CookSafe

COOK ISLANDS
CHAMBER OF COMMERCE
Punanga Kimi Puapinga o te Kuki Airani

Privacy and Security Information for the CookSafe Contact Tracing System

CookSafe is a voluntary Contact Tracing system for the Cook Islands which has been endorsed by the Office of the Prime Minister, and Te Marae Ora (TMO, Ministry of Health). The system has been developed by the Cook Islands Chamber of Commerce.

1. Overview

A Contact Tracing System for COVID-19, called **CookSafe**, is being operated in the Cook Islands, effective from 19th June 2020.

The Purpose is to:

1. keep people safe within the Cook Islands
2. quickly trace possible COVID-19 infections and carriers
3. identify and locate their contacts
4. identify locations of interest
5. allow early testing and interventions

CookSafe Cards are available to:

1. All visitors to the Cook Islands
2. All returning Cook Islanders and Work-Permit holders
3. All persons wishing to access **CookSafe Venues**: tourist facilities, bars, restaurants, nightclubs, government agencies, businesses and other venues as notified by TMO (Te Marae Ora, Ministry of Health)

CookSafe Cards have unique QR codes, linked to the cardholder's contact information via an encrypted database. CookSafe Cards are issued to arriving passengers on board the aircraft, and to people already resident in the Cook Islands. Residents can obtain a CookSafe Card from the CookSafe Support Office at the Chamber of Commerce, and other participating outlets.

CookSafe Venues (tourist facilities, bars, restaurants, nightclubs, government agencies, businesses and other venues as notified by TMO) are strongly encouraged to:

- Register their venue with the CookSafe Support Office
- Install a scanning 'app' on an Android device / iPhone / iPad
- Scan all visiting CookSafe cardholders into their premises
- Maintain accurate staff attendance records

CookSafe Cardholders need to keep their cards with them at all times, and present their cards for tagging in at all CookSafe Venues. The cards can be photographed on a phone and the picture can be used to tag in.

CookSafe Database

- The unique QR code (encoding a random number) on each CookSafe Card, is linked to the cardholder's contact details, and stored in a secure database only accessible by TMO.
- Cardholders present their card for scanning when entering all CookSafe Venues.
- The scanner automatically uploads to the secure database:
  - the Cardholder's QR code number,
  - the date and time and
  - the location.

No other identifying information is taken or stored.

CookSafe Methodology

In the event of a COVID-19 carrier being identified as being, or having been, present in the Cook Islands:

- The database will be searched by authorised TMO staff for CookSafe Cardholders who were present in the same location as the carrier at the same time.
- Staff attendance records for CookSafe Venues will be similarly searched
- Persons identified as likely to have been in contact with a COVID-19 carrier will be approached by TMO for testing and intervention.

2. Privacy Information

Any personal information and contact details you provide when registering for a CookSafe card is provided to TMO so contact tracers can quickly get in touch if you are identified as a close contact of someone who has COVID-19.

Any information you register with CookSafe will never be used for enforcement purposes. It also will not be shared with another government agency unless that agency is directly involved in the COVID-19 response and sharing the information is necessary for public health purposes during the pandemic.

Any contact tracing information you register with CookSafe is stored securely on TMO's database, where only authorised TMO personnel can see it. This includes the contact information you provide, and the locations and times that you 'Tag-in' to public places. Please note that records maintained by TMO are subject to Section 29 (5) of the Ministry of Health Act 2013, relating to legal rights of confidentiality. At the end of this document we have put this section for reference.

Anonymised statistical information
Anonymised statistical information is provided to support staff for reporting purposes. It is not possible for this data to be linked to an individual CookSafe user.

QR Codes
The randomised CookSafe QR codes used in CookSafe contact tracing tracing do not contain any information other than a unique number. When these are scanned at CookSafe locations, the number, date, time and location are securely transmitted to the TMO database. The information is then deleted from the scanner. All scan data is deleted after 60 days, and is only accessed for the purpose for contact tracing. CookSafe has been assessed by security experts to ensure the data is managed securely.

3) Security and Stability - CodeReadr Platform:

- **Stability & Uptime**

  The codeREADr platform has an uptime of more than 99.9%. In other words, the downtime is less than 4.38 minutes/month on average. It is understand that your business depends on the uptime of our servers. Thus, focus has been to keep them available and fast.

- **User Authentication & Permissions**

Whether you're on the website or the app, codeREADr requires you to go through an authentication process. The website account holder (admin) must give all of the mobile app users unique usernames and passwords. Then, the admin can set specific permissions for each user. In this way, users have access to only what they need.

- **Encrypted App Communication**

When data travels from your mobile device to our servers it is securely encrypted via TLS. This means that all of the data within your scans, such as its service type, user, device and location, go through this cryptographic protocol. This ensures that your data is safe, secure, and only accessible to an administrator with a valid username and password to the website.

- **Encrypted Website Communication**

The login to CodeREADr.com is also encrypted by TLS. This means that all of the data transferred between CookSafe and their web browser when your admin is viewing or downloading scans is encrypted. Also, just in case someone forgets to type in the "s" , there is an automated redirection of browsers from http:// to https://. Thus, any authentication, login, or view of data between is secure.

- **Encrypted API Communication**

The APIs you can call to retrieve data or configure codeREADr in the cloud are also encrypted by TLS. The API utilizes token-based authentication and IP filtering to ensure it is only your server that is connecting to your information. You are able to revoke and reset your API keys at any time.

- **Data at Rest Encryption**

In addition to encrypting data while 'moving' (app-to servers, servers-to app, browser-to-web services, etc.), data stored on our servers is also encrypted. Typically, this is referred to as 'Data at Rest Encryption'.

- **Replicated & Redundant Databases**

With codeREADr, you don't need to be concerned about losing data. Our database is highly scalable. If something should happen to the main database server, it synchronously replicates the data across multiple data centers. Thus, if one database server goes down, there are others waiting in standby mode to immediately take its place. These backup databases support an automatic failover feature. Therefore, the system will switch from the failed database to the duplicate database without human intervention. Ultimately, there is no waiting for a repair of the connections.

- **Continuous Data Backup**

Backup snapshots of your data are taken so that should a disaster occur, this can be restored information from any point in time, and from the past three days. Weekly and monthly backups are also stored in our databases. Everything is backed up except barcode images which can simply be re-generated.

- **Database Technical Details**

Our databases are replicated across multiple data centres and support automatic failover. If any problems occur with our primary database server, a switch over to a replicated database without human intervention occurs. Patches and updates to the database software can also be applied without any downtime.

Maintenance is conducted via the following steps:

1. Perform maintenance on stand-by
2. Promote stand-by to primary
3. Perform maintenance on old primary, which becomes the new standby.

Databases are continually backed-up, storing the backups for a defined retention period of 30 days. Both Point-In-Time-Restore and Snapshot Restore are supported. The Point-In-Time-Restore allows specification for any minute (except the previous 5 minutes) during the past 30 days and restore the data. Also, automatic full daily snapshots are done of our Database and copies of these are retained for a month.

An automated replication service is utilised for the file system. The service stores data in multiple facilities and on multiple devices within each facility. To increase durability, this system synchronously stores data across multiple facilities at the time of file creation. The service calculates a checksum on all network traffic to detect corruption of data packets when storing or retrieving data.

SECTION 29 OF THE MINISTRY OF HEALTH ACT 2013

29. General principles relating to medical records and health information

(1) The provisions of this section apply to medical records and other information relating to a patient or user of health services, held by the Ministry and by any health service provider, and any health professional or allied health professional.

(2) The general principles applying to the keeping, use and divulging of medical records and other information relating to a patient or user of health services are as follows—

(a) the Ministry is entitled to collect information (including information derived from medical records and other information relating to a patient or user of health services) for any purpose relevant to its functions, responsibilities and powers under this Act, and any other law for which the Ministry is responsible:

(b) patients and users of health services, and their legal guardians and representatives, are entitled to access their medical records, subject to the imposition of a reasonable fee:

(c) medical records and other information relating to a patient are to be disclosed to any other party only on any of the following grounds-

- (i) the disclosure is to the patient or user, or his or her legal guardian or representative:
- (ii) the patient or user has given written authority for the information to be disclosed:
- (iii) the disclosure is ordered by a court, or relates to an investigation by the police in relation to the commission of an offence:
- (iv) the disclosure relates to a notifiable disease and is required by the Ministry:
- (v) the disclosure of the information is otherwise necessary to prevent or lessen a serious threat to public health or public safety, or to the life or health of the individual concerned or another person:
- (vi) the information must be disclosed in accordance with any law that requires such disclosure, and subject to such procedures or rights of confidentiality as that law imposes:

- (d) information may be divulged by the Ministry to the parents or legal guardians of minors.

(3) The Minister may, by written Order, require any health service provider, and any health professional or allied health professional to disclose medical records or other information obtained in relation to a patient or user of health services, if such information relates to any of the following—

- (a) abuse, malnourishment or neglect of a child:
- (b) abuse, malnourishment or neglect of an elderly or infirm person:

- (c) sexual abuse or sexual assault of a person:
- (d) a non-accidental injury:
- (e) a sexually transmitted infections:
- (f) HIV infection or other notifiable disease:
- (g) any disease or medical condition for which the Ministry maintains a registry:
- (h) a mental illness.

(4) Information disclosed under subsection (3) must be kept confidential, and may only be disclosed by the Ministry in accordance with subsection (2).

(5) Legal rights of confidentiality and privilege relating to medical records and other information relating to a patient or user of health services are subject to the provisions of this Part.