# Considerations for strengthening legal frameworks for digital contact tracing and quarantine tools for COVID-19

Interim guidance

15 June 2021

World Health Organization
Western Pacific Region

## 1. Introduction

### 1.1 Background

There has been rapid development and uptake of digital contact tracing and quarantine (DCTQ) tools as part of the response to coronavirus disease 2019 (COVID-19). Such tools are designed to support contact tracing and quarantine efforts and overcome challenges associated with resource limitations and timeliness. The range of tools being developed and utilized across the Western Pacific Region is wide and continually evolving, encompassing different forms and applications of technology, many of which are novel and have limited evidence of effectiveness *(1)*.

There are critical legal and ethical dimensions to the use of DCTQ tools, including issues relating to privacy and surveillance, which differ depending on the technology being used and its application. These tools should be governed by effective legal frameworks grounded in sound ethical principles to ensure their use is lawful, proportionate and properly managed. Doing so will foster public trust, acceptance and voluntary uptake, enhancing the effectiveness of selected tools as well as overall public health efforts *(2)*.

Member States in the Western Pacific Region have taken different approaches to addressing the legal and ethical dimensions, which may be instructive for other jurisdictions.

### 1.2 Purpose

This document aims to support Member States in the Western Pacific Region to review, develop and monitor their legal frameworks for DCTQ tools, guided by the ethical principles for digital proximity tracking technologies suggested by the World Health Organization *(3)*. It is designed to be considered alongside guidance for Member States on selecting DCTQ tools for COVID-19 *(4)* and may also be instructive for digital tools used for other public health purposes.

### 1.3 Target audience

Policy-makers and legal officials at national and subnational levels advising on the design and implementation of DCTQ tools as part of the COVID-19 response.

## 2. Use of DCTQ tools during the COVID-19 pandemic

As countries transition through the various stages of the pandemic and gradually ease physical distancing requirements and other non-pharmaceutical interventions (NPIs), mechanisms to strengthen and sustain the “test, trace, track and treat” paradigm are more important than ever to contain the spread of the disease *(1)*.

To allow societies to continue functioning while limiting the risk of transmission, Member States will need to maintain the capacity to rapidly identify and inform cases and potential contacts and manage their quarantine and isolation as appropriate *(5)*. Effectively implementing these

functions at the scale necessary to suppress COVID-19 requires substantial resources and capacity amidst unprecedented time and resource constraints. Critical elements in the implementation of contact tracing, for example, include a workforce of trained contact tracers, logistics support to contact tracing teams, and well-designed information-systems to collect, manage and analyse data in real time *(1)*. Member States are looking to digital technologies to overcome resource constraints and improve the effectiveness of these core public health functions.

## 2.1 Legal and ethical dimensions

DCTQ tools have the potential to enhance contact tracing and quarantine efforts to suppress COVID-19 and contribute to longer-term objectives, such as generating data for research and pandemic preparedness. Yet, they raise a number of legal and ethical issues that require careful consideration and management in order to maximize their effectiveness.

These tools generally involve the collection and use of information from or about individuals. This presents an incursion into private and social life, impacting the right to privacy and raising issues of data protection and control *(6)*. The information DCTQ tools utilize is often highly sensitive and capable of being misused, including information about the movements and health status of individuals and communities. Seemingly benign information including so-called metadata may also identify individuals and reveal personal information that is sensitive in a given context *(7)*. These issues also arise with respect to manual contact tracing and quarantine functions, but are amplified by the larger scale of information DCTQ tools are capable of processing *(2)*.

**Right to privacy**

Privacy is a fundamental human right recognized in several international and domestic legal instruments, including the International Covenant on Civil and Political Rights *(8)*. The United Nations General Assembly adopted a resolution in 2018 reaffirming the right to privacy in the digital age and calling upon States to respect and protect the right to privacy, including by considering developing or maintaining and implementing legislation that protects individuals against its violation *(7)*. The resolution recognizes the importance of the right to privacy to the realization of other rights, including the right to freedom of expression and opinion, the prevention of violence, including gender-based violence, abuse and sexual harassment, and as a foundation of a democratic society.

The application of DCTQ tools can also impact other rights and freedoms. Individual autonomy may be diminished where governments or employers mandate the use of a digital tool. A person's freedom of movement and ability to realize other rights may be impacted by a DCTQ tool that is used to determine access to public spaces or other premises based on perceived public health risk.

Existing inequities may be exacerbated by the deployment of DCTQ tools. Disparities in access and capacity to make use of digital technologies may mean that the potential benefits of such tools are not shared, including among older persons, marginalized populations and other groups vulnerable to the health and socioeconomic impacts of COVID-19.

There is also a risk that DCTQ tools could be used for purposes outside public health and beyond the COVID-19 pandemic, including broader population surveillance and law enforcement. The involvement of private actors in the development and implementation of these tools also increases the potential for data to be extracted and processed for commercial purposes, as well as for public health infrastructure to build a dependency on commercial products.

## 2.2 Role of legal frameworks

Clear legal frameworks, preferably in the form of legislation, are needed to address the legal and ethical dimensions of DCTQ tools and ensure their use is lawful, proportionate and in the interest of public health.

It is particularly important that legal frameworks are in place to govern the use of personal information and other data to ensure that privacy is respected and to prevent loss, unnecessary

intrusion and commercial exploitation. This will also help to secure public trust and acceptance of DCTQ tools, encouraging voluntary uptake and usage, which are critical to the effectiveness of many tools *(2,9,10)*. Failing to assure the public that data are adequately protected and not able to be used for purposes other than public health could also have broader implications for trust and participation in public health efforts *(11,12)*.

Legal frameworks in these are areas are growing, but not universally. In 2015, WHO found that 91% of high-income countries, 81% of upper-middle-income countries and 79% of lower-middle-income countries reported general privacy legislation to protect personally identifiable information *(13)*. This contrasted to only 45% of low-income countries reporting the same. Of the six WHO regions, the Western Pacific had the lowest percentage.

Legal frameworks also play an important role in ensuring that oversight of the use of DCTQ tools is adequate and that processes are in place for their eventual dismantling once the public health need has ended.

## 3. Steps for strengthening legal frameworks for DCTQ tools

The urgency of the COVID-19 pandemic and the speed at which DCTQ tools have been developed have left little time to understand their implications and assess relevant legal frameworks. Despite these pressures, it is vital that Member States integrate consideration of legal and ethical issues in the design, implementation and operation of DCTQ tools and take the opportunity to assess, strengthen and develop the legal frameworks governing their use.

A simple three-step approach is suggested to strengthen legal frameworks that can be integrated within projects to design and implement DCTQ tools and adapted to different jurisdictional processes. The checklist in the annex is intended to aid policy-makers when considering the ethical and legal dimensions throughout the three-step process.

**Terms of use and privacy policies**

A number of voluntary DCTQ tools include terms of use that seek to govern their use, including the rights and responsibilities that users have with respect to their data. For a number of reasons, these are generally not sufficient to govern the use of DCTQ tools on their own, including:

1. Terms of use are usually lengthy, complex documents that are difficult for users to understand and are rarely read in practice. Further, there is a knowledge imbalance about the methods digital technologies use to process data between service providers and users.
2. Terms of use are almost always unidirectional and set by the service providers with no scope for negotiation.
3. The use of DCTQ tools is often a broader policy issue affecting the community and requires the kind of deliberation and debate that generally occurs as part of the legislative process.
4. Terms of use put the onus on users to monitor and investigate misuse, and they are unlikely to provide satisfactory avenues of recourse accessible to most users.

### Step 1: Identify and review existing legal frameworks

#### A. Identify existing legal frameworks

Member States are likely to have existing legal frameworks that are relevant to DCTQ tools. These may determine the scope of the government's power to implement a tool, govern the collection and use of personal information and other data, and protect rights and freedoms. A number of laws administered by multiple government bodies are likely to be relevant, including:

- general privacy/data protection frameworks, which may apply to all data or only the government, private sector or information technology/communication sectors;
- health information frameworks, including those dealing with health records and data;

- emergency powers, public health/infectious disease control and quarantine laws, which may provide a lawful basis for the application of DCTQ tools;
- anti-discrimination laws;
- intellectual property laws; and
- frameworks concerning rights and freedoms, including the right to privacy, freedom of movement and protection from unlawful detention.

Other legal frameworks, including those at a subnational level, may be relevant, depending upon national legal and governance structures. Member States may also need to consider the operation of foreign laws, such as in the case data are stored overseas. During the identification process, engage legal experts to assist with the review to ensure that all relevant legal frameworks are identified.

### B. Review existing legal frameworks

Undertake a review to assess how the existing legal frameworks address the legal and ethical issues raised by the use of DCTQ tools.

Potential legal and ethical issues are varied and the checklist in the annex outlines general questions for governments to consider. The list is not exhaustive; as more information becomes available about the technology and its uses and impact, additional ethical and legal issues may arise, necessitating ongoing monitoring and evaluation. Consider setting principles to guide the review. Assessment tools such as the UN Global Pulse Risk, Harms and Benefits Assessment Tool may be useful reference points *(14)*.

The review should involve legal experts with relevant expertise in areas such as privacy, data protection and public health, as well as technological experts to understand and communicate the functions and potential implications of the tool.[1] This process should be grounded in an understanding of the practical implications of the tool, including with respect to vulnerable and marginalized communities. Policy-makers may consult with communities and civil society organizations, among others, to gain a deeper understanding.

## Step 2: Develop and implement new legal frameworks

Develop and implement new legal frameworks if the process in step 1 reveals that existing frameworks are inadequate (or no relevant framework exists). The process will need to be realistic and aligned to time frames for the proposed deployment of the DCTQ tool, as well as the jurisdictional requirements in each Member State. Depending on the need, available resources, and other context considerations, this may involve one or more of a range of legislative steps, including:

- amending existing laws;
- making temporary arrangements, such as by order, to govern specific DCTQ tools; or
- establishing new, complete legal frameworks to govern DCTQ tools and strengthen laws relating to data protection and digital technology generally.[2]

As far as possible, investments should contribute to broader efforts to strengthen legal frameworks for digital health and data protection.

To advance the development and implementation of new legal frameworks, consider the following actions, as appropriate to their context:

- Establish a project team and a detailed project plan that identifies its aims, time frames, approval processes, available resources and lines of responsibility. Team members should be drawn from relevant government sectors and include a mix of backgrounds and expertise. Senior leadership and stewardship of the project will be necessary to secure political support and buy-in.

[1] For example, the New Zealand Ministry of Health carried out a privacy impact assessment of the NZ COVID Tracer mobile app, which involved the Office of the Privacy Commissioner among other stakeholders *(15)*.

[2] For example, the Australian Minister for Health made an emergency determination under the Biosecurity Act 2015 to govern the use of the COVIDSafe app during its initial deployment *(16)*. Subsequently, the Government amended the national privacy law to incorporate those initial measures and introduce additional measures to protect privacy and bring COVIDSafe data within its scope *(17)*.

- Develop a consultation strategy based on the size and nature of the process and the groups most likely to be affected. Ensure consultations are as wide as possible within the time available. Stakeholders may include: relevant government sectors; subnational authorities; oversight bodies; experts in law, public health and technology; the private sector, including technology providers and users; civil society and privacy advocates; and the community, including vulnerable and marginalized groups and those that face barriers to accessing digital technologies.
- Tailor consultation activities to different audiences to encourage inclusivity and enable participation.
- Make information about the DCTQ tool and how it operates, including the source code, available to stakeholders to enable analysis and scrutiny of its impact, including on privacy and data security, and the adequacy of existing legal frameworks.
- Draft laws that translate the policy intention into an effective and enforceable legal instrument. This should be based on country needs and context, including the legal environment. Ensure that the laws are consistent with and can function alongside other relevant legal frameworks.
- Consider implications for current contractual arrangements, including intellectual property, with private entities involved in the design and implementation of the DCTQ tool. Also, preparing template contracts and other legal instruments.
- Develop an implementation plan for the new legal framework. This plan should include establishing processes and upskilling officials to ensure that the practical application of the DCTQ tool complies with the new law. Also, identify the necessary resources.
- Develop a communication strategy to inform users about the new legal frameworks and their rights and obligations with respect to the DCTQ tool, including avenues of redress. Information should be provided in a range of formats taking into account access to information, language and literacy.
- Develop a monitoring and evaluation framework to review the effectiveness of the legal framework.
- Establish or designate authorities to monitor compliance with the legal framework and provide oversight, and ensure they are properly resourced. Consider including accessible, efficient avenues of recourse for breach of the new law, for example of an individual's privacy.

## Step 3: Monitor and evaluate the effectiveness and impact of the new legal frameworks

Monitor and evaluate the effectiveness of legal frameworks governing the use of DCTQ tools throughout their operation. The checklist in the annex can be used to guide monitoring and evaluation and assess the effectiveness of new laws in addressing the legal and ethical issues raised by the tool. The process should consider any impact the frameworks had on the effectiveness or uptake of the tool.

Public and user views can be monitored and sought through a variety of methods, including regular public engagement and monitoring of traditional or social media. This could be done within the Government or with the assistance of external civil society groups that can review the legal frameworks and complete an independent, third-party review and analysis. Consider publishing or providing the source code and details about the security protocols for the DCTQ tool to allow for comprehensive auditing and testing.

Legal frameworks are never perfect, and policy-makers should use the monitoring and evaluation process as an opportunity to identify areas that can be addressed and improved. Possible actions may include making further amendments to legislation or enhancing its implementation and enforcement.

## Annex: Checklist of legal and ethical considerations to assess legal frameworks

This table provides a non-exhaustive list of legal and ethical considerations that may be relevant. Member States are encouraged to assess their legal frameworks based on their own context and the DCTQ tool involved.

| | |
|---|---|
| **Proportionality** | Is there a legitimate public health need for collecting the data? |
| | Is the use of the tool necessary to meet the public health need? |
| | Is the use of the tool reasonable to meet that need, having regard to the impact on individuals and the community? |
| **Time limits** | Does the legal framework identify that the collection of data is temporary and will continue only as long as the public health need exists? |
| | Does the legal framework identify how the end date of the data collection will be determined? |
| | Does the legal framework outline how long the data will be retained and how it will be destroyed at the end of the period? |
| **Data minimisation** | Does the legal framework state that only the minimum amount of data necessary will be collected? |
| | Does the legal framework outline the exact type or types of data that will be collected? |
| **Transparency and explainability** | Are users of the technology required to be provided with a clear and unambiguous explanation of the technology and how it processes data? |
| | Is the technology behind the tool (including the source code) required to be published and open to third-party analysis and audit? |
| | Are users required to be informed about the existence of any automated decision-making processes and how risk predictions will be made? |