eHealth Network

Mobile applications to support contact tracing in the EU's fight against COVID-19

Common EU Toolbox for Member States

Version 1.0

15.04.2020

The eHealth Network is a voluntary network, set up under article 14 of Directive 2011/24/EU.
It provides a platform of Member States' competent authorities dealing with digital health. The Joint Action supporting the eHealth Network (eHAction) provides scientific and technical support to the Network.

Adopted by consensus by the eHealth Network, Brussels, Belgium, 15 April 2020

CONTENT

EXECUTIVE SUMMARY

Mobile apps have potential to bolster contact tracing strategies to contain and reverse the spread of COVID-19. EU Member States are converging towards effective app solutions that minimise the processing of personal data, and recognise that interoperability between these apps can support public health authorities and support the reopening of the EU's internal borders.

This first iteration of a common EU toolbox, developed urgently and collaboratively by the e-Health Network with the support of the European Commission, provides a practical guide for Member States. The common approach aims to exploit the latest privacy-enhancing technological solutions that enable at-risk individuals to be contacted and, if necessarily, to be tested as quickly as possible, regardless of where she is and the app she is using. It explains the essential requirements for national apps, namely that they be:

* *voluntary;*

* *approved* by the national health authority;

* *privacy-preserving* - personal data is securely encrypted; and

* *dismantled* as soon as no longer needed.

The added value of these apps is that they can record contacts that a person may not notice or remember.

These requirements on how to record contacts and notify individuals are anchored in accepted epidemiological guidance, and reflect best practice on cybersecurity, and accessibility. They cover how to prevent the appearance of potentially harmful unapproved apps, success criteria and collectively monitoring the effectiveness of the apps, and the outline of a communications strategy to engage with stakeholders and the people affected by these initiatives.

Work will continue urgently to develop further and implement the toolbox, as set out in the Commission Recommendation of 8 April, including addressing other types of apps and the use of mobility data for modelling to understand the spread of the disease and exit from the crisis.

I THE ROLE OF MOBILE APPS IN COMBATING COVID-19

1. BACKGROUND

The World Health Organisation (WHO) has declared the COVID-19 to be a pandemic[1]. Mobile applications ('apps') can support health authorities at national and EU level in monitoring and mitigating the ongoing COVID-19 pandemic, facilitate the organisation of medical follow-up of patients and provide direct guidance to citizens on playing their part in the control of the disease.

In a number of countries, both within the EU and worldwide, national authorities or developers have announced the launch of apps offering varying levels of functionality to support the fight against the virus. Member States recognise the value of such apps needs to be considered within the context of wider public health measures and the stage of the spread of the contagion. Apps that support contact tracing in particular have emerged as the most promising, from a public health perspective. These apps offer the possibility of alerting/ warning citizens that they have been in close proximity with an individual who has been confirmed positive for Covid-19. (For the purposes of this toolbox 'contact tracing and warning apps' refers to apps with such a functionality).

2. CONTACT TRACING AND WARNING

Contact tracing and warning can play an important role in all phases of the outbreak especially as part of containment measures during de-escalation scenarios. Its impact can be boosted by a strategy supporting wider testing of persons showing mild symptoms.

The aim of contact tracing and warning is for public health authorities to rapidly identify as many contacts as possible with a confirmed case of COVID-19, ask them to self-quarantine if possible, and rapidly test and isolate them if they develop symptoms. The aim of contact tracing could also be to have anonymised and aggregated data of infection patterns in society, as a means to make containment decisions at local level. At EU and world level, the ECDC and WHO have asked Member States to identify and follow up nationally contacts linked to each case so as to interrupt transmission and, as a secondary objective, understand transmission dynamics.

Contact tracing is normally carried out manually by public health authorities. This is a time-consuming process where cases are interviewed in order to determine who they remember being in contact with from 48 hours before symptom onset and up to the point of self-isolation and diagnosis. Longer contact duration and closer proximity means a higher risk of infection. This process relies on the recall of the case by the patients – who may be very ill at the time of interview – both in terms of who they have met and the proximity and duration of that meeting, as well as the ability to produce names and phone numbers of these people (or 'contacts'). Such manual processes relies on the patient's memory and obviously cannot trace individuals who have been in contact with the patient but are who are unknown to him/her.

3. TRACING AND WARNING APPS

Digital tools such as mobile apps with tracing functionalities can be of substantial support in this process, identifying both known and unknown contacts of a confirmed

[1] http://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19/news/news/2020/3/who-announces-covid-19-outbreak-a-pandemic

case and possibly help in their follow up, in particular in settings with large numbers of cases where public health authorities can get overwhelmed. Such functionalities can help identify more contacts and speed up the overall process substantially, which is of essence in this pandemic. The functionality in such apps, if rolled out on a large scale so that they reach well over 50% of the population[2], could be useful for Member States to rapidly detect contacts of cases, collect information on these contacts and to inform contacts on the need for follow-up and testing if required. In addition, the apps can provide contacts of COVID-19 cases with the information on how to reduce the risk of further transmission and advice on what to do if they develop symptoms.

Such apps should only be developed and implemented in close coordination with and under the oversight of the relevant public health authorities. Public health authorities will coordinate the local contact tracing process in line with international guidance which defines which contacts should be followed up and what the management of these contacts should be.

In parallel with mobile applications, manual contact tracing will continue to play an important role, in particular for those, such as elderly or disabled persons, who could be more vulnerable to infection but less likely to have a mobile phone or have access to these applications. Rolling-out mobile applications on a large-scale will significantly contribute to contact tracing efforts also allowing health authorities to carry manual tracing in a more focussed manner. Public health authorities will continue using currently available software (e.g. national contact tracing systems and Go.Data from WHO/GOARN) to manage the contact tracing and contact management process. The apps should be able to interact/complement the contact management tools used by Member States. These apps should include functionality to ensure that any communication with contacts is undertaken securely and in line with local public health guidance.

4. RATIONALE FOR A COMMON EU APPROACH TO TRACING AND WARNING APPS

Contact tracing apps are the present focus of a common approach to the use of mobile apps and data, although other functionalities may be addressed in future iterations of the Toolbox, as set out in the Commission Recommendation of 8 April 2020.

Close proximity to individuals affected seems to be the main means of transmission of the virus. This digital technology, if deployed correctly, could contribute substantively to containing and reversing its spread. Deployed without appropriate safeguards, however, it could have a significant negative effect on privacy and individual rights and freedoms. This common approach to contact tracing apps aims therefore to ensure interoperable and privacy-preserving digital contact tracing of EU citizens, to be applied consistently by all Member States with the full support of the EU. A fragmented and uncoordinated approach to contact tracing apps risks hampering the effectiveness of measures aimed at combating the COVID-19 crisis, whilst also causing adverse effects to the single market and to fundamental rights and freedoms.

A common approach therefore requires a cross-border interoperability mechanism – complementing current solutions such as the Early Warning and Response System. It

[2] A study quoted here by researchers at Oxford University's Big Data Institute said 60% of a country's population would need to be involved for the approach to be effective.

must ensure that citizens moving between countries are all benefiting from Member State approved apps wherever in the EU the device happens to be, thus supporting the relaxation of containment measures across the different Member States.

The common approach discussed in this document builds on the information and best practice shared by Member States in the eHealth Network. Contact tracing apps need to be fit for purpose, compliant with applicable laws and respecting the values and fundamental rights and freedoms of the EU. At a national level, the available app should be officially recognised by the public health authority. Their acceptance and take-up by individuals depends on whether the public perceive them as effective, accurate, privacy-protective and trustworthy, avoiding mass surveillance and strictly limited in time to the duration of the current crisis.

In particular, Member States are considering the need for public health authorities to process personal data in the interests of public health while at the same time minimising the limitation of rights to personal data and privacy through, for example, processing of personal data at the level of the mobile device. This common approach is therefore complemented by guidance from the Commission on data protection and privacy aspects of the use of these apps. Furthermore, the large volume and sensitivity of the data that will be processed require robust cybersecurity measures (set out in this toolbox) to mitigate the risk of security and data breaches which could have the devastating effect on the trust of public in the use of those apps.

5. OBJECTIVE AND STRUCTURE

In this first version, this toolbox sets out the various relevant parameters to enable a coordinated development and use of officially recognised contact tracing applications and the monitoring of their performances.

For this purpose, it provides a detailed list of baseline requirements and functionalities that should be taken into account throughout this process.

These requirements and functionalities have been identified collectively by Member State authorities who are considering the launch of an app to support contact tracing.

Overall, this constitutes a pan-European approach for officially recognised COVID-19 mobile applications. In Section II, this document provides an overview of existing frameworks and measures regarding contact tracing apps, both globally and at Member State level.

In Section III, this document outlines the various requirements and elements of a common EU approach to mobile contact tracing applications. They reflect the Member States' collective understanding of the requirements for officially recognised contact tracing apps from a public health perspective taking into account specific scenarios of the spread of the contagion. They cover several key aspects including the epidemiological framework, technical requirements, how to ensure interoperability across the EU, address accessibility, governance, exchange of information between Member States, evaluating the performance of the apps and the prevention of non-official apps that could be harmful or contradict this common approach. **These requirements and elements are described in detail in the table in Annex 1**. In particular, this section addresses the options for privacy preserving solutions in support of public health efforts.

Section IV addresses the importance of clear and regular communications with the public on the use of tracing and warning apps.

Section V outlines next steps notably concerning implementation of this toolbox and its evaluation as well as other actions included in the Commission Recommendation of 8 April 2020

Annexes apart from Annex 1 that sets out the EU common approach include other documents that detail various relevant aspects of the toolbox.

6. SCOPE

This common approach applies to apps that are voluntarily installed, and alert people who have been in proximity for a certain duration to an infected person, in order to get tested or to self-isolate (contact tracing and warning functionality).

A common approach to other functionalities, in particular on information and symptom tracking functionalities, is likely to be developed in future iterations of the toolbox.

II OVERVIEW OF COVID-19 APPS CURRENTLY AVAILABLE

1. GLOBAL DEVELOPMENTS

Since the beginning of the COVID-19 pandemic, many smartphone apps have been developed, some of them by public authorities. Singapore was one of the first to introduce digital tools for combating COVID-19, where the Ministry of Health developed a contact tracing application that registers contacts between users and that sends a notification to those that have been in contact with infected patients. Singapore recently published the source code of their application. The World Health Organization (WHO) is working on the development of an application that would provide medically-approved information and advice to users based on their symptoms[3]. This standalone application comes besides the WhatsApp-based messaging service launched in late March 2020 that provides up to date information on Covid-19[4].

On 10 April 2020, Google and Apple jointly announced an initiative related to the use of the Bluetooth protocol to support contact tracing apps.[5]. The protocol would support the use of Bluetooth LE (Low Energy) for proximity detection of nearby mobile phones, and for the data exchange mechanism that alert participants of possible exposure to someone who they have recently been in contact with, and who has subsequently been positively diagnosed as having the virus[6].

[3] More technical information is available in the official GitHub repository of the WHO (work in progress at the time of writing): https://worldhealthorganization.github.io/app/.

[4] https://www.who.int/news-room/feature-stories/detail/who-health-alert-brings-covid-19-facts-to-billions-via-whatsapp

[5] https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/ The announcement included the publication of three draft technical documents on Bluetooth and cryptography specifications and framework documentation.

[6] To implement the protocol, in May, they intend to launch application programming interfaces (APIs) and operating system-level technology that enable interoperability between Android and iOS devices for such apps that support contact tracing apps and that are officially approved by public health authorities. As a second step, in the coming months, they intent to build this functionality into the underlying platforms of

2. EUROPEAN INITIATIVES

Different consortia, gathering mainly academia and private actors, are developing approaches that could be used for developing contact tracing applications, in line with European privacy values. Many of them are open initiatives and several health authorities are following up their work and progress.

In Europe, the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)[7] consortium intends to support the development of national initiatives that pursue a fully privacy-preserving approach by providing ready-to-use, well-tested, and validated modules and tools. It also aims to enable tracing of infection chains across national borders. Initiatives under the umbrella of PEPP-PT, aim at an open protocol for COVID-19 proximity tracing using Bluetooth Low Energy on mobile devices and an architecture that ensures that personal data stays entirely on an individual's phone.

National initiatives

Several Member States in the EU and EEA have launched or intend to launch initiatives that involve contact tracing apps in the fight against Covid-19. The following is a brief, non-exhaustive list of ongoing initiatives, more detailed information can be found in Annex III:

Type	**MS**	**Description and status**
Contact tracing	AT	Similar to Singapore/ PEPP-PT platform. It builds on the exchange of (manual and automatic) digital handshakes via Bluetooth (BLE). U Uses ultrasound and WLAN only to estimate the distance between two devices. This is done using Google Nearby (with data storage in the U.S.) and P2P kit Mobile number is communicated by the user only once he or she is confirmed infected Austria "Epidemics Law"
Contact tracing	CY	Uses geo location data based on MIT SafePaths

their operating systems, which users of the device could opt into. The companies promised to provide further information but did not commit to release the source code.
The protocol excludes processing of any location data – unless the user opts in, applies 'Rolling Proximity Identifiers' that prevent identification of the user, processes proximity identifiers obtained from other devices exclusively on the device, permits only users to decide whether to contribute to contact tracing by sharing Diagnosis Keys with the 'Diagnosis Server' if diagnosed with COVID-19, resulting in the alert to other users. Matches stay local to the device are not revealed to the server. The details and implications of this announcement from a medical and privacy perspective requires further analysis and discussion.

[7] https://www.pepp-pt.org/

Contact tracing	CZ	Uses location data from mobile operators to construct "memory maps" (visualization of locations the person spent significant time in the last 5 days), which help specialists to lead more effective and efficient contact tracing call with infected people. Endorsed by the Ministry of Health and currently in pilot operation in 3 regions.
Contact tracing and warning	DE	Under consideration, probably based on PEPP PT and Bluetooth
	EE	Analysing different options with a preference to privacy enhancing solutions based on consent such as PEPP-PT, emphasizing the need for cross-border interoperability.
	FI	Aiming for privacy enhancing approach International developments under consideration
Contact tracing	FR	Uses Bluetooth to detect transmission chains for the coronavirus and help limit the spread. Under development in cooperation with PEPP-PT and with input from the French data protection authority.
Symptom checking and contact tracing	IE	Provides citizens with a way to check their Covid-19 symptoms and receive reliable advice. This data can be submitted to inform national heat maps. Contact tracing app also informs national heat maps and modelling of the spread of the disease. Currently in test. Will launch in advance of the lifting of restrictions on movement of citizens (or just before)
Contact tracing	IT	Launched and completed an open call to assess the state of the mobile apps for contact tracing, and selected two candidate solutions, currently at the beta version stage, to be tested in the field, before national roll-out. IT Strategy proposed by the Governmental COVID-19 Task-force has been evaluated by the Italian Government and it is going to be implemented over the next weeks.
Contract tracing	IS	Helps to analyse individuals' travel and trace their movements against those of other people when cases of infection or suspected infection arise. Available
Contact tracing	NL	The Ministry of Health of The Netherlands, together with the National Privacy Authority, is in the process of developing an app

Contact tracing	NO	Combines Bluetooth and GPS data to rapidly detect and give advice to people who may be infected with the coronavirus and to monitor the spread of the infection and to assess the effects of the infection control measures. Based on central storage of encrypted information. Twofold purpose: Individual tracing and warning of close contacts, and anonymised tracking of infection patterns in society. Under development
Contact Tracing and self-diagnostic app and quarantine enforcement application[8], since 1 April (the latter is not in the scope of this toolbox)	PL	Downloaded voluntarily, the application uses Bluetooth to record contacts, informs users (and health authorities) of exposure to an infected person, and provides users with verified medical advice. The risk-assessment is supplemented with a "health diary" self-diagnostic monitoring tool as well as a dedicated helpline. In the final stages of development. Interoperability with domestic health authority's backend has been ensured and the majority of the code has been published online. Launch is to occur imminently and an information campaign is ongoing since late March.
Contact tracing	PT	Interoperability between existing system will be guarantee in the mApp, symptom checker (this functionality will be used in the app as well), connected with "TRACE COVID-19 System" (Surveillance and Monitoring) and NHS24 referral system. Under consideration

III A COMMON APPROACH TO MOBILE CONTACT TRACING AND WARNING APPLICATIONS

Requirements for contact tracing and warning apps will necessarily vary to some extent according to the situation in individual Member States. The following requirements represent Member States' collective understanding of best practice and constitute common European approach.

The requirements are divided into four parts: 1) essential requirements covering the epidemiological framework, technical functionalities, cross-border interoperability requirements as well as cybersecurity measures and safeguards 2) measures aimed to ensure accessibility and inclusiveness 3) governance/role of public health authorities covering approval of tracing apps and their access to data generated by tracing apps, 4) supporting actions covering sharing of epidemiological information and cooperation with ECDC, measures to prevent proliferation of harmful apps and monitoring of effectiveness of apps.

A more detailed overview of each functionality and/or type of app, as well as the relevant actors concerned is presented in ***Annex 1.***

[8] https://www.gov.pl/web/koronawirus/aplikacja-kwarantanna-domowa--od-dzis-obowiazkowa

1. ESSENTIAL REQUIREMENTS FOR NATIONAL APPS AND CROSS-BORDER INTEROPERABILITY

a. Epidemiologic framework

With regard to the epidemiologic framework, Member States should consider the following:

i. An approach based on epidemiological heuristics

- Adopt the heuristics as commonly agreed by ECDC (guidance on contact tracing[9]) with epidemiological bodies in each Member State and, where necessary, allow the update thereof in particular with regard to what is epidemiologically sufficient in terms of: proximity, distance, historical importance of the proximity (that is, 14 or 16 days), as well as definitions of different types of contact[10].

ii. Notification of contacts

- Clearly define and observe procedures at the level of each Member State for how to inform and manage persons who may have been exposed to the virus.

- Allow only authorized public health authorities or other authorized parties such as laboratories to confirm an infection and define how the warning alert should be triggered.

- Provide immediate information to the users at risks (i.e. the 'contacts' of an infected person) about potential infection and what to do next. The content of this message should be designed by public health authorities, including best practices for suspected cases who have not yet confirmed by testing. The message could include, for example, information on self-quarantine, what symptoms to look for and what to do if symptoms develop.

- Depending on the national laws, the health authorities may contact directly the user that was in close contact with a COVID-19 patient. The users should however be informed at the time of the installation of the app, that he/she may be contacted by the authorities.

- When a user has tested positive, the public health authority should authorise the app to notify and manage different levels of risk related to the intensity and the proximity of contacts, other concerned users that their device has been in proximity to a device whose user has tested positive for COVID-19 or has

[9] https://www.ecdc.europa.eu/en/covid-19-contact-tracing-public-health-management-second-update

[10] See COM guidance on data protection. The ECDC provides guidelines of what the definition is of different contacts ('high-risk exposure contacts' have had contact with the case for a longer duration and in closer proximity, whereas 'low-risk exposure contacts' have more fleeting exposure. Member States ultimately determine their own definitions of different types of contacts. As the public health community come to understand more about transmission dynamics – for example around the risk of transmission via smaller droplets that can travel over larger distances – these definitions may have to be revised. It is essential that the functionality can be re-programmed in an iterative manner. In fact, by collecting and analysing data from contact tracing apps, and by cross checking these with actual test result data, public health authorities can learn whether they are casting the net too wide or too narrowly in terms of the proximity and duration parameters they have programmed in the app.

signalled significant symptoms, while ensuring that the app does not reveal the identity of the user who has tested positive.

- Put in place adequate security and privacy safeguards for data collection, retention and sharing policies.

- Apps should be disabled once the pandemic has passed. If it is not possible to disable or remove apps from individual phones, authorities should no longer collect data or seek Covid-19 related data from citizens. Techniques like notifications should be considered to prompt users to disable or completely remove these apps from their phone.

iii. Privacy-preserving app solutions that support public health efforts

Member States have been considering the most appropriate app solutions for their specific situations that comply with applicable laws and minimise the processing of personal data. Some apps have already been launched, are close to launching or still under development. These apps can be grouped into at least two general categories:

1) Decentralised processing

The proximity data related to contacts generated by the app remains only on the device (mobile phone). The apps generate arbitrary identifiers of the phones that are in contact with the user. These identifiers are stored on the device of the user with no additional personal information or phone numbers.

The provision of mobile phone numbers or other personal data by the user at the time of the app installation is not necessary, because an alert is automatically delivered via the app the moment that a user notifies the app – with the approval of the health authority - that he/she has test positive.

Public health authorities determine the content and timing of the notification message. The message may, for example, ask the person to stay at home and/ or to contact the public health authorities, should they develop symptoms and to facilitate testing.

This approach would considerably reduce the risks to privacy as close contacts would not be directly identifiable and this option would thereby enhance the attractiveness of the application. Public health authorities would not, however, have access to any anonymised and aggregated information on social distancing, on the effectiveness of the app or on the potential diffusion of the virus. This information can be important to manage the exit of the crisis.

Although not necessary for the functioning of the app, an alerted person (that she/he was in contact with a positively tested person) may wish to provide personal information (e.g. phone number) to the public health authorities in order to get further support and guidance. The app can provide an option to do so. This should be an "opt in" option and clearly indicated as "opt in". The authority can then make contact with the individual and advise him or her accordingly.

2) Backend server solution

In this option, the app functions through a backend server held by the public health authorities and on which are stored the arbitrary identifiers. Users cannot be directly

identified through these data. Only the arbitrary identifiers generated by the app are stored on the server. The advantage is that the data stored in the server can be anonymised by aggregation and further used by public authorities as a source of important aggregated information on the intensity of contacts in the population, on the effectiveness of the app in tracing and alerting contacts and on the aggregated number of people that could potentially develop symptoms.

Through the identifiers, users who have been in contact with a positively tested user will receive as in the previous version an automatic message or alert on their phone. As in the previous version, an alerted person (that she/he was in contact with a positively tested person) may wish to provide personal information to the public health authorities in order to get further support and guidance. The user should express his/her consent, in case they wish to be contacted by the health authorities. The app can provide an option to do so. This should be an "opt in" option and clearly indicated as "opt in". The authority can then make contact with the individual and advise him or her accordingly. Some public health authorities have a policy to phone all contacts directly rather than rely on automated notifications, in which case users of the app should be given the option to provide their contact numbers as part of the registration process and based on explicit consent of the user.

This supplements manual contact tracing effort (where positive cases are interviewed), notably because penetration of the contact tracing app in the population is likely to be incomplete, and particularly because many vulnerable individuals such as the elderly are may not have access to this app. It would help authorities detect surges in cases, as well enabling them to follow up in a more personalised way contacts who are at risk of infection.

None of the above two options includes storing of unnecessary personal information. Options where directly-identifiable data on every person downloading the app is held centrally by public health authorities, would have major disadvantage, as noted by the EDPB in its response to consultation on Commission draft guidance on data protection and tracing apps. These options would not keep personal data processing to the absolute minimum, and so people may be less willing to install and use the app. Centralised storage of mobile phone numbers could also create risks of data breaches and cyberattacks.

b. Technical functionalities

In order to ensure effectiveness of the apps, several requirements concerning technical functionalities should be considered by the Member States. These concern aspects related to:

i. Proximity technology and recording

Member States should consider specifications which allow contact detection to an accuracy of one metre[11], in order to minimise false positives. Such specifications should concern, among others, aspects related to the sending and receiving of Bluetooth signals, the capability to estimate proximity with precision, the capability to record and store unique, ephemeral, pseudonymised IDs observed from other mobile phones or devices in

[11] For example, Bluetooth detection could deliver false positives when it detects proximity to the device of someone wearing a face mask or even on the opposite side of a wall.

epidemiologically relevant proximity on the device. They should also allow the recording of the device's proximity to another device, and the duration of this proximity, on which is running any COVID-19 app officially recognised by national health authorities.

ii. Generated ID and code

Member States should ensure that the ephemeral ID is generated pseudo-randomly and changes periodically to enhance the protection against eavesdropping, as well as hacking and tracking by third parties. Likewise, the code (a one-time-password) created by the relevant health authorities to confirm that a user is infected should be generated pseudo-randomly be single-use, and change frequently in order to ensure that it cannot be used by malicious individuals to pollute the data collected on the server. *See also the cybersecurity requirements in sub-section III.1.d) below.*

iii. Performance

Member States should ensure that the apps' performance allows, among others: (i) *accuracy*, and notably that it records accurately actual physical proximity and duration of contact; (ii) *completeness*, and notably that it holds a complete history of relevant contacts as in traditional manual contact tracing, in a irrefutable way; (iii) *integrity*, and notably that it only records authentic contact events with at-risk individuals and (iv) *scalability and (v) security*, and notably backend architecture and technology that can be deployed with local IT infrastructure and can scale to billions of users, while ensuring a high level of network and information security.

c. Cross-border interoperability requirements

i. Necessity of interoperability between mobile tracing and warning apps

Infection transmission chains do not stop at national or regional borders. To collaborate and manage cross-border transmission chains, national health authorities should be technically able to exchange available information about individuals infected with and/or exposed to COVID-19. Tracing and warning apps should therefore follow common EU interoperability protocols so that the previous functionalities can be performed, and particularly safeguarding rights to privacy and data protection, regardless of where a device is in the EU. Such protocols should be created and provided to developers to ensure three key requirements:

1) the alignment of epidemiological criteria to define close contacts for a high risk exposure, following WHO and ECDC guidance[12] on the determinants of contact tracing, including the definition of close contact (distance and duration of exposure) and the period for which contacts are stored (for how long);

2) contact tracing apps to register a user's proximity contacts with other users using different contact tracing apps (indicated as (1) in the diagram below); and

[12] ECDC, Contact tracing: public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union – second update, technical report, 8 April 2020, https://www.ecdc.europa.eu/sites/default/files/documents/Contact-tracing-Public-health-management-persons-including-healthcare-workers-having-had-contact-with-COVID-19-cases-in-the-European-Union–second-update_0.pdf.

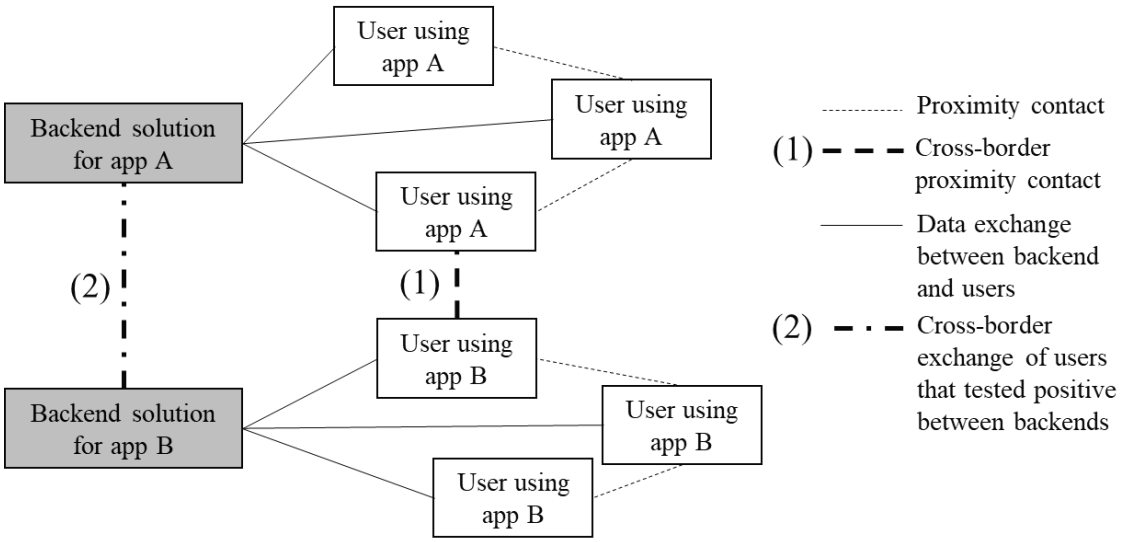
3) national authorities to exchange data on infection transmission chains by means of backend solutions, in order to interrupt cross-border transmission chains (indicated as (2) in the diagram)[13].

ii. Technical requirements

By envisioning a scenario where several mobile apps exist in the EU (e.g. one app per country or region), it is necessary to create common foundations for these different pieces of technology to work together to an EU-wide contract tracing network. Three of the main building blocks of such foundations are:

1) the proximity-based contact tracing mobile apps installed in each smartphone, and
2) backend information systems used to manage the information flows with such apps, deployed nationally or regionally.
3) epidemiological agreements - all Member States in Europe would use the same definitions (eg proximity, etc), based on ECDC guidance on contact tracing[14].

Those building blocks and the relevant information flows are depicted in the following diagram, for two separate contact tracing systems (A and B). The white building blocks represent the users and their devices, equipped with a contact tracing app from their respective Member State or region. They are capable of recording proximity contacts with other users, and exchange limited non personal information with the corresponding backend solution. The grey building blocks represent the backend solution which sends and receives information from the apps. The backend solution also must exchange data with other backend solutions. The data sent and received from the apps heavily depends on the architecture of the overall systems.



[13] The contact tracing protocol released by Apple and Google on 10 April 2020 appears to address requirement 2) and 3). An example of a protocol covering Requirement 3 is the one established in the context of the Early Warning Response System (EWRS), which links the European Commission, ECDC and public health authorities in the EU and EEA countries responsible at national level for notifying alerts and determining the measures required to protect public health (Articles 8, 9 and 10 of Decision No 1082/2013/EU).
https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

[14] https://www.ecdc.europa.eu/en/covid-19-contact-tracing-public-health-management-second-update

Figure 1. Two proximity-based contact tracing systems, including data flows and interoperability requirements.

iii. Implementing interoperability

Cross-border data flows between apps depend on consistency between epidemiological frameworks and technical functionalities.

Interoperability may therefore require agreements between national health authorities, for instance those cooperating under EWRS[15]. The Member States in the eHealth Network, in collaboration with Health Security Committee and supported by the Commission, should cooperate in order to define the criteria that would allow for cross-border interoperability; these criteria will be listed in the toolbox that can be updated within an iterative process.

d. Cybersecurity

Cybersecurity for these mobile applications, as well as the backend and any associated services is critical. Member States' authorities and the developers of these applications should therefore take a series of measures to ensure adequate cybersecurity throughout the lifecycle of the applications.

The cybersecurity requirements detailed in *Annex 1* have been compiled by ENISA, the EU Agency for Cybersecurity, and based on current best practices as regards the secure design, development and deployment of mobile applications.

The requirements concern measures to address the most common cybersecurity risks associated with this type of application, including possible abuse scenarios. They include technical requirements such as on the use of encryption, communications security, secure development practices and user authentication.

The cybersecurity requirements also address the need to enhance both national authorities' but also citizens' trust in the proper functioning of the applications and to provide transparency. Independent testing of the applications, access to source code and a policy for vulnerability handling and disclosure are in this respect deemed necessary.

Finally, Member States are recommended to carry out a national risk assessment to identify and mitigate possible risks of abuse. Furthermore, as the applications are deployed, national and European health and cybersecurity agencies, including Computer Security Incident Response teams, are expected to cooperate in responding to any potential incidents including the disclosure of new vulnerabilities.

e. Safeguards

Any contact tracing and warning app officially recognised by Member States' relevant authorities should present all guarantees for respect of fundamental rights, and in particular privacy and data protection, the prevention of surveillance and stigmatization. To this end, Member States should ensure that strong safeguards are in place, including but not limited to:

[15] https://www.ecdc.europa.eu/en/early-warning-and-response-system-ewrs

i. Temporary and voluntary nature

- Automated/gentle self-dismantling, including deletion of all remaining personal data and proximity information, as soon as the crisis is over.

- The apps' installation should be consent-based, while providing users with complete and clear information on intended use and processing.

ii. Data processing in line with Commission Guidance

- A necessary and proportionate data retention policy[16].

- Compliance with applicable law, particularly on data protection and confidentiality of electronic communications.

- Location data is not necessary nor recommended for the purpose of contact tracing apps, as their goal is not to follow the movements of individuals or to enforce prescriptions. Collecting an individual's movements in the context of contact tracing apps would violate the principle of data minimisation and would create major security and privacy issues.

- Safeguards to prevent stigmatization of infected persons or close contacts of infected persons.

- Safeguards to ensure the storing of proximity data on the device and data encryption.

2. ACCESSIBILITY AND INCLUSIVENESS

"Inclusiveness" is a foundational principle not only from a fundamental rights perspective, but also from an effectiveness perspective (as the success of the solution approach depends on factors such as "user penetration as a percentage of population", "percentage of the population using a mobile device", "the number of people who have downloaded the application"). Inclusiveness is all the more important for those, like children, vulnerable groups, and elderly persons, who often do not have a smartphone and/or connected device, or may not be digital-savvy enough to install and properly use the tracing app. In addition, healthcare workers may not be using their mobile phone while at work and additional contact tracing efforts are needed in the healthcare setting.

The contact tracing apps complement the important manual contact tracing efforts, which will continue, given that the penetration of the tracing functionality (or app) in the population or among certain groups of people may be incomplete.

Mobile apps will not reach all citizens given that they rely on the possession and active use of a smart phone. Evidence from Singapore[17] and a study by Oxford University[18] indicate that 60-75% of a population need to have the app for it to be efficient.

[16] Insert reference to final published version of guidance

[17] Singapore case: To date, about one million people have downloaded Singapore's contact-tracing app, but the tool has not been beneficial yet. At least three-quarters of Singapore's population - or 4.3 million people - need to use the app for the tool to be truly effective in combating Covid-19, National Development Minister, Lawrence Wong previously said. https://www.straitstimes.com/tech/google-launches-new-tool-to-help-public-health-officials-plan-social-distancing-measures

However, non-users will benefit from any increased population disease control the wide-spread use of such an app may bring.

In addition to citizens who do not possess a smart phone at all, there may be others that do but who require particular and additional functionalities. For example, the elderly, or persons with disabilities.

The digitally excluded, or harder to reach, categories will include persons with disabilities, including those that are dependant of support services (carers, support workers, personal assistants and deafblind interpreters). Moreover, not all assistive technology applications have Bluetooth capabilities.

Helplines could be envisaged at national level to support the uptake of the app for people who own a smartphone and would benefit from guidance and support in installing and using the app. Complementary, location-based solutions could be used to increase the coverage of digital excluded people (e.g. elderly, children, health and care workers). Standalone devices or wearables which do not need a smartphone to operate could be considered for these groups. Such devices would need to be compatible with the tracing app system. They would entail manufacturing and distribution costs but the devices would be immediately usable, without the need for app configuration or heavy customer service. It is also possible to include in such groups Domotics and home based ICT solutions to broaden the number of people reached by the solutions.

Content of tracing apps should meet the accessibility requirements set out in the transposition legislation of the Web Accessibility Directive[19], which include reference to Harmonised European Standard (HEN) 301549.

3. GOVERNANCE AND APPROVAL OF TRACING APPS

In doing their assessment, the authorities in Member States should take into account this toolbox with focus on interoperability, privacy and security elements. As regard the endorsement of contact tracing apps by Member States, the preferable arrangement should be that the national competent authorities in charge of the health crisis is ultimately accountable for the app. Preferably, the health authority of the Member State should be controller for the processing of personal data (either the national competent authority designated under article 9 of the Decision 1082/2013 or another health authority decided by the Member States).

For the acceptance of different types of apps (and underlying infection transmission chains information systems) and for ensuring that they fulfil the aimed purpose of epidemiological surveillance, the underlying policies, requirements and controls must be aligned and implemented in a coordinated way by the responsible national health authorities.

In general, to fight pandemics, it proved successful to evaluate and re-use existing tools to communicate COVID information in order to ensure increased information and accelerate the outreach. The experience of several Member States that started introducing

[18] Oxford University Research: a study quoted here by researchers at Oxford University's Big Data Institute said 60% of a country's population would need to be involved for the approach to be effective.

[19] Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (Text with EEA relevance) *OJ L 327, 2.12.2016, p. 1–15.*

contact tracing apps shows that, in order to increase the acceptance, an integrated governance is needed to prepare and implement the measures, involving not only health, but also other authorities, as well as private sector, experts, academics, data protection authorities etc. A wide communication model is needed, as well.

4. SUPPORTING ACTIONS

a. Sharing of epidemiological information between national public health authorities and cooperation with ECDC

Public health authorities may use anonymised/aggregated data from contact tracing to learn more about the transmission dynamics and adapt the public health response.

Aggregated data from tracing functionalities or results of the research may be shared with relevant health authorities and/or ECDC to help in the overall understanding of the epidemic and transmission dynamics, subject to applicable data protection guidelines.

b. Prevent proliferation of harmful apps

In order to prevent the proliferation of unlawful or harmful apps, each Member States should consider setting up a national system of evaluation/accreditation endorsement of national apps, possibly following a common set of criteria (to be defined), allowing the national health authorities to control the setting up of the system, as well as the activation of the different levels of alert (based on a code provided by the healthcare professional or triggered by the healthcare professional after the positive testing of a COVID-19 case) (governance above). A close cooperation between health and digital authorities should be sought whenever possible for the evaluation/endorsement of the apps.

Close cooperation with app stores will be needed to promote national apps and promote uptake while delisting harmful apps.

Should apps that are not endorsed by national health authorities send notifications, relevant legal or administrative measure should be pursued by the Member States.

Finally, in order to provide a wide uptake of the beneficial apps, a solid communication strategy will need to be put forward (*see section V*).

c. Monitoring the effectiveness of the apps

Member States should develop a set of KPIs to assess/reflect the effectiveness of the apps in supporting contact tracing.

Peer-reviews at national level, but also among Member States and coordinated at EU level, to allow the review of the effectiveness and functioning of the chosen mobile applications, as well as the balancing with the fundamental rights requirements, are particularly encouraged. This should include independent technical reviews, including in-depth audits of the apps in terms of security, privacy or accessibility, ideally coordinated at European level (e.g. via an independent testing facility). Such independent assessments can be coordinated with the assessments conducted by national authorities, for example cybersecurity agencies, and will help increase trust, a vital condition for uptake and success.

IV. COMMUNICATIONS

Clear and regular communication is paramount to ensuring public trust when combating the COVID-19 crisis. As set out in the Recommendation, in paragraph (9), Member States authorities and the Commission should ensure regular, clear and comprehensive communication to the public on the actions taken and provide opportunities for the public to interact and participate in discussions.

Communication strategies for the overall response to the COVID-19 crisis, including the aspects related to the use of mobile applications, are already in place in the Member States. A clear and coherent communication approach across the EU, promoting good communication practices in relation to the development and use of mobile applications, could only reinforce the benefits of EU coordination in the response to the COVID-19 crisis, help ensuring accountability of the relevant national and EU authorities, institutions and networks and public trust for the decisions taken and measures implemented.

This section sets out the main elements of a framework for a coherent communication approach at the level of Member States and the Commission, with the aim of ensuring transparency towards the general public and accountability for the decision-making process in relation to the development and use of COVID-19 related mobile apps covered by this Toolbox.

Principles for communication[20] strategies in relation to the COVID-19 related mobile apps, as covered by this Toolbox include:

- Establish a clear framework setting out the communication approach, including single points of communication to the public, the type of information to be communicated, the format in which the communications are made and the timing of such communications;
- Ensure timely, regular, clear and comprehensive communication to the public;
- Ensure that the means of communication guarantee visibility and accessibility of information provided to the public;
- Set out a framework fostering public debates and interaction with stakeholders;

[20] Key messages to public could include cautions against the use of non-authorised mobile applications; the relevant and non-confidential parts of system's security and privacy evaluation; clear and streamlined information in relation to the mobile applications being tested and/or approved and/or promoted at national/federal and regional level, and in particular information on: how the apps were developed or procured and by whom; the purpose of the apps (including whether they are part of the exit strategies or not); the individual and societal benefits to using the app; the functionalities and features; the context in which they are used or going to be used; the envisaged timeframe for using such apps; the control mechanisms in place; the safeguards in place to protect fundamental rights, including on use, storage, collection, processing and transfer of data and limitations thereof; mechanisms in place to assess the efficiency of the apps, the entities in charge of such assessment and the outcome of the assessment; the publication of the source code is also encouraged. Member States should consider establishing a single communication point at national level: preferably national/federal-level health authorities or task forces/crisis governance centres set up at national/federal level for managing the COVID-19 crisis. Member States should consider: communicating information to the public on the development and use of mobile applications as part of the regular COVID-19 crisis communication related to the health emergency and lockdowns. Such communication should be done on a regular basis, at a timing and with a frequency widely known to the public, publishing updated information concerning the relevant mobile applications on dedicated official COVID-19 information websites widely known to the public and, where relevant, as part of the alert systems developed by national authorities. the information provided and published should be visible, clear and accessible to all members of the public, including to persons with disabilities.

- Establish strategies to counter the dissemination of fake news, as well as misleading or unfounded rumours, while keeping all necessary guarantees in place to preserve freedom of expression and freedom and information.
- Ensure the involvement of the technical community in the review process of the effectiveness and functioning of the mobile applications (e.g. independent testing facility).

The strategies could include opportunities for public debates on the development and use of the COVID-19 mobile applications and their impact on society and individuals. This could be done, among others, via dedicated online fora, regular events, press conferences or similar, where the media, stakeholders and civil society may raise questions and provide comments to the relevant decision-makers and app developers. Written documents should also be available to the public with the possibility to return comments and suggestions.

Finally, stakeholders should be involved as much as possible in the preparation of the apps and dissemination of information about them.

V TOWARDS A COMMON SOLUTION: CONCLUSION AND NEXT STEPS

Member States are collectively determined to return to normal life without harming our fundamental rights and freedoms. They are seeking to converge in their use of digital health tools that have a significant and growing role to play in fighting the pandemic. Implementing this common approach across the EU to the use of mobile tracing and warning apps is an important first step forwards.

Intensive work within the eHealth Network will continue with the Member States reports in May, the Commission assessment of progress in implementing Recommendation C/2020/2296 in June as well as other follow up actions and possible further recommendations to the Member States.

The Network will meet every two weeks during the COVID-19 crisis (as long as the COVID-19 is declared a pandemic by WHO and longer if considered necessary by the eHealth Network). The Commission will ensure the secretariat of these meetings.

In particular, Member States will focus on five particular areas of priority follow-up:

a. Developing further the interoperability framework, evaluating and extending the toolbox to additional functionalities

Public health authorities will assess the effectiveness of the apps at national and cross-border level *(see also Annex 1 and section III.4 above)*. This may be done by crosschecking contact tracing data with actual test result data and checking the proportion of contacts who test positive by type of contact exposure. This can help public health authorities tailor prevention efforts and also help them understand whether they cast the net too wide or too narrowly in terms of the proximity and duration parameters they have programmed in the app. Public health authorities can also learn about different settings where transmission is more likely to take place which can guide public health action. These data can help authorities understand the impact of mitigation measures and the lifting of these.

The toolbox will be expanded, particularly in close liaison with the Health Security Committee. In particular, Member States will consider the potential for symptom trackers to inform allocation of resources to areas of need, new models for healthcare (monitoring of the vulnerable at home) and informing epidemiological models within and across Members States.

By 31 MAY 2020: Member States will report to the Commission on the actions taken and provide updates in their bi-weekly meetings, as long as the crisis persists.

The Commission will publish by 30 June 2020 the report evaluating the progress made which may include proposals for further follow-up actions

b. Urgent engagement with owners of the mobile operating systems

BY END APRIL 2020: Member States with the Commission will seek clarifications on the solution proposed by Google and Apple with regard to contact tracing functionality on Android and iOS in order to ensure that their initiative is compatible with the EU common approach.

c. Use of mobility data to inform anti COVID-19 measures and exit strategy

FOR JUNE 2020. A common approach for the use of anonymised and aggregated mobility data will be developed, focusing on data necessary for: (1) modelling to map and predict the diffusion of the disease and the impact on needs in the health systems in Member States and (2) optimising the effectiveness of measures to contain the diffusion of the COVID-19 virus and to address its effects, including confinement (and de-confinement), and to obtain and use those data.

d. Cybersecurity

FOR MAY 2020. The NIS Cooperation Group, within its work stream on Cybersecurity in the health sector, will facilitate the exchange of good practices for national authorities dealing with cybersecurity of COVID applications including identifying effective testing and evaluation methods in cooperation with the European Cybersecurity Certification Group established by the Cybersecurity Act. The CSIRTs network will continue to provide relevant EU wide situational awareness and information sharing on related threats, incidents and vulnerabilities.

On the basis of the Member States reports, the Commission will assess in June 2020 the progress and the effect off the Recommendation C/2020/2296 and may make further recommendations to the Member States.

In order to support transparency and interoperability, the publication/sharing of the source code and the peer reviews are encouraged and are highly recommended for the apps supported by the national authorities (this could be done, if relevant, against a fair compensation).

e. Explore cutting-edge and privacy enhancing technical solutions

AS OF APRIL 2020 Technical input will also be sought at national and EU level. In this respect, the Commission can support in organising ad-hoc meetings with m-health hub and New Generation Internet Communities.

ANNEX I: RECOMMENDATIONS FOR A COMMON APPROACH TO MOBILE TRACING APPS

Essential requirements for national apps and cross-border interoperability

a) Epidemiological framework

Apps should be operated under the control of the relevant public health authorities (use of service providers acting on behalf of the authorities is possible) and be developed and implemented in close cooperation with them, in order to support and complement existing epidemiological processes and procedures in the Member States. Public health authorities should coordinate the local contact tracing process in line with national legislation and international guidance that defines which contacts should be followed up and what the management of these contacts should be. Member States may decide to use proximity data in the contact tracing process. Users should be fully informed about the follow-up process before consenting to the activation of the app.

Id	Functionality/ type of app	Description and Recommendation	Relevant actors[21]
EF-01	Epidemiological relevance for "close contacts"	Adopt the heuristics as commonly agreed by ECDC (guidance on contact tracing[22)] with Member States as to what is epidemiologically sufficient in terms of proximity as: (i) time duration, (ii) distance, (iii) environmental context.	Public health authorities / ECDC
EF-02	Epidemiologically relevant retention period for contact tracing data	Adopt the heuristics as commonly agreed by ECDC on the historical importance of the proximity (that is, 14 or 16 days)	ECDC guidance / public health authorities
EF-03	Information to users at risk	MS determine how to inform users at risk, e.g. via the app or directly by the NHAs Adequate safeguards be put in place in light of data collection, storage and sharing policies	Relevant public health authority
EF-04	Timing of notification to users at risk	Users at risk should be notified immediately after a positive Covid-19 test.	

EF-05	Encoding COVID-19 status	Only authorized public health authorities or other authorized parties such as laboratories should be entitled to confirm an infection and trigger a warning alert; for instance by providing a (QR) code/sending a notification to enable the user to trigger a warning alert; alternatively the authorized public health authorities or other authorized parties such as laboratories themselves should be entitled to trigger a warning alert.	
EF-06	Information to be provided to the user	Users at risk should be informed about potential infection due to a close contact with an infected person and what to do next. The content of this message shall be determined by public health authorities and could include information on self-quarantine, what symptoms to look for and what to do if symptoms develop. Depending on the national laws, the health authorities may contact directly the user that was in close contact with a COVID-19 patient. In that scenario, the users have to be informed at the moment of the app installation, that they may be contacted by the health authorities and that their data may be processed by the health authorities.	
EF-07	Privacy-preserving app solutions that support public health efforts	Member States have been considering the most appropriate app solutions for their specific situations that comply with applicable laws and minimise the processing of personal data. Solutions can be grouped into at least two general categories: 1) Decentralised processing The proximity data related to contacts generated by the app remains only on the device (mobile phone). The apps generate arbitrary identifiers of the phones that are in contact with the user. These identifiers are stored on the device of the user with no additional personal information or phone numbers. The provision of mobile phone numbers or other personal data by the user at the time of the app installation is not necessary, because an alert is automatically delivered via the app the moment that a user notifies the app – with the approval of the health authority - that he/she has test positive. Public health authorities determine the content and timing of the notification message. The message may, for example, ask the person to stay at home and/ or to contact the public health authorities, should they develop symptoms and to facilitate testing. This approach would considerably reduce the risks to privacy as close contacts would not be directly identifiable and this option would thereby enhance the attractiveness of the application. Public health	Health authorities, app developers

		authorities would not, however, have access to any anonymised and aggregated information on social distancing, on the effectiveness of the app or on the potential diffusion of the virus. This information can be important to manage the exit of the crisis. Although not necessary for the functioning of the app, an alerted person (that she/he was in contact with a positively tested person) may wish to provide personal information to the public health authorities in order to get further support and guidance. The app can provide an option to do so. This should be an "opt in" option and clearly indicated as "opt in". The authority can then make contact with the individual and advise him or her accordingly. 2) Backend server solution In this option, the app functions through a backend server held by the public health authorities and on which are stored the arbitrary identifiers. Users cannot be directly identified through these data. Only the arbitrary identifiers generated by the app are stored on the server. The advantage is that the data stored in the server can be anonymised by aggregation and further used by, public authorities as a source of important aggregated information on the intensity of contacts in the population, on the effectiveness of the app in tracing and alerting contacts and on the aggregated number of people that could potentially develop symptoms. Through the identifiers, users who have been in contact with a positively tested user will receive as in the previous version an automatic message or alert on their phone. As in the previous version, an alerted person (that she/he was in contact with a positively tested person) may wish to provide personal information to the public health authorities in order to get further support and guidance. The app can provide an option to do so. This should be an "opt in" option and clearly indicated as "opt in". The authority can then make contact with the individual and advise him or her accordingly. This supplements manual contact tracing effort (where positive cases are interviewed), notably because penetration of the contact tracing app in the population is likely to be incomplete, and particularly because many vulnerable individuals such as the elderly are may not have access to this app. It would help authorities detect surges in cases, as well enabling them to follow up in a more personalised way contacts who are at risk of infection. Some public health authorities have a policy to phone all contacts directly	

		rather than rely on automated notifications, in which case users of the app should be given the option to provide their contact numbers as part of the registration process and based on explicit consent of the user. None of the above two options includes storing of unnecessary personal information. Options where directly-identifiable data on every person downloading the app is held centrally by public health authorities, would have major disadvantage, as noted by the EDPB in its response to consultation on Commission draft guidance on data protection and tracing apps. These options would not keep personal data processing to the absolute minimum, and so people may be less willing to install and use the app. Centralised storage of mobile phone numbers could also create risks of data breaches and cyberattacks.	

b) Technical functionalities			
Id	**Functionality**	**Description** **Recommendation**	**Relevant actors**[23] **Supporting actions**
TF-01	Proximity technology	In order to reliably determine the epidemiologically targeted 1.5 meters distance, a resolution of 0.5 meters should be provided, minimizing false positives. 1) App (in conjunction with device/OS) should be able to send and receive and record Bluetooth signals even in the background mode (even when the phone is locked). 2) App should be able to estimate with sufficient accuracy the proximity between mobile phones via Bluetooth signals or other effective and non-tracking techniques 3) App should advertises continuously its presence using a temporary anonymous ID that permits establishing contact with other app users in proximity. 4) App should records and store IDs observed from other mobile phones in epidemiologically relevant proximity on the device 5) App should be able to indicate the Member State in which it is registered	
TF-02	Physical proximity	Actual physical proximity should be recorded accuratly. Only if a mobile phone is in "epidemiologically relevant" proximity to another mobile phone for an "epidemiologically relevant" period of time as commonly agreed by NHAs (see rows 1 and 2 in part a above), the ID of each phone is stored in encrypted form in the respective other phone.	TF-04
TF-03	Ephemeral ID	The ephemeral ID should be generated pseudo-randomly and change periodically to enhance the protection against eavesdropping and hacking and tracking by third parties. The ephemeral ID includes the (encrypted) information necessary to identify the device (without being the device ID) to send it push notifications, if needed.	

TF-04	Code produced by health authority to confirm COVID-19 cases	The code created by the competent national healthcare authority should be generated pseudo-randomly and be single-use. This ensures that it cannot be used by malicious individuals to pollute the data collected on the server. This code should be as user friendly as possible (e.g. QR codes) to avoid an error prone input from the user.	Health authorities
TF-05	Scalability	Scalability to more than 100 million users within a month. In order to reach this scale, the technological requirements of the devices should be kept to the minimum possible and avoid technical capabilities only available on latest or recent technological platforms.	
TF-06	Devices	The contact tracing capabilities should be supported by virtually all devices with Bluetooth connectivity, independently from their technological platform. The contact tracing capability should be available in all possible operating systems and safeguards are needed to avoid excessive battery use.	
TF-08	Open source	Openly publish the technical specifications and the source code for the apps, as a way to maximise re-use, interoperability, auditability and security.	App developers

c) Essential cross-border interoperability requirements			
Id	**Functionality/type of app**	**Description and Recommendation**	**Relevant actors[24]** **Supporting actions**
IOP-01	eHealth European Interoperability Framework[25]	Framework to model the interoperability landscape to describe and discuss interoperability challenges and solutions. This framework is endorsed by the eHealth Network, and is composed of the following layers: a) Legal and regulatory; b) Organisational (policy and care process); c) Semantic (data and information); d) Technical (applications and infrastructure).	eHealth Network
IOP-02	Epidemiological criteria must be aligned to define close contacts for a high risk exposure	App developers and public health authorities should align with WHO and ECDC guidance on the determinants of contact tracing, including the definition of close contact (distance and duration of exposure) and the period for which contacts are stored (for how long).	ECDC and WHO App developers Public Health Authorities
IOP-03	A contact tracing app must be able to record its user's proximity contacts with users using different contact tracing apps	Apps must be able to determine a proximity contact, following the agreed epidemiological criteria, independently from the technological platform and mobile app each individual is using.	App developers Public Health Authorities
IOP-04	Backend solutions must be able to communicate to other MSs/regions about users that have tested positive	Public Health authorities should align on the protocol for data exchange of cross-border contact chains, namely about infected individuals that may have been in contact with individuals from another country.	App developers Public Health Authorities
IOP-05	Infection exposure notifications	Public Health authorities should align on the protocol to inform exposed individuals	Public Health Authorities

[25] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co03_en.pdf

d) Cybersecurity			
Id	**Requirement**	**Description**	**Relevant actors[26]**
Requirements for national authorities			
CS-01	National risk assessment, information sharing, incident response	National authorities should conduct an overall risk assessment focused on the potential cybersecurity risks of COVID applications, taking into account known security issues in the underlying platforms and communication protocols as well as recent incidents and threats. The relevant parts of this national risk assessment should be shared with the project team(s) developing the applications. Information sharing and collaboration should be established on cybersecurity and vulnerability management between the project team(s) and the relevant national authorities and bodies, including the national CSIRT, cybersecurity agencies, relevant medical product CSIRTs, etc. Regular threat briefings are an important tool to create awareness of cybersecurity threats at all levels in the project team(s). It is important to have plan for incident management and vulnerabilities, including adequate procedures for the notification and involvement of national CSIRTs and relevant cybersecurity and data protection authorities.	National health authorities; National cybersecurity authorities. National CSIRTs
CS-02	Security testing and independent review. *2.*	National authorities should ensure that the security of the app and the backend is reviewed and tested by independent experts before deployment and after each change. To build trust and provide transparency, national authorities should ensure that the architecture and the code of the application (the app and the backend) are made available for review by independent technical experts. Publishing the source code for independent review is key, as well as providing a clear contact point to raise potential security issues. It is important that security researchers, experts, citizens and organizations, are able to report errors and/or	National Authorities; Project Teams Independent evaluators; Security

[26] This column aims at identifying the main owners of the measures, i.e. actors responsible for developing, enforcing and/or implementing a measure.

		vulnerabilities to the project team(s). Developers should have vulnerability handling procedures in place and provide an appropriate vulnerability disclosure framework. National authorities may also consider further activities to enhance trust in the applications such as a bug bounty program.	researchers;
Requirements for developers			
CS-03	Data minimization and minimum permissions	Developers should limit as much as possible the permissions of the app, minimize the data processed, where possible pseudonymize and/or anonymize data, protect any remaining sensitive data processed by the app or the backend, and delete it when no longer needed. Sensitive data may include personal information, health information, critical security data, metadata, etc.	Project teams;
CS-04	Secure software development	Developers should follow good practices, secure coding principles, secure design principles and development of the applications and the backend services. Developers should use the latest and up to date development environments. Developers should test their app as much as possible, using automated tools for testing and integration, which cover not only functional tests, but also security tests like fuzz testing, vulnerability scanning, code quality checks, (static and dynamic) code analysis tools, source code scanning for libraries and developed code. The back-end platform and any related services should be hardened and/or patched to mitigate the risk of compromise of data and the interface between the app and the back end should be secure. Developers should consider threats to their development environments. It is important to consider that cyber attackers often target software developers, system administrators, development platforms, because they may have system passwords, sensitive credentials, access to source code, access rights to sensitive assets, passwords to the backend, etc.	Project teams;

CS-05	Built-in security for apps, protocols and backend.	Developers should make best use of smartphone operating systems built-in security functions, such as user authentication, app sandboxes, encrypted per-app storage, etc. It is important to use the dedicated app storage, which comes with built-in security controls.	Project teams;
CS-06	Communication security, encryption, cryptography	All network communications between the application and the backend should be encrypted using well-known and publicly recommended cryptographic libraries. It is essential to use transport layer encryption to encrypt data in transit, when communicating over mobile networks and WiFi networks. Developers should use existing, well-known and publicly recommended cryptographic algorithms and protocols, and well-tested implementations. Special care should be given to the requirements for the secure use of each algorithm and protocol (e.g. random initialization vectors or nonces). Identifier relay/replay prevention safeguards should be implemented to prevent those attacks, meaning that User A should not be able to record an identifier of User B and, afterwards, send User B's identifier as his/her own.	Project teams;
CS-07	Secure-by-default and user-friendly	COVID applications will have to be used by a large portion of the population, not only the few tech-savvy. The apps should be secure out-of-the-box with settings that are secure-by-default. It is important to design an intuitive and user-friendly application to avoid security issues due to misconfiguration or mistakes by the user.	Project teams;
CS-08	User authentication	Developers should make use of the user authentication methods available on the smartphone platform in particular as regards access to sensitive information.	Project teams;

CS-09	Secure use of libraries and third party code	The application should rely to the extent possible on the low-level libraries provided by the operating system and avoid depending on third parties libraries. When third party libraries are used, particular attention should be given to ensure they are kept up to date and their source code is available for review. Application developers have to invest in vetting libraries, third party code and integrate them securely in their application.	Project teams;
CS-10	Handling insecure smartphones	Developers should consider that not all smartphones run the latest versions of operating systems. The devices may be running vulnerable software, and some built-in security functions may not be available. Many smartphones are running outdated and vulnerable operating systems, some smartphone are rooted or jailbroken, or otherwise modified.	Project teams;
Further references		**ENISA** - ENISA Smartphone guidelines and tool: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smartphone-guidelines-tool - ENISA report on pseudonymisation techniques: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices **Industry** - OWASP mobile security project https://owasp.org/www-project-mobile-security/ , - OWASP Mobile Security Testing Guide https://owasp.org/www-project-mobile-security-testing-guide/ - Android developers security documentation- https://source.android.com/security - iOS developers security documentation- https://developer.apple.com/documentation/security **Member States** - The SOG-IS cryptography catalogue https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.1.pdf - Germany - Requirements for OEM regarding Smartphone Security https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/requirements/Requirements-Smartphones.html - France - Recommandations de sécurité relatives aux ordiphones - https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-aux-ordiphones/	

e) Safeguards			
Id	**Functionality/type of app**	**Description and recommendation**	**Relevant actors[27]** **Supporting actions**
SG-01	Temporary app/ Data deletion	App should be deactivated automatically and all remaining personal data and proximity data should be erased, as soon as the crisis is over.	
SG-02	Voluntary character	App should be consent-based with full information of intended processing of data	
SG-03	No tracking	Location data is not necessary nor recommended for the purpose of contact tracing apps, as their goal is not to follow the movements of individuals or to enforce prescriptions. Collecting an individual's movements in the context of contact tracing apps would violate the principle of data minimisation and would create major security and privacy issues.	
SF-04	No stigmatization	The app should ensure that no user knows the identity of any infected persons or of close contacts of infected persons	
SG-05	Proximity data stored on the device	In order to enhance privacy and security, proximity data (close contacts) should be stored only on the device, and be deleted after the epidemiologically relevant period as recommended by ECDC (14-16 days). Only after a user has been confirmed infected, the proximity data of that user may be uploaded to the central server and/or the competent health authorities, depending on the system chosen by the Member State.	

SG-06	ID generation	The ephemeral IDs transmitted between devices via BLE should be generated pseudo-randomly and changed periodically. They should neither allow any user to identify the user of the specific device nor to associate multiple signals to the same device.	
SG-07	Pseudonyms	Pseudonyms should have no relation to long-lived personally identifiable information (PII).	
SG-8	Encryption	The app should encrypt data as much as possible in order to enhance security and privacy	

Accessibility and inclusiveness				
Id	**Functionality/type of app**	**Description and Recommendation**		**Relevant actors[28]** **Supporting actions**
M01	Accessibility standard	Web Accessibility Directive[29]: Content of tracing apps should meet the accessibility requirements set out in the Harmonised European Standard (HEN) 301549 whose references may be updated from time to time by the Commission. Specific group of people/circumstances: consider also specific device that users could carry (eg relevant for digitally excluded people, outdoor workers, healthcare workers etc.)	Harmonised European Standard (HEN) 301549[30]	
M02	UX standards, where relevant	Considerations could be given to the CEN/ISO 82304-2 Quality Requirements Conformity Assessment (QRCA) work that could help assessing medical safety, usability, safety of personal data and technical quality of health apps and issues a Health App Quality Label.	CEN/ISO 82304-2	Ongoing work CEN/ISO

Public health authorities' governance mechanisms

[29] https://ec.europa.eu/digital-single-market/en/web-accessibility

[30] Commission Implementing Decision (EU) 2018/2048 of 20 December 2018 on the harmonised standard for websites and mobile applications drafted in support of Directive (EU) 2016/2102 of the European Parliament and of the Council C/2018/9056 *OJ L 327, 21.12.2018, p. 84–86*

Id	Governance action	Description	Relevant actors Related measure(s)
GA01	Overall coordination	The underlying policies, requirements and controls must be aligned and implemented in a coordinated way by the responsible national health authorities	Depending on the national setting: • Overall coordination: authorities in: charge of the crisis (usually government or ministry of health); • digital health authorities; • epidemiological institutions; • national research institutions
GA02	Cooperation within MS	Integrated strategy to develop the apps, involving cooperation with other authorities, as well as private sector, experts, academics, data protection authorities	• Other relevant ministries (e.g. digital ministry, ministry of state administration, ministry of internal affairs etc) • Involvement of other authorities (eg data protection authorities)
GA04	Endorsement of the app	Health authorities are accountable for the app and use the tool-box when evaluating/endorsing it As regards the quality and reliability assessment of the apps, the member states should take on the principles of the ongoing CEN TC251 work that provides a common integrated framework for all EU Member States	Depending on the national setting: • Institutions coordinating the crisis response; • digital health authorities, in cooperation with epidemiological institutions; • digital ministries or other settings
GA05	Cooperation within EU	The Member States supported by the Commission, should cooperate in order to define the criteria that would allow for cross-border interoperability; these criteria will be listed in the toolbox that can be updated within an iterative process.	• Member States, represented in the eHealth Network, collaboration with Health Security Committee

		Cooperation across border to exchange information concerning infected patients and their contacts, complementing the work carried in the framework of Decision 1082/2013 of the EU Parliament and of the Council	• Support of the European Commission • Cooperation between the institutions cooperating in the framework of the Early warning and response system and Health Security Committee

SUPPORTING ACTIONS			
Id	**Supporting action**	**Description**	**Relevant actors** **Related measure(s)**
SA01	Information sharing/ Sharing of epidemiological information	Depending on national settings, possibility to transmit anonymised/aggregates or pseudonymised data to national epidemiological and/or research institutions (based on consent or national law) for analysis. Transmission of aggregated data to national authorities and ECDC – to be defined (eg distribution of number of contacts per cases by age and gender and changes over time (for example before and after lifting of containment measures), or percentage of contacts testing positive by type of contact exposure (proximity and duration) Member States in the eHealth Network will set up a system that will allow for an iterative process of continuous monitoring and evaluation of the functioning of their apps. When doing this analysis, the eHealth Network will seek input from the Health Security Committee. Ad-hoc meetings between the eHealth Network and Health Security Committee could be set up.	• National health data authorities, epidemiological institutions • research institutions • ECDC eHealth Network • Health Security Committee • Input from technical communities (m-health, New Generation Internet etc)

		Technical input will also be sought at national and EU level	
SA02	Prevent proliferation of harmful apps	Member States should set up a national system of evaluation/accreditation endorsement of national apps, allowing the national health authorities to control the setting up of the system, as well as the activation of the alert Close cooperation with app stores in order to promote national apps and delist harmful apps Pursue legal or administrative measures in case of not-endorsed apps sending notifications	• MS representatives in the eHealth Network, in cooperation with digital and epidemiological authorities • Cooperation with law enforcement authorities
SA03	Monitoring the effectiveness of the COVID-19 applications (including interoperability)	Technical input will be sought at national and EU level The publication/sharing of the source code is highly encouraged. Peer-reviews at national level, but also among Member States, to allow the review of the effectiveness and functioning of the chosen mobile applications, as well as the balancing with the fundamental rights requirements, are particularly encouraged. This should include independent technical reviews, including in-depth audits of the apps in terms of security, privacy or accessibility. Such independent assessments can be coordinated with the assessments conducted by national authorities, for example cybersecurity agencies, the National Monitoring Bodies in charge of monitoring accessibility of websites and mobile apps under the Web Accessibility Directive, and will help increase trust, a vital condition for uptake and success.	• eHealth Network • Health Security Committee • Input from technical communities (m-health hub, New Generation Internet etc)National health data authorities, epidemiological institutions • research institutions • ECDC

ANNEX II: BACKGROUND INFORMATION ON CONTACT TRACING

Contract tracing distinguishes from social distancing in that it aims at stopping further transmission once an infected person is confirmed to be positive for Covid-19.

The WHO defines contact tracing as a monitoring process consisting of three steps[31]:

3. "Contact identification: Once someone is confirmed as infected with a virus, contacts are identified by asking about the person's activities and the activities and roles of the people around them since onset of illness. Contacts can be anyone who has been in contact with an infected person: family members, work colleagues, friends, or health care providers.
4. Contact listing: All persons considered to have contact with the infected person should be listed as contacts. Efforts should be made to identify every listed contact and to inform them of their contact status, what it means, the actions that will follow, and the importance of receiving early care if they develop symptoms. Contacts should also be provided with information about prevention of the disease. In some cases, quarantine or isolation is required for high risk contacts, either at home, or in hospital.
5. Contact follow-up: Regular follow-up should be conducted with all contacts to monitor for symptoms and test for signs of infection."

Contact tracing is a key part of the public health response to COVID -19 and is done by public health authorities, involving the identification of persons who may have been exposed to COVID-19 as a result of being in contact with an infected person.

Contact tracing can be conducted manually, based on interviewing the infected person and then contacting the people who have been exposed. However, this can prove difficult as the infected person may not be able to recall all past encounters, or there may not be sufficient means for proper follow-up. Given the high reproduction rate of Covid-19 and the saturation of healthcare systems, mobile contact tracing applications provide the advantage of being able to efficiently register such contacts, and to automate the contact listing. Mobile applications should be one component of a comprehensive national strategy for contact tracing. Such mobile apps should be combined with appropriate testing plans and medical follow-up procedures by the public health authorities and national health authorities. Contact tracing is important in all transmission scenarios but can be challenging to carry out due to lack of resources, mobile technology could help to make the process more efficient.

Contact tracing can benefit from different approaches:

1. Identifying people at risk based on proximity and duration of contact with an infected case.
2. Identifying people at risk based on environmental transmission

This information is also useful for national authorities, ECDC and WHO in the context of studies aiming at understanding transmission dynamics such as which contacts are at higher risk of infection when there is less virus circulation, where transmission takes place and the impact of mitigation measures, in order to target public health measures.

[31] https://www.who.int/features/qa/contact-tracing/en/

ANNEX III: BACKGROUND INFORMATION ON SYMPTOM CHECKER FUNCTIONALITIES

Symptom checker functionality refers to a website or mobile application that allows people to answer a set of questions about different symptoms compatible with COVID-19. The functionality can then provide recommendations such as whether a test is needed and on ways to reduce the risk of transmission to others.

Symptom checker functionalities can sometimes be combined with contact tracing functionalities which opens the possibility of alerting contacts of people with symptoms compatible with COVID-19 before they have received a test. This is e.g. being considered in the United-Kingdom.

The symptom checker functionality of apps could be useful for Member States to complement primary care surveillance and understand more about of COVID-19 in the population. These data are collated together with data from more widespread testing of those with symptoms as part the COVID-19 surveillance systems. This would complement existing surveillance systems and, in particular, overcome the challenges for surveillance of COVID-19 in many countries which recommend that patients with respiratory symptoms should not visit their general practitioner.

Data from symptom checker functionalities combined with laboratory testing data could help in estimating the positive predictive value of respiratory symptoms in a given community, and providing information on the level of virus circulation as well as the impact of mitigation measures (and their lifting) on transmission.