“Flu Smart”

*By Dr Hamish Rodda, MBBS BMedSci FACEM*

*Emergency Physician & Medical Informatician*

*Melbourne, Australia*

[*hamishrodda@icloud.com*](mailto:hamishrodda@icloud.com) *|* [*https://www.linkedin.com/in/hamishrodda*](https://www.linkedin.com/in/hamishrodda) *|* [*@hamish\_rodda*](https://twitter.com/hamish_rodda)

A Design Document for a System to Technically Enable Individuals and Communities with Critical Data and Capabilities against the Novel Coronavirus, **SARS-CoV-2**

# Introduction

A substantial threat exists to global public health in the form of the novel coronavirus SARS-CoV-2. Societies have expressed that their ability to contain this threat through existing manual contact tracing methods will not be sustainable in pandemic conditions. Techniques that can slow the advance of the illness will at least buy time for vaccine development, if not greatly contribute to putting a stop to unrestricted transmission.

This idea is to combine existing personal mobile technology and cloud computing to form a system capable of real-time automatic contact tracing and epidemiologic monitoring. This will enable communities with active community transmission to track and quarantine chains of infection remotely and at scale. Other communities will achieve earlier, and more complete detection should novel coronavirus arrive. Through digital interaction, personal contact and risks are decreased, and frontline medical resources are reserved for individuals that truly require emergency medical care.

The “Flu Smart” applications that would be created will have utmost regard for personal privacy and will ask for permission when sharing of sensitive data is needed. They will ask individuals to contribute their private data for the good of their community only once they become unwell; even when this occurs, the system must be engineered to permit only the minimum necessary information to be revealed, such that the actual identity of the volunteer participants is maximally concealed.

The applications can also deliver other benefits, such as empowering improved personal hygiene. Handwashing alerts can be delivered at the right time; for example, when arriving at home or at work, and after contact with large numbers of people. Individuals would receive a custom haptic alert and know that it is time to wash their hands even without touching their phone or watch.

Community application of this system will allow visualisation of the distribution of suspected and actual cases, better informing community control actions such as travel restrictions and voluntary quarantine. Global application of this system will dramatically improve the data that is made available to decision makers, as well as making gravity of the threat being faced much clearer to the world.

In the future, if successful this system could be re-used for more effective control of existing transmissible infectious diseases such as influenza and measles, as well as future pandemic diseases.

Table of Contents

[Introduction 1](#_Toc33516187)

[Copyright 3](#_Toc33516188)

[Design and Naming 3](#_Toc33516189)

[System Overview 3](#_Toc33516190)

[Detailed Workflows 3](#_Toc33516191)

[Local Mode 3](#_Toc33516192)

[Networked Mode 4](#_Toc33516193)

[Proximity Detection 4](#_Toc33516194)

[Location & Contact Privacy 5](#_Toc33516195)

[Symptom Monitoring 5](#_Toc33516196)

[Identification of Cases 5](#_Toc33516197)

[Positive Case Handling 6](#_Toc33516198)

[Exposed Individual Determination (Automated Contact Tracing) 7](#_Toc33516199)

[Community Detection + Response Improvements 7](#_Toc33516200)

[Special Populations 9](#_Toc33516201)

[Families 9](#_Toc33516202)

[Residential Care 9](#_Toc33516203)

[Privacy 9](#_Toc33516204)

[Individual Privacy Control 10](#_Toc33516205)

[Security Considerations 10](#_Toc33516206)

[Governance of system use 10](#_Toc33516207)

[Defence against System Misuse 10](#_Toc33516208)

[Responsive Design 11](#_Toc33516209)

[System Creation 11](#_Toc33516210)

[Funding 12](#_Toc33516211)

[Version Control 12](#_Toc33516212)

[Glossary of Terms 12](#_Toc33516213)

# Copyright

All design work in this document is original content by Dr Hamish Rodda. Any rights to the intellectual property of this work is hereby waived in the interest of public good.

## Design and Naming

The name and design of the system are indicative only, suggestions and changes are welcome. It is acknowledged that Flu Smart suggests influenza, however the main disease target is novel coronavirus; however ‘SARS Smart’ / ‘COVID Smart’ and variants may not be as well received by individuals.

# System Overview

The **Flu Smart** system captures individual location, time, and Bluetooth contact data to enable automatic contact tracing in the event of verified COVID-19 diagnosis. The application protects individual privacy primarily through storing sensitive data only on the well individual’s device, and through allowing anonymous participation up to the point of confirmed or presumptive diagnosis. After diagnosis, the system requests additional permissions for community good. However, individual identities will not be directly revealed; only through the difficult task of determining patterns in revealed overlapping contact would others be able to determine the identity of the now unwell contacts.

Identified community groups have key roles in the success of the system. The local health department’s infectious diseases unit participates by deciding who should be screened for COVID-19, and in return can access anonymous statistics on symptom prevalence and tracking of confirmed disease. The World Health Organisation participates by validating that only government-authorised people have access to this functionality, and WHO also receives access to the anonymous information.

# Detailed Workflows

## Local Mode

**Flu Smart** will provide a client application that will be voluntarily installed on personal mobile devices. This app will ask for permission to access location data (eg. calculated through GPS and WiFi) in the background. When permission for these is granted, the device will commence recording location information, saving this securely and only on the device. The app will automatically purge this sensitive information after the majority of **incubation period**, i.e. currently thought to be two weeks. The app will then be able to produce a report on the device which shows a timeline of personal locations; times arrived and departed the location; and the app may also be able to plot this information on a map. This report should be able to be emailed or printed on user request. The use case of this information is in its application to individual health care, and in manual contact tracing activity should an individual wish to still contribute to community good after diagnosis but decline to use the networked methodology below.

It is expected that community uptake of the **Flu Smart** application would be swift; however, if uptake turns out to be poor, the platform vendors may be requested to send push notifications to individuals in a geographic area where the local health department is in need of better uptake of the system.

## Networked Mode

To provide the main community benefit, the app will ask for voluntary participation in the automated contact tracing system. If the individual wishes to participate, the app will additionally request permission to upload approximate locations visited during each time period, for the purposes of subscribing to possible exposure alerts. This approximation could be done by converting the GPS coordinates to a **geohash**, for example the 5 character precision with a reported accuracy of +/- 2.4km. For each one-hour time period, a list of these approximate locations visited would be uploaded to the cloud. Any locations on the border of the geohash region would result in the neighbour geohash also being included, as it would be better to over-subscribe than under-subscribe. In addition, if location information suggests a commute has occurred but this commute potentially crosses several geohash regions, these interval regions should also be included. The use case would be if an individual was on a train and not receiving GPS signal, they should still subscribe to the proximity so their phone can check for potential proximity exposures.

At no point will the app requested any login or other identifying information; instead the **Cloud Service** will allocate an anonymous identifier (a **Flu ID**) specific to each device to new devices to allow two-way communication. As each ID will effectively relate to one person, this identifier should not be used in other correspondence (see the **Case ID** below for persistent tracking purposes).

## Proximity Detection

As well, the app will request Bluetooth and activity data access. If this is granted, the phone will monitor in the background for other Bluetooth devices, and intermittently announce its presence at pre-defined time points as well; for example, an announcement period of 30 seconds every 15 minutes that is shared by all Flu Smart apps. A list of Bluetooth identifiers observed will be saved against each location and time period. Time in proximity to each identifier will be saved on individual devices; separated into time in close proximity (eg. less than 5 metres, to be confirmed by experts), and time in any proximity. This is used later for improved accuracy in the calculation of exposure risks.

The amount of Bluetooth scanning performed will be regulated by the phone’s battery state, and the individual’s activity. Higher preference may be given to scanning when an individual is stationary, or when an individual may be using public transit (intermittent fast motion, and also if the device is already contextually aware) or occasionally during private transit (e.g. determining others sharing a car ride). It would likely be impractical to attempt to determine all contact when individuals walk through large crowds and would also result in low specificity alerting, especially when the individual is outdoors. In order to create an app with acceptable battery performance it is probable that Bluetooth scanning be sensibly aligned with activity data. Note that there would be no need to actually record activity data. Also, as the Bluetooth identifiers will be distributed with an Exposure Record, only one of each pair of individuals’ devices would need to record the others’ presence in order for a link to be created. There may also be a need to determine a baseline of normal ‘always’ or highly frequent Bluetooth contacts for each individual, to save on storage of useless information.

## Location & Contact Privacy

To enhance privacy controls, individual users may be permitted to exclude certain geographical areas from alert subscription (for example, in proximity to their home), and/or for the app to insert at random some incorrect information e.g. locations and times not visited. The app must also have a mode to temporarily disable all data collection for a specified time period, and the ability to erase on-device information covering a specified time, geographical area, or all recorded information at the individual’s request. The app may also be able to ask the **Cloud Service** to remove all records pertaining to the individual’s device, although it is acknowledged that implementing this would be a lower priority than having the service operational; a better option may be for a device to request that it is provided with a new anonymous **Flu ID**.

## Symptom Monitoring

Next, the app will allow for individuals to self-report any symptoms, after permission is granted to anonymously upload this information as well. For example, the app will be able to collect the onset date/time of any significant fever, cough, or shortness of breath. The individual should be able to indicate the severity of the symptoms. Commencing this data entry starts the creation of a **Case Record**, and upload to the cloud platform assigns a **Case ID**. This identifier would initially be anonymous and would persist only for the duration of the person’s illness.

The self-reporting will be more useful in the automated contact tracing if it is able to estimate the individual’s infectivity over time, and what methods the individual used to control their activity. Thus, once an individual has indicated that they are symptomatic, the app should regularly request the individual to track their symptoms: how often are they coughing, the amount of secretions being generated, the use of masks, etc. This should be of low burden (eg a quick update) to improve compliance. The app could also increase the frequency of reminders to attend to hygiene. All of the information contributes to the **Case Record**. The app can display a QR code which represents the individuals **Case ID** for use if the individual interacts with a healthcare service or the health department.

In this section of the app, there should be a link to the World Health Organisation information on SARS-CoV-2, plus a link to the local health department’s online resources and information. There should also be information on when to seek emergency medical care, and an ability to request emergency care if the individual requires it (eg. a call to the local emergency service). This self-reporting and uploading alone would provide prevalence and trend information for flu-like symptoms.

## Identification of Cases

Taking this further, each local health department should be able to participate at this point in the screening and diagnosis of individual cases and/or at the population level. **Case Records** are uploaded to the cloud and can be reviewed by the local health department. Symptomatic individuals that self-rate that they do not require emergency medical care can be sent an authorised request for pathology testing; the local health department decides who is provided this option (eg. all patients with symptoms, or a random sample, or all patients in a cluster as determined by cloud-based machine learning / AI). The local health department would be provided with the individual’s **Case ID** for further interaction. Options for the individual to be tested include:

* receiving a test kit in the mail, containing instructions on collection and return of the sample to a collection point; or
* presenting to a dedicated testing facility to have a test carried out; or
* the health department could request their location so they can attend and perform this testing.

This proposal is undecided as to whether the Flu Smart app should offer its own two-way communication or refer two-way communication needs to existing messaging platforms. All of the above should use existing communication/messaging platforms; as it is essentially not possible to have formal testing performed without revealing your identity to a healthcare provider, and thus the privacy can no longer be protected in a greater way.

This system will then allow for enhanced community screening of the incidence of novel coronavirus, without requiring this service provision to be performed by primary care providers or emergency medical services – both of whom are likely to become extremely overloaded in a sustained community transmission scenario.

If a negative result is returned for novel coronavirus, the app could potentially receive and relay this result to the user based on the Case ID provided on the test request form, and HL7 FHIR integration. However, this must also reinforce the requirement to maintain quarantine despite a negative initial result.

## Positive Case Handling

Once a patient returns a positive result for novel coronavirus; or where sufficient testing is not possible, self-rated determination of meeting the current case definition; the automated contact tracing kicks in. In the confirmed case scenario, the diagnosed individual is flagged as infected in the central system on the basis of their **Case ID**, and their device is sent this diagnosis and a request to upload an **Exposure Profile**: the list of exact locations, and all Bluetooth contacts, in the potential incubation period for their illness; plus the **Case Record** including generated scores of the estimated infectivity. The individual has the ability to allow or decline this request and is provided detailed information about what will happen to their information if they do allow it to be shared. The individual is also provided information about voluntary quarantine; how to carry it out, and how to get help if they need in order to avoid breaking their quarantine. They can indicate in the app that they have placed themselves into quarantine, which then allows the local health department and the WHO to monitor self-quarantine trends.

If the individual agrees to the provision of the **Exposure Profile**, the information is assembled and uploaded to the **Cloud Service**. The **Cloud Service** determines a list of all **Flu ID**s that may have potentially crossed paths with the affected individual – i.e. those devices that have subscribed to alerts for the same **geohash** location, and the same one-hour time band (plus possibly the next one-hour time band to account for inaccuracies across the hour boundary). Push requests are automatically sent to these devices advising them to contact the service for an update. The devices automatically then contact the service with their latest **subscription request**, and in response the **Cloud Service** sends any **exposure profile**(s) that need analysis to these devices.

## Exposed Individual Determination (Automated Contact Tracing)

On these devices that have received **Exposure Profile**(s) for matching, the device systematically compares the received exact location and time information, plus the received Bluetooth identifier(s) of the affected individual, to the historical record saved on that device. An **Exposure Profile** with no overlap in location and time is discarded. An **Exposure Profile** with some overlap i.e. a match for location and time is then used to generate an **Overlap Record**. A request is sent to the **Cloud Service** for the associated **Case Profile** to be provided, plus to record this **Flu ID** as a potential contact for the case, and requesting any specific updates related to the source **Case ID**.

This will contain details of the overlap, an estimate of the exposure risk involved; and the **Case ID** number of the exposure individual for purposes of transmission chain calculation. The risk calculation takes into account whether there is any Bluetooth proximity matching, for how long, and what level of proximity; plus the infectivity information within the exposure profile. All **Overlap Records** from this calculation are combined, and a report of potential individual exposure is generated. The user then receives an alert to review this exposure information if the generated estimate is moderate risk or greater. Note that all of the above calculation may be intensive for the personal device involved, so this would most likely be best performed when the individual is asleep, and their device is connected to power; the individual would then receive this information when they wake. Note also that information about the exposure individual’s movements, or other potentially identifying information, is never presented to the alerted individual, and the entire Exposure Record is deleted, leaving only the matched information copied into the Overlap Record on the device.

When an individual receives an alert that they have had a moderate or greater risk of exposure to novel coronavirus, it is important that as much as is possible this alert does not engender panic. Information must be immediately available about the specific exposure detected (location, proximity (if known), length of time, infectivity of the other individual(s)) but not information that deliberately identifies who they were exposed to. Thus, the app generates an exposure risk report, and provides suggestions/options; such as increased symptom vigilance, decreased contact measures, and voluntary self-quarantine. If the individual is participating in symptom monitoring and anonymous statistics, the app can also upload the summary of estimated exposures, and individual’s current self/community mitigation status.

## Community Detection + Response Improvements

Should an individual who has a known exposure develop symptoms, this should be flagged to the local health department as a priority case for investigation. The **Cloud Service** retains a record of all **Flu IDs** that have self-declared they are potentially exposed. The aforementioned screening process for the known contacts could also be instituted automatically, or after manual review.

Should there be specific information to disseminate to all potential contacts of a specific case, a message would be able to be pushed to all of these individuals’ apps.

Should a health department detect a concerning pattern of illness, the department should be permitted to push an alert to all devices currently or recently in a particular region advising increased vigilance or other controls. The alert should allow the individuals to open a website to read further information.

Functionality available to local health departments should include:

* View local case distribution
  + Symptomatic only
  + Probable case – by case definition
  + Confirmed cases
* Manage Potential Cases
  + Enable/Disable automatic contact tracing of potential cases
  + Set public health screening capacity
  + Design pathology request form template
  + Configure FHIR integration
* View individual Case Record
  + Exposure Profile: heat map and detailed log of exposures, plus a timeline of infectivity score
  + Manage testing requests
  + Manage test results
  + View potential contacts
    - Click through to view other individual cases, where these contacts have registered symptom onset and thus created a Case Record
  + Message potential contacts
  + Message symptomatic contacts
* Message Community
  + Send message(s) to all individuals in a geographic region

Functionality available to individuals within their apps should include:

* View Location and Contact History
  + Email / print record
* Report and Track Symptoms
  + Enter symptom onset date
  + Answer health questionnaire
  + Update severity
  + Select individual prevention strategies employed (eg. handwashing, mask, decreased contact with others)
    - Commence and complete voluntary self-quarantine
  + View and print pathology request(s)
  + Check pathology results
  + View Case ID and QR code
* Family Options
  + Add dependent child(ren)
  + Add schools, year level, and classrooms
  + Exclude attendance over date(s)
  + View alerts for attended schools
* View Status
  + Nearby population incidence
  + Community alert level
* Privacy
  + Location, Bluetooth, Activity, Alert, Cloud interaction permissions
  + Exclude data collection in location(s)
  + Delete on-device data: particular geographic region, particular time period, or all
  + Subscribe from cloud service
    - Resuming this allocates a new **Flu ID**
* Hygiene Alerts
  + Enable / disable / frequency

# Special Populations

## Families

As young children will not often have access to a personal mobile device, an adult should be able to add their children to their own app. The app should also be able to collect the school of enrolment and class name, and to be able to record whether school has been attended or not for each child on each school day (with the default being attended). This could be used for symptom monitoring and quarantine information, and also be used to send alerts if the local health department identifies a particular school, and/or class(es), as having sustained a significant exposure risk.

## Residential Care

As the elderly or infirm will often not have personal mobile devices, this application will not be able to function the same way. However, as the physical location of most residents remains quite static, alerts would be able to be delivered if a confirmed case visited a facility whilst symptomatic. The **Flu Smart** app could have a separate mode for residential facilities so that their management can receive an alert and be able increase vigilance and take other preventative measures in their population.

# Privacy

The primary protection for well individuals is storing their detailed information on-device only. By uploading **geohash** location information in time bands, it is possible that an identifying pattern could be created, although the low precision of the information being uploaded is the primary defence. It should be possible for apps to upload some incorrect location/time data to disguise the real data if developers wish to pursue this.

To avoid unintended leak of information eg. to unauthorised implementations of the protocols for information exchange, technology vendors should implement their best existing solution for verifying the authenticity of the software that is being interacted with.

To avoid allowing malicious actors to receive large amounts of confidential location and time data, limitations should be provided on subscription to alerts. Subscriptions allowed should be physically possible eg. not request information from separate cities in the same consecutive time periods. In addition, subscription should be disallowed for example 36 hours after a time period passes.

To enhance control of the data, depending on final system design it may be possible to allocate separate ID numbers for anonymous status reporting, and alert subscription. It may also be possible to allow different cloud providers to handle the two functions; and/or to allow individuals to determine which cloud provider they use to subscribe to alerting (a named cloud provider or rotating amongst all options). Clearly, an exposure report submitted to a cloud provider providing the alerting service would need to be passed on to all other participating cloud providers for distribution to the subscribed devices.

## Individual Privacy Control

Individuals have a clear voluntary participation role in this system. Apps should consider implementing limitations on the duration that consent can be provided for ongoing data capture and sharing features.

# Security Considerations

Information about message exchange between devices and the **Cloud Service**(s) must be encrypted end-to-end, and secondary identifiable information for example around IP addresses should be discarded once messages have been exchanged.

Information stored in cloud systems should also be subject to regular purges, for example discarding alert subscription information after two weeks.

# Governance of system use

It is suggested that a central agency should determine and govern primary and secondary use cases for the data collected centrally – for example the World Health Organisation should oversee what is permitted to be persisted past the two-week cut-off.

Secondary uses that benefit the contributing communities – such as information on the burden of disease – should be shared publicly so it can be given back to those that have contributed.

## Defence against System Misuse

Should a health department or government attempt to use the system to unfairly target individuals or communities, instead of aiding them, the World Health Organisation must have the ability to revoke access to the central systems whilst diplomatic discussions can take place. It is understood that some measures taken by governments in these times may appear extreme but are ultimately for the good of the broader community.

It is possible that individuals may attempt to misuse the system in order to falsely simulate an increased burden of disease. The main control against this is that in order to report a case, the individual must upload their location and Bluetooth data; many individuals wishing to misrepresent themselves will not want to share this information. If a local health department makes a decision to allow automated contact tracing without confirmed COVID-19 diagnosis, the chance of this misuse is increased although may not be a significant impost compared to the impact on public health already being experienced to trigger the decision.

# Responsive Design

Assumptions and settings provided in the system, such as the 2 week quarantine period, should be a downloadable setting to allow for centrally managed changes to this without requiring endpoint upgrades. In addition, it should be possible to send an alert to all subscribed devices that an upgrade of their app is required to improve functionality, in the case that the app does not automatically update through existing app distribution mechanisms.

Iterative improvements are to be expected in all areas, and a focus should be ensuring that the health departments can deal with the demands they will be experiencing – the system should ensure that it prioritises the efficient management of a high demand scenario.

# System Creation

If this system is to be designed, assembled and implemented promptly, a large amount of cooperation and investment effort amongst technology leaders is required.

The following services will be required:

* Project management and coordination
* Experts in infectious diseases and emergency management to confirm the use cases
* Technical and Functional specification development, including data protocols
* Cloud hosting development and implementation
* Client application development and implementation
* Interactive cloud portal for health departments and allocation of access by the World Health Organisation
* Data collection of regional health department online resource links and phone numbers to be provided to individuals should they need assistance within their apps

The implementors of the client applications should remain separate from the cloud hosting providers to ensure the balance of individual privacy protection. The main platform vendors (ie. Apple, Google & Samsung) should create the client applications themselves as they have the most expertise and will be able to give the client applications elevated permissions if their platforms require this in order to implement the required features.

The following would be reasonable extensions for development after implementation

* Systems for integration of pathology requests and results, eg. using HL7 FHIR
* Ability to integrate with local health department software platforms
* Analytics of anonymous data and publication of summary information for the public

The following non-exhaustive list of technology leaders should be approached to assist

* Apple
* Alphabet/Google
* Samsung
* AWS
* Microsoft
* IBM
* Health Level 7
* A leading technology project management firm

# Funding

Technology firms should strongly consider contributing their services for the greater good; certainly, better control of the global spread of this disease will result in improved economic performance and relatively more purchase of their goods and services than if the disease spread unchecked. In addition, providing the app and service to their employees will increase community confidence and may provide a more effective control over staff sick leave; especially the appropriate use of leave avoiding other staff members from becoming unwell.

It would not be advisable to ask the general public to fund the system through purchase of the application or through provision of service; as the service’s strength will be when a large proportion of the population is participating.

# Version Control

|  |  |  |
| --- | --- | --- |
| Date | Author | Change |
| 14/2/2020 | Hamish Rodda | Initial idea conceived |
| 24/2/2020 | Hamish Rodda | Initial documentation |
| 25/2/2020 | Hamish Rodda | New idea for residential facilities. Add details of Flu Smart app capabilities |

# Glossary of Terms

**SARS-CoV-2**: The novel coronavirus first detected in Wuhan, China

**COVID-19**: The disease caused by the novel coronavirus

**Geohash**: An efficient approximation of a location; the geohash algorithm with precision 5 provides a location which is +/- 2.4km in accuracy

**Flu Smart**: A preliminary name for the proposed system to allow

**Individual**: A person participating in the Flu Smart system

**Flu ID**: A unique identifier automatically assigned to each individual’s personal mobile device by the cloud platform. This number is only used to allow communication between an individual’s device and the cloud platform.

**Exposure Profile**: A list of an individual’s presence at specific GPS locations, with start and end date/times; plus all Bluetooth identifiers encountered at that location, the and the duration of time in each band of proximity (as possible), plus the **Case Profile** and **Case ID**

**Case Record**: The date and time of symptom onset, list of symptoms, and progression of symptoms, with particular focus on aspects that suggest high infectivity

**Case ID**: A unique identifier automatically assigned to a self-reported illness

**Overlap Record**: A combination of a healthy individual’s exposure profile and an infected individual’s exposure record, resulting in a time period, proximity of exposure

**Incubation Period**: the sensible maximum reported time between exposure to an infectious agent, and the development of clinical disease.