HHR
Health and Human Rights Journal

Human Rights and Digital Health Technologies

NINA SUN, KENECHUKWU ESOM, MANDEEP DHALIWAL, AND JOSEPH J. AMON

Abstract

Digital health technologies have been heralded as a critical solution to challenges and gaps in the delivery of quality health care and essential to achieving the Sustainable Development Goals. Yet they also present threats to privacy and confidentiality, which can lead to discrimination and violence, resulting in violations of the rights to health, housing, employment, freedom of assembly, expression, protection from arbitrary detention, bodily autonomy, and security. More broadly, without proper planning and safeguards, digital health technologies can contribute to expanding health inequity, widening the "digital divide" that separates those who can and cannot access such interventions. This article outlines key harms related to digital technologies for health, as well as ethical and human rights standards relevant to their use. It also presents several strategies for mitigating risks from digital health technologies and reviews mechanisms of accountability, including recent judicial rulings.

Nina Sun is Deputy Director of Global Health and Assistant Clinical Professor in the Department of Community Health and Prevention, Dornsife School of Public Health at Drexel University, Philadelphia, USA.

Kenechukwu Esom is Policy Specialist with the HIV, Health and Development Group of the United Nations Development Programme's Bureau for Policy and Programme Support, New York, USA.

Mandeep Dhaliwal is Director of the HIV, Health and Development Group of the United Nations Development Programme's Bureau for Policy and Programme Support, New York, USA.

Joseph J. Amon is Director of Global Health and Clinical Professor in the Department of Community Health and Prevention, Dornsife School of Public Health, Drexel University, Philadelphia, USA.

Please address correspondence to Nina Sun. Email: nys28@drexel.edu.

Competing interests: None declared.

Copyright © 2020 Sun, Esom, Dhaliwal, and Amon. This is an open access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/4.0/), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original author and source are credited.

Introduction

In early 2020, facing the challenge of limiting transmission from a poorly understood and fast-moving virus, governments took steps to implement measures to reduce mobility—including lockdowns, travel bans, and restrictions on large gatherings. Without a vaccine or cure, countries sought to increase social distancing; identify and isolate individuals infected by the SARS-CoV-2 virus that causes COVID-19 disease; and quarantine close contacts of those infected and individuals coming from areas with high levels of transmission.[1]

Many countries also turned to the development and use of digital technologies to support their COVID-19 response. Basic eHealth approaches, including online COVID-19 data dashboards and mobile phone apps for symptom screening and case management, have complemented new digital technologies such as infrared thermal screening cameras and wearables (for example, smartwatches) that monitor temperature, pulse, and sleep to screen for the disease.[2] The use of artificial intelligence (AI) and machine learning has allowed for the analysis of large data sets ("big data") for prediction, forecasting, contact tracing, and drug and vaccine development.

The development of digital apps for contact tracing and for the monitoring and enforcement of quarantine and social distancing orders has been especially prevalent—and controversial—in national responses and in global discussions of how to control COVID-19 and reconcile individual rights to privacy and confidentiality with control efforts. For example, in March 2020, Ecuador's health ministry released an app for individuals to report COVID-19 symptoms. The application can connect individuals with a health care worker—however, to use the app, users must provide personal information, as well as their geolocated address. Human rights organizations raised concerns about the country's lack of legislation or independent oversight body to protect the sensitive data collected.[3] Similarly, in Israel, an emergency law authorized Israel's internal security service to collect information, without user consent, to predict which citizens may have been exposed to the virus.[4] Under the program, the health ministry sends alerts to people's phones ordering them to self-quarantine. In the United Kingdom, the development of a contact tracing app by the National Health Service was met with concerns from parliamentarians about the lack of legal protections and clarity in terms of what data would be collected, what that data will be used for, who will have access to it, and how it will be safeguarded from hacking.[5]

Apps have also been developed to enforce quarantine and social distancing orders. For example, in China, the government funded private tech companies to jointly develop an app that determines who needs to quarantine and for how long.[6] The app assigns users one of three colors: green enables unrestricted movement, yellow requires seven days of quarantine, and red requires fourteen days of quarantine. Users must scan a QR code in order to enter buildings (including their homes), go to the supermarket, or use public transport. Human rights organizations have raised concerns that the app shares data on users' locations with the police and that the app's decisions can be arbitrary and difficult to appeal, leaving some individuals confined to their homes indefinitely.[7] South Korea, Singapore, Germany, France, Australia, and India have also piloted or adopted mobile phone apps to support COVID-19 contact tracing.[8]

These examples from the COVID-19 response did not emerge from nowhere. For the past few decades, digital health technologies have been increasingly employed in clinical medicine and public health practice. While not new, the profile of digital technologies for health has risen with the COVID-19 pandemic, alongside questions and concerns about what safeguards exist that adequately balance potential benefits and harms. The HIV response has long had discussions related to how to best advance public health, taking a right-based approached to mitigate harms.[9] Many of these HIV and human rights standards are also relevant across other health issues, including COVID-19. Building on that framework, this article provides an overview of some potential harms related to digital health technologies and then describes the ethical and human rights standards that can guide

governments and other stakeholders in mitigating the rights-related concerns of these technologies.

Key harms related to digital health technologies

There are various potential human rights-related concerns that may arise out of the use of digital technologies for health, including lack of access (the "digital divide") and the privatization of health information and services. Three potential harms related to digital health technologies that can relate to privatization, as well as public health systems, include data breach, bias, and function creep. Understanding each is critical to minimizing the harms of digital health technologies.

Data breach

A data breach refers to any breach of security that leads to the "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data."[10] Data breaches are common in the health sector and have a variety of causes—from malware and hacks to accidental or purposeful disclosure of personal health information by health care employees.[11] One study found that in 2016 and 2017, there were over 1,300 recorded incidents of protected health information data breaches across 27 countries.[12] In 2019, a data breach in Singapore resulted in the release of the personal information of more than 14,000 people living with HIV.[13] Data breaches violate an individual's right to privacy and erode trust in the health care system. As technology evolves and health systems become more complex, the likelihood of data breaches increases. To combat this risk, health systems must invest in information security and data protection, but not all health systems may have the resources to do so.

Bias and discrimination

Differentiated treatment has been repeatedly documented as a result of algorithmic biases in AI and other automated processes. This phenomenon can, for example, amplify discrimination in criminal justice proceedings and predictive policing, facilitate discriminatory hiring decisions, or produce targeted online marketing campaigns with discriminatory effects.[14] Within health care, studies examining applications of AI have also demonstrated that algorithms do not provide equally accurate predictions of health outcomes across race, gender, or socioeconomic status.[15] This raises concerns that AI will further entrench discrimination and prejudice against individuals based on these grounds. To highlight these concerns, the United Nations Special Rapporteur on contemporary forms of racism is developing a report on new information technologies, nondiscrimination, and racial equality.[16] Additionally, certain types of algorithmic decisions evade current nondiscrimination laws, leading to unfair differentiation that is technically legal (for example, offering differing prices for the same product based on speed of internet access) but can undermine the goal of achieving the right to health for all.[17]

Function creep

Function creep occurs when data that are collected for a specific purpose (for instance, personal information provided as a part of medical screening) are used for another purpose (such as to check immigration status). Concerns about function creep are relevant for all forms of digital health technologies but are especially pertinent to biometrics, where, for example, biometric data collected for digital health purposes could be used for forensics or criminal proceedings.[18] This concern has been highlighted in the HIV response, where many communities disproportionately affected by HIV may be stigmatized or criminalized groups.[19] Function creep can also lead to data breaches, when, for example, wearables such as fitness apps reveal information that can be used to identify individuals' homes, places of work and worship, or businesses frequented. Government partnerships with private companies, including big technology companies, have also raised alarms related to the potential for function creep with the exploitation of data for surveillance or commercial purposes.[20]

Global overview: Ethics and human rights approaches

To date, discussions around strategies to address potential harms from digital health technologies have emphasized the adoption of ethical principles and guidelines. There have also been discussions around the application of legally binding international human rights obligations.[21] While there may be some conceptual overlap in principles, ethics and human rights should be seen as separate yet complementary systems that aim to protect individuals and promote accountability for effective, just, and people-centered digital health technologies.

Ethical approaches

Various groups, such as the Institute of Electrical and Electronics Engineers, the World Economic Forum, and the European Commission's High-Level Expert Group on Artificial Intelligence, have developed resources related to ethics and digital technologies.[22] The United Nations' Chief Executive Board is also currently in the process of developing recommendations on the ethics of artificial intelligence.[23] Key ethical principles coming from these organizations highlight ethical principles familiar to public health and biomedical researchers, including beneficence, autonomy, consent, privacy, participation, transparency, nondiscrimination, equity, and accountability.

Most ethical frameworks emphasize that digital health technologies should "do no harm," and they include an obligation to be aware of, and mitigate, any harms that may occur. In addition to minimizing harmful effects, technologies should also maximize benefits for humanity.[24] The frameworks also stress that all individuals should be recognized as having agency over themselves and their personal information; that any personal information collected should be done with fully informed consent; and that safeguards should exist to protect the integrity and security of personal information.

Ethical frameworks also encourage inclusiveness and participation, calling on developers and government authorities to ensure that end users are meaningfully engaged in the development of digital technologies. Further, the development, adoption, and implementation of digital health technologies should be done in an open, discoverable manner that allows for public feedback, monitoring, and consultation—including, for example, ensuring algorithmic transparency. Ethical frameworks also emphasize that digital health technologies should not deliberately or unintentionally discriminate against individuals. Moreover, ethics underscore the importance of equity and encourage those developing digital technologies to account for the needs of vulnerable and marginalized groups, including women, children, racial and ethnic minorities, and migrants. This includes ensuring that effective nondigital options be available and accessible to all as an alternative to digital technologies.

Establishing ethical frameworks on digital health technologies can be important for advancing rights and mitigating harms, and these frameworks are often used to regulate private actors, whether individuals or organizations. However, ethical principles can lack specificity, and enforcement mechanisms can be weak. Thus, adopting and implementing human rights norms and standards that enshrine basic ethical principles into law can provide important opportunities for enforceability and accountability.

International human rights framework

While there is no specific global human rights agreement for digital technologies, many existing human rights obligations are applicable. Within the context of health, the HIV movement has been a leader in integrating human rights to facilitate more just, effective responses. This has also included discussion on the rights-related standards on the use of digital technologies for populations at increased risk of HIV. Based on this work, as well as the discussion raised by COVID-19, the most relevant standards in the adoption of digital health technologies are the rights to health, nondiscrimination, benefit from scientific progress, and privacy.

Right to health

The adoption of digital technologies for health must align with the right to health. Enshrined in

several human rights treaties, the right to health outlines four key elements: availability, accessibility, acceptability, and quality.[25] The use of digital technologies for health must, at minimum, satisfy these four key elements. These obligations mean that governments should ensure the availability and accessibility of digital infrastructure throughout the country, both in terms of hardware (for example, computers, mobile phones, mobile phone towers, internet, and broadband accessibility) and in terms of software (for example, applications). This also includes providing digital literacy trainings for all users, including those in leadership, health care, and communities.[26] Addressing the availability and accessibility of digital health technologies supports efforts to bridge the digital divide. Digital health technologies should be a step toward supporting countries in realizing the right to health, which means that they must be acceptable to all communities and must be of good quality (meaning that they must be able to deliver on their clinical or public health purpose).

Right to nondiscrimination

Emerging and new technologies raise two main categories of concerns related to nondiscrimination. The first relates to access and availability of the technologies, while the second centers on implicit biases within the technologies themselves. On access and availability, due to a myriad of issues—including limited technical infrastructure (for example, broadband access, satellite towers, and electricity), lack of digital literacy, expense, and lack of access to digital hardware (for example, mobile smart phones and computers)—relying on digital technologies as a primary system or strategy within the health sector may inadvertently exacerbate inequalities, contributing to the digital divide.[27] On biases within digital technologies, human rights and technology experts recognize that the design of various technologies may include implicit and inadvertent biases. Engineers and software developers tend to design technologies with limited engagement and input from communities with diverse backgrounds, such as racial, gender, and socioeconomic backgrounds.[28]

To realize the right to nondiscrimination in the context of digital technologies, states and technology companies alike should proactively identify risks of discrimination in access to and the availability of technologies. If violations occur, states should hold private businesses to account for preempting, identifying, mitigating, and redressing discriminatory outcomes.[29] States should also ensure transparency and accountability related to the development, adoption, implementation, and evaluation of digital technologies for health, as well as provide access to justice where the right to nondiscrimination or other rights have been violated. Finally, there should be an effective, nondigital option that achieves the same goal for those who are unwilling or unable to use digital technologies.[30]

Right to benefit from scientific progress

The right to enjoy the benefits from scientific progress can be a critical component in achieving the right to health. Countries have a duty to ensure the availability and accessibility of "all the best available applications of scientific progress necessary to enjoy the highest attainable standard of heath," on a nondiscriminatory basis, with a focus on the most marginalized.[31] On emerging and new technologies, states should balance the benefits and risks. New technologies should be developed and used within an inclusive, rights-based framework, highlighting the principles of transparency, nondiscrimination, accountability, and respect for human dignity. States should also develop laws that impose an obligation for human rights due diligence on private and other nonstate actors (see section below on obligations of private enterprises). Finally, states should regulate the control and ownership of data collected through new technologies to prevent misuse and exploitation, as well as ensure informed consent and privacy.[32]

Right to privacy

Human rights law recognizes the right to be free from arbitrary or unlawful interference with one's privacy.[33] Any lawful interference with this right must be precisely outlined in relevant legislation.[34] Moreover, states must regulate the collection and

storage of personal information—these measures must be effective in preventing the unauthorized disclosure or use of personal information.[35] Such information can never be used for any purpose that is incompatible with the aims of human rights law. In addition, individuals have the right to know what personal data is stored in databases, and the purposes of such storage. They also have the right to request the rectification or elimination of files that contain incorrect personal information or "have been collected or processed contrary to the provisions of the law."[36] These obligations are further built on by regional agreements on data privacy and protection (see corresponding section below). Moreover, the Special Rapporteur on the right to privacy's *Recommendation on the Protection and Use of Health-Related Data* also outlines important rights-related considerations.[37] It covers key topics such as rights of the data subject, security and interoperability, transborder data flow, and considerations related to data and gender, indigenous populations, and persons with disabilities.

Human rights-related obligations of private enterprises

States have specific human rights obligations related to private businesses. First, states must protect against human rights abuses by third parties, an obligation that covers private actors. This includes ensuring access to justice when business-related human rights violations arise. Governments should also set expectations for businesses domiciled or operating within their jurisdiction to respect human rights, including through crafting, monitoring, and enforcing protective legislation, as well as conducting human rights due diligence that accounts for issues related to gender and marginalization.

Private companies also have human rights-related obligations, including, at a minimum, the duty to respect human rights standards.[38] Respecting human rights means that private companies must

> *(a) avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur; [and] (b) seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.*[39]

In alignment with these principles, companies should develop and enact human rights policy commitments and conduct human rights due diligence. This due diligence comprises ongoing processes that assess the human rights impacts of companies' operations, preventing or mitigating impacts, tracking to see how concerns are addressed, and remedying any actual violations that the operations caused or to which they contributed.[40] Rather than framing private sector obligations solely within the realm of voluntary or unenforceable ethical standards, business enterprises should treat the obligation to respect human rights as a legal compliance issue.

Regional data-protection frameworks

One human right that has been firmly established in regional-level agreements is the right to privacy. Such agreements include the African Union Convention on Cyber Security and Personal Data Protection, Asia-Pacific Economic Cooperation Privacy Framework, European Union's General Data Protection Regulation, Standards for Personal Data Protection for Ibero-American States, and Council of Europe's Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data.[41] Many of these frameworks have a specific focus on data privacy and surveillance and have developed safeguards related to data processing and the rights of individuals whose data are collected (that is, the "data subjects").

Under these regional frameworks, data should be collected and processed in a manner that (1) is lawful, fair, and transparent to the data subject; (2) aligns with a legitimate purpose that is clearly specified and agreed to by the data subject; (3) is the minimum necessary for the legitimate purpose; (4) is stored only for as long as necessary for the specified, legitimate purpose; (5) ensures appropriate security, as well as data integrity and accuracy; and (6) ensures that the entity that controls the data demonstrates compliance with all principles

of data processing.[42] Informed consent must also be obtained prior to data collection and processing. This consent must be voluntarily given—an unambiguous agreement to a request presented in clear and plain language.[43] Furthermore, entities (that is, states or companies) that process data must implement safeguards to ensure data security, including anonymization or pseudonymization, as well as the encryption of personal data.[44]

These regional frameworks also enshrine a set of positive rights for data subjects. These "rights of the data subject" include the following:

- right to be informed about what data are and are not collected;
- right to access stored data;
- right to rectification;
- right to erasure (commonly known as the "right to be forgotten");
- right to restriction of processing;
- right to be notified of rectification or erasure or restriction of processing;
- right to data portability;
- right to object; and
- rights related to automated decision-making and profiling.[45]

Strengthening human rights-aligned governance of digital health technologies at the national level

To ensure that all individuals can enjoy the benefits of digital health technologies while mitigating the harms, it is critical for all stakeholders—including governments, civil society, and the private sector—to take steps to protect human rights in this context. Part of the solution, especially related to concerns around data breaches and function creep, is to establish safeguards aligned with regional and global human rights and ethical standards in national legal frameworks on data collection and processing, as well as on the rights of the data subject. But these are minimum standards—a floor on which to build. Not only should digital health technologies ensure privacy, but they should be leveraged to advance the right to health in an equitable, nondiscriminatory manner. There are three opportunities that allow countries to assess whether there is sufficient consideration of ethical principles and integration of human rights protections when digital health technologies are adopted: health technology assessments (HTAs), national digital health strategies, and judicial review.

Health technology assessments

One strategy for preventing rights violations arising from data breaches, biases, and function creep is the requirement for a robust system of HTA prior to the authorization for use of a new (or updated) digital health technology. An HTA is a multidisciplinary process that evaluates the "value of health technology at different points in its lifecycle" (including the technology's properties, effects, and impacts).[46] It aims to inform policy makers and influence decision-making in health care, with a focus on how best to allocate funding for health programs and technologies. Components of such an assessment include the validation of technical aspects (for example, the accuracy of the product or system), clinical considerations (for example, contribution toward improving or maintaining a specific health condition), and systems compatibility (for example, connection with or integration into patients' lives, health service provision, and health systems, including medical records).[47] It can be applied to different types of interventions, such as piloting tests, medicines, vaccines, procedures, and programs.

Applying HTAs to digital technologies provides an opportunity for governments to assess the ethical and human rights risks of these technologies, including considerations related to equity. HTAs can face challenges in this role, however, as digital health technologies evolve rapidly and the technology sector's ethos of "moving fast and breaking things" stands in contrast with the conventional process of health technology devel-

opment and testing for patient safety and clinical efficiency (upholding a "do no harm" approach).[48] To better tailor HTAs to digital health technologies with a focus on ensuring equity in availability and access, there are several key considerations. In addition to assessing the traditional technical, clinical, and systems elements, integrating a strong focus on usability and human-centered design is critical. Digital technologies should be co-designed with end users (for example, health care providers, systems administrators, patients, and communities) and should have effective mechanisms for subsequent feedback and iteration. This speaks to a cornerstone of product design, which is that they must meet the needs of end users. This also facilitates the uptake and effectiveness of digital technologies and fulfills the key ethics and human rights principle of meaningful participation and engagement. HTAs should also assess the risks for bias or discrimination as a result of access to and use of the digital health intervention. This includes reviewing a digital technology's accessibility and availability for all users, including those most left behind.

National digital health strategies

Another approach to review country-level standards for digital health technologies is the development of a national digital health strategy. These strategies facilitate coordination, set standards for interoperability, and establish policies related to digital health.[49] A country-wide strategy is also helpful for identifying gaps and opportunities where digital technologies can be best leveraged to improve health outcomes. The process of developing a national digital health strategy is an opportunity to define the human rights standards, advance rights-based principles (such as participation via broad-based consultations), and develop the trust necessary for effective implementation. According to the World Health Organization's 2015 global survey on eHealth, 72 countries have national digital health strategies and corresponding implementation plans.[50] The 2019 report of the Global Digital Health Index (GDHI) indicates that out of the 22 current GDHI countries, Jordan, Portugal, Bangladesh, Thailand, Malaysia, and the Philippines have the most advanced processes, policies, and practices for digital health.[51]

Accountability through the judicial system

Courts have historically played a key role in protecting human rights and clarifying the obligations of states, particularly on the right to health.[52] Within the HIV response, for example, judicial decisions have advanced a range of rights and freedoms, including the right to access antiretroviral treatment.[53] Similarly, for the use of digital technologies, some judiciaries have led the way in weighing the need for digital technologies while mandating the protection of human rights. While the cases below are not focused specifically on health issues, their rulings have a direct impact on the adoption and use of digital health technologies.

The Indian Supreme Court's decision in *Justice K.S. Puttaswamy (Rtd) v. Union of India and Others* is noteworthy because the court read the right to privacy into the Indian Constitution, which otherwise does not explicitly enshrine this right. It noted that "[p]rivacy is concomitant of the right of the individual to exercise control over his or her personality" and that privacy is "the necessary condition precedent to the enjoyment of any guarantees in Part III [fundamental rights]."[54] The court underscored that fundamental rights and freedoms such as those to life, dignity, and equality cannot be enjoyed without respecting the right to privacy. In elaborating on this right, the court noted that a critical aspect of the right to privacy is control over the dissemination of personal information. It also noted that every individual should have the right to exercise control over his or her own life and image as portrayed in the world and to control the commercial use of his or her identity.[55]

The Supreme Court's judgment paved the way for the development of a comprehensive privacy and data protection bill in India. The bill, released in mid-2018, has many positive features, including data-protection impact assessments, a right to be forgotten, and enforcement penalties. But there are also concerns, such as the use of personal data by law enforcement; while the bill notes that this use

should be "necessary and proportionate," it nevertheless contains broad exemptions.[56]

In the context of data and digital technologies, the Supreme Court of Jamaica considered legal standards within an explicit constitutional right to privacy in the case of *Julian Robinson v. The Attorney General of Jamaica*.[57] Specifically, the case analyzed the legality of the National Identification Registration Act (NIRA), which aimed to facilitate people's enrollment in a national identification system. Enrolment in the national identification system was mandatory for all citizens and residents of Jamaica, with the failure to enroll subject to criminal sanctions. In *Robinson*, the court struck down the NIRA, holding that the law violated the country's constitutional Charter of Fundamental Rights and Freedoms. It found that the act did not "provide sufficient safeguards against misuse and abuse of the data collected" and that the compulsory collection of biographical and biometric data violated various rights under the charter, including the rights to privacy and nondiscrimination. The court also found that the NIRA did not comply with the standard of data minimization (in other words, taking no more data than necessary for a legitimate purpose).[58]

Similarly, on the topic of biometrics, the High Court of Kenya, in January 2020, held that the government's initiative to assign each citizen a unique biometric ID, known as Huduma Namba, needed stronger privacy and data protections before it could proceed. Moreover, the court prohibited the government from collecting individuals' DNA and location data as part of this initiative.[59]

On privacy and differentiated treatment, the Hague District Court in the Netherlands struck down the government's use of SyRI, an "automated program that analyzes a wide range of personal and sensitive data to predict how likely people are to commit tax or benefits fraud."[60] SyRI's risk calculation system was kept secret by the Dutch government so that surveilled individuals could not challenge the fraud investigations against them. The court ruled that the government must respect citizens' right to privacy and that transparency is critical as a safeguard against intrusion. It also noted that because SyRI was implemented only in low-income neighborhoods, this use could amount to discrimination on the basis of socioeconomic or immigrant status.[61]

Conclusion

Digital technologies hold much promise for addressing inequities and barriers to health care quality and access. They have the potential to reduce health care costs, transform health systems to provide more accurate and responsive care, and break down silos between sectors. But fears about digital technologies resulting in rights violations are real and grounded in the experiences of populations who are already subject to discrimination, social marginalization, and surveillance. In the future development of digital health technologies, more attention should be given to the development of community-owned technologies, aligned with ethical principles, that explicitly seek to advance accountability and justice. For example, within the HIV response, eHealth apps may be used by community members to monitor medication stockouts (for example, antiretroviral therapies) or to address discriminatory treatment in health care facilities.[62] They may also facilitate reports of abusive law enforcement practices against vulnerable and key populations. Governments should also ensure that digital health interventions directly address the digital divide and inequities in access. Furthermore, governments should take advantage of the data provided by digital health technologies to advance transparency and facilitate dialogue with populations—to both inform and validate the findings.

The diversity and sophistication of digital health technologies can make it difficult for nonexperts—or anyone—to understand the consequences of hitting "accept" when a five-thousand-word notice in five-point font appears on the screen of their phone. Combatting this, and leveraging the potential of digital health technologies, requires the meaningful adoption of standards and principles that ensure that these technologies truly protect rights, empower individuals, and do no harm.

References

1. For an overview of human rights issues related to the COVID-19 response, see J. J. Amon and M. Wurth, "A virtual roundtable on COVID-19 and human rights with Human Rights Watch researchers," *Health and Human Rights Journal* 22/1 (2020), p. 399.

2. S. Whitelaw, M. A. Mamas, E. Topol, and H. G. C. Van Spall, "Applications of digital technology in COVID-19 pandemic planning and response," *Lancet Digital Health* (June 29, 2020); J. Budd, B. S. Miller, E. M. Manning, et al., "Digital technologies in the public-health response to COVID-19," *Nature Medicine* (2020), pp. 1–10.

3. Human Rights Watch, *Ecuador: Privacy at risk with Covid-19 surveillance* (July 1, 2020). Available at https://www.hrw.org/news/2020/07/01/ecuador-privacy-risk-covid-19-surveillance.

4. N. Lomas, "Israel passes emergency law to use mobile data for COVID-19 contact tracing," *Tech Crunch* (March 18, 2020). Available at https://techcrunch.com/2020/03/18/israel-passes-emergency-law-to-use-mobile-data-for-covid-19-contact-tracing.

5. UK Parliament Human Rights Committee, *Human rights and the government's response to Covid-19: Digital contact tracing* (May 7, 2020). Available at https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/343/34305.htm#_idTextAnchor011.

6. M. Wang, "China: Fighting COVID-19 with automated tyranny," *Diplomat* (April 1, 2020). Available at https://thediplomat.com/2020/03/china-fighting-covid-19-with-automated-tyranny.

7. Human Rights Watch, *Mobile location data and Covid-19: Q&A* (May 13, 2020). Available at https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa.

8. Whitelaw et al. (see note 2).

9. See, for instance, Office of the United Nations High Commissioner for Human Rights and UNAIDS, *International guidelines on HIV/AIDS and human rights* (Geneva: Office of the United Nations High Commissioner for Human Rights, 2006).

10. European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016).

11. Center for Internet Security, *Data breaches: In the healthcare sector.* Available at https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/.

12. Verizon, *Protected health information data breach report: White paper* (2018). Available at https://enterprise.verizon.com/resources/reports/2018/protected_health_information_data_breach_report.pdf.

13. S. Leyl, "Singapore HIV data leak shakes a vulnerable community," *BBC News* (February 22, 2019). Available at https://www.bbc.com/news/world-asia-47288219.

14. F. J. Z. Borgesius, "Strengthening legal protection against discrimination by algorithms and artificial intelligence," *International Journal of Human Rights* (March 25, 2020). For more information on AI biases and human rights, see M. Latonero, *Governing artificial intelligence: Upholding human rights and dignity* (Data and Society, 2018).

15. I. Chen, P. Szolovits, and M. Ghassemi, "Can AI help reduce disparities in general medical and mental health care?," *AMA Journal of Ethics* 21/2 (2019), pp. E167–E179.

16. To be released in 2020; see Office of the United Nations High Commissioner for Human Rights, *New information technologies, racial equality, and non-discrimination: Call for input.* Available at https://www.ohchr.org/EN/Issues/Racism/SRRacism/Pages/Info-Technologies-And-Racial-Equality.aspx.

17. Borgesius (see note 14).

18. M. Kavanagh, S. Baral, M. Milanga, and J. Sugarman, "Biometrics and public health surveillance in criminalized and key populations: Policy, ethics and human rights considerations," *Lancet HIV* (2018).

19. Global Commission on HIV and the Law, *Risks, rights and health: Supplement* (New York: UNDP, 2018); for COVID-19 concerns, see S. L. M. Davis, "Contact tracing apps: Extra risks for women and marginalized groups," *Health and Human Rights Journal* (April 29, 2020). Available at https://www.hhrjournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups.

20. See, for instance, Privacy International, *Amazon: Alexa, what is hidden behind your contract with the NHS?* (December 2019). Available at https://privacyinternational.org/node/3298; Privacy International, *(Sort of) Trust but verify: Palantir responds to questions about its work with NHS* (May 2020). Available at https://privacyinternational.org/long-read/3751/sort-trust-verify-palantir-responds-questions-about-its-work-nhs; Privacy International, *Google: Give Google an inch and they'll take a mile!* (November 2019). Available at https://privacyinternational.org/node/3280.

21. See, for example, S. L. M. Davis, K. Esom, R. Gustav, et al., "A democracy deficit in digital health?," *Health and Human Rights Journal* (January 16, 2020). Available at https://www.hhrjournal.org/2020/01/a-democracy-deficit-in-digital-health/. See also S. L. M. Davis, "Contact tracing apps: Extra risks for women and marginalized groups," *Health and Human Rights Journal* (April 29, 2020). Available at https://www.hhrjournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups/.

22. See IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically aligned design: A vision for prioritizing human well-being with autonomous and intelligent systems*, 1st edition (Piscataway: IEEE, 2019); T. Philbeck, N. Davis, and A. Engtoft Larsen, *Values, ethics and innovation rethinking technological development in the*

fourth Industrial Revolution (World Economic Forum, 2018). Available at http://www3.weforum.org/docs/WEF_WP_Values_Ethics_Innovation_2018.pdf; European Commission, High Level Excerpt Group on Artificial Intelligence, *Ethics guidelines for trustworthy artificial intelligence* (Brussels: European Commission, 2019).

23. United Nations, Chief Executives Board for Coordination, *First version of a draft text of a recommendation on the ethics of artificial intelligence* (July 2020).

24. See National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, US Department of Health, Education and Welfare, *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research* (1979).

25. Committee on Economic, Social and Cultural Rights, General Comment No. 14, The Right to the Highest Attainable Standard of Health, UN Doc. No. E/C.12/2000/4 (2000); for articles on the right to health, see International Covenant on Economic, Social and Cultural Rights, G.A. Res. 2200A (XXI) (1966), art. 12; Convention on the Elimination of All Forms of Discrimination against Women, G.A. Res. 34/180 (1979), arts. 11(1), 12; Convention on the Rights of the Child, G.A. Res. 44/25 (1989), art. 24; International Convention on the Elimination of All Forms of Racial Discrimination, G.A. Res. 2106A (XX) (1965), art. 5; Convention on the Rights of Persons with Disabilities, G.A. Res, 61/106 (2006), art. 25; African Charter on Human and People's Rights, OAU Doc. CAB/LEG/67/3 rev. 5 (1981), art. 16; Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights (1988), art. 10.

26. United Nations, *Report of the Secretary General: Roadmap for digital cooperation* (June 2020).

27. See, for example, P. Alston, Report of the Special Rapporteur on Extreme Poverty, Digital Technology, Social Protection and Human Rights, UN Doc. A/74/493 (2019), paras. 44–49.

28. See Amnesty International and Access Now, *Toronto Declaration on the protecting the right to equality and non-discrimination in machine learning systems* (2018). Available at https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems. See also Alston (see note 27).

29. Amnesty International and Access Now (see note 28).

30. Alston (see note 27).

31. Committee on Economic, Social and Cultural Rights, General Comment No. 25, Science and Economic, Social and Cultural Rights, UN Doc. E/C.12/GC/25 (2020), para. 70.

32. Ibid., paras. 75–76.

33. International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI) (1966); see also Convention on the Rights of the Child, G.A. Res. 44/25 (1989); International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, G.A. Res. 45/158 (1990), art. 14.

34. Human Rights Committee, General Comment No. 16, Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (1988).

35. Ibid., para. 10.

36. Ibid.

37. Mandate of the United Nations Special Rapporteur on the Right to Privacy, Task Force on Privacy and the Protection of Health-Related Data, *Recommendation on the protection and use of health-related data* (2019). Available at https://ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf.

38. Office of the United Nations High Commissioner for Human Rights, *Guiding principles on business and human rights* (New York: United Nations, 2011); see also Shift and Institute for Human Rights and Business, *ICT sector guide on implementing the UN Guiding Principles on Business and Human Rights* (European Commission, 2014); Committee on Economic, Social and Cultural Rights (2020, see note 31), paras. 75–76; Amnesty International and Access Now (see note 28); D. Puras, Report of the Special Rapporteur on the Right of Everyone to the Highest Attainable Standard of Physical and Mental Health, UN Doc. A/HRC/44/48 (2020), para. 78.

39. Office of the United Nations High Commissioner for Human Rights (2011, see note 38), principle 13.

40. Shift and Institute for Human Rights and Business (see note 38).

41. African Union Convention on Cyber Security and Personal Data Protection (2014); Asia-Pacific Economic Cooperation Privacy Framework (2005); European Union (2016, see note 10); Standards for Data Protection for the Ibero-American States (2017); Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, amended by the Protocol CETS No. 223 (1981).

42. European Union (2016, see note 10), art. 5.1-2; African Union Convention on Cyber Security and Personal Data Protection (2014), arts. 13, 22; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, amended by the Protocol CETS No. 223 (1981), art. 5; Standards for Data Protection for the Ibero-American States (2017), ch. II; see also Asia-Pacific Economic Cooperation Privacy Framework (2005), part III.

43. European Union (2016, see note 10), art. 7; African Union Convention on Cyber Security and Personal Data Protection (2014), art. 13; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, amended by the Protocol CETS No. 223 (1981), art. 5; Standards for Data Protection for the Ibero-American States (2017), art. 12; Asia-Pacific Economic Cooperation Privacy Framework (2005), principle V.

44. European Union (2016, see note 10), art. 32; see also

European Union, *Recital 78: Appropriate technical and organizational measures*. Available at https://gdpr.eu/recital-78-appropriate-technical-and-organisational-measures/; African Union Convention on Cyber Security and Personal Data Protection (2014), arts. 13, 20–21; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, amended by the Protocol CETS No. 223 (1981), art. 5; Standards for Data Protection for the Ibero-American States (2017), art. 7; Ibero-American Standards (see note 41) articles 19, 21, 23; APEC Privacy Framework (see note 41) principle VII. Security safeguards.

45. Synthesized from key principles in EU GDPR (see note 10) articles 12-23; AU Convention (see note 41) articles 16-19; Standards for Data Protection for the Ibero-American States (2017), arts. 24–32; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, amended by the Protocol CETS No. 223 (1981), art. 5; Standards for Data Protection for the Ibero-American States (2017), art. 9.

46. Health Technology Assessment International, *About Health Technology Assessment International*. Available at https://htai.org/about-htai; see also World Health Organization, *Health technology assessment*. Available at https://www.who.int/medical_devices/assessment/en.

47. S. C. Mathews, M. McShea, C. L. Hanley, et al. "Digital health: A path to validation," *NPJ Digital Medicine* (2019).

48. Ibid.

49. Inter-Telecommunications Union, *Digital health strategies*. Available at https://www.itu.int/en/ITU-D/ICT-Applications/Pages/e-health-strategies.aspx.

50. N. Cory and P. Stevens, "Building a global framework for digital health services in the era of COVID-19," Information Technology and Innovation Foundation (2020). Available at https://itif.org/publications/2020/05/26/building-global-framework-digital-health-services-era-covid-19; see also World Health Organization, *Global Observatory for Health: Global survey*. Available at https://www.who.int/goe/data/en.

51. P. Mechael and J.K. Edelman, *The state of digital health: 2019, Global Digital Health Index* (2019). Available at https://static1.squarespace.com/static/5ace2doc-5cfd792078a05e5f/t/5d4dcb80a9b364000183a34/1565379490219/State+of+Digital+Health+2019.pdf.

52. P. Bergallo, "Argentina: Courts and the right to health; Achieving fairness despite 'routinization' in individual coverage cases?" in A. E. Yamin and S. Gloppen (eds), *Litigating health rights: Can courts bring more justice to health?* (Cambridge, MA: Harvard University Press, 2011).

53. See, for example, South African Constitutional Court, *Minister of Health v. Treatment Action Campaign (TAC)* (2002) 5 SA 721.

54. Supreme Court of India, *K. S. Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012 (August 24, 2017).

55. Ibid.

56. R. Chirgwin, "India mulls ban on probes into anonymized data use—with GDPR-style privacy laws," *Register* (July 31, 2018). Available at https://www.theregister.com/2018/07/31/india_privacy_boffin_ban.

57. Supreme Court of Jamaica, *Robinson, J. v. the Attorney General of Jamaica*, [2019] JMFC Full 04.

58. Ibid.

59. High Court of Kenya, *Nubian Rights Forum v. Attorney-General* (2019).

60. A. Toh, "Dutch ruling a victory for rights of the poor," Human Rights Watch (February 6, 2020). Available at https://www.hrw.org/news/2020/02/06/dutch-ruling-victory-rights-poor#; *Nederlands Juristen Comité voor de Mensenrechten tegen Staat der Nederlanden [Netherlands Jurists Committee of Human Rights v State of the Netherlands*], Rechtbank Den Haag [Hague District Court], C/09/550982/HA ZA 18-388 (February 5, 2020).

61. Toh (see note 60); see also J. Henley and R. Booth, "Welfare surveillance system violates human rights, Dutch court rules," *Guardian* (February 5, 2020). Available at https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules?CMP=Share_iOSApp_Other.

62. For an example of medical stockouts and digital technology, see Stop Stockouts Project. Available at https://stockouts.org; for an example of an access to justice reporting system in the HIV response, see R. T. Williamson, P. Wondergem, and R. Amenyah, "Using a Reporting system to protect the human rights of people living with HIV and key populations: A conceptual framework," *Health and Human Rights Journal* 16/1 (2014).