result in disciplinary action.

Associated Documents

MMH Registration Process
SOP for Provider
MMH Information Materials (FAQs, Term of Use, etc.)

Other Information

For queries, contact the Planning and Funding Directorate in Tupapa at 29664.