Research Report

Data-Driven/App-enabled Pandemic Responses: Data Protection Issues, Risks, and Recommendations

Version Control

Version	Date	Changed By	Comment
1.0	2020/03/30	Daragh O Brien Katherine O'Keefe PhD Peter Davey	Consolidation of research into final report format.
2.0	2020/04/23	Daragh O Brien	• Updated to broaden from Irish market focus • Updated Contact Tracing Use Case to incorporate latest developments; • Updated to reflect EDPB guidance • Added reference to remote monitoring • Updated to include references to latest Apple/Google API design • Updated to include reference to Germany adopting DP-3T based solution • Updated to include references to OpenTrace calibration testing • Report retitled to reflect broader scope
2.5	2020/04/26	Daragh O Brien	• Updated to include reference to Germany adopting DP-3T based solution • Updated to include references to latest Apple/Google API design

Contents

Acknowledgements

As with the first edition of this report, we acknowledge the early input of independent experts such as Phil Booth in MedConfidential, Pat Walshe of Privacy Matters, and others.

In this edition, I would like to acknowledge the various academics and researchers who have contributed to the rapid evolution and development of frameworks in this space, in particular for contact tracing. I would especially like to commend those consortia who have adopted a high level of transparency in their publication of materials and their response to questions and their willingness to discuss pros and cons of their proposed approaches and alternative technologies.

I would also like to thank Digital Rights Ireland for their insights on some topics.

Caveats

This report represents a 'best efforts' analysis of the current state of the nation as of the 22nd April 2020 when the desk research activity was concluded. Some additional minor changes were made based on information that became available on 26th April 2020.

It does not constitute legal advice and it will, by reason of the rapid evolution of the debate and research in these areas in response to Covid-19, contain errors, omissions, and gaps.

Where these are highlighted to us, every effort will be made to update and correct the analysis in a later edition of this report.

Furthermore, the conclusions and recommendations made are based on the information and analysis available to us at the time of writing. If the facts change, our opinions and recommendations may alter also.

Executive Summary

Castlebridge have prepared this research report for the purposes of supporting Data Protection Impact Assessment activity in respect of contact tracing apps and associated mobile device-based interventions in public health response to pandemic scenarios or other infectious disease outbreak scenarios.

Since the first edition of this research report, which focussed on the implementation of contact tracing in Singapore, there has been extensive further research in this area and critical assessment of the suitability of the technology approaches proposed. In addition, there has been the development of a number of frameworks for centralised and decentralised processing of Bluetooth identifiers to support contact tracing, and Apple and Google have collaborated on a technical API standard to address many of the operational issues that have affected previous generations of contact tracing apps from the dim and distant past of mid-March 2020.

Outline of Methodology

Castlebridge applied a variant of our Data Protection Impact Assessment/Ethical Impact Assessment methodologies to the analysis of a set of defined use cases derived from media discussion of various uses for smartphone/mobile phone data to support covid-19 response initiatives.

In doing so, we have drawn on our international network of experts in data protection, telecommunications, and clinical data study design, as well as individuals with personal experience of some of the applications discussed, to develop the best possible analysis. The business needs/use cases we identified for analysis in this report are set out below.

Business Need	Summary Approach
Identification of Close Contacts and support for contact tracing	Use mobile phone data (location or other) to identify close contacts and support contact tracing.
Provide symptom tracking and recording to support epidemiological data capture/analysis	Provide a smartphone app where users can log symptoms they are experiencing.
Notify individuals if they have had close contact with someone who has tested positive	Send push notification from smartphone app to notify the person who has been in close contact
To track population movements to support analysis/prediction of disease trends and effectiveness of containment	Use mobile phone data to identify movements people
Provide information to app users	Use push notification to give targeted information to app users

Summary of Conclusions and Recommendations

Our conclusions and recommendations are summarised below.

Contact Tracing

Since the first edition of this research report, which focussed on the implementation of contact tracing in Singapore, there has been extensive further research in this area and critical assessment of the suitability of the technology approaches proposed. In addition, there has been a rapid pace of development in respect of protocols to implement a technical approach to support contact tracing. Based on our review of the published information at this time, we recommend:

1) Pragmatism and clear management of expectations in respect to the effectiveness and accuracy of BT-LE as a means for measuring proximity. While it is better than other technologies and is potentially the most privacy preserving technology currently available, it is being implemented to do something the protocols were not developed to do and there are significant technical challenges that need to be recognised.

2) Adoption of a decentralised Exposure Notification/Contact Tracing application strategy based on DP-3T, with an intent to implement the Apple/Google API. It is our assessment that this provides the best balance against the data protection rights of individuals and the obligations of organisations. There is a clear roadmap for supporting interoperability across borders, and the mechanisms for processing apply the data minimisation principle and avoid disclosing the social graph of any individual. Additional data capture can be implemented at the application level, subject to a valid legal basis and a DPIA.

   With the implementation of the Google/Apple API as a decentralised exposure notification solution that addresses at operating system level many of the challenges regarding battery life and, in the latest iteration, accuracy of proximity calculations, it is difficult to see how a centralised architecture that cannot implement these features at an API level in their application could be implemented without challenges to user adoption.

   Furthermore, with a number of EU member states abandoning centralised architectures in favour of DP-3T based frameworks, future interoperability could become problematic for Centralised approaches.

3) Any DPIA should distinguish between the process of identifying Bluetooth Identifiers (what Apple/Google now term 'Exposure Notification') and the other potential data requirements of a contact tracing process. Consideration should be given to explicit use cases that define the business need and approach through the life cycle of the data.

4) The design of any application should consider the User Personas who will interact with it. Consideration should be given to the potential impacts on children, persons with diminished capacity, or other vulnerable persons.

5) Push notifications should be implemented with caution and in a manner that supports existing manual contact tracing but does not replace it. Consideration should be given to how inbound versus outbound calls to action will be implemented, and processes should be designed accordingly. Furthermore, any messages should be

6) The EDPB guidance on the requirements for contact tracing applications are quite clear and should be considered and applied in any DPIA. Note that this may require domestic legislation to give effect to appropriate safeguards for data and for fundamental rights.

   Applications should be voluntary, and any additional data processed must be for a specific and lawful purpose. Authorities should avoid any suggestion that an application is "mandatory but not compulsory" in the user experience that is being implemented.

7) Transparency is essential during the design and development of any application. Furthermore it is a key success factor in implementation and adoption by communities.

8) Contact tracing should preserve the "human touch" in design and execution of processes, particularly for vulnerable persons, children, or persons with diminished capacity.

9) A clear contact centre strategy is required. While inbound calling by individuals is the most privacy preserving, outbound calling may be a

more appropriate mechanism. Both bring with them issues. A potential solution is a hybrid model supporting inbound and outbound calling. Process design is an essential aspect of ensuring optimal outcomes.

Symptom Tracking

Symptom tracking apps provide a potentially rich source of epidemiological data relating to the progression of the illness. They may also provide data to help differentiate the symptoms of other commonly occurring illnesses from those of Covid-19.

There are potential issues of data quality in the context of self-reported symptoms and also consistency of completion of self-reporting which could impact the effectiveness of logged data.

We recommend that they be deployed as a "second wave" application in the context of contact tracing to support the management of close proximity contacts of infected persons. This will help reduce the "noise" in the data that is gathered and will enable causation and correlation factors to be more readily identified.

We also make a number of high level recommendations regarding the security of data in such applications.

We advise that self-reported symptoms should not be used as a trigger for exposure risk notification/contact tracing alerts due to the subjectivity of the data and the risk of it being maliciously abused. This increases the risk of "alert fatigue".

An exception to our recommendations regarding symptom tracking would be the use of clinically prescribed remote monitoring / telemedicine solutions to support diagnosed or suspected cases of Covid-19 who are self-isolating. We believe these have a potentially significant value in an overall system optimisation approach to the pandemic response.

Push Notification of Close Contact

It is questionable if the push notification of a close proximity contact to a person who has tested positive is **necessary** to protection the vital interest of the data subject or another or if it is **necessary** to pursue the public health objective.

It is also possible that push notifications could cause unnecessary distress to data subjects and, absent appropriate context in communication, could trigger

unexpected and undesirable consequences for third parties. Consideration should also be given to the risk of 'Alert Fatigue'.

In particular, the risk of sending a push notification to a child, or to a vulnerable person, cannot be ignored.

Push notifications should be a supplement to and not a replacement for existing contact tracing and follow up protocols. It is essential that the "human touch" is not lost.

Furthermore, consideration should be given to the "next action" that would be taken by persons in receipt of a push notification. Any action that results in a substantial increase in calls to local primary care facilities should be avoided. Likewise, if the call to action is to contact a central number, this must be adequately resourced to ensure callers are answered in a timely manner and ideally on their first attempt.

Analysis of Population Movement using Mobile Data

Analysis of population movement using mobile data represents a significant risk of mass surveillance and would require either processing on the basis of consent or the processing of anonymised data.

A range of very clear safeguards would be required to balance data protection and data privacy obligations against the objectives of processing this data.

It is important to note that the data is of insufficient granularity to support contact tracing but would, in an aggregate form, potentially support measurement of effectiveness of social controls on movement.

Push Notifications to App Users

Push notifications of a general nature to app users have a lawful basis either on the basis of consent or on the basis of processing in the public interest.

We would question the need for these to be implemented as part of an application or application framework and would recommend instead that an SMS subscription service where people can subscribe for general updates would be sufficient to meet the need of general communication.

Application Strategy

We recommend against the development of a single application to perform both multiple functions given the potential for complexity which may impact usability and acceptance of the application. Where such a strategy is adopted, there should be a clear application roadmap indicating what functionality will be enabled when and under what circumstances/in response to what triggers.

Ultimately any application must be seen in the context of the overall response system. In that context, any barriers to adoption should be minimised and explicit consideration should be given to how the applications interact with and support existing public health response processes such as contact tracing, testing, and hospital care.

Introduction

The information processing capabilities of mobile devices have increased significantly in recent years since the introduction of the App Store by Apple a decade ago. Today, app-based data capture can represent an efficient mechanism for engaging with citizens on a variety of topics.

Coupled with this, the near ubiquitous penetration of mobile phones means that mobile devices represent a potentially valuable source of data in the context of contact tracing and other public health functions. As mobile phones allow for a two-way flow of information between the data subject and the public health authority, they can also support the delivery of validated and authoritative information to individuals through official channels.

However, this potential must be put in context of an uneven distribution of technologies (e.g. smartphone versus "feature phone") and a variation of technical capability even within the context of the smartphone segment. It must also be considered in the context of the relevant legal and regulatory frameworks which exist to govern and protect data relating to individuals, their communications, or their location from misuse and abuse in a manner which might disproportionately impact their fundamental rights and freedoms.

Furthermore, more data does not necessarily mean more useful information. It is important that any increased information gathering or information sharing capability is focussed on informing right actions to prevent illness and support recovery in society as part of an appropriately evidence-based response.

Since the end of March there has been a growing body of research, development, and debate about the optimum approaches that can be applied to use data of various types to support pandemic response. This research paper will examine the data protection and privacy implications of several generic use case that have been identified. We also endeavour to summarise some of the recently published research and guidance in key areas to help inform decision making.

It is essential that the development and deployment of applications to process data in support of the pandemic response are not considered a panacea to the challenges of managing a pandemic response. They offer a potentially useful set of capabilities, but governments must ensure transparency as to the purpose, functions, and limitations of these technologies so as to avoid unfounded assumptions as to their capability.

Purpose of this Research Report

The purpose of this research report has evolved since the first iteration in late March 2020. The scope of the research is to consider the data protection and data governance implications of identified use cases for data-driven strategies for pandemic response, primarily relating to the use of mobile phone apps and data derived from mobile phones or their use, as part of an overall response strategy for Covid-19 or other pandemics. While the first iteration of this report focussed on the specifics of legislation in the Republic of Ireland, this iteration aims to address a broader audience.

In preparing this report we aim to inform data protection impact assessments, the definition of requirements and the implementation of functionality in smartphone applications to support public health responses to pandemic in a manner that will support:

1) The timely collection of quality information to support contact tracing.
2) The effective communication with affected persons of relevant information in a timely manner.
3) The effective management of cases to minimise the impact on healthcare systems
4) The establishment and maintenance of trust between the individual and the public health authority to ensure that there is a timely sharing of information to support decisions and inform actions to prevent illness and support recovery

To this end we have applied the Castlebridge Ethical Information Assessment Model to a series of defined “use cases” which may arise in the context of the use of different approaches to mobile data or apps. We also consider wider implications and considerations in respect of the safety and security of data subjects, and the protection of their wider fundamental rights and freedoms to ensure appropriate balance is struck.

Disclaimer

This report has been produced using the best efforts of Castlebridge and based on a review of the available research that was known to us and accessible to us at the time of preparation of the report. New research, information, or the specifics of the regulatory frameworks in a specific jurisdiction may affect the application of or relevance of findings in any specific context.

It does not purport to be, nor are we presenting this report, as legal advice.

Methodology and Approach

The methodology we have applied in preparing this report is adapted from the Ethical Impact Assessment/Privacy Impact Assessment methodology developed by Castlebridge[1]. This methodology applies a quality systems-based approach to the evaluation and assessment of data protection and information ethics risks in proposed processing of data.

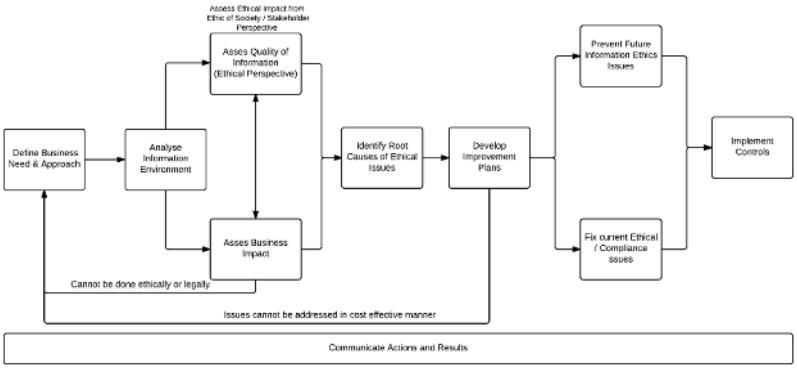


Figure 1 Castlebridge EIA/DPIA Framework

In this framework, the definition of Business Need and Approach is a critical first step which defines the Use Case for the processing activity against which the information environment can be assessed. Our framework allows for iterative elaboration of use cases and the consideration of alternate approaches in a structured and repeatable manner.

The Analysis of the Information Environment for the identified business need and approach addresses the context of personal data, legal and regulatory considerations, and the process environment relating to each Use Case.

In considering the process environment, Castlebridge applies a simple three stage life cycle for the end to end processing of data.

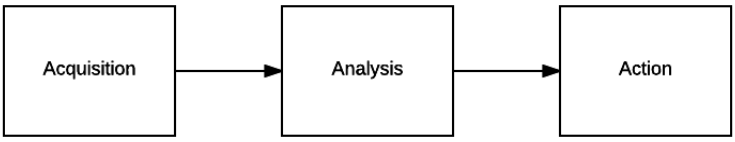


Figure 2 The Simplified Information Life Cycle

Based on our analysis we make recommendations for how data derived from or gathered through mobile devices and apps might best be used as part of a response strategy.

[1] Details of the methodology can be found in *Ethical Data and Information Management: Concepts, Tools, and Methods*, O'Keefe, Katherine, O Brien, Daragh, Kogan Page, 2018

Business Needs and Approaches

This section of our analysis has been updated to reflect the emergence of competing approaches to contact tracing applications, and the identification of an additional Business Need in the form of strategies to reduce demand on hospitals for the treatment of mild or suspected cases of Covid-19.

Identified Business Needs and Approaches

A "Use Case" reflects "the requirements of business processes, and business processes are supported by information systems and automated business processes" (Finneran-Dennedy, Dennedy, & Fox, 2014). In the Castlebridge methodology, we term a high-level use case a "Statement of Business Need and Approach".

A structured "problem statement" template[2] is defined for each use case which captures, as completely as possible, a statement of the proposed processing, the purposes for the processing, and the identified benefits to data subjects and to the organisation proposing the processing activity.

The identified use cases for review in this report are set out in the table below:

Business Need	Summary Approach
Identification of Close Contacts and support for contact tracing	Use mobile phone data (location or other) to identify close contacts and support contact tracing. This may be implemented as a centralised or decentralised model.
Provide symptom tracking and recording to support epidemiological data capture/analysis	Provide a smartphone app where users can log symptoms they are experiencing.
Notify individuals if they have had close contact with someone who has tested positive	Send push notification from smartphone app to notify the person who has been in close contact
To track population movements to support analysis/prediction of disease trends and effectiveness of containment	Use mobile phone data to identify movements people
Provide information to app users	Use push notification to give targeted information to app users

The identification of business need should be an essential precursor step to the adoption of technology solutions such that the requirement and level of tolerance for technical constraints can be clearly evaluated and understood.

[2] This template is based on the framework set out in Chapter 4 of (Finneran-Dennedy, Dennedy, & Fox, 2014) and Chapter 10 of (O'Keefe & O Brien, 2018)

Analysis of Needs and Approaches

We conducted a review of the business needs and proposed approaches described above. For each use case we followed the standard DPIA/Ethical Impact Assessment approach used with Castlebridge clients.

Business Need #1: Contact Tracing

Since the first iteration of this report, which focussed on the development of the TraceTogether application in Singapore, there has been a significant wave of developments in the adoption and evaluation of contact tracing applications in a number of jurisdictions. We have also seen the emergence of competing models for standard frameworks for contact tracing using mobile phone technologies in either a centralised[3] or decentralised[4] mode of operation.

In addition, there has been a substantial amount of guidance and other supporting documentation published by both the EU Commission[5] and the European Data Protection Board[6] [7] in recent days which reaffirm the broad parameters that need to be considered and applied when considering applications which operate within an EU member state or a jurisdiction that applies EU data protection principles in their domestic legislation.

Finally, there has been the announcement from Google and Apple[8] of the development of a draft technical specification and framework API to enable the use of Bluetooth LE without some of the limitations identified in earlier applications such as Singapore's TraceTogether application.

In this section of the report we will provide a summary overview of the current state of the nation in relation to the different approaches and the issues, risks, and opportunities that arise in the context of these types of applications.

In the context of the analysis for this report we have limited our research to the use of applications based on the Bluetooth LE technology.

---

[3] https://en.m.wikipedia.org/wiki/Pan-European_Privacy-Preserving_Proximity_Tracing
[4] https://en.wikipedia.org/wiki/Decentralized_Privacy-Preserving_Proximity_Tracing
[5] *Mobile Applications to support contact tracing in the EU's fight against Covid-19: Common EU Toolbox for Member States v1.0,* EU eHealth Network, 15th April 2020
[6] *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 Outbreak,* EDPB, 21st April 2020
[7] *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the Covid-19 outbreak,* 21st April 2020
[8] *Privacy Preserving Contact Tracing,* Google, Apple, April 2020
https://www.apple.com/covid19/contacttracing/

Statement of Business Need and Approach

Proposed Processing Activity (What we propose to do)	To process information about the proximity of smartphone users to other individuals using data derived from smartphone to support contact tracing
For the Purpose of	So that close contacts of individuals who have tested positive for Covid19 can be identified quickly and accurately for the purpose of testing and isolation
To achieve benefit (to the organisation)	• To improve speed and accuracy of contact tracing • To reduce potential span of population which may be infected through follow-on contact infection • To allow for more timely testing of potentially infected people
To achieve benefit (to the data subject)	To protect the vital interests of the data subject or others through more efficient use of public health resources

Approach

The key functional requirement identified here is the collection of information relating to close contact between individuals to identify and alert who may have been exposed to COVID-19. As such, the key to quality data required to fulfil the goal is the ability to identify and trace proximity and duration of contact between individual regardless of their geographical location, and to enable communication with individuals who have had close contact with people who have tested positive for COVID-19.

Irrespective of whether the application is using a decentralised or centralised model for operation, the consensus on the underlying technology has shifted towards the potential application of Bluetooth Low Energy (BT-LE) as a protocol for measuring the proximity of individuals. The duration of that contact can then be derived by measuring the time between the first and last logged interaction between two devices.

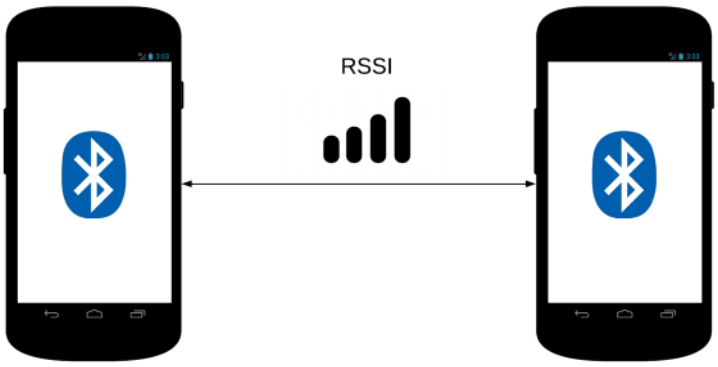


Figure 3 Bluetooth Signal Strength as Proxy for Proximity

Analysis of Information Environment

In analysing the information environment for BT-LE contact tracing applications we have reviewed the various framework approaches and the available information on applications that are proposed in some jurisdictions in the context of the three-stage information life cycle described earlier in this document. This allows us to consider the process, technology, regulatory, and social implications of the application of different implementation approaches through a common lens.

Categories of Data Subject in Scope

The categories of data subject in scope for the proposed processing are:

1) Smartphone app users
2) People who are in close proximity to smartphone app users

Categories of Personal Data in Scope

The categories of personal data that are in scope within the application are:

- Proximity to other devices (based on Bluetooth relative signal strength)
- Pseudonymised identifier for app users.

In addition, depending on the mode of implementation or the specifics of any application for implementation, the personal data in scope for contact tracing may also include, for example:

- Mobile phone number for users
- Non-pseudonymous identifiers for users
- Age of the user
- Name of the user

Note that self-reported symptom data is not considered as part of this use case other than as a potential trigger (arising from the Analysis phase) of an Action (a notification or other outcome).

Information Life Cycle Analysis

Applying the three-stage life cycle model to the analysis, a number of issues potentially arise. However, it is necessary to provide a brief overview of the different approaches that currently appear to be in discussion as a basis for these kinds of contact tracing applications.

Overview of Approaches

A range of approaches have been proposed over the past few weeks to enable BT-LE to be deployed as the basis for a contact tracing tool. It is important that

the differences between the approaches are understood. Likewise, it is important to distinguish between an application, a framework, and an API for the purposes of this analysis.

- An **application** is the instantiation of software installed on a device, along with any supporting back-end or server-side components necessary to make the application work.
- A **framework** is a design schema or specification defining the architecture, functions, and processing actions that would be implemented in an application. It establishes foundational design principles and priorities.
- An **API** is an application interface sitting between the Operating System on a device and an Application which 'pre-packages' certain features or functionality in a standardised manner eliminating the need for application developers to develop bespoke code to achieve those objectives.

Common Aspects

Both centralised and decentralised approaches to BT-LE proximity tracking rely on the use of pseudonymised "Ephemeral IDs" which the apps broadcast as a type of "beacon", and on-device logging of identifiers which are encountered by app users as they go about their day to day activities.

These Ephemeral Ids are generated from the Bluetooth

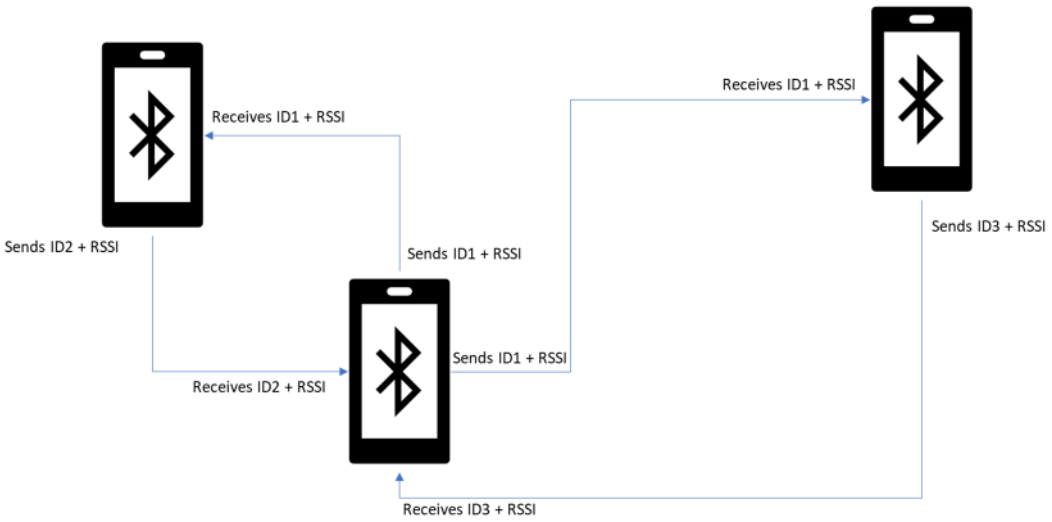


Figure 4 Simplified Common Approach to Ephemeral ID sharing and Proximity Finding

These Ephemeral IDs broadcast from devices that are detected as being in proximity are recorded and stored on-device with a calculation of the duration

that they were in proximity. The Ephemeral IDs are pseudonymised using a randomly generated seed or a centrally generate encryption key.

As these apps record based on the proximity of a device, they do not need to record the location data from the device (e.g. device GPS) and, as such, are not processing location data of the device which could be associated with the user. This non-recording of location data provides a work-around for the restrictions on the processing of location data in Article 9(1) of the ePrivacy Directive (Directive 2002/58/EC).

However, as data is being written to devices, it does fall within the restrictions of Article 5(3) of the ePrivacy Directive and, as such, consent is required where the processing is not necessary the delivery of an information society service requested by the user. In this context it is important to consider if the logging of close proximity contacts as part of a pandemic response constitutes an "information society service" under EU law. This term is defined in Article 1(2) of the Technical Standards and Regulations Directive (Directive 98/48/EC) as being a "service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

It is not clear that a contact tracing service would fall within the scope of being an Information Service under Article 5(3) and therefore, notwithstanding any other lawful basis that may apply to the processing of personal data under GDPR, consent would be required for the storage of data on-device. This consent, however, could be demonstrated by an affirmative act of downloading the app or through the permissions management in the interaction with the operating system on the device.

The Apple/Google API

The Apple/Google initiative is an API (or set of APIs) to allow applications to interact with the Bluetooth layer in the Operating system on devices in a different way. This removes the requirement for apps to remain running in the foreground and provides a standardised way for contact tracing applications to interact with the Bluetooth stack on the devices to obtain identifiers that are pseudonymised using a rotating ephemeral id that changes every 10 to 15 minutes. This mitigates against linkage-based attacks through reidentification of individuals from their device identifiers.

It is important to note that the Apple/Google API does not perform contact tracing but provides a basis for Exposure Notification based on the recording of Bluetooth beacons with an Ephemeral identifier[9].

[9] https://www.apple.com/covid19/contacttracing/

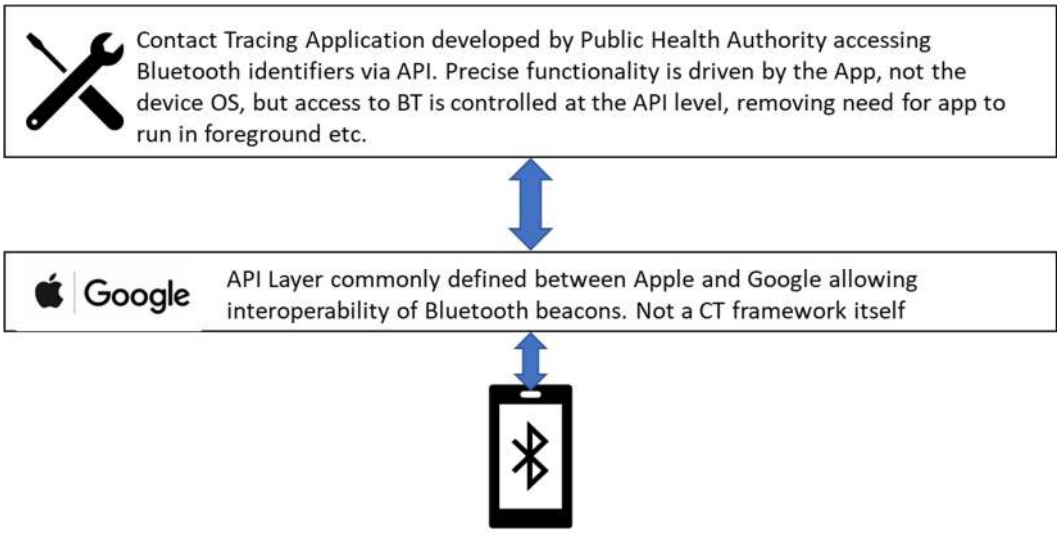


Figure 5 High Level Conceptual View of Apple/Google Framework

In the event that an individual has a positive diagnosis for Covid-19 and enters that fact via the Public Health Authority app, this will allow the upload of the identifiers logged for his device to the public health authority, who then publish that list to their app[10] installed on other users' phones.

In the Apple/Google API, the comparison of this list is performed on-device and, if the identifier of the positive diagnosis app matches any of the identifiers logged on another user's application, they will receive a notification through their app.

The Apple/Google API does not define or prescribe any form of operation by a Public Health Authority contact tracing application, and therefore does not appear to constrain the development of apps that capture additional information from users for the purposes of the contact tracing functions in that jurisdiction.

The implementation of the API does require light-weight server-side capabilities to be provided by the Public Health Authority to support diagnosis verification (e.g. the use of an authorisation key to verify a reported diagnosis is not fraudulent) and also to hold the repository of uploaded Ephemeral keys for infected persons.

A key data protection enhancing control within the Apple/Google Framework is that it is a curated API which will only be accessible by approved public health authorities and cannot be accessed by any other developers. Furthermore, it is part of the Apple/Google governance for this API that access to it would be turned off within jurisdictions when the pandemic/epidemic has ended.

[10] https://re.livecasts.eu/webinar-on-contact-tracing-applications at approximately 1hr 5 minutes in.

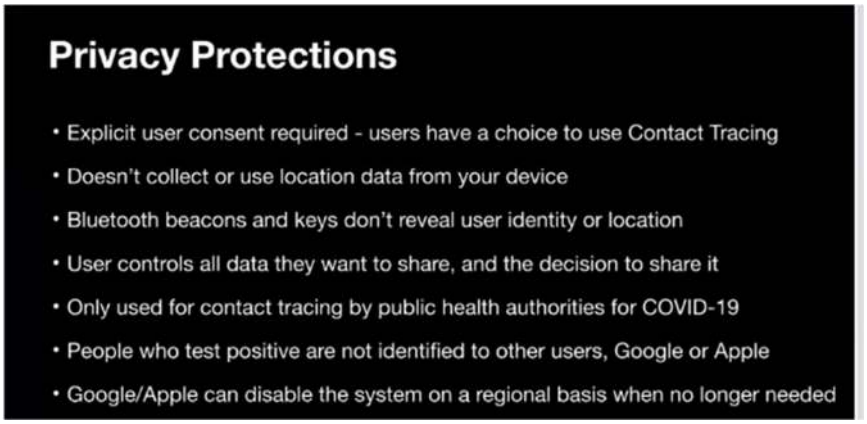


Figure 6 Screenshot from presentation given by Gary Davis, Apple, 24th April 2020

A key focus of the Apple/Google API initiative is to support platform and geographic interoperability for Bluetooth enabled contact tracing.

The current timeline for deployment of this API is for prototype API to be delivered to developers in early May with a full deployment to devices running Android 6.0 and higher or iOS 13 or higher.

It is not mandatory for apps to use the Apple/Google API to deliver a contact tracing application. As such, this does not prevent the deployment of applications that operate in a centralised model but it may affect the efficacy of centralised model applications due to the identified power management issues of Bluetooth on certain devices.

Apple/Google have identified the introduction of cross-border interoperability as being a requirement of the API currently in development, which draws heavily on the DP3-T framework.

Apple/Google identify the impact on battery life as being a potential barrier to adoption of contact tracing applications as if the use of Bluetooth runs down the battery it may result in users turning off the application or turning off Bluetooth, reducing the effectiveness of BT-LE solutions for contact tracing.

Centralised Framework Specific Aspects

Centralised contact tracing frameworks, such as Singapore's TraceTogether or applications based on the PEPP-T[11] framework. Other frameworks that have emerged in recent days include the ROBERT framework[12] which is being proposed as the basis for contact tracing in France and Germany and appears to be based on the PEPP-T framework.

The key characteristic of a centralised contact tracing framework is that:

- Applications upload the entire data set of identifiers that the user has been in proximity with to a central server
- The server decrypts the pseudonymous identifiers to match against data shared from other users
- The risk calculation is performed on the server-side and the result of that calculation then triggers a required action (e.g. push notification to an app user)

The ROBERT framework also explicitly references the interoperability with other jurisdictions operating a similar centralised protocol, allowing for cross-border operation of contact tracing. However, this is dependent on the specific implementation of the framework in a particular application. Furthermore, the PEPP-T framework has not defined formally the mechanisms for interoperability at this time.

Among the concerns and criticisms raised in respect of centralised contact tracing applications is the ability of the State (via the Public Health Authority) to develop a detailed map of an individual's social graph, with potentially significant impacts on the privacy and data protection rights of individuals.

However, this risk should be considered as a feature of the approach that has been taken by centralised solutions to solving the problem of speeding up the provision of information to individuals and to public health authorities which results in the emphasis being placed on securing the server-side and "official-side" of the process from malicious action or data breach.

A more pertinent criticism of a centralised solution, which is highlighted by the EDPB in their guidance on contact tracing applications, is that, by design, they are less able to comply with the data minimisation principle in GDPR with

[11] The PEPP-T framework was not reviewed in detail for this research due to the low level of transparency of publication of information about this framework. We also note a significant exodus from this group over recent days arising from the perceived issues with transparency and accountability.

[12] https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_0.pdf

respect to the data that is transferred to Public Authorities as they require the upload of *all* contacts logged on a device to the central authority. This also raises issues in the context of necessity and proportionality as it may not be *necessary* to process data in this way to meet the public health objective. A key consideration in the context of GDPR compliance is comparison with the "state of the art" as required under Article 25 of GDPR .

This issue also arises in the context of the provision of data to epidemiologists as it may require the centralised solution to provide data of all

As such, centralised models may fall foul of the requirements under Article 25 of GDPR, particularly in the context of technical approaches which better align with and implement data protection principles.

Decentralised Framework Aspects

There are a variety of decentralised frameworks proposed, but they operate on a broadly similar basis. The currently prevalent decentralised solution proposed in Europe is the D3P-T framework developed by a consortium of academics from computer science, law, and epidemiology. As mentioned earlier, the Apple/Google Framework is developing an API layer that follows a decentralised model.

The general characteristic of decentralised model is that operates as a peer-to-peer data exchange of the "ephemeral identifiers" between devices that are in proximity to each other. A log of identifiers that are received and identifiers that have been sent is held on-device. When a user receives a positive test (or a probable diagnosis), their app sends the list of all identifiers that they have broadcasting to the central server. These identifiers are then broadcast to other users of the app and the list of "infected" ephemeral identifiers is then matched on the device and risk calculations are performed locally and the application then triggers any appropriate notifications to the user.

Decentralised approaches minimise the amount of data that is being processed or transferred and minimises the need for a Public Authority "server-side" involvement beyond:

1) Providing a mechanism to validate / verify a diagnosis (to mitigate risk of false reporting).
2) A repository server for reported "infected identifiers" which are broadcast to other phones.

There is nothing in the design of a decentralised model for contact tracing that prevents the application layer (the part that a user would interact with) capturing additional information about the user for use in the Contact Tracing

process. While the processing of the proximity protocol data is decentralised, once an appropriate trigger event arises (e.g. an identification of a close proximity contact) the Public Health Authority can trigger the processing of other data (e.g. some basic patient information for the purposes of a contact from a public health doctor or contact tracer). Any such processing would need to be executed in compliance with the principles of necessity and proportionality and in line with obligations under GDPR.

A decentralised framework avoids the issues of potential social graph exposure as only the identifiers of the infected person is shared with the central server. As such, no data is generated that allows for the mapping of contact relationships between people at the server-side.

Furthermore, the DP3-T protocol can support interoperability through the identification of countries that users have visited (based on GPS co-ordinates or mobile carrier information which is available from the device). This allows an application built to the DP3-T standard to:

1) Upload the user's identifiers to another country's backend if the user reports they are infected, allowing their identifiers to be downloaded to apps in the other country
2) Applications can poll the server in other countries to download lists of infected identifiers to process on-device and calculate risk scores etc. as would be done in a single country implementation.

The interoperability would be managed through a configuration file in the application that would contain the addresses and connection details of the relevant servers, allowing for countries to be added easily.

It is notable that a number of EU countries previously promoting the adoption of a centralise model for identifying close contacts have, as of the 26th of April 2020[13], shifted their focus to a decentralised solution based on DP-3T.

Acquisition

As outlined above, data is acquired through the exchange of pseudonymised identifiers over a Bluetooth radio signal in which each device acts as a beacon. There is fundamentally no difference between the Centralised and Decentralised approaches in this context. The Apple/Google API represents a method for the technical implementation of this data acquisition.

[13] https://www.reuters.com/article/us-health-coronavirus-europe-tech-idUSKCN22807J

The proximity of devices is inferred from the RSSI (Radio Signal Strength Indicator) value for the Bluetooth beacon detected by a device. This is used to calculate an approximate distance between the devices.

When an individual registers a positive test result or diagnosis, the data is processed onwards as described above in the description of the Centralised and Decentralised approaches.

Legal Basis

The legal basis for processing data broadcast or transmitted in this context is set out below:

Legislation	Legal Basis	Comment
GDPR	Article 6(1)(e)	This requires the processing to be necessary for a public interest function.
ePrivacy Directive	Article 5(3) – Consent is required	Data is being read from/written to a device connected to a public communications network for a purpose that is not an information society service.
GDPR	Article 9(2)(a)	Explicit Consent will need to be obtained for the sharing of contact data with epidimiologists. In some jurisdictions, there may be a legislative basis for this processing as well allowing Article 9(2)(h) or Article 9(2)(i) to possibly be relied on as well, but DP3-T framework requires double opt-in consent

In terms of the freedom of choice of individuals in using the application, the fact that an application must be downloaded and installed on a device constitutes a meaningful and transparent choice but only in circumstances where the installation of the application and its use to gather identifiers is freely given.

Furthermore, the operation of the application requires revocable consent to be given in the mobile device operating system to access functions such as the Bluetooth functionality and also on-device storage. Therefore, consent must be obtained and it can be withdrawn even temporarily through on-device controls.

While jurisdictions may have enacted legislative powers that would give a legal basis for the adoption or use of an app such as this, an important factor in adoption is the maintenance of trust between individuals and public health authorities. Therefore, the reliance on statutory powers to enforce the use of such an application should be considered carefully given the potential impact on wider public health surveillance activities (e.g. sexually transmitted diseases) which require a high degree of community trust in the confidentiality of the processing of health-related data so as to avoid deterring reports of disease.

This requirement for a voluntary aspect to contact tracing applications is explicitly referenced in the guidance from the European Data Protection Board

issued on the 22nd April. Therefore, it is highly questionable whether any "mandatory but not compulsory" approach to implementation of a contact tracing application would be considered compatible with EU law.

The legal basis for processing other data that might be obtained by a specific instance of an application would need to be assessed in the context of the purpose that that data would be used for and also the trigger for requesting that information. We would recommend that no data be shared off-device to the public health authority until clear trigger criteria have been met, but there may be justification for capturing data on-device such as:

- Age of the user (to ensure children are not contacted in appropriately or to ensure appropriate guidance is provided)
- Whether they share a common party wall with a neighbour (e.g. living in a flat or a semi-detached house).

A DPIA would be required for the specific application design to validate the compliance of any supplementary data capture and it is outside the scope of tis report to comment further on that.

Analysis

The analysis action of the processing activities for the purposes of contact tracing takes place either on-device in the case of decentralised processing or on-server in the case of a centralised framework. In addition, data may be sent to epidemiologists for scientific research purposes based on the consent obtained during the setting up of the app.

Centralised Framework

In a centralised framework the upload process sends all the identifiers for people who an infected person was in contact with to the server. Risk scores are calculated on the server based on the criteria defined by the Public Health Authority for risk.

This does not comply with the data minimisation principle under GDPR as it is not *necessary* for the purpose of tracing contacts with an infected person for the data of all identifiers that they have had contact with to be transferred to the central server. It is likely that the majority of identifiers that are uploaded will not match the risk profile that has been set and, therefore, this constitutes excessive processing. This point is alluded to in the EDPB guidance on Contact Tracing applications where they note that decentralised solutions are better able to comply with the data minimisation principle.

This data minimisation challenge also arises in the context of the transfer of data to epidemiologists where, absent formal controls on the server-side of the

centralised framework implementation, a proportion of the data that will be transferred will not relate to persons who have been in contact with infected persons. This may actually have a negative impact on the usefulness of the data for epidemiological studies due to a high volume of irrelevant data.

Legal Basis

The legal basis for performing the analysis of data in this context is:

Legislation	Legal Basis	Comment
GDPR	Article 6(1)(e)	This requires the processing to be necessary for a public interest function.
ePrivacy Directive	Article 5(3) – Consent is required	The uploading of data from the device requires consent under ePrivacy Directives. This will usually be part of the verification process and should be stated processing purpose.
GDPR	Article 9(2)(c) 9(2)(h) and Article 9(2)(i)	The processing of data for the purposes of contact tracing is addressed under these provisions. However, necessity remains a key issue and it is unclear how the processing of data of uninfected people is necessary for the purposes of contact tracing

As identified above, there is a significant question whether the processing of data relating to persons who are not infected as part of the upload and analysis process is strictly speaking necessary for the purposes of contact tracing.

Decentralised Framework

In a decentralised framework, once a user reports a confirmed diagnosis, only their ephemeral identifiers (and the other ephemeral identifiers they have broadcast over the preceding number of days) are uploaded to the server. Those identifiers are then loaded to other user's apps and the risk calculation processing happens on-device.

This means that only the identifiers of people who are infected are shared and processed. This is in keeping with the data minimisation principle under GDPR.

In the context of sharing data with epidemiologists, the fact that the data that is transferred is limited the people the infected person has had close contact with, as determined on-device, reduces the potential risk of non-relevant data being transferred for processing by epidemiologists. The DP3-T framework sets out a clear methodology and protocol for extracting and transferring data for epidemiological analysis purposes that has started from a *de minimis*

position and is explicitly being developed out with epidemiologists to ensure that the data minimisation principle is respected.

Legislation	Legal Basis	Comment
GDPR	Article 6(1)(e)	This requires the processing to be necessary for a public interest function.
ePrivacy Directive	Article 5(3) – Consent is required	The uploading of data from the device requires consent under ePrivacy Directives. This will usually be part of the verification process and should be stated processing purpose.
GDPR	Article 9(2)(c) 9(2)(h) and Article 9(2)(i)	Different EU member states may have specific legislation providing a range of powers to public health officials to request and process data subject to appropriate safeguards in addition to the GDPR provisions.

Action

The "Action" phase of this Information Life Cycle relates to the action that is taken by the Public Health Authority, either directly (through an action of a human actor) or indirectly (through the operation of the application) once a close proximity contact has been identified and a user of the application is identified as being at risk of infection.

These actions essentially fall into three categories:

- Outbound call by Public Health Authority (similar to manual contact tracing)
- Push notification for a call
    - to trigger an inbound call to the Public Health Authority or;
    - to trigger a process within the app for the user to provide information to the Health Authority to phone them
- Push notification for information
    - Advice to self-isolate
    - Advice on next steps to take (e.g. installing or activating symptom tracking functionality in the app)

The details of the push notification processes will be addressed in Business Need #3.

Common Aspects

The common aspects of this processing activity between both the centralised and decentralised models are that the output of the analysis phase will have identified a risk profile. Depending on the nature of the containment strategy implemented by the Public Health Authority, individuals may be categorised at different risk thresholds based on contact proximity and duration, which may trigger different actions.

One key factor of the action to be taken that should be considered is the ethical issues of patient care, avoiding distress, and ensuring that individuals are aware of the alert and understand the implications of the contact and the actions they need to take to protect health and promote recovery.

It is important for Public Health officials to determine what follow up actions they would like to take as part of their Contact Tracing process as this may have implications for the design of an application and the capture of data other than the contact proximity data such that the data that is processed by the application is adequate for the purposes envisaged.

Therefore, it is *essential* in our view that applications be designed from a "Business Need /Approach"/ Use Case perspective to ensure that the required capabilities are identified and that data is acquired and analysed as needed to allow the desired action to be taken. For example, basic demographic details (e.g. age, type of accommodation, contact details of parent/guardian) could be relevant in different contexts depending on the nature of the action that is to be taken.

Note that neither the Centralised nor DeCentralised frameworks nor the Apple/Google API prevent the definition of and development of additional data collection functions in an application. However, any such collection must be necessary and proportionate and comply with obligations under GDPR. A DPIA is an essential component of ensuring and evidencing that compliance from the design stage of the application.

Centralised Framework

In a centralised framework, the processing of the risk classifications will be done on the central server and this will trigger the next action.

In a centralised framework, it may be more likely that users will have had to register a contact phone number when installing the application (e.g. the TraceTogether app in Singapore requires a phone number to be registered as part of the application installation process).

If a phone number is not available, it is assumed that a push notification via the application will be used as the only mechanism for contact to trigger an action on the part of the app user.

In a 'data-light' Centralised model, where only the data about identifiers is processed and no other personal data is captured or retained by the Public Health Authority there is a risk that children or people with diminished capacity will receive notifications and the design of the "Action" processes must consider the risks to the rights and freedoms of those categories of individual and how to ensure the Public Health Purpose is satisfied effectively in such contexts.

Decentralised Framework

In a decentralised framework approach, the Public Health Authority has no data about the user of an application who is identified as being at risk due to contact proximity and duration. This is by design.

Therefore, for any communication strategy other than a push notification via the application, it will be necessary for the application to be designed in such a way as contact information can be captured if required.

Therefore, careful consideration needs to be given to the required action and the potential issues, risks, and impacts on users of the application. In a 'data-light' De-Centralised model, where no data is held by the Public Health Authority about users there is a risk that children or people with diminished capacity will receive notifications and the design of the "Action" processes must consider the risks to the rights and freedoms of those categories of individual and how to ensure the Public Health Purpose is satisfied effectively in such contexts.

Constraints and Issues Identified

A range of constraints and issues are identified in the context of the acquisition of data using these methods.

Fitness for Purpose/Data Quality

Neither Bluetooth nor BT-LE are primarily designed as protocols to measure proximity and are subject to a range of factors that affect the variability of the data. The assessment of proximity is a calculated value that is influenced by a range of variables and factors including:

- Signal absorption by the body if a phone is in a pocket
- Signal absorption from walls, glass, clothing (including PPE)
- Differences in device hardware such as antennae, even in devices of the same general type
- Interference from other devices
- Signal attenuation as a result of proximity to metal
- Humidity or other weather conditions.

According to a blog post published on the Bluetooth SIG website:

> "*When you use RSSI for your proximity applications, you may need to consider the difference in definition from different chipset vendors. The absolute value of RSSI may vary from different radio circuits but trending of the RSSI from the same chip could still give you lots of information. To avoid the influence from the environment, you may want to define your own sampling algorithm to get rid of the noise*." [14]

A paper published on the GitHub repository for OpenTrace, the open sourced version of the Singapore TraceTogether app provides extensive detail of the calibration methodology that has been developed for that application with respect to the variability in Transmitter and Receiver devices[15]. We note that this method requires identifying the device model type (TAC Code) derived from the IMEI number of the devices transmitting and receiving beacons.

This paper indicates that data from mobile phone operators for the devices that are active on networks in the operative jurisdiction would be required to allow for appropriate calibration of the application's proximity assessment, at least in the model implemented as part of the OpenTrace/TraceTogether application. A comment posted on the GitHub repository summarises the

[14] https://www.bluetooth.com/blog/proximity-and-rssi/
[15] https://github.com/opentrace-community/opentrace-calibration/issues/4#issue-599877202

importance of appropriate calibration for the delivery of the required outcomes from these applications in a pessimistic manner:

> *"If the systematic errors are not removed by the calibration method, then BLE will be completely unsuitable for the intended purpose of interrupting the infection chains."*[16]

Even where the derivation of proximity is performed with appropriate calibration to control for variability in the Transmitter and Receiver, there are additional environmental variables associated with radio frequencies potentially affecting the RSSI values and the calculation of proximity.

A related issue is the inability of a BT-LE app to identify any barriers that might exist between devices that are detected near each other. The commonly cited example is people living next door to each other or in separate rooms with a physical barrier between them being identified as "close contacts" by an app, resulting in data being processed/shared if one or other of the device owners has tested positive for Covid-19. While there is discussion in the DP3-T community[17] about extending the app to use ultrasonic ranging in addition to BT-LE proximity to potentially reduce false positives in this context, this is also an imperfect solution and has not yet been implemented.

This raises a potential issue in respect of the Adequacy principle in GDPR (Article 5(1)(c) and the Accuracy Principle in Article 5(1)(d) as any DPIA will need to assess whether a proximity estimation based on a potentially uncalibrated algorithm will allow the objectives to be met, and whether the potentially high level of "false positives" that could arise from proximity detection through barriers would be excessive for the identified purpose.

However, the words of Dr Michael Ryan of the WHO should be considered in this context:

> *"Perfection is the enemy of the good when it comes to emergency management"*[18]

In this context, it is important that jurisdictions implementing a BT-LE enabled contact tracing platform make a formal determination in their DPIA as to the margin of error and imperfection that is acceptable in their use of these technologies. Appropriate measures will need to be taken to control for false

---

[16] https://github.com/opentrace-community/opentrace-calibration/issues/2#issuecomment-616154944

[17] https://github.com/DP-3T/documents/issues/185

[18] Speaking at WHO press conference, 13th March 2020 (https://web.archive.org/save/https://www.youtube.com/watch?v=AqRHH6e-y6I, last accessed 21 April 2020)

positives in a way that engenders and maintains trust in the Public Health response.

Some mitigation strategies to false positive risk triggers include:

- Maintain the "human in the loop" aspect of traditional contact tracing
- Implement rapid testing to minimise impact of unneeded self-isolation controls
- Careful preparation of messaging in any push notifications (see Business Need #3 below)

However, there remains insufficient data to show that BT-LE enabled contact tracing will actually work to a sufficient degree. The real benchmark test to be considered is this:

- Will it provide insights faster than a traditional interview?
- Will it be more or less fallible then human memory?

In this context, the definition of the required purpose and the parameters for what is considered "adequate" for that purpose must be clearly defined as part of the DPIA process and, if the technology does not meet that threshold it should be retired.

It is noted that the DP-3T consortium has commenced testing and calibration of their application with the Swiss Army as of 26th April. It is also noted that version 1.1 of the Apple/Google Framework has introduced additional processing capability using another component of the BT-LE stack in an attempt to improve accuracy[19].

"Gaming" the Application

The issue of "gaming" the application, either through the misuse or abuse of self-reporting triggers (as is apparently proposed in the UK[20]) or through some other mechanism[21] arises.

Under the currently proposed UK system, individuals would self-report symptoms of Covid-19 and, if they matched the disease profile, a push notification of a "Yellow Alert" would be pushed to any device that that that

[19] https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.1.pdf (published 24th April 2020)
[20] https://www.bbc.com/news/technology-52263244
[21] In February 2020, a German performance artist famously spoofed the traffic flow algorithms of Google Maps using 99 mobile phones in a handcart to trick the system into identifying traffic jams on streets that were otherwise empty of traffic. https://www.theguardian.com/technology/2020/feb/03/berlin-artist-uses-99-phones-trick-google-maps-traffic-jam-alert

individual had been in contact with. As we will discuss later in reference to the use of push notifications, there is a significant risk of "Alert Fatigue"[22], an issue that should be familiar to clinicians.

While Alert Fatigue is a risk to the individual, the potential for abuse of the self-reporting to initiate a lockdown or quarantine of an individual or a group of individuals, either through malice or accident, cannot be overlooked.

The DP3-T framework references the validation of a diagnosis/test result against a validation server as a control to minimise the risk of misuse/abuse of self-assessment.

Equality of Access

The need for the application to run on a smartphone which is enabled with BT-LE raises significant issues with regard to equality of access and de facto exclusion of individuals who may not, either through choice, constrained financial circumstances, age, or disability not be in possession of an appropriately equipped device. According to the GSMA, at the end of 2019 smartphones only accounted for 76% of the total connections in Europe[23].

Research by Pew Research published in Q1 2019[24] shows that, in the UK, 76% of survey respondents reported owning a smartphone, with 19% owning a "featurephone[25]" and a further 5% reporting no mobile phone use. Other countries in Europe reported lower smartphone use, with Greek respondents only reporting a 59% penetration of smartphones versus 32% for "feature phones".

In the Pew study, the penetration of smartphones within the 50+ age group is reported as being 60% of the sample population. Therefore, it is reasonable to conclude that a smartphone-app centred strategy for contact tracing risks overlooking a recognised "high risk" segment of the population for severe Covid-19 impacts.

Therefore, when electing to implement a smartphone app-based approach to support contact tracing, any DPIA should specifically address the potential "digital divide" that is created by favouring a technology that may not be accessible or useable by a potentially significant portion of the population. It is

---

[22] https://psnet.ahrq.gov/primer/alert-fatigue

[23] https://www.gsma.com/mobileeconomy/europe/ Last accessed 21 April 2020

[24] https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/ Last accessed 21 April 2020.

[25] A feature phone is a type of mobile phone that has more features than a standard mobile phone but is not equivalent to a smartphone. Feature phones can make and receive calls, send text messages and provide some of the advanced features found on a smartphone.

important when documenting your DPIA to consider what proportion of your population is likely to fall within the addressable market for such an app so you can correctly determine the likelihood of obtaining sufficient contact tracing data for the strategy to be effective and also so you can determine the potential risk to the fundamental rights of those portions of your population who do not have smartphones.

Again, while perfection may be the enemy of good, it is important that the expectations of effectiveness of any smartphone app approach are effectively managed. This will require conscious decisions to be made as part of any DPIA and these should be as evidence based as possible.

Consideration of User Personas

One significant gap in the research and analysis, and indeed a glaring oversight in the guidance from the European Commission and the European Data Protection Board, is a consideration of the impacts of the use of this technology on children who may have smartphones and may download the application. In addition, users with visual impairments, or cognitive impairments, or other factor that might affect their capacity to interact with or understand any notifications or messages initiated by the app also seem to have been overlooked in the haste to define a technical solution to this problem.

Children

As applications of this type are not Information Society Services under EU law, they do not fall within the scope of Article 8 of GDPR. However, the probability of an in-app notification or call from a Public Health official to a child resulting in distress to the child cannot be ignored. Therefore, the design and implementation of any contact tracing application should:

1) Consider how child users of the application can or should be identified, and what the appropriate point in the process should be for doing so. We would suggest that a prompt on installation of the application should allow users who are children to create an on-device profile for their parent or guardian and the “Action” phase of any contact tracing process should check to determine if there is a “Parent” profile created and direct communication to that nominated parent.
2) Consider the phrasing and structure of push notifications or other text communication that may be targeted to children to ensure that they are intelligible and do not cause unnecessary distress.

Diminished Capacity / Visually Impaired

Similar considerations arise for those with diminished capacity or who are visually impaired. Consideration should be given as to how relevant public

health information will be communicated to these categories of individual or to their carers. Such processes may need to consider any relevant domestic legislation with regard to Assisted Decision making in the context of care for persons with diminished capacity.

Alternative Approaches

It is important to consider that smartphones are not the only category of devices which operate with BT-LE capability. Smartcard technologies are available which provide the same beacon broadcast capability and can provide on-card storage of logged beacon data, similar to the functionality of the smartphone apps[26].

These technologies address the challenges of older users and smartphone device penetration in a particular jurisdiction and potentially allow for the introduction of additional features and functions over time. Access to the logged close contact identifiers could be triggered by a public health official scanning a QR code on a card when a person has tested positive (similar to the provision of a security code in the DP3-T decentralised framework).

New Zealand[27] is reportedly considering rolling out a smart-card based contact tracing solution but, as of the time of writing, details of how it will function and whether it will align with a decentralised or centralised model are unavailable (but due to the limitations of on-device processing in a smart-card, we assume this would be a centralised solution).

[26] https://www.linkedin.com/pulse/covid-19-response-needs-wake-up-reality-stephan-engberg/

[27] https://www.newsroom.co.nz/2020/04/17/1132682/nz-considering-100m-contact-tracing-covidcard

Figure 7 Screenshot of a potential New Zealand "CovidCard"

From the published information it appears that the proposed model would work similar to the smartphone-based approach, with log data being downloaded from the card by public health officials once a person tests positive for Covid-19[28]. This suggests that a database of cards linked to contact details of card-holders will be required to enable contact tracers to notify potentially infected individuals.

Analysis of Information Environment

There insufficient information available at this time to fully assess the information environment for this alternative approach. However, conceptually the model would appear to be similar to the smartphone approaches but using a different platform for initial data acquisition.

Acquisition

BT-LE enabled cards would be provided to individuals and (it is assumed) would be registered to them either through an application form process or some other mechanism.

The cards would act as Bluetooth beacons, similar to the smartphone applications already discussed and would log other beacons which come into proximity.

In this context, the lawful basis for processing would likely fall under Article 6(1)(d) and Article 6(1)(e) of GDPR. As the smart card is not a device connected to a public communications network it would not fall within the ePrivacy

[28] https://www.slashgear.com/covidcard-phone-free-contact-tracing-proposed-in-new-zealand-20617380/

Directives. In practice, it would be easy for individuals to opt-out of the contact tracing by leaving the smartcard at home.

As part of deploying the solution however, it would be necessary to register the card in some way against a contact phone number or other mode of contact. This might be achieved through a partner smartphone app or through a registration process.

We note from the limited available information that the smartcard proposed in New Zealand has a built-in "kill switch" arising from the expected battery life of the cards, after which time they would need to be replaced. This supports the EDPB requirement that a procedure would need to be put in place to stop the the collection of identifiers once public health officials identify that the pandemic has ended[29].

Analysis

From the available information, we infer that the process for analysis of the data will be triggered by a positive test for Covid-19 which will in turn trigger a process where by a Public Health Official will download the logged data from the device.

This download would need to be triggered by and controlled through an appropriate security mechanism to prevent unauthorised access to or disclosure of data. It would also require an appropriate legislative authority to be in place underpinning contact tracing, as per other mechanisms.

The analysis of "at risk" individuals would likely be similar to the processing in a smartphone-based implementation, with similar issues and risks.

Action

The action phase of this mode of operation will depend on the processes implemented as part of the wider contact tracing programme in any jurisdiction.

It will not be possible to send a push notification to an app in this context, unless the smartcard is paired with an app (and again, this raises the issue of smartphone penetration in vulnerable population demographics).

As the operation of the system would apparently have to rely on a register of cards against a database of user contact information, it would be possible to

[29] *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 Outbreak,* EDPB, 21st April 2020, at page 13

implement either an SMS-based notification or a telephone call-based notification and follow up process, depending on requirements.

A 'hybrid' model of operation could be implemented with a registration of the card via a smartphone app which would provide other Covid-19 related functionality (e.g. symptom tracking) and allow for receipt of push notifications in the event of a close-proximity contact testing positive.

Constraints and Issues Identified

While a smart-card based solution may appear to address many of the challenges presented by smartphone-based solutions. However, there are a number of constraints and limitations that arise with these types of technologies.

Security of IDs and potential for linkage-based attacks

An apparent limitation of this solution is the absence of Ephemeral IDs (frequently-generated temporary IDs), which can pose a risk of reidentification for users should broadcast identifiers be logged and the ability to link cards/ids and patterns of behaviour to individuals. We would recommend that consideration be given to the implementation of such a mechanism as part of any implementation of a smart-card based solution.

Technical Feasibility of Solution

From the information that is currently available it is unclear how technically feasible a card-based solution would be. Concerns arise with respect to battery life, the potential manufacturing lead times and the mechanics of distribution of cards.

Further information would be required to properly assess the technical feasibility of a card-based solution and, even in New Zealand, there is minimal publicly available information on how this proposal would work based on our enquiries with our contacts in the data management and data protection consulting community in New Zealand.

Conclusion

Alternative technologies may emerge to support contact tracing and should be considered, however a card-based solution brings with it logistical challenges in respect of battery life and manufacturing timescales that may mitigate against this technology as a longer term solution. Further detail is required before this can be recommended as a target solution in the short to medium term.

Summary Conclusion

The rapid pace of evolution in protocols and technical frameworks for BT-LE enabled contact tracing makes it impossible at this time to provide a detailed

Information Risk assessment for each option. Also, this iteration of this report has focussed on the frameworks and APIs. Additional data protection risks and potential mitigations may arise based on the specific implementation of an application in a given context by a Public Health Authority.

However, based on a balanced assessment of the options that present themselves for Authorities looking to develop an application that provides the maximum potential for compliance with EU Data Protection laws (both the GDPR and the ePrivacy Directives) while allowing for flexibility of implementation and the potential for interoperability with applications in other jurisdictions, we would consider an architecture built on the Apple/Google API and implementing the DP3-T decentralised approach is most likely to meet these requirements in a sustainable way that will support user adoption through:

- Robust data protection controls and protection of individual user privacy
- Minimal impact on battery life, which will affect both adoption of the application and effectiveness of day to day usage.

The guidance of the EDPB provides a clear set of benchmark criteria for considerations in any DPIA. However, the question of whether this technology will actually provide a sufficiently greater effectiveness of contact tracing over traditional manual methods remains to be seen as there is, as of yet, no evidence as to the percentage of population who must adopt it to be effective or whether the underlying technology is fit for this new and innovative purpose.

It is our assessment, based on the currently available information, that an architecture based on a decentralised model for contact identification, but with other features and functionality implemented at the application level as required by a public health authority (subject to data protection laws) would be the most appropriate solution as it provides a

Business Need #2 Symptom Tracking

This section examines the use of mobile location data and/or other mobile phone technologies to support the logging and tracking of symptoms. For the purposes of this research paper we have identified the Covid-19 symptom tracker deployed by Zoe Global Limited and Kings College London (https://covid.joinzoe.com/) as a reference model to conduct analysis against. We also looked at PatientSphere for Covid-19 by the Open Cancer Network in the United States.

Statement of Business Need and Approach

Proposed Processing Activity (What we propose to do)	To gather data about health symptoms from app users, whether they have tested positive for Covid-19 or not through a smartphone app
For the Purpose of	To develop a better knowledge of symptomatic progression and improve clinical case definitions to help differentiate Covid-19 from other seasonal respiratory infections (e.g. colds)
To achieve benefit (to the organisation)	• To improve clinical epidemiological information about Covid-19 • To support the identification of possible infection trends
To achieve benefit (to the data subject)	• To protect the vital interests of the data subject or others through more efficient use of public health resources

Analysis of Information Environment

This category of application can either process data as direct input into a remote database (Covid.Zoe approach) or it can log data locally on a device which can then be submitted to a public health official or doctor (PatientSphere approach).

Legal Environment (Basis for Processing)

As these categories of application would be processing special category data within the meaning of Article 9 of Regulation 2016/679/EU (GDPR), a higher standard of care is required in respect of the processing of this data.

Relevant Lawful Processing Conditions.

The relevant lawful processing conditions under GDPR are set out in the table below. It must be noted that *necessity* of the data to the processing purpose is a key requirement under the various provisions of Article 9.

Applicable Processing Condition	Rationale
Article 9(2)(a)	Individuals can be asked to give explicit consent. However, this must be explicit consent to each SPECIFIC processing activity that will be undertaken using the data.
Article 9(2)(g) Article 9(2(i)	Subject to the existence of an appropriate provision in domestic legislation with appropriate safeguards, these articles may also be relevant as legal basis for processing. However, **necessity** is a key test.

It is important to note, however, that these provisions carry with them a requirement to ensure appropriate safeguards for the processing of data.

Article 9(2)(c) does not apply in this context as:

1) The information processed is not *necessary* to protect the vital interests of the data subject (notwithstanding its helpfulness)
2) The data subject is capable of providing consent.

Application of ePrivacy Directives

Under the ePrivacy Directives, location data processed from the device such as GPS co-ordinates will require consent.

Likewise, if logged symptom data is stored on-device prior to being uploaded, processing will require consent under Article 5(3) of the ePrivacy Directives as this processing may not fall within the context of an information society service.

Considerations regarding Health Research

The lawful processing conditions in respect of scientific research arising from self-reported symptom tracing are different to those underpinning a public health response purpose. They will be addressed by Article 89 of Regulation 2016/679/EU and will require appropriate ethics governance and oversight of approved researchers. As this varies from jurisdiction to jurisdiction from a process and governance perspective, further analysis of this question is out of scope for this iteration of this research report.

Process Environment (Description of Processing Activities)

Both Covid.Zoe and the Planetsphere Covid Symptom tracker record data relating to:

- Personal profile (name, contact number, age)
- Symptoms (current symptoms, symptom history)
- Whether user or a co-habiting person has tested positive (Planetsphere only)
- Medications being taken (Planetsphere)
- Hospital treatments received (Covid.Zoe)

Screenshots of each of the applications from the Apple app store are provided in an appendix to this document.

The PlanetSphere application logs data locally on-device and allows it to be shared by email with a third party. The Covid.Zoe application logs entries directly to a backend database. It is not clear from the available documentation whether local logging of data takes place.

Users are identified primarily by their mobile phone number in both applications and mobile phone numbers are validated using a One-time-password code (similar to the TraceTogether implementation).

Necessity of Processing

For the purpose identified in the statement of business need and approach, it is necessary for public health officials to:

1) Identify and contact the data subject (name, mobile number)
2) Identify the data subject's general location
3) Identify self-reported symptoms
4) Identify medications being taken or medical interventions that have been undertaken in hospital

In the context of applications that are being deployed by Public Health authorities, there is no requirement for the application to record that the data subject or a person connected to them has tested positive for Covid-19 (this is functionality in the PlanetSphere app) as this information should already be available to the Public Health Authority.

Adequacy / Accuracy of Data

A limitation of "crowd-sourced" data gathering applications of this kind is that the quality of self-reported symptoms can be variable. Also, this kind of data

gathering requires users to continue to log data in order for it to be useful for analytics purposes.

This may be easier to control for in the context of application users who have tested positive for Covid-19 or are identified close contacts of persons who have tested positive as part of a case-management approach.

In addition, the use of mobile phone location data to register the user's location may not provide appropriate level of data quality for accuracy in analysis.

Security of Processing

The Covid.Zoe implementation of symptom tracker logs data and uploads to a central server. The PlanetSphere implementation logs data locally on-device and allows for reports to be emailed off device to a user-input email address.

Any local storage on-device must be secure and encrypted.

It is our view that, in the context of a public health authority deploying an app to support symptom tracking, the app should not require the need to send data to a third party by email.

The exception to this would be if the symptom tracker information was required by a medical professional outside the public health environment. In such cases, the application should be capable of uploading the symptom tracking report to a secure location which can be accessed by authorised healthcare professionals.

Technical Environment

Mobile Network

The use of smartphone applications assumes a consistent and reliable mobile phone network connection that can support upload of data to remote servers. While mobile network coverage has improved in many areas, there are a large number of locations where operator coverage can be weak to non-existent due to local topographical issues or as a result of operator decisions re: investment in masts in a given area.

It should also be borne in mind that solutions that are designed and developed with an assumption of good to excellent mobile network coverage or smartphone-level device capabilities will be unusable in:

- Countries with poor network coverage, small bandwidth packages for mobile data on phone subscriptions, or expensive costs for data usage
- Countries with low penetration of smartphones (e.g. reliance on "feature phones" or older devices)

On-Device

The application can record a variety of items of data from mobile devices. If a user's location is required, their location can be derived from GPS data on the device. This will require consent and this should be clearly sought in the user registration process for the application.

Alternatively, users can be asked to provide their postcode. Again, the purpose for this information needs to be made explicitly clear.

Risks and Root Cause Analysis

We have identified a number of risks in relation to the proposed use of symptom tracing applications modelled on the Covid.Zoe and PlanetSphere reference applications.

Issue	Title	Description	Risk Priority	Criticality	Category
ST_005	Retention of data	The retention of symptom and medication data linked to an identifiable individual is not necessary once the public health emergency has ended. Data may be relevant for research.	160	36	Governance
ST_001	Quanity of low quality data	Mass roll out of the symptom tracking application capability could result in excessive data of variable quality of self-reported symptoms which could reduce quality of analysis and actions	158	39	Governance
ST_003	Unauthorised access to symptom data in transfer	Special category data from symptom tracker needs to be transferred securely.	111	23	Technology
ST_002	Mobile network access may impede use of app	The use of an app to upload symptom data assumes existence of an "always on" data capability and reliable mobile network. This may exclude people in certain areas from the use of this app.	88	25	Governance
ST_004	Inaccurate Location Data	Users registering the app at a location that is not their home address may be mis-identified as being based in the other location leading to inaccuracy in any analysis	52	24	Process

The root causes for the identified issues are as follows:

Issue	Root Cause
ST_005	Storage limitation is a requirement under GDPR. Clarity on retention period/purpose is an essential element of ensuring user trust.
ST_001	Individual perception of symptoms can be subjective. Submission of irrelevant symptom data from a large population can result in symptoms correlated to a link to a diagnosed case being missed/overlooked.
ST_003	Email is an insecure data transfer mechanism. Unless app supports an encrypted email client internally, potential breach of Article 32 obligations to ensure security of data.
ST_002	This is a function of mobile networks and is outside the scope of an app to address. An alternative mechanism needs to exist for individuals to log their symptoms where necessary
ST_004	People may download app at GP surgery or at a location not their home. Also, mobile network location data can be inaccurate.

Recommended Mitigations

Based on our analysis, we would make the following recommendations for mitigation, which we believe will reduce the residual risks involved in processing.

Issue	Title	Recommended Mitigation	Residual Risk Priority	Residual Criticality
ST_005	Retention of data	A defined retention schedule is required BEFORE the application is deployed to define how long de-identified symptom and medication data will be retained and for what purpose. There is no basis to retain this in an indentifiable format	17	4
ST_001	Quanity of low quality data	Recommend targetting roll out of symptom tracker to close contacts of positive test subjects	92	20
ST_003	Unauthorised access to symptom data in transfer	For app implementations that communicate directly with server, HTTPS protocol must be applied, data should be encrypted in transit. Where data is stored locally, email should not be used for data transfer off app, use an upload process similar to TraceTogether data upload.	50	10
ST_002	Mobile network access may impede use of app	Need to consider alternative mechanisms for symptom tracking for people with low/no mobile coverage or access to internet	84	25
ST_004	Inaccurate Location Data	Request home eircode for the purposes of mapping symptoms. This should be an OPTIONAL field and should NOT be used for any other purpose	36	16

Summary Comment on Approach

The Business Needs and Approach, and Information Environment of an app for symptom tracking is significantly different to the goals, contexts, and purposes for processing of the previously reviewed app to support contact tracing, requiring completely different datasets for different purposes, and presenting a different risk profile.

The quality and fitness for purpose of data collected may vary significantly with implementation decisions in developing the app in addition to the variable quality of crowd-sourced symptom data. The processing of location data presents compliance and privacy risks which may not be adequately answered by benefit of quality data for analysis.

In addition, as the data gathered in such an app would be self-reported, design of the data flow and analysis must take into consideration data quality for information collected from people who become too unwell to self-report using the app.

Furthermore, our analysis presumes a “self-hosted” application, not a rebadged version of an externally provided application which would introduce additional risks.

Alternative Technologies

A related category of application to symptom trackers is the domain of remote patient monitoring. These applications are normally categorised as a Class 1 medical device and are used in tandem with external sensors such as pulse oximeters. As such, while they may appear to share characteristics with symptom trackers, these applications are more clinically focussed and process quantitative clinical telemetry data as well as qualitative self-reported symptom data.

They are a prescribed device that allows patients or suspected cases of Covid-19 to be treated at home while still being under clinical supervision. This is identified as a benefit in reducing the demand on hospital beds.

The lawful basis for processing in these contexts would be Article 9(2)(c), Article 9(2)(h), and Article 9(2)(i) of GDPR.

As Castlebridge works with a provider of this category of technology we will not provide a detailed analysis of this use case in this report to avoid any ethical conflict.

Business Need #3: Push Notification of Contacts

This section examines the use of mobile location data and/or other mobile phone technologies to support the push notification through an app of alerts regarding close contact with an infected person. For the purposes of this research paper we have identified a Covid-19 close contact tracking application from the EU which provides this functionality as a reference model for assessment.

Statement of Business Need and Approach

Proposed Processing Activity (What we propose to do)	To send a push notification alert to an application user when they are identified as having been in close contact with another individual who has tested positive for Covid-19
For the Purpose of	• Advising the individual as to the required public health actions (self-isolation etc.) • Advising individual re: testing or symptom tracking requirements
To achieve benefit (to the organisation)	• Reduces human involvement in contact tracing process • Improved efficiency of contact tracing and follow up
To achieve benefit (to the data subject)	• To protect the vital interests of the data subject or others through more efficient use of public health resources

Analysis of Information Environment

Legal Environment (Basis for Processing)

As these categories of application would be processing special category data within the meaning of Article 9 of Regulation 2016/679/EU (GDPR), a higher standard of care is required in respect of the processing of this data.

Relevant Lawful Processing Conditions.

The relevant lawful processing conditions under GDPR are set out in the table below. It must be noted that *necessity* of the data to the processing purpose is a key requirement under the various provisions of Article 9.

Applicable Processing Condition	Rationale
Article 9(2)(a)	Individuals can be asked to give explicit consent. However, this must be explicit consent to each SPECIFIC processing activity that will be undertaken using the data.
Article 9(2(i)	There is a public interest in the context of public health, but this must be subject to a statutory basis in domestic legislation

It is important to note, however, that these provisions carry with them a requirement to ensure appropriate safeguards for the processing of data.

Article 9(2)(c) does not apply in this context as:

1) The information processed is not *necessary* to protect the vital interests of the data subject (notwithstanding its helpfulness)
2) The data subject is capable of providing consent.

Article 9(2)(g) does not apply in this context as:

1) The sending of a push notification is not NECESSARY given the existing and established processes for contact tracing and follow-up that exist.

In general, a key requirement will be demonstrating the necessity for use of push notifications. When considered in light of the EDPB guidance that contact tracing applications should support and integrate with existing contact tracing methodologies, there should be appropriate documentation of and alignment of processes in this context to ensure that necessity for the purpose is clearly demonstrated and that the benefits over traditional manual contact tracing methods are clearly articulated.

These benefits may include (for example):

- Speed of response/speed of action
- Improved provision of information in a timely manner

Application of the ePrivacy Directives

As the communication in this context will not be for the purposes of marketing, the requirements for consent under the ePrivacy Directives do not arise for the sending of messages such as SMS messages.

Process Environment (Description of Processing Activities)

The reference application identified which triggers push notifications to users is primarily a contact tracing application that, once a close proximity contact of a user is confirmed as having tested positive for Covid-19 generates a push notification to any app user who has been in contact with the positive test subject.

In a centralised implementation, this messaging would be triggered from the central application server based on a risk profiling analysis performed there.

In a decentralised implementation, the messaging would be triggered by on-device processing of risk profiling on-device.

Therefore, the operative processing mechanism is similar to the “Action” phase of the contact tracing scenario examined earlier in this report, with the outbound calling from a contact tracer being replaced with a push notification delivered to the app.

However there a number of significant differences that need to be considered in the implementation of a push-notification based approach which relate to the specific action that is to be undertaken by a recipient of a message. Our analysis considered three basic scenarios:

Notification of Risk and Instruction for Next Steps

The notification of risk may provide additional information for the next steps to be taken by the recipient. The precise nature of these next steps will depend on the contact tracing and containment strategy being implemented. This may involve either:

- The public health authority contacting the individual to provide further information;
- The individual being asked to contact the public health authority to give further information; or
- The individual being given instructions to self-isolate and perhaps implement symptom monitoring or other measures.

It is outside the scope of this research to make recommendations on the appropriate strategies for public health authorities to implement with respect to pandemic containment. However, we would make the following comments.

Inbound versus Outbound calling

There is a process capability question that must be set against data protection and privacy concerns with respect to the performance of a contact tracing function.

Inbound Calling

Assuming the implementation of a decentralised exposure notification/contact tracing approach, the most privacy preserving approach is to generate a notification to people who are at risk requesting that they phone a specific number to speak to a public health doctor so further information can be obtained or provided.

In this scenario, no personal data is shared with the Public Health Authority until such time as the individual makes contact themselves. However, this then requires individuals to make contact, which triggers two sources of risk:

Risk 1: People do not call

There is a risk that people do not call the contact tracing team in the Public Health Authority. The reasons for this may be manifold (fear, not recognising the message, language barriers, diminished capacity, message recipient is a child).

This deprives the Public Health Authority of their ability to perform human-driven information gathering and to provide contextually relevant information to the affected person which might influence decisions on prioritisation of treatment responses such as testing or other interventions (e.g. are they co-habiting with an immune-compromised person? are they lone-parents who cannot self-isolate from children?)

Risk 2: Inbound Call Volumes exceed call handling capacity

The risk in this context is that a high volume of risk notifications being sent out will trigger an equally high volume of inbound calls to the contact tracing team over a compressed time period. This is analogous to the public health concerns with regards to hospital facilities becoming swamped if faced with a surge.

Therefore, in any response strategy which relies on inbound calling from persons who receive a push notification, consideration must be given to how that will be implemented as part of the human contact tracing process in a way

that does not result in people who have received a risk notification message being left with long on-hold times or having to make multiple calls to speak to a contact tracing team member.

If the objective is to improve speed of processing of contact tracing, consideration would need to be given to a two-strand process whereby outbound calls could be used in tandem to manage surges. For example, an overflow queue could be created where callers could leave a voicemail with basic information and arrange a call back. Alternatively, an SMS or chat-bot based interaction might be initiated which would allow for asynchronous conversation prior to a human call handler becoming available.

However, any additional technology intermediation in the process would need to consider the challenges for people with diminished capacity, children, or non-technically adept individuals who would have to interact with the process.

In order to ensure effectiveness, the user experience has to be kept as simple as possible and as scalable as possible.

Outbound Calling

Outbound calling has an immediate benefit of allowing the Public Health Authority to map resources to workload more directly in a manner that is controllable by the Public Health Authority. This process is also more in-line with the traditional methods for contact tracing and follow up used by Public Health Authorities.

A key data point that is required to enable outbound calling is, of course, a phone number. The key issue that needs to be determined in the design of the contact tracing process that any application will sit within is what the appropriate point in the process is for the phone number to be requested. It would not be in keeping with the principles of necessity and proportionality or the data minimisation principle under GDPR for a phone number to be obtained by the Public Health Authority for all users of the app given the purpose for which the number is required is an outbound contact.

Therefore, two options arise:

1) The phone number could be registered with the app but held on-device until such time as a user is identified as being at risk, at which point the number could be provided to the Public Health Authority. Article 5(3) of the ePrivacy Directives would suggest that this transfer would need to be by consent at that time (e.g. implemented via a popup or as part of the

notification or as a stated purpose with consent at the time the app is installed)

2) The phone number could be requested as a response to the push notification being received (similar to in-app notifications in other contexts).

In either scenario, the Public Health Authority receives contact information at the time it is needed, for a specific purpose, aligning with requirements of the GDPR.

There remain, however, a number of practical risks with an outbound calling strategy:

Risk 1: Children and people with diminished capacity

As there is no age-barrier to the installation of any app, there is a risk that notifications may be sent to children and that, as a result, children may be contacted by Public Health officials as part of contact tracing activities.

Likewise, persons with diminished capacity may also be recipients of calls in this way.

Therefore, the overall strategy for the use of apps needs to consider how the process and user experience will be designed to cater for scenarios such as this. Possible design choices might include:

- In-app contact profile registration where a secondary contact can be nominated for children or persons with diminished capacity
- Call scripting and training for contact tracers to handle calls with children or persons with diminished capacity (we assume that this is already standard practice but it should be reinforced as there is a higher potential for the manifestation of this risk in this context).

There will be issues in this context in respect of the autonomy of children, particularly teenagers and young adults. However, the process must take consideration of the variability in the population who may receive outbound calls in this context.

Risk 2: Verification of Outbound Caller

It will be necessary for there to be some form of verification mechanism built into the process to control for malicious actors in any outbound calling process. This has already been recognised in Singapore in respect of contact tracing, and is a consistent criticism of the data security practices of banks performing outbound calling.

The process must include an appropriate verification mechanism (code word, code number, 'colour of the day' passphrase) that the data subject can use to verify the identity of any caller. This could be implemented in-app as a security feature either through a push notification of a passphrase or a verification code displayed in the app that the caller must be able to repeat to verify that they are calling from the Public Health Authority.

Notification of Risk and Provision of Information

Push notifications that provide notification of risk and provision of information only, without a Contact Tracing follow-up from the Public Health Authority, should be carefully drafted to take into consideration:

- Literacy and language skills of recipients
- The profile of recipients (i.e. will they be received by children or people with diminished mental capacity)

We would recommend that any push notification providing information should also include an inbound contact call to action for people who have questions or require clarification.

Notification of Risk Only

We see no benefit in a call to action that notifies an individual only of their risk and would strongly advise against such a strategy as it is likely to result in unnecessary distress for recipients.

Adequacy / Accuracy of Data

In this context, the key driver of the trigger to send notification is the identification of a close proximity contact between two users of the application. This will be accurate within the following constraints:

- Accuracy of Bluetooth range estimation and contact logging
- Uptake and adoption of the contact tracing application
- Functionality constraints in iOS environment

We note that the Apple/Google API initiative will be addressing the identified constraints in the iOS environment.

Security of Processing

In a fully centralised model of operation, the security of processing of the data will be dependent on the security of the mobile app and associated back-end database. In a decentralised model, this risk is lessened as the notification will be an in-app generated event on the device.

However, irrespective of the mode of operation of the application, there is a risk that push notifications could be accessed by 3rd parties (e.g. family members). This could lead to distress, particularly if the 3rd party is a related child or person with reduced intellectual capacity to understand the nature of any message.

Potential for Unintended Consequences

It should be borne in mind that there is a significant risk of unintended consequences from the use of push notifications in this context.

There is a risk that a push notification without supporting context information could cause unwarranted distress to a data subject or another (e.g. a child). This is particularly the case in vulnerable persons (e.g. people with depression, mental illness, or intellectual disability, or cognitive impairment). This has already been referenced in Business Need #1 analysis.

There is also a risk that in circumstances where a data subject has a small social group or lives in a sparsely populated area that a push notification of close contact could provoke a negative reaction and create a risk of harm to a 3rd party. While this is a low probability risk, it would be damaging to trust in the application if it was to occur.

Therefore, the reliance on push notifications as a primary method of communicating close contact events to data subjects should be treated with caution to ensure appropriate social and clinical responses are delivered.

Risks and Root Cause Analysis

We have identified a number of risks in relation to the proposed use of push notifications for communication of close proximity contact with infected persons.

Issue	Title	Description	Risk Priority	Criticality	Category
PN_001	GPs swamped with inbound calls, affecting delivery of care	The provision of a push notification of close contact may result in an increase in calls inbound to GPs or health clinics, impacting on operations and delivery of care	175	39	Process
PN_005	Push notification to children in error	Unless application captures year of birth, there is a risk that push notifications will be issued to children, who have downloaded a contact tracing app	160	33	Process
PN_003	Distress to data subject	The impersonal nature of push notifications means that this may cause distress to data subjects who receive a message and do not understand the message or who are vulnerable to negative interpretations	158	35	Process
PN_002	Unauthorised disclosure of contact with infected person via 3rd party accessing phone	If a 3rd party acesses a users phone they will be able to see any push notifications received. This may include children using a parent's device	88	35	Governance
PN_004	Injury to a 3rd party	If push notification received by a person in a small social group/small population area, it may give rise to aggressive response (driven by fear/lack of understanding)	70	14	Process

The root causes we have determined for these risks are identified below.

Issue	Root Cause
PN_001	Human reaction on receipt of a push notification of close contact with positive case will be to seek further information or take further action. This will result in calls to primary healthcare provider.
PN_005	If children register for apps without any check to verify age/identify age, push notification will be issued to children
PN_003	Lack of human touch and absence of immediate response to queries that might arise will lead to distress
PN_002	Nature of phones and push notifications. User may expose data themselves
PN_004	Lack of “human touch” and absent immediate response to queries and information in context could result in a negative emotional response (anger) towards a small/identifiable population set.

Recommended Mitigations

Our recommended mitigations for the risks identified above are summarised below, along with our estimation of the residual risk inherent in the proposed processing as a result of applying these mitigations.

Issue	Title	Recommended Mitigation	Residual Risk Priority	Residual Criticality
PN_001	GPs swamped with inbound calls, affecting delivery of care	An existing process for contact tracing follow up exists. Push notification should supplement not replace this process. Recommend use of push notifications AFTER contact attempt by contact tracer. Message sent needs to have clear and specific call to action. Alternatively: establish dedicated INBOUND call line for queries but must ensure capacity.	100	23
PN_005	Push notification to children in error	Contact tracing apps should capture year of birth as part of registration. Children (<18, or potentially <16) should be excluded from push notification contact	32	7
PN_003	Distress to data subject	Push notifications should support/supplement standard human-driven contact tracing follow up processes. Messaging must be exceptionally clear to minimise distress	87	20
PN_002	Unauthorised disclosure of contact with infected person via 3rd party accessing phone	This is outside the direct control of the health authority to mitigate. Users should be advised of the risk of push notifications if this is to be deployed	88	35
PN_004	Injury to a 3rd party	Push notifications should support/supplement standard human-driven contact tracing follow up processes. Messaging must be exceptionally clear to minimise distress	44	9

As a general principle, push notifications should be used to supplement not replace standard public health tracing and follow up processes.

The communication and “call to action” in any push notification should be extremely clear for individuals and need to ensure that people with literacy or language issues will be capable of understanding the message and what their next action should be.

A Hybrid Approach?

A hybrid approach may be the optimum strategy for push notification-based engagement with people who have been in close proximity to a person who has been diagnosed as infected. In this approach, both an inbound and outbound call centre would be required to both receive inbound calls triggered by a push notification and also to make outbound calls, either in response to an explicit request triggered via the app for an outbound call response, or on foot of a voicemail that has been left requesting further contact.

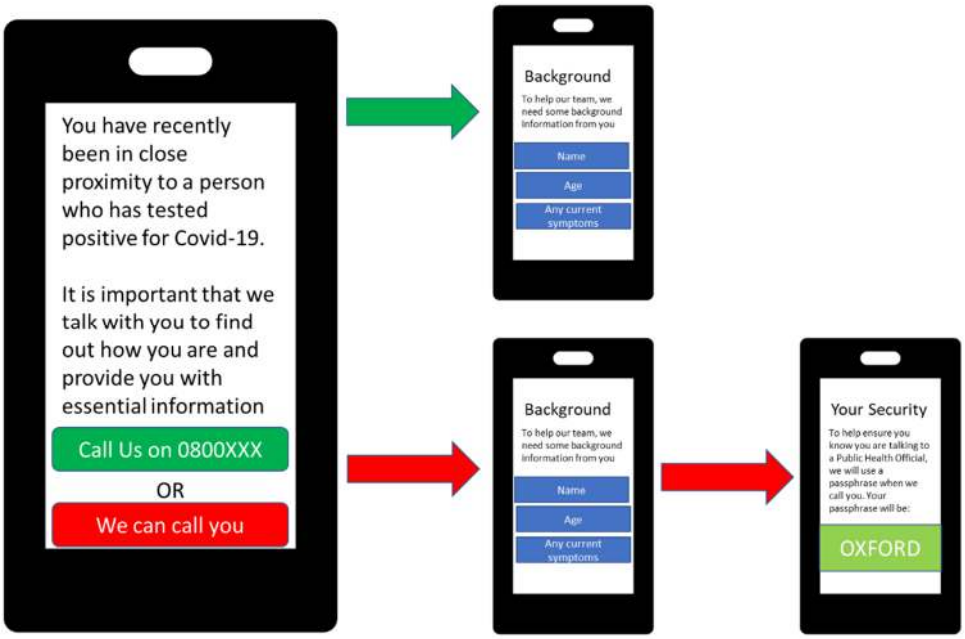


Figure 8 Mockup of Choice-based Call To Action with Hybrid Call Option and Security Control

Summary Comment on Approach

This approach presents numerous risks of unintended consequences. Reliance on push notifications as a primary method of communicating close contact events to data subjects should be treated with caution to ensure appropriate social and clinical responses are delivered.

However, if an appropriate end-to-end process is defined, with appropriate resourcing to mitigate the risks identified above, push notifications could be an appropriate mechanism to trigger the next phase of a contact tracing process or to provide appropriate information to individuals.

Business Need #4: Population Movement

This section examines the use of mobile location data and/or other mobile phone technologies to support tracking of population movements. For the purposes of this research paper we have referenced against the use of mobile phone location data during the most Ebola outbreak to inform our assessment.

Statement of Business Need and Approach

Proposed Processing Activity (What we propose to do)	To use mobile network CDR (call data record) or network location data to develop statistical analysis of population movements
For the Purpose of	• To support statistical analysis of the effectiveness of restrictions on movement. • To identify higher risk areas for community transfer due to statistical non-compliance with movement restrictions
To achieve benefit (to the organisation)	• To assist in infection trend prediction • To inform of effectiveness of public health controls
To achieve benefit (to the data subject)	• To protect the vital interests of the data subject or others through more efficient use of public health resources

Analysis of Information Environment

The primary source for data for the purposes of this type of tracking would be the mobile phone networks. The location data from CDRs (Call Data Records) in the network allows for the identification of an approximate location of an individual based on the mobile phone mast that their device has connected with to connect to the network.

Legal Environment (Analysis of Legal Basis)

The processing of location data from devices connected to a public communications network is governed by the ePrivacy Directives 2002-2009, as enacted in Ireland through SI336/201. The ePrivacy Directives are *lex specialis* and therefore need to be considered outside the parameters of GDPR.

The ePrivacy Directive addresses the use of location data and requires data to be either made anonymous or be processed solely on the basis of consent "to the extent and duration necessary for the provision of the value added service" (which in this context we will interpret as mobile operator assisted infectious

disease control, but normally this relates to value added services in a mobile network).

Anonymisation and Reidentification

The term “anonymised data” is often misused to refer to data that has had the directly identifiable portions removed or truncated. However, if there is the possibility for an individual to be identified *indirectly* from data it still falls within the definition of personal data under Regulation 2016/679/EU and should be more accurately described as pseudonymised data.

Therefore, for any processing of location data derived from the telecommunications network to be used without having to obtain freely given, specific, unambiguous, and informed consent from each data subject, the data must be aggregated such that an individual user cannot be reidentified from the data. However, it must be noted that granular location data has a very high risk of reidentification, to the point that location pattern information derived from CDR data is functionally impossible to truly anonymise under the EU Data Protection legislation.

Technical Environment (Summarised)

Mobile phone networks record both CDR data for the purposes of billing. In this data is the Home Location Register data which records which network mast a device was connected to when making a call. The network records the number of devices connected to a Home Location as part of its network logging data.

It is therefore possible to identify for a given subscriber what HLR they were connected to at a specific time, which is a traditional use of CDR data in law enforcement applications. It is also possible to report on the number of mobile phones connected to a given Home Location at particular times, allowing for statistical comparisons of network usage and device movement over time.

The granularity of location data derived from the network is down to the Home Location / Mast level and within the signal radius of a given network mast. It is not sufficiently granular for close proximity contact tracing but could be relevant for statistical analysis of population movements.

FlowMindr has published information on the approaches taken to processing mobile network data for epidemiological analysis based on their work supporting mobile operators using data to assist in the response to the Ebola outbreak in 2014. They recommend the following approaches to minimise data protection, privacy, and security risks:

1) MISISDN and IMEI numbers should be hashed and stretched using SHA-3
2) Anonymised data should be retained within operator's environments and not be shared. Analysis should take place in the Operator's environment with access via VPN

Process Environment

The general processing approach to processing this data is to perform statistical analysis of population movements between locations defined by network locations. The analysis would show a percentage increase or decrease of devices connecting to the network in particular locations.

This data can be used to evaluate the level of changing population mobility as a measure of effectiveness of restrictions on movement in the society as part of disease control measures.

Risks and Root Cause Analysis

We have identified the following risks.

Issue	Title	Description	Risk Priority	Criticality	Category
PT_001	Mass Surveillance risk	Where users consent to the use for mobile location data, it constitutes a mass surveillance risk	350	70	Governance
PT_003	Excessive retention of data	Data may be retained for longer than is needed	171	39	Governance
PT_002	Disclosure of individual calling patterns	If a malicious actor knows the cell tower a person is calling from, they can potentially identify calling patterns that would identify an individual	132	33	Governance

These risks assume that consent has been obtained for processing or that the processing is being undertaken in a manner that aggregates and effectively anonymises data using appropriate clustering.

The root cause for these risks is that they arise from the volume of data and the potential desire of organisations to retain data for research or analytical purposes.

We set out a number of mitigations to these risks.

Recommended Mitigations

Issue	Title	Recommended Mitigation	Residual Risk Priority	Residual Criticality
PT_001	Mass Surveillance risk	Appropriate safeguards need to be implemented to mitigate riskof mass surveillance. This includes deletion of data once public health emergency has abated, restriction on use of data to purely statistical analysis, and limitation on the access to data by individuals	175	35
PT_003	Excessive retention of data	Need to have a defined retention period for any data that is not aggregated statistical data. Retained data should be aggregated using K-anonymity approach to cluster data and remove data where group sizes are small	30	7
PT_002	Disclosure of individual calling patterns	Limit access to data to specifc persons. Retain data within operator environments to reduce risk of reidentification	53	13

Key controls that are recommended in respect of the use of mobile network data include:

- The mobile phone numbers of subscribers making and receiving calls or text messages will be anonymised by mobile operators inside their premises and on their equipment. This is achieved by replacing the mobile phone numbers with an anonymous code before being analysed. This is done through a hashing process using the secure SHA-3 algorithm.
- Anonymised CDR data will not be transferred outside of the operator's system/premises: The anonymised data will be kept secure and encrypted within the operator's premises. Access to the data will be controlled and given only to pre-approved and authorised personnel. A record of access will be maintained and auditable. Access to the algorithm and the ability to decrypt the data will be further protected by also limiting access to pre-approved and authorised personnel.
- All analysis will take place on mobile operator's systems, in their premises and under operator supervision. Once anonymised by the mobile operator, the data will be analysed on-site by approved research entities that agree to abide by strict ethical standards on the use of data.
- No analysis will be undertaken that singles out identifiable individuals. No attempts will be made to link the data to other data about an individual and which may impact on their privacy or otherwise cause harm.
- Only the output of the analysis (i.e. the resulting non-sensitive data on population mobility estimates, aggregate statistics, indicators, etc.) will be made available to relevant and approved aid agencies, government or research agencies that can use these inputs in their modelling and planning efforts. No sensitive data will be shared with or made available to any third parties.

In addition to these mitigations, we would recommend the consideration of pure statistical analysis of device connections to different Home Locations in the HLR data set. Analysis of this data over time, using hashed data, would allow for a statistical analysis of movement between locations without the call data associated to a CDR that could potentially allow for reidentification.

This data could be prepared for analysis by operators and aggregated by a small area statistical code to further cluster mobile network masts into defined geographical areas not directly linked to individuals.

Summary Comment on Approach

The use of CDR data, in particular location data, is complicated by the Legal Environment and the difficulty of truly anonymising granular location and CDR data, as it carries high risk of reidentification. Mitigations must be taken to ensure that individuals cannot be singled out from a crowd in analysis.

Business Need #5: Push Notification of Updates

This section examines the use of mobile location data and/or other mobile phone technologies to support the logging and tracking of symptoms. For the purposes of this research paper we have referenced against the use of mobile phone location data during the most Ebola outbreak to inform our assessment.

Statement of Business Need and Approach

Proposed Processing Activity (What we propose to do)	Push notifications to be sent to app users to provide information to data subjects about infection control measures or other public health measures.
For the Purpose of	• Supporting public health communications and updates on social control measures in effect in an area
To achieve benefit (to the organisation)	• Improved targeting of communication • Improve efficiency of communication
To achieve benefit (to the data subject)	• More timely provision of targeted information relating to their specific situation.

Legal Environment (Analysis of Legal Basis)

Assuming push notifications would be of a general nature and would not be relating to the health of an identified data subject, the legal basis for processing would need to be found under Article 6 of GDPR.

Consent under the ePrivacy Directives/SI336 would not be required so long as the messages did not contain a direct marketing call to action (e.g. requesting people purchase an app or subscribe to a service).

Applicable Processing Condition	Rationale
Article 6(1)(a)	Data subjects can "opt-in" to receive push notifications
Article 6(1)(e)	The processing may be necessary to provide updates and information necessary to the public health function but not necessary to the protection of vital interests

Process Environment

The processing environment for push notifications of this kind is that a message is formulated and then submitted for broadcast via the application.

However, this is dependent on network coverage and an active data connection and may discriminate against persons who have poor network coverage, particularly for data services.

Risks and Root Cause Analysis

We identify few risks associated with this proposed processing activity, assuming the purpose of processing to distribute push notifications is clearly explained and disclosed to data subjects.

Issue	Title	Description	Risk Priority	Criticality	Category
PN2_001	Push notification to children in error	Notification messages may be sent inappropriately to children. Less significant impact than contact trace push notifications but may cause upset/distress	90	20	Governance
PN2_002	Retention of contact information	A defined retention period would be required for retention of subscriber lists	144	32	Governance

The root causes here are related to the potentially open nature of the applications to download.

Recommended Mitigations

Issue	Title	Recommended Mitigation	Residual Risk Priorit..	Residual Criticality
PN2_001	Push notification to children in error	Implement appropriate safeguards to ensure age appropriate messaging is used	28	6
PN2_002	Retention of contact information	Recommend a retention period of 12 months after date of last message, benchmarked against SI336	26	6

The above mitigations substantively address the risks identified, however we would also recommend an alternative strategy be considered. The retention period for SMS contact information in this context is benchmarked against the “soft opt-in” provisions for electronic marketing to existing customers set out in the Irish legislation giving effect to the ePrivacy Directives.

Summary Comment on Approach

Rather than pursuing the strategy of a push notification via an application, we would recommend the creation of a subscription SMS service where individuals can subscribe directly, with .

This reduces the reliance on push notification, and removes any dependence on mobile network data services.

Conclusion and Recommendations

The development of contact tracing and symptom tracking applications has a clear benefit in the context of public health responses to infectious diseases, not just in the immediate context. However, the convenience and capability of smartphone application-based technologies needs to be balanced against the fundamental rights of individuals, particularly given the *de facto* introduction of a mass surveillance capability in response to a public health emergency.

Since the end of March there has been a rapid development of technical designs and approaches in this area, but we would caution that the rush to define the most perfect solution from a data protection and security perspective may have overlooked the need to consider the User Personas and the Business Needs and Approaches that need to be implemented to ensure the maximum effectiveness of these technologies in supporting the containment and (hopefully) eradication of Covid-19 as a public health threat.

The need to strike an appropriate balance has been recognised by the WHO, the EU Commission, the EDPB, and other key stakeholders. With great power comes great responsibility. But equally, the perfect is the enemy of the good, so it is essential that the decisions made in the design and execution of any application or the implementation of any technology clearly identify and address the trade-offs that are being made.

Transparency is an essential building block that any data-driven strategy for combating Covid-19 must be built on. This is the explicit consensus of the WHO, the European Commission, the European Data Protection Board, and international commentators. That we have seen the opposite of transparency from some national governments in their rush to develop applications (e.g. Ireland, the UK, and others), and from some of the consortia that have been promoting different frameworks for developing BT-LE enabled applications is disturbing.

There is no panacea at this time. We would strongly recommend that contact tracing be considered as part of a solution strategy encompassing hospital demand management, rapid testing, and a maintenance of good hygiene and social distancing practices until the effectiveness of the new technologies that are being developed to combat this new virus are proven, or until an effective vaccine is developed. We would also recommend that the temptation to develop a “swiss army knife” application should be tempered with the need to

ensure that each function that is deployed works effectively so as to build and maintain trust.

Recommendations

Consider the Life Cycle of the Process and Optimising the System

Any application or technology should be considered in the context of the overall process of pandemic response, whether it is managing a contact tracing process or minimising the immediate load on clinical care environments through remote monitoring.

Focussing on one aspect of the overall response process at the expense of others will result in a suboptimal overall outcome. The objective should be to optimise the overall response system through improved speed of contact tracing, faster deployment of and prioritisation of testing, and better management of clinical resources.

Therefore, consideration will need to be given to those areas of the target population who cannot be addressed or served through technology-enabled solutions.

Contact Tracing

1) Expectations should be managed in respect of Contact Tracing through a smart-phone model. There is, as of yet, no empirical evidence of the effectiveness of BT-LE for measurement of proximity in this way and there are a range of factors that will influence accuracy and the level of false positives and false negatives. There remains an open question as to the adequacy of this data for the purposes identified which may or may not be addressed through solutions implemented in device OS level APIs being developed.

2) Contact tracing applications should be built on a decentralised model and leverage the Apple/Google API when it is available. This, in our assessment based on the information available at this time, represents the architecture with the most likely potential to deliver effective interoperability, minimise impact on device battery life (and hence adoption), and meet user and Regulator expectations with respect to Data Protection by Design.

   A Centralised solution may be appropriate in the context of a specific jurisdiction where there may be economy of scale or operational dependencies on a neighbouring jurisdiction that has implemented a

centralised architecture . A DPIA is required to evaluate this and document that decision making process. It is important to note in this context that Germany, previously a strong proponent of a centralised solution, has abandoned the implementation of PEPP-PT based solutions in favour of a decentralised approach.

3) It is important to distinguish between the processing of Bluetooth Ephemeral identifiers, which may be processed in a decentralised manner, and the potential requirements for additional data being required by Public Health Officials. Therefore, a DPIA should consider the Use Cases and Business Needs/Approaches that arise throughout the Acquire/Analysis/Action life cycle. The shift in terminology by Apple/Google to describe the Bluetooth beacon processes as "Exposure Notification" is a subtle but important distinction that should be drawn.

4) The design of any application should consider the User Personas of those likely to be interacting with it. Consideration should be given to the potential impacts on children or persons with diminished capacity or other vulnerable persons.

5) Push Notifications should be implemented with caution and in a manner that supports and does not replace manual contact tracing.

6) The EDPB guidance is robustly clear on the requirements for the implementation of any application and those criteria should be considered in any DPIA. Note that a DPIA may highlight a requirement for domestic legislation to give effect to additional safeguards for personal data or fundamental rights and freedoms.

7) Transparency with Data Subjects during the design and development of any application is essential to ensuring trust in the process.

8) It is essential that Contact Tracing preserves the "human touch" in the design and execution of processes, particularly for vulnerable persons such as children or persons with diminished capacity.

9) The "call to action" from any push notifications from contact tracing functionality should be clear, intelligible, and accessible. It should be

capable of being understood by people with limited literacy or other language constraints.

10) A clear contact centre strategy is needed for any call to action arising from a push notification. Inbound calling is the most privacy preserving but has practical operational challenges that could limit effectiveness, not least the need to ensure that the inbound channel is appropriately resourced to handle large spikes in call volumes. Outbound calling raises another set of challenges and complications that will need to be considered. On-balance, a hybrid approach combining inbound and outbound call teams may be the best solution, with individuals potentially having a choice.

Symptom Tracking

11) Symptom tracking applications should be used in tandem with contact tracing and should be deployed with people who have been identified as a close contact to support monitoring of disease progression (or not) while these close contacts self-isolate. Wide spread public deployment risks creating a large volume of data but a low value of information due to data quality issues in self-reporting of symptoms and variances in self-reporting discipline among individuals.
12) Self-reported symptom tracking should NOT be used as the basis for triggering Contact Tracing alerts. This is easily gamed and will result in "alert fatigue".
13) Clinically monitored reporting of symptoms via an app, with appropriate clinical controls and quantitative data, should be considered as a strategy to support self-isolated case management and reduce hospital bed load for mild or suspected cases.

Location Data Analysis

14) Mobile network data analysis has a potential application in assessing population movements *en masse* and in assessing the effectiveness of population movement controls to limit spread, but they require substantial safeguards to be put in place to limit their impact on fundamental rights and freedoms

Application Strategy

15) Public Authorities should avoid the temptation to build all features into a single app, particularly when deadlines are tight and there is a need for

the delivered software to function with minimal error. There are (at least) two applications to consider:

a. **Contact tracing** – a *de minimis* app should allow for identification of close proximity contacts and communication with them
b. **Symptom tracking <u>for close contacts</u>**: - a *de minimis* application in this context should allow for the close proximity contacts of infected persons to record their symptoms and for that data to be accessible by public health officials.

Where the decision is taken to develop a single application with multiple functions (a "Swiss Army Knife"), we would recommend that a clear application functionality roadmap be defined and communicated to data subjects. This roadmap should set out the planned functionality, the planed sequencing for delivery, and the trigger events or factors that would make the implementation of that functionality in the application necessary and proportionate as requirements.

Excessive complexity in an application through scope creep or feature bloat in early releases will increase the likelihood of failure of the application and will impact adoption and acceptance by the community.

Transparency and Trust

We further recommend an excessive focus on transparency and communication of what is being done with people's data to ensure that data subjects can trust the processing. This extends to robust clarity on retention periods for identifiable data and the methods that will be used to aggregate data for research purposes which may arise subsequent to the initial response periods.

The importance of trust in this process cannot be understated to ensure that the right information is obtained in the right way to inform appropriate public health actions to support recovery and promote health. If any concept is to be adopted from the software development world into this process it should be the concept of the **minimum viable product**.

DPIAs should be published as "living documents" throughout the life cycle of the project and engagement with relevant civic society organisations is essential.

Ultimately, as Dr. Michael Ryan has pointed out, "The perfect is the enemy of the good" in pandemic response, but "mushroom management" of key stakeholders, the community, is the antithesis of trust.

References

de Hert, P., & Wright, D. (2012). *Privacy Impact Assessment.* Brussels: Springer.

DPC. (2018, November). *List of Types of Data Processing Operations which require a Data Protection Impact Assessment.*

DPC. (2019, September). *Guide to Data Protection Impact Assessments (DPIAs).* Retrieved from Data Protection Commission: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/190926%20Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29.pdf

EDPB. (2017, October 4). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whetherprocessing is "likely to result in a high risk" for the purposes of Regulation 2016/679.* Retrieved from European Data Protection Board: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Finneran-Dennedy, M., Dennedy, T., & Fox, J. (2014). *The Privacy Engineer's Manifesto.* Apress.

Justice, A., Rabeneck, L., Hays, R., Wu, A., & Rozzette, S. (1999). Sensitivity, specificity, reliability, and clinical validity of provider-reported symptoms: a comparison with self-reported symptoms. . *Outcomes Committee of the AIDS Clinical Trials Group*.

McDonald, S. (2016). *Ebola: A Big Data Disaster.* Dehli: The Centre for Internet and Society.

O'Keefe, K., & O Brien, D. (2018). *Ethical Data & Information Management: Concepts, Tools, and Methods.* Kogan Page.

Vokel, F. (2020, 03 23). *TraceTogether - Under the Hood.* Retrieved from Medium.com: https://medium.com/@frankvolkel/tracetogether-under-the-hood-7d5e509aeb5d

Appendices

Appendix 1: Mapping Castlebridge Framework to EDPB/DPC Guidance

Description of Methodology and Approach

The Castlebridge DPIA Framework

The analysis in this report has been carried out using the Castlebridge DPIA Framework. This methodology has been developed based on a proven quality management system for information management, which we have adapted to meet the requirements of a structured Data Protection Impact Assessment methodology. This assessment addresses the first six steps in this framework.

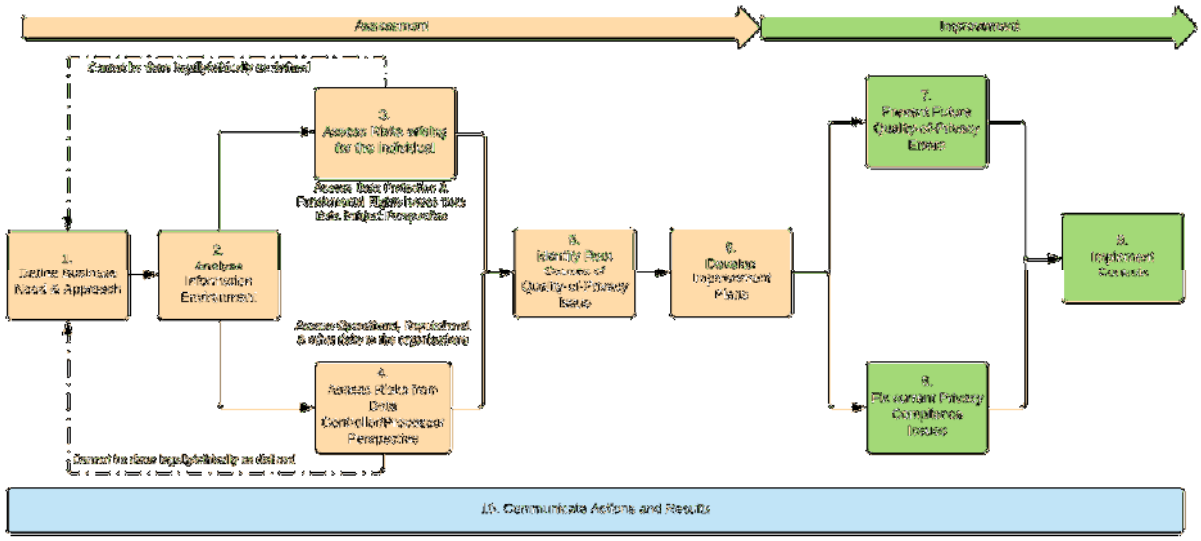


Figure 9: The Castlebridge DPIA Framework

The Castlebridge Ethical Impact Assessment Framework builds on the DPIA framework and extends it to consider wider ethical issues as appropriate. The full Ethical Impact Assessment model is described in (O'Keefe & O Brien, 2018)

Step	Summary Description
1	This step defines the processing purposes and seeks to break out the description of processing into discrete goals. It is also where an assessment of whether a DPIA is required is undertaken.
2	In this step we assess the broad information environment of the processing environment from different perspectives, including legal basis, necessity, proportionality, technology etc.
3	In these steps we conduct an assessment of the impacts on data protection rights, fundamental rights and freedoms, and organisation objectives to establish risks.
4	
5	In this step we determine the root cause of the issues /risks identified
6	In this step we develop remediation and mitigation plans to address the root causes of the risks identified in steps 3 to 5.

Data Protection Impact Assessments are intended to "identify and mitigate against any data protection related risks arising from a new project, which may affect your organisation or the individuals it engages with[i]". The primary concern at all times has to be the impact on data subjects. All impacts on data subjects, regardless of relative criticality or priority, have to be mitigated or addressed.

The Castlebridge DPIA methodology used in this Research Paper is a proprietary methodology developed to take account of the requirements under Recital 75 of GPDR and Recital 58 of the Law Enforcement Directive for organisations to assess risks from the perspective of the impact on the fundamental rights and freedoms of data subjects, while at the same time taking account of the c7ompeting interests of Data Controllers, to ensure that informed decisions are made regarding safeguards and other mechanisms envisaged to protect personal data, minimise the impact on fundamental rights and freedoms, and to demonstrate compliance with relevant legislation.

The methodology is adapted from a proven risk assessment methodology in quality management systems, Failure Modes and Effects Analysis[ii], and it explicitly recognises the impact of identified issues and risks to both the individual and to the organisation. These impacts are ranked on a 1 to 10 scale to allow for granularity of assessment. The likelihood of occurrence is also ranked on a scale of 1 to 10 and the likelihood of detecting the risk event (i.e. recognising that it is occurring) is also scored on a scale of 1 to 10. A composite "Risk Criticality" score is calculated based on the Impact on Individuals, Impact on the Organisation, and the Likelihood of Occurrence. A "Risk Priority" score is calculated by including the Likelihood of Detection. Therefore, highly critical risks which would be easy to detect and mitigate are given a higher priority score.

These scores are assigned to both the inherent risk assessment (before mitigations and controls are applied) and the residual risk assessment (after mitigations and controls are implemented). Mitigations usually focus on reducing the impact of the risk or its likelihood of occurrence.

Further information about the Castlebridge Risk Assessment Methodology can be obtained directly from Castlebridge.

The European Data Protection Board (EDPB) and Ireland's Data Protection Commission (DPC) have both published guidance on the conduct of Data Protection Impact Assessments. Our methodology maps to the high-level framework recommendations of both the EDPB guidance of 2017 (EDPB, 2017) and the guidance note from the DPC in September 2019 (DPC, 2019).

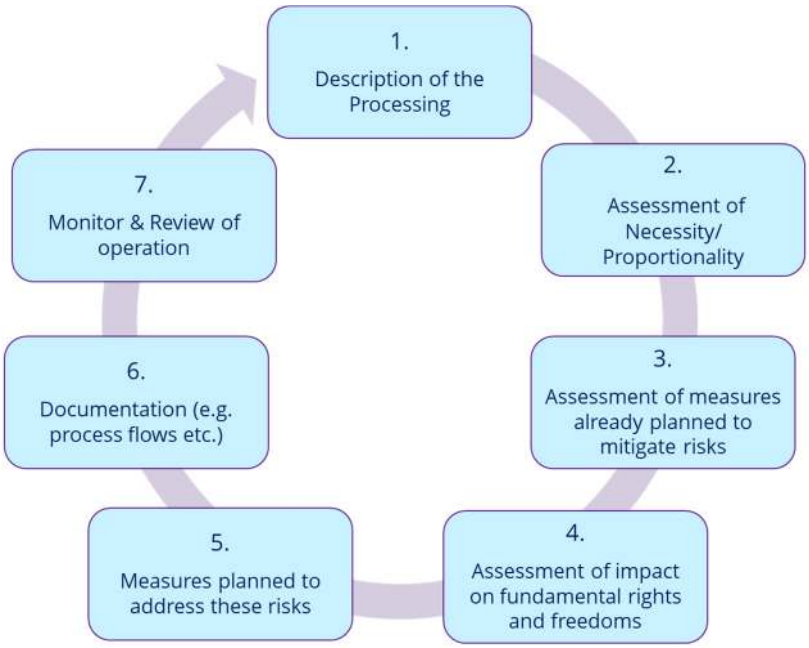


Figure 10 EDPB Data Protection Impact Assessment Process (source: WP248, rev.01, October 2017)

EDBP Step	Castlebridge Mapping	Comment
Step 1	Step 1- Business Need & Approach Definition	This is essential for the correct scoping and framing of the DPIA process.
Step 2	Step 2 – Assess Information Environment	Castlebridge Methodology breaks these activities into different task clusters from the EDPB generic format but the same activities are performed.
Step 3	Step 2 – Assess Information Environment Step 3 – Assess Data Subject Privacy Impact Step 4 – Assess Business Risk	
Step 4	Step 3 – Assess Data Subject Privacy Impact Step 5 – Identify Root cause	
Step 5	Step 2 – Assess Information Environment Step 5 – Identify Root Causes Step 6 – Develop Improvement plans	
Step 6	Step 2 – Assess Information Environment Step 10 – Communicate Step 7 - Fix current issues Step 8 - Prevent future issues	Documentation is provided for review as part of Step 2, documentation would be updated as part of implementation of PIA recommendations
Step 7	Step 9 – Implement Controls	PIA will recommend controls as part of improvement plans

Table 1: Mapping Castlebridge Methodology to EDPB Guidance

Risk Assessment Methodology

The Risk Assessment Methodology applied by Castlebridge is a proprietary risk assessment approach we have developed for Data Protection/Privacy Impact Assessments. It takes account of the clear requirement under Recital 75 of Regulation 2016/679/EU and the implied requirement in Recital 58 of Directive 2016/680/EU for organisations to assess risks from the perspective of the impact on the fundamental rights and freedoms of data subjects. The methodology applied also takes account of the competing rights and interests of Data Controllers for the purposes of informing decisions regarding safeguards and other mechanisms envisaged to ensure the protection of personal data and to demonstrate compliance with relevant legislation.

We apply a variant of the Failure Mode Effects Analysis[iii] methodology that is commonly applied in quality management systems. Within this analysis, we rank the following variables to calculate a risk criticality score. The variables we rank are set out in the table below. Rankings are performed on a 1 to 10 scale. The rubric and process for calculating risk criticality is also described below.

Variable	Definition
Impact on Individual (**IoI**)	An assessment of the impact on the fundamental rights and freedoms or choice/agency of individuals arising from or as an outcome of the proposed processing activity
Impact on Organisation (**IoO**)	An assessment of the impact on objectives of the organisation or on the brand or operations of the organisation in the event that this risk materialises
Likelihood of Detection (**LD**)	An assessment of how likely it is, in the normal course of operations and in light of the identified controls and mitigations that have been or will be implemented, that the occurrence of a risk would be identified in a timely manner sufficient to minimise impact on individuals or organisations
Probability of Occurrence (**PO**)	An assessment of the probability that a given risk would manifest itself as an actual event impacting individuals or the organisation.
Weighted Impact on Individual (WIOI)	Where a Risk weighting bias is included in the calculation to reflect a priority to the Individual or organisation this is calculated as (IoI * Risk Bias)
Weighted Impact on Organisation (WIOO)	Where a Risk weighting bias is included in the calculation to reflect a priority to the Individual or organisation this is calculated as (IoO * Risk Bias)
Criticality of Risk (**CoR**)	A calculation of the severity of the risk without consideration of ease of detection. ***COR=(Average(WIoI:WIoO)*PO***
Risk Priority (**RP**)	A calculation of the relative priority of a risk taking into account of the likelihood of detection. It is calculated as follows: ***RP=(Average (WIoI:WIoO)*LD*PO)***

Table 2 Risk Calculation and Assessment Variable

Presentation of Risk Assessment

The Risk Assessment is presented in a standard grid format that allows for summarisation by Risk Priority Score or Risk Criticality score. For the purposes of colour coding risks, the maximum and minimum risk scores are calculated as hidden values to ensure an appropriate Red/Amber/Green coding across all values. The maximum Risk Priority Score is 1000 and the minimum is 1. The maximum Risk Criticality is 100.

The Risk Bias value allows for a weighting between the right of the individual and the interests of the organisation to be explicitly applied. This bias is on a scale of 0 to 100 and results in the calculation of a Weighted Impact score for Individuals and Organisations which is used as the basis for Risk Priority and Criticality calculation.

The template also captures the recommended remediation for the specific risk and the Residual Risk Priority and Risk Criticality scores based on the recommended remediations being applied.

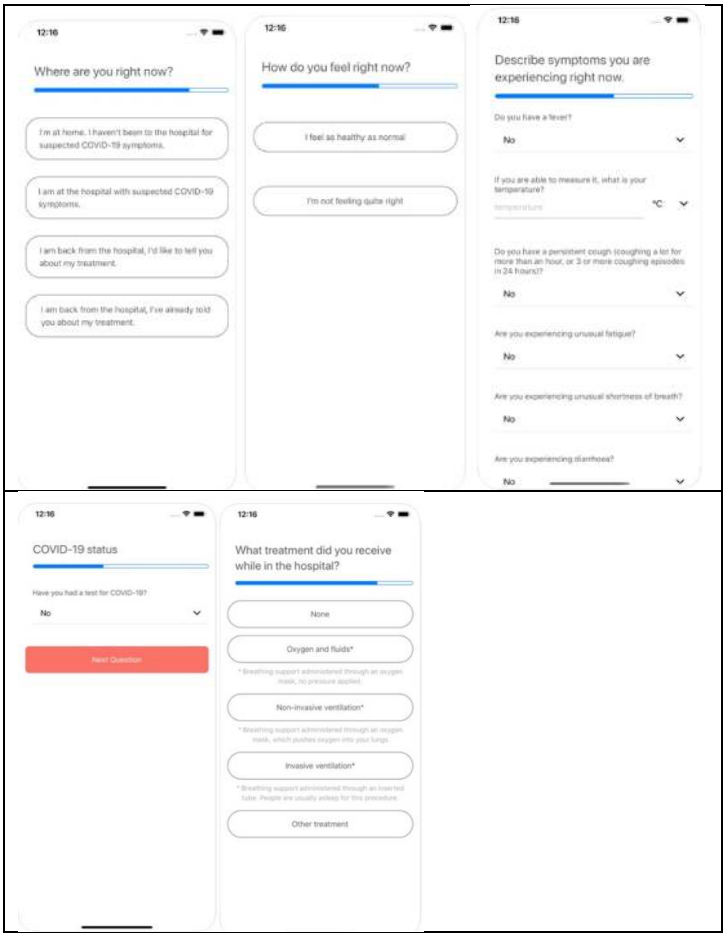
Risk Bias	Individual	Organisation																	
	60	40																	
Issue	**Title**	**Description**	**Impact on Individual**	**Impact on Organisation**	**Probability of Occurrence**	**Likelihood of Detection**	**Weighted Impact Individual**	**Weighted Impact Org**	**Risk Priority**	**Criticality**	**Category**	**Recommended Mitigation**	**Residual Impact on Individual**	**Residual Impact on Organisation**	**Residual Probability of Occurrence**	**Residual Likelihood of Detection**	**Weighted Impact Individual**	**Weighted Impact Org**	**Residual Risk Priority**	**Residual Criticality**
Unique ID	**Failure mode / Risk**	**Failure mode / Risk description**	**1- 10 Score**	**1 -10 score**	**1 -10 score**	**1 - 10 Score**	Individual score * Weighting	Organisation score * Weighting	RPN Score	Criticality Sore	**Categorisation of Root Cause Type**	**Recommended Mitigation**	**1- 10 Score**	**1 -10 score**	**1 -10 score**	**1 - 10 Score**	Individual score * Weighting	Organisation score * Weighting	RPN Score	Criticality Sore

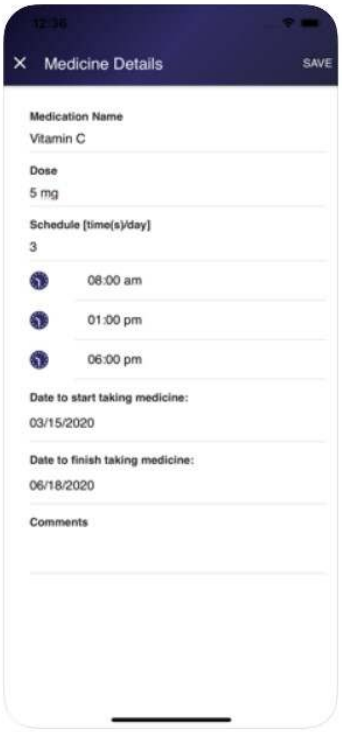
Figure 11: Example of Risk Assessment Template

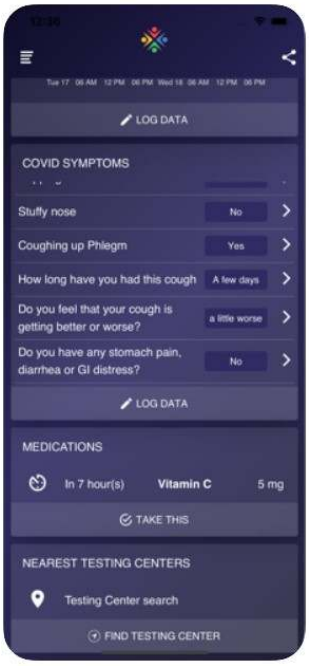
Appendix 2: Screenshots from Symptom Tracing Apps

Castlebridge reviewed two Symptom Tracking applications as part of this research review. These screenshots are sourced either from the application itself or from the Apple Appstore page for the application. It must be noted that there is a substantial transparency deficit in many of the Covid-19 symptom tracker applications.

Covid19.Zoe







[i] Source: Data Protection Commissioner Guidance on DPIAs: https://dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments

[ii] Failure Mode and Effects Analysis is a standard process analysis tool used in quality management systems initially developed by the US military in the 1940s and forming the basis of quality management systems such as Total Quality Management and Six Sigma. The objective of an FMEA analysis is to support a cross-functional assessment of the things that might go wrong in a proposed process (Failure Modes) and the likely impacts or consequences of these failures (Effects). Failure modes are prioritised based on the severity of their impact, the likelihood of their occurrence, and the likelihood that they can be detected (and therefore prevented or mitigated). Further information on the FMEA methodology can be found at the American Society for Quality (ASQ.org).

Castlebridge has adapted the FMEA approach from quality systems to apply to the objective assessment of issues arising in data protection assessments. This adapted methodology explicitly recognises impacts on individuals and on the organisation in respect of an identified risk materialising. This allows for risks to be prioritised accordingly for treatment in any remediation plan or preventative definition of controls as part of a DPIA. This methodology is proprietary to Castlebridge and has used in a number of DPIAs for public sector projects since 2012. Training in the methodology has also been delivered extensively to Public Sector organisations and government departments either in-house or through Public Affairs Ireland. The methodology is also taught on the Law Society Certificate in Data Protection Practice since 2013 and in the UCD Sutherland School of Law Diploma in Data Protection and Governance

[iii]