

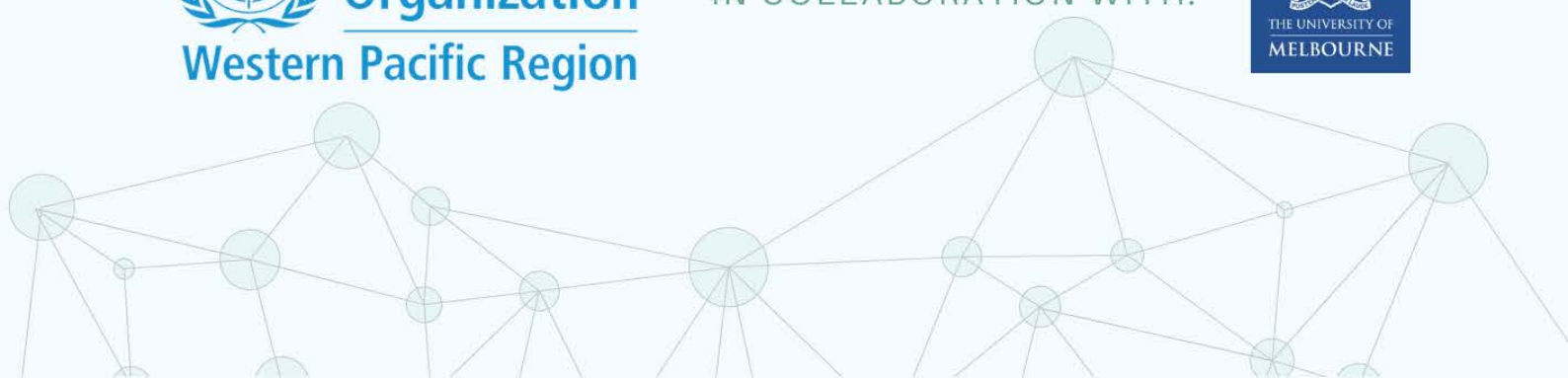


LEGAL DIMENSIONS OF COVID-19 SERIES
PAPER # 1

DIGITAL TECHNOLOGY AND
COVID-19 IN THE WESTERN
PACIFIC REGION



IN COLLABORATION WITH:



Legal Dimensions of COVID-19 Series: Paper #1

DIGITAL TECHNOLOGY AND COVID-19 IN THE WESTERN PACIFIC REGION

21 January 2021



WPR/DHS/2021/001

©World Health Organization 2021

Some rights reserved. This work is available under the CC BY- NC-SA 3.0 IGO licence.

This publication is part of a series developed in collaboration with the University of Melbourne. The main authors of the series of publications are the following: Jonathan Liberman (Associate Professor, University of Melbourne) and Ben Lilley and Darryl Barrett (WHO Regional Office for the Western Pacific).

The named authors alone are responsible for the views expressed in these publications.

Key points

- Digital technology plays a critical role across all aspects of health and has the potential to accelerate progress in attaining the Sustainable Development Goals related to health and well-being.
- The coronavirus disease 2019 (COVID-19) pandemic is highlighting the potential benefits of digital technology as well as its risks and limitations, including the so-called digital divide within the Western Pacific Region.
- Legal frameworks are essential for harnessing digital technologies, minimizing their risks and ensuring benefits are shared.
- COVID-19 presents an opportunity for Member States to build lasting legal and regulatory infrastructure that helps bridge the digital divide and realize the benefits of digital technology for health.

Purpose

To support WHO Member States in the Western Pacific Region in developing legal frameworks and related regulatory capacity to effectively use digital technologies in the COVID-19 response, as well as for health beyond the COVID-19 pandemic.

Background

Digital technology plays a critical and growing role across all aspects of health.

The 2018 World Health Assembly resolution on digital health recognized:

the potential of digital technologies to advance the Sustainable Development Goals, and in particular to support health systems in all countries in health promotion and disease prevention, and by improving the accessibility, quality and affordability of health services

The resolution urged Member States to “develop, as appropriate, legislation and/or data protection policies around issues such as data access, sharing, consent, security, privacy, interoperability and inclusivity consistent with international human rights obligations”.

The adoption of the resolution has stimulated increased global, regional and national activity towards harnessing the power of digital technologies for health. WHO has issued the new WHO Guideline: Recommendations on Digital Interventions for Health System Strengthening, the Global Strategy on Digital Health 2020–2025 and a Digital Implementation Investment Guide (DIIG): Integrating Digital Interventions into Health Programmes. In For the Future: Towards the Healthiest and Safest Region, laying out the vision for its work in the Western Pacific, WHO has highlighted innovation, including the use of digital technologies, as a key enabler to meet current and future health challenges. Vast disparities exist in countries’ access to digital technologies and capacity to make use of them. These disparities – or “digital

divide” – extend well beyond health and health systems. The Secretary-General of the United Nations recently issued a Roadmap for Digital Cooperation, which aims to “accelerate global digital cooperation, seizing on the opportunities that are presented by technology – while mitigating the risks – so that progress towards achieving the [Sustainable Development] Goals by 2030 can be made collectively”.

The digital divide also manifests disparities between the legal frameworks and regulatory capacities of countries to advance digital technology for health and manage its risks. For example, in 2015, WHO found that 91% of high-income countries (HICs), 81% of upper-middle-income countries (UMICs), and 79% of lower-middle-income countries (LMICs) reported general privacy legislation to protect personally identifiable information. This contrasted with only 45% of low-income countries (LICs) reporting the same protection. Regarding the more specific protection of the privacy of individuals’ health-related data in electronic health records, over 80% of HICs, 53% of UMICs, 28% of LMICs, and 30% of LICs reported such legislation. Of the six WHO regions, the Western Pacific had the lowest percentage of countries with general privacy legislation to protect personally identifiable information and the third highest percentage of legislation to protect the privacy of individuals’ health-related data in electronic health records.

The digital divide has significant impacts on all aspects of the COVID-19 response, including, for example, preparedness, surveillance, contact tracing and the delivery of health services. Yet, for all of the challenges it poses, COVID-19 also offers opportunities for digital development and capacity-building in all countries, including lower-resource countries.

Discussion

Digital technology and COVID-19

The COVID-19 pandemic has underscored the value and risks of digital technology for health and the implications of the digital divide between and within countries. These realities have been dramatically underlined by the speed with which SARS-CoV-2 – the virus that causes COVID-19 – spreads, the need for rapid interventions to control its spread, and the vulnerability of many health systems in the face of the pandemic. As the United Nations Secretary-General recently said, “the digital divide is now a matter of life and death for people who are unable to access essential health-care information. It is threatening to become the new face of inequality”.

Digital technology is playing an important role across virtually all aspects of the COVID-19 response, including collecting and analysing population data to drive decision-making, communicating vital information to and with the public, enabling and supporting contact tracing, monitoring population-level and individual responses to public health measures (such as quarantine, isolation and lockdowns), and delivering health services.

The urgency and exceptional nature of the COVID-19 pandemic also amplifies risks associated with the use of digital technology. Many of these risks are not unique to digital technology, but manifest differently and are exacerbated by technology, in particular due to the volumes and scale of data now capable of being collected and utilized. The speed with which digital technologies are being deployed increases the risk that legal frameworks will be ill-equipped to regulate their use and that the necessary safety, quality and governance arrangements will not be applied. The exceptional nature of COVID-19 may also be used to justify encroachments on rights and freedoms by governments and private actors and limit ordinary democratic processes and accountability mechanisms.

Building digital technology capacity for COVID-19 and beyond

Countries have greatly varying capacities to make use of digital technologies, including infrastructure (such as internet connectivity and mobile/broadband), availability of the technologies (for the country as a whole, and among population groups and subgroups), effective and interoperable data systems, workforce capability, digital literacy, trust in technology, capacity to fix problems when they arise and enabling legal frameworks.

This digital divide is apparent in the Western Pacific Region, for example, in the differences between a number of countries in Asia, Australia, New Zealand and Pacific island countries. Divides also exist within countries, such as between central islands/capital cities and outer islands/remote areas, which are less likely to have reliable and consistent digital access.

Despite this and all the challenges that COVID-19 presents, there are opportunities in all settings to build capacity in digital technology. Efforts to take advantage of these opportunities need to move at an appropriate pace, driven by national (and subnational) governments in accordance with local needs, cultures and values. Wherever possible, efforts should build on existing strategies and investments in digital health. These opportunities should be pursued in partnership with the community, including through co-design, to develop lasting participation and trust.

Responses should take into account immediate needs as well as future uses of any new technologies developed for the COVID-19 response. The use of technologies by individuals requires appropriate hardware, meaning that models chosen need to be appropriate for use with technologies (such as mobile phones) used in the country, both to ensure sufficient uptake to be effective and to minimize exclusion of particular population groups and subgroups.

Particular attention is needed to ensure that responses support, build on and do not

undermine existing health practices, nor disadvantage members of the community. The *WHO Guideline: Recommendations on Digital Interventions for Health System Strengthening* cautions against excluding or jeopardizing “the provision of quality non-digital services in places where there is no access to the digital technologies or they are not acceptable or affordable for target communities”. Inequity in accessing the benefits of digital technologies may extend beyond access to the technologies themselves and include the way technologies are applied. For example, algorithms supporting resource allocation and clinical decision-making may be biased and reflect and reinforce existing health inequities if based on data collected from non-representative samples of populations.

The vital role of legal frameworks

Effective legal frameworks are essential to harnessing the power of digital technologies for health generally and in combating COVID-19 in particular. Legal frameworks can act as a critical enabler for technology by establishing governing and coordinating structures, reducing barriers to innovation, and enabling actions to bridge the digital divide. Effective legal frameworks are also necessary to ensure that the use of digital technology is safe and of high quality, promotes equity, and accords with ethical and human rights principles, including that the privacy of individuals is respected and their personal data protected from misuse.

Besides having varying digital technology capacities, countries have different legal frameworks and related regulatory capacities for managing digital technologies. This applies across a range of relevant frameworks such as health and medical law, privacy and data protection law, discrimination law, consumer protection law, contract law, intellectual property law, occupational health and safety law, and the human resources capacity to develop, monitor and enforce laws and regulations.

Regulation of digital health information, and of digital information generally, is complex. Depending on the technology used,

information involved and domestic context, several sectors beyond health are likely to be involved. Information can be instantaneously made public and/or transmitted across jurisdictions. The digital landscape is constantly evolving and private sector expertise generally develops in advance of public sector knowledge.

The scale and unprecedented nature of the COVID-19 pandemic is putting pressure on existing legal frameworks relevant to digital technology and highlighting gaps and areas for strengthening. Pertinent to the use of technology, the COVID-19 response is characterized by:

- the central role of personal information, including sensitive health information which is subject to mandatory notification;
- the need to understand individual and population-level movements and behaviour to implement public health measures, and the technological means to systematically extract and analyse large volumes of data from various sources, including social media, e-commerce, mobile devices, satellite imagery and environmental sensors (big data);
- information needing to be shared quickly across multiple actors such as governments, clinicians, hospitals, laboratories and researchers;
- private sector actors often having significant roles, including as technology providers, health service providers and employers;
- errors potentially having enormous implications, for both individuals and the population as a whole – for example, if the virus spreads because incorrect information is communicated; and
- the global nature of the crisis and of the response, meaning that information of different kinds is shared with various actors across jurisdictions.

The health and related social and economic urgencies of COVID-19 cannot await the development of perfect or near-perfect legal frameworks. Countries need to make

judgements about how to avail themselves of the benefits of digital technologies while minimizing the risks.

Regulation of personal data and health information

Of particular concern and consideration for WHO are legal frameworks relating to the collection, storage, sharing, use of and access to information. This includes, for example:

- what information is to be collected and used and whether individuals are required to provide personal health information or are encouraged and permitted to do so;
- how information, once provided, can be stored and shared;
- for what purposes information can be used and under what conditions, such as with individual consent or alternate legal justification; and
- who may collect and use the information and who will have access to information once provided, such as individuals to whom the information relates or their treating clinicians.

Such frameworks are likely to encompass a range of laws administered by health and other sectors. They should be developed, as far as possible, in partnership with the community, including targeted engagement of vulnerable and disadvantaged groups, and their justification clearly explained. Any breaches should be taken seriously, appropriate remedies provided and necessary improvements made. Individuals should be given rights to challenge and correct information collected about them.

These are critical considerations because interventions to reduce the spread of COVID-19 rely on individuals coming forward, such as for testing. This is supported by building a sufficient degree of trust that personal information will be used appropriately – for instance, that it will not be disclosed in unethical ways and individuals will not be denied access to services or otherwise subjected to discrimination or stigma. These matters are also critical

because those involved in the collection and handling of information need sufficient clarity to enable them to use and share the information in a timely fashion for public health purposes.

One area that has received significant attention is the use of digital contact tracing apps, which governments may either require or request individuals to download and use. Each country will need to decide on the appropriate use of digital technology in contact tracing. There is generally a trade-off between the potential effectiveness of such apps in terms of their ability to trace and their intrusiveness, in the sense of how much personal information is provided. There are various models to support contact tracing, from centralized models operated by governments or on their behalf, through to decentralized models that are open source, or contact tracing capabilities developed by mobile software operating systems, such as from Apple and Google. These varying models involve different trade-offs, have different levels of effectiveness and require different kinds of regulation.

Regulation of private technology providers

Digital technological solutions are dominated by private technology providers, which have a range of commercial interests in the use of both their products and information that is collected through their products. Many of these companies have greater resources than a number of countries in the Western Pacific Region. Arrangements with such private providers entered into by governments should have sufficiently robust data-sharing and service agreements, with enforceable requirements relating to such matters as purpose specification, data use (and misuse), restricted access and disclosure, derived data, data enhancements, intellectual property, staff training, auditing, and accountability. Countries may benefit from the development of model or sample agreements addressing these matters.

Actions for consideration

Eight actions for WHO and Member States to work together and consider:

1. Review and, as necessary, strengthen legal frameworks governing collection, storage, sharing, use of and access to information. This will require collaboration across government and may involve reform of laws administered by sectors other than health.
2. Support investments in universal health coverage, through the review of health services, social insurance and other laws to reduce unnecessary barriers to innovation and identify opportunities to incentivize effective use of digital technologies, such as expanding access to telehealth services.
3. Identify legal barriers to equitable access to the benefits of digital technologies for health and advocate measures beyond the health sector to bridge the digital divide.
4. Review and, as necessary, strengthen regulatory capacity to enable the optimal use of digital technologies for health, including: professional standards, training and competencies; quality and safety; and efficiency in health-care applications.
5. Building on existing digital health strategies and structures, strengthen governance frameworks to build capacity across sectors and levels of government and promote accountability over the development and use of technology. Accountability mechanisms may include independent oversight, participatory governance, being open (such as source code, data, algorithmic models), and data protection impact assessments.
6. Consider arrangements with private technology providers, and, as necessary, strengthen arrangements to address data use (and misuse), data sharing and intellectual property.
7. Review and implement laws and related programmes in partnership with the community, including vulnerable and disadvantaged groups, to ensure the effectiveness and equity of responses and to build and maintain community participation and trust.
8. Prioritize the protection of personal information to avoid discrimination and stigma, including the exacerbation of existing health and social inequalities.