Privacy International's Submission to the UN Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health

Input for the thematic report titled "Digital innovation, technologies and the right to health"

November 2022

Privacy International ("PI") is a London-based non-profit, non-governmental organization (Charity Number: 1147471) that works internationally to protect people's privacy, dignity, and freedoms. Through our work we aim to build a world where technology will empower and enable us, not exploit our data for profit and control. [1] PI works globally with partners[2] to challenge overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

PI welcomes the opportunity to engage once again with the mandate by submitting comments, evidence, and recommendations to the UN Special Rapporteur on the right to health, Ms. Tlaleng Mofokeng. We hope that our input will contribute to the forthcoming report, "Digital innovation, technologies and the right to health".

I. Introduction

Technology has contributed significantly to the planning and delivery of health information, services and care. We have seen the use of data and technology across the healthcare sector from health apps, electronic medical records, to smart supply-chain management, the use of drones for the delivery of medication, and nascent technology on automated diagnostics.

The introduction of digital technologies in the health sector have been portrayed as "a critical solution to challenges and gaps in the delivery of quality health care and essential to achieving the Sustainable Development Goals."[3] The WHO draft Global Strategy on Digital Health 2020 – 2025 presents its vision of digital health technologies "that allow people to manage their health more

[1] For more information about PI, please visit our website at www.privacyinternational.org and in particular: https://privacyinternational.org/strategic-areas

[2] For more information about our global network of partners, please see: https://privacyinternational.org/where-we-work

[3] Privacy International, Digital Health: what does it mean for your rights and freedoms, 8 November 2021. Available at: https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms; United Nations Development Programme, Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes, 12 July 2021. Available at: https://www.undp.org/publications/guidance-rights-based-and-ethical-use-digital-technologies-hiv-and-health-programmes

effectively, improve caregiver-patient communication and monitor the impact of policies on population health."[4]

We agree that digital technologies can potentially improve the delivery of health information, services and care. However, before the inception of any technology-assisted initiatives, there need to be open, inclusive decision-making processes and human rights assessments as to whether to deploy them in the first place in a particular setting or for a particular purpose. Once this first step has been concluded, and the deployment of such technologies is justified, then safeguards and due process guarantees need to be considered in order to identify and mitigate risks. Otherwise, the same programmes that are intended to facilitate access will amplify pre-existing shortcomings and injustice.

This submission is based on the work we have done as well as our Network of partners as we've monitored and responded to developments associated with the use of data and technology in the health care sector by governments and companies.

II. Discrimination and Exclusion

Digital technologies for health can exclude particular groups based on whether or not they rely on a technology, platform or requirements which are not practically or reasonably accessible to those groups.

The UN Development Programme (UNDP) has warned that relying on digital technologies as a primary system or strategy within the health sector may impact access and availability, and inadvertently exacerbate inequalities, contributing to the digital divide.[5] Similar concerns were echoed by Asociación por los Derechos Civiles (ADC), which cautioned against full reliance on digital health services, on account of Argentina's enduring inequality and the difficulties potentially faced by low-income sectors to access services when these are predicated on computer/smartphone access or Wi-Fi connectivity.[6] Specifically in the context of reproductive and maternal health services and telemedicine,[7] obstacles to connectivity have been flagged as a key bottleneck issue.[8]

These lessons were reinforced during the COVID-19 pandemic with the development of contact-tracing apps, with many sponsoring governments incorrectly assuming that their populations had widespread use of smartphones and access to connectivity,[9] or over-estimating the extent to which specific groups would be able or willing to engage with contact-tracing apps.[10]

---

[4] WHO, Global Health Strategy, 2020-2025. Available at: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf

[5] United Nations Development Programme, Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes, 12 July 2021. Available at: https://www.undp.org/publications/guidance-rights-based-and-ethical-use-digital-technologies-hiv-and-health-programmes,

[6] Asociación por los Derechos Civiles, Privacy is Health: A preliminary review of the legal framework and technological developments on electronic health records and telemedicine in Argentina, March 2021, pp. 16-17. Available at: https://adc.org.ar/wp-content/uploads/2021/06/ADC-Privacy-is-health.pdf

[7] Privacy International, Telemedicine and data exploitation, 28 October 2021. Available at: https://privacyinternational.org/long-read/4655/telemedicine-and-data-exploitation

[8] Galle A, Semaan A, Huysmans E et al., A double-edged sword – telemedicine for maternal care during Covid-19: findings from a global mixed-methods study of healthcare providers. BMJ Global Health 2021;6;e004575. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7908054/pdf/bmjgh-2020-004575.pdf

[9] Privacy International, Colombia: Coronapp fails at public information purpose, 9 March 2020. Available at: https://privacyinternational.org/examples/3435/colombia-coronapp-fails-public-information-purpose

[10] Sara L. M. Davis, Contact Tracing Apps: Extra Risks for Women and Marginalized Groups., 29 April 2020. Available at:https://www.hhrjournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups/

Furthermore, digital health can be exclusionary when connected services are made conditional upon the presentation of a single document, usually a national ID. Digital health exclusion on this basis can be direct or indirect. For example, it can be directly exclusionary if it requires prospective patients to present ID when they don't have one. It is well-documented that there are individuals and communities who are less likely to have ID, such as the poor and disadvantaged, women, older persons, members of some occupational groups, people with disabilities, and people whose name and gender are not properly reflected in the ID system.[11]

There have been examples of individuals being denied healthcare as a result of lacking the required ID with some tragic consequences. In India, a woman in labour was turned away by her local hospital for not having an Aadhaar card and later passed away during delivery at home.[12]

The COVID-19 pandemic yielded fresh lessons about the impact of requiring a single form of identification as a condition to access health services.[13] In Uganda, a petition launched by Unwanted Witness challenged the requirement for people seeking vaccination to present ID in order to receive it.[14] As a result the Ministry changed the policy to allow other forms of ID to be accepted. In India, providing an ID number (known in India as an Aadhaar number) was a requirement to register for coronavirus vaccine appointments on a mobile app using Aadhaar, effectively excluding millions of people without an ID.[15]

A requirement to present ID can be indirectly exclusionary when its implications deter prospective patients from engaging with the service. This is especially true when accessing the health service may lead to stigmatisation, if confidentiality is not respected and personal data is being made available to third parties. For example, there have been reports that some stopped looking for treatment for HIV/AIDS after treatment was linked to the biometric identity system Aadhaar.[16]

III. The use of AI

The pitfalls of AI in the field of digital health are varied and well-established. A primary concern relates to the quality, representativeness and objectivity of data used to train AI systems.[17] In the absence thereof, AI systems may lead to bias and discrimination, which may further entrench inequalities and exclude historically disadvantaged groups such as girls and women, ethnic minorities, elderly people, rural communities and other disadvantaged groups.[18]

[11] A/HRC/43/29, para 33

[12] S Bhuvaneshwari, Karnataka: Turned away bu Tumakuru govt hospital, mom & twin newborns die, The Times of India, 4 November 2022. Available at: https://timesofindia.indiatimes.com/city/mysuru/turned-away-by-tumakuru-govt-hospital-mom-twin-newborns-die/articleshow/95287187.cms

[13] Privacy International, International Health Day during a pandemic: an opportunity to reflect, 10 April 2020. Available at: https://privacyinternational.org/news-analysis/3619/international-health-day-during-pandemic-opportunity-reflect

[14] Unwanted Witness, Covid-19 vaccine: CSOs petition court challenging national ID requirement. Available at: https://www.unwantedwitness.org/covid-19-vaccine-csos-petition-court-challenging-national-id-requirement/

[15] Rina Chandran, Fears of vaccine exclusion as India uses digital ID, facial recognition, Reuters, 15 April 2021. Available at: https://www.reuters.com/article/us-india-health-coronavirus-trfn-idUSKBN2C217V

[16] Menaka Rao, Why Aadhaar is prompting HIV positive people to drop out of treatment programmes across India, Sroll.in, 17 November 2017. Available at: https://scroll.in/pulse/857656/across-india-hiv-positive-people-drop-out-of-treatment-programmes-as-centres-insist-on-aadhaar

[17] World Health Organisation, Ethics and governance of artificial intelligence for health, 28 June 2021, p.11. Available at: https://www.who.int/publications/i/item/9789240029200

[18] Ibid., pp. 54-57.

For example, automated decision-making used for health decisions has led to less spending in Black communities than on white patients despite the same level of need.[19] Even when AI aims to be inclusive, it can be discriminatory. A project carried out by an Argentinean local government in partnership with Microsoft to use AI to predict teen pregnancy was built on a database capturing the data of 200,000 female residents of Salta, including highly sensitive data ranging from nationality, ethnicity and disability status to access to hot water. The aim was to predict which girls from low-income areas would become pregnant in the next five years, although it was never made clear how the information would be used. Despite this, the project has now been expanded to other provinces in Argentina. [20] Concerns were expressed that this was yet another tool to control the bodily autonomy of economically disadvantaged communities by preventing and avoiding abortions.[21]

AI similarly carries with it privacy risks which take particular relevance in the healthcare context. The large amounts of personal datasets that AI often relies on can make people vulnerable if the data is not handled securely or transparently. Data breaches can put millions of people at risk, and obscure data-sharing practices - which we've formerly documented[22] - can result in health data being made available to countless third parties in the absence of the data subject's informed consent.[23] In the healthcare context, unauthorised disclosures can be particularly harmful depending on the nature of the illness. Our partner KELIN, based in Kenya, has documented the harm of unauthorised disclosures relating to the status of HIV-positive individuals.[24]

In light of these risks, Privacy International is pleased to see a growing understanding among international organisations of the need to place human rights at the centre of the design, development and deployment of any artificial intelligence technologies in the field of health. This imperative has been echoed most recently by the World Health Organisation in their report on Ethics and Governance of Artificial Intelligence for Health.[25]

Nevertheless, we remain concerned by the sustained "technosolutionism". We must continue to challenge the assumptions that the use of AI in healthcare will lead to more efficient healthcare systems, despite as of yet little evidence to support this assumption. The effectiveness and relevance of AI technologies in healthcare systems need to be carefully reviewed and AI applications need to be designed in ways that respect and protect human rights from the outset. As we have argued elsewhere,[26] there is a real risk that the use of AI technologies by states or industry will have a negative impact on human rights, including the right to privacy.

IV. Access to health information and services through web platforms and social media

[19] Obermeyer Z, Powers B, Vogeli C, Mullainathan S., Dissecting racial bias in an algorithm designed to manage the health of populations. Science. 2019; 366(6464): 447-53. Available at: https://www.science.org/doi/abs/10.1126/science.aax2342
[20] WIRED, The case of the Creepy Algorithm that 'Predicted' Teen Pregnancy, 16 February 2022. Available at: https://www.wired.com/story/argentina-algorithms-pregnancy-prediction/
[21] Peña, P. and Varon, J., Teenager pregnancy addressed through data colonialism in a system patriarchal by design. 3 May 2021 (updated 26 April 2022) Available at: https://notmy.ai/news/case-study-plataforma-tecnologica-de-intervencion-social-argentina-and-brazil/
[22] Privacy International, Privacy International study shows your mental health is for sale, 3 September 2019. Available at: https://privacyinternational.org/long-read/3194/privacy-international-investigation-your-mental-health-sale
[23] Privacy in the Digital Age 2021, para. 14, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement
[24] KELIN and Privacy International, Report of the launch of the research findings on the right to privacy and confidentiality for PLHIV accessing health services, 18 December 2014. Available at: https://kelinkenya.org/wp-content/uploads/2010/10/PI-report-pdf.pdf
[25] Privacy International, Our analysis of the WHO report on Ethics and Governance of Artificial Intelligence for Health, 20 July 2021. Available at: https://privacyinternational.org/news-analysis/4594/our-analysis-who-report-ethics-and-governance-artificial-intelligence-health
[26] Privacy International, Artificial Intelligence. Available at: https://privacyinternational.org/learn/artificial-intelligence

Over the course of our work, we have raised concerns about how web platforms and social media are spreading misinformation which is curtailing access to healthcare and consequently leading to other harms such as discrimination.

The 'adtech' industry is contributing to undermining the right to health by supporting an ecosystem in which health data is commoditised, shared with and used by third parties.
Numerous mental health websites include trackers from known data brokers and AdTech companies, which enables them to access information about the users' behaviour on a given website. We investigated some depression test websites and found that a number of them store users' answers to the test as variables and share answers, as well as test results with third parties in the URL.[27] In a separate 2021 investigation, we found that some of the most popular dieting apps and platforms were sharing health information with third parties.[28] These practices are concerning, not least because they enable the use of an individual's health information by third-parties, not all of whom may act in good faith.

Access to information on sexual and reproductive healthcare has also become a battle ground for targeted advertising and misinformation, to restrict access to reproductive healthcare. Through our research with our global partners, we identified targeted advertising of scientifically inaccurate health information as a tactic deployed by those opposing access to reproductive services.[29] By way of example, ads about "abortion pill reversal" have continued to make the rounds on social media platforms since we first spotted them in 2020.[30] Another example of misleading advertising was reported by Le Monde who exposed anti-IVG (anti-abortion) advertising on Facebook as part of a broader campaign led by anti-abortion website IVG.net.[31] The advertisement relied on stock photos and purportedly genuine testimonies posted in public Facebook groups and promoted to young women. Most of the posts attempted to promote the idea that abortion leads to mental health issues, an assertion that scientific research has thoroughly disproven.[32]

Targeted advertising, some of it enabled through geo-fencing - the creation of a virtual boundary around an area that allows software to trigger a response or alert when a mobile phone enters or leaves an area – has reportedly allowed groups opposing abortion to target people going to abortion clinics with ads.[33] When put to the service of the opposition to abortion, geo-fencing can result in

[27] Privacy International, Privacy International study shows your mental health is for sale, 3 September 2019. Available at: https://privacyinternational.org/long-read/3194/privacy-international-investigation-your-mental-health-sale; Privacy International, Taking a depression test online? Go ahead, they're listening, 2 September 2019. Available at: https://www.privacyinternational.org/news-analysis/3188/taking-depression-test-online-go-ahead-theyre-listening
[28] Privacy International, An unhealthy diet of targeted ads: an investigation into how the diet industry exploits our data, 4 August 2021. Available at: https://privacyinternational.org/long-read/4603/unhealthy-diet-targeted-ads-investigation-how-diet-industry-exploits-our-data
[29] Privacy International, Country case studies: Reproductive Rights. Available at: https://privacyinternational.org/learning-resources/country-case-studies-reproductive-rights
[30] Lauren Kirchner, Maddy Varner, and Angie Waller, As Demand for Medication Abortion Increases, Facebook Allows Ads for Potentially Dangerous "Abortion Reversal" Procedure, 19 July 2022. Available at: https://themarkup.org/citizen-browser/2022/07/19/facebook-allows-ads-for-potentially-dangerous-abortion-reversal-procedure; Privacy International, A documentation of data exploitation in sexual and reproductive rights, 21 April 2020. Available at: https://privacyinternational.org/long-read/3669/documentation-data-exploitation-sexual-and-reproductive-rights
[31] Laura Motet, Les anti-IVG ciblent les jeunes femmes grace aux publicités sur Facebook, Le Monde, 11 July 2018. Available at: https://www.lemonde.fr/les-decodeurs/article/2018/07/11/les-anti-ivg-ciblent-les-jeunes-femmes-grace-aux-publicites-sur-facebook_5329906_4355770.html
[32] American Psychological Association, The facts about abortion and mental health, 23 June 2022. Available at; https://www.apa.org/monitor/2022/09/news-facts-abortion-mental-health
[33] Christina Cauterucci, Anti-Abortion Groups Are Now Sending Targeted Smartphone Ads to Women in Abortion Clinics, Slate, 26 May 2016. Available at: https://slate.com/human-interest/2016/05/anti-abortion-groups-are-sending-targeted-smartphone-ads-to-women-in-abortion-clinics.html

visitors of abortion clinics - many of them in a vulnerable position - being placed in the difficult situation of dealing with potentially unwelcome or disturbing advertising.[34]

V. The impact on the right to privacy

Complementing some of the examples already provided elsewhere in this submission, we would like to highlight some additional concerning trends and practices by States, companies or other third parties.

Limited or no consideration for right to privacy

Despite the recognised risks associated with the use of new technologies in the health sector to people and their rights,[35] we are seeing the absence of human rights and privacy considerations and comprehensive impact assessments in the design and implementation of digital health in general.[36]

In particular we have explored how this has been a shortcoming in the development of Reproductive and Maternal, Newborn, Child and Adolescent Health (RMNCH) digital health services.[37] While the intention is to tackle ongoing concerns such as maternal and child mortality, without the necessary safeguards these tools have the potential to undermine human rights if risks of mission creep, unregulated data sharing, failure to protect the identity of users as well as exclusion are not mitigated from the onset.[38]

For example, despite not having a data protection framework in place, the Ministry of Health and Family Welfare in India introduced India's Mother and Child Tracking System (MCTS).[39] It is a system that collects vast amounts of data about pregnant women, children, and families from conception to 42 days postpartum. As of 2018, 120 million pregnant women and 110 million children were registered on the portal, with research undertaken by the Center for Internet and Society suggesting that the

[34] Privacy International, How opposition groups are using misinformation to delay people accessing safe abortion care, 18 April 2020. Available at: https://privacyinternational.org/video/3673/how-opposition-groups-are-using-misinformation-delay-people-accessing-safe-abortion-care

[35] WHO, Global Health Strategy, 2020-2025. Available at: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf

[36] Privacy International, Digital Health: what does it mean for your rights and freedoms, 8 November 2021. Available at: https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms

[37] Reproductive and Maternal, Newborn, Child and Adolescent Health (RMNCH) digital health services include digital information registries facilitating scheduling through SMS; remote access to care and counselling; telemedicine; health workers using a mobile phone to track pregnant people throughout their pregnancy or a child over their immunisation cycle, as well as the use of sensors and wearable devices. See: Privacy International, The use of SMS in the delivery of reproductive and maternal healthcare, 12 January 2022. Available at: https://privacyinternational.org/long-read/4735/use-sms-delivery-reproductive-and-maternal-healthcare; Privacy International, Telemedicine and data exploitation, 12 January 2022. Available at: https://privacyinternational.org/long-read/4655/telemedicine-and-data-exploitation; Privacy International, Privacy International, How digital health apps can exploit users' data, 4 March 2022. Available at: https://privacyinternational.org/long-read/4804/how-digital-health-apps-can-exploit-users-data;

[38] Privacy International, Protecting Privacy in The Digitalisation of Reproductive Healthcare. Available at: https://privacyinternational.org/campaigns/protecting-privacy-digitalisation-reproductive-healthcare; Privacy International, Health Tech In Sexual and Reproductive Rights. Available at: https://privacyinternational.org/learn/health-tech-sexual-and-reproductive-rights; Mohammad S. Alyahya, Niveen M. E. Abu-Rmeileh, Yousef S. Khader, Maysaa Nemer, Nihaya A. Al-Sheyab, Alexandrine Pirlot de Corbion, Laura Lazaro Cabrera Sundeep Sahay, Maturity Level of Digital Reproductive, Maternal, Newborn, and Child Health Initiatives in Jordan and Palestine, Methods of Information in Medicine,15 November 2022. Available at: https://www.thieme-connect.com/products/ejournals/abstract/10.1055/s-0042-1756651#info

[39] Privacy International, India's Mother and Child Tracking System, 11 August 2021. Available at: https://privacyinternational.org/long-read/4610/indias-mother-and-child-tracking-system; Centre for Internet & Society, Big Data and Reproductive Health in India: A Case Study of the Mother and Child Tracking System, 17 October 2019. Available at: https://cis-india.org/raw/big-data-reproductive-health-india-mcts

categories of data captured by the system in practice are broader than those listed in the official statement introducing the system. The vast troves of personal data managed by the MCTS in the absence of data protection legislation are a considerable risk factor for the numerous women and families involved.

Vast data processing and data-sharing by the private sector

We have conducted research into period-tracking apps and how extensive data collection and data-sharing practices by companies directly impact on users' privacy.[40] Our 2019 research into 5 period-tracking apps uncovered that many of them were sharing data with third-party entities not disclosed in the apps' privacy policies and a couple were conducting what could be described as extensive data-sharing with Facebook. There are many other documented examples of the ways data collected by period-tracking apps can be shared with third parties emerging from research conducted by other CSOs with concerns about such practices.[41]

Companies developing period-tracking apps present as offering transparent and efficient means for users to keep on top of their reproductive health. However, even if that is the intention ultimately, they are still companies whose continued existence relies on making a profit. One way in which companies make their profit from apps that are marketed as "free" is to collect, share or sell user's personal data to third companies for advertising purposes. For example, the data of pregnant people is particularly valuable to advertisers as expecting parents are consumers who are likely to change to their purchasing habits. These concerns have been borne out in practice. For example, in the UK, the company Bounty was fined £400,000 by the UK's data protection authority for illegally sharing the personal information of mums and babies as part of its services as a "data broker".[42]

Access and use of health data by law enforcement

Data protection laws - where they exist - generally exclude law enforcement processing from their scope of application. Therefore, in certain circumstances, and depending on the legal framework in place, companies and even public sector bodies can be compelled by law enforcement bodies or courts to hand over personal data for criminal investigation purposes. This is particularly relevant in countries where some medical procedures are outlawed, such as abortion. For example, as recent experience from the US shows, different period-tracking apps apply different approaches to law enforcement requests: while some refuse to disclose data in the absence of a warrant legally compelling them to do so, others have previously offered to disclose data to law enforcement voluntarily.[43]

Security and integrity concerns: expanding the exposure and attack surface

Governments around the world are embracing innovations in technology and digitising their health systems. However, technologically complex systems are inherently vulnerable to cyber security

[40] Privacy International, No Body's Business But Mine: How Menstruation Apps are Sharing Your Data, 9 September 2019. Available at:https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data; Privacy International, We asked five menstruation apps for our data and here is what we found, 4 December 2020. Available at: https://privacyinternational.org/long-read/4316/we-asked-five-menstruation-apps-our-data-and-here-what-we-found

[41] Felizi N. and Varon, J., MENSTRUAPPS – How to turn your period into money (for others), Coding Rights. Available at: https://chupadados.codingrights.org/en/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/

[42] Privacy International, How a company exploited the data of 14 million mothers and babies, 15 September 2021. Available at: https://privacyinternational.org/long-read/4620/how-company-illegally-exploited-data-14-million-mothers-and-babies

[43] Privacy International, Privacy and Sexual and Reproductive Healthcare in the Post-Roe world, 22 July 2022. Available at: https://privacyinternational.org/long-read/4937/privacy-and-sexual-and-reproductive-health-post-roe-world

incidents and data breaches.[44] The results can be significantly harmful for the privacy of individuals as well as the delivery of healthcare services.

There are numerous high-profile examples of digital health systems being breached due to poor data security management, even within some of the most well-resourced governments. For example, in 2019 there was a HIV data leak in Singapore,[45] a leak of over 2.5M medical records in the United States in 2020,[46] and the leak of 500,000 medical records in France in early 2021[47]. There have been reports of hackers having broken into databases containing the details of women having sought abortion care. In a recent example from the US, the data of 400,000 Planned Parenthood users was stolen in a ransomware attack.[48] In August 2022, the NHS was impacted by a ransomware attack on one of its software suppliers, Advanced, which provides services for NHS 111 and patient records.[49]

VI. Current state of digital health governance

Although there are some examples of welcoming developments, below we outline some fo the overarching weaknesses which persist in the current approach to digital health governance.

The lack of a human-rights based approach

While some issues around equality and access (i.e. digital divide) are increasingly discussed with regards to digital health and health in general, there is limited consideration of the protection of all rights including the right to privacy beyond data protection compliance issues.[50] The adoption of a human rights approach is still a nascent idea in the health sector, and in practice such an approach informs very little in regard to the initial decision to adopt digital technologies, let alone to inform their design and implementation.

Whilst this was already a documented concern,[51] the approach taken to respond to the Covid-19 pandemic saw a lack of clear principles and effective enforcement of existing human rights obligations of governments and private entities which led to short-sighted decision-making with little consideration of what was needed for an effective public health response and limited understanding of the impact on individuals and communities, in particular those in vulnerable positions.[52]

---

[44] Privacy International, Digital Health: what does it mean for your rights and freedoms, 8 November 2021. Available at: https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms

[45] Sharanjit Leyl, Singapore HIV data leak shakes a vulnerable community, BBC News, 22 February 2019. Available at: https://www.bbc.co.uk/news/world-asia-47288219

[46] Matthew Humphries, Report: AI Company Leaks Over 2.5M Medical Records, PCMag, 18 August 2020. Available at: https://uk.pcmag.com/encryption/128228/report-ai-company-leaks-over-25m-medical-records

[47] France24, France investigates leak of almost 500,000 medical records, including HIV and fertility status. Available at: https://www.france24.com/en/europe/20210225-france-investigates-massive-leak-of-medical-records

[48] Kevin Collier, 400,000 Planned Parenthood users' data stolen in ransomware attack, NBC News, 2 December 2021. Available at: https://www.nbcnews.com/news/hackers-held-planned-parenthood-ransom-accessed-data-400000-users-rcna7336

[49] Dan Milmo, NHS ransomware attack: what happened and how bad is it? The Guardian, 11 August 2022. Available at: https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it

[50] Nina Sun, Kenechukwu Esom, Mandeep Dhaliwal, and Joseph J Amon, Human Rights and Digital Health Technologies, Health and Human Rights Journal, Volume 22/2, December 2020, pp.21-32. Available at: https://www.hhrjournal.org/2020/12/human-rights-and-digital-health-technologies/

[51] Privacy International, Digital Health: what does it mean for your rights and freedoms, 8 November 2021. Available at: https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms;

[52] Privacy International, PI's contribution to the first public consultation for an International Pandemic Treaty, 12 April 2022. Available at: https://privacyinternational.org/advocacy/4838/pis-contribution-first-public-consultation-international-pandemic-treaty; Privacy International, PI's submission on the working draft of the WHO's Pandemic prevention, preparedness and response accord, 21 September 2022. Available at: https://privacyinternational.org/advocacy/4957/pis-submission-working-draft-whos-pandemic-prevention-preparedness-and-response

Lack of comprehensive protection frameworks

Nearly 150 countries around the world have adopted comprehensive data protection laws to protect people and their data.[53] Such developments provide better protection frameworks to regulate the use of data and technology in the health sector.

However, there is a need to ensure safeguards across cross-cutting sectors and consideration of wider human rights obligations. For example, complementary safeguards associated with the use of technology in the health sector must be adopted and enforced across policy domains such as immigration enforcement, border management, and social protection, to name a few. These are important because developments in these sectors may negatively impact on the right to health of specific individuals and communities. This was seen with the "immigration exemption" provision within the UK Data Protection Act 2018, which was then ruled unlawful by the High Court.[54]

First deployment and then regulation

Too often, governments jump to adopt digital tools and technologies without ensuring the relevant regulatory mechanisms are in place, and where they are in place there is little evidence that they are capable of effectively monitoring and addressing potential abuses to mitigate the risks and protect people and their rights.

For example, before adopting a data protection law, Kenya proposed several digital health initiatives which had severe implications for persons living with HIV (PLHIV) and other key populations, namely sex workers, LGBT people, and people who use drugs including a study of these communities and a proposed presidential directive to collect up-to-date data and prepare a report on all school-going children living with HIV and AIDS.[55]

IPANDETEC documented that the governments of Costa Rica, Guatemala and Panama were deploying digital apps for contact tracing and self-diagnostic, health certificates, and digital vaccination forms, amongst others as part of their response to the Covid-19 pandemic without having the necessary legal and regulatory safeguards in place.[56]

In India, the Centre for Internet and Society has observed that healthcare policy is being developed and secondary legislation passed in the absence of enforceable data protection legislation, raising questions about the risks to patients' data.[57]

Even where legal and regulatory safeguards exist, they may not always be effective which highlights how important enforcement and accountability are key. When exploring digital health initiatives in Argentina, ADC reviewed a variety of laws and decrees aimed at effectively regulating personal data

[53] In addition, around 30 countries have initiated a legislative process with a data protection bill in progress. See: David Banisar, National Comprehensive Data Protection Laws and Bills 2022, 28 October 2022. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

[54] UK Home Office, Immigration exemption policy document: data protection legislation, 4 February 2022. Available at: https://www.gov.uk/government/publications/immigration-exemption-policy-document-iepd/immigration-exemption-policy-document-data-protection-legislation-accessible-version; Open Rights Group, "Immigration Exemption" ruled unlawful under GDPR. Available at: https://www.openrightsgroup.org/campaign/immigration-exemption-campaign-page/

[55] KELIN, "Everyone said no" Biometrics, HIV and Human Rights - A Kenya Case Study, 2018. Available at: http://www.kelinkenya.org/wp-content/uploads/2018/07/%E2%80%9CEveryone-said-no%E2%80%9D.pdf

[56] IPANDETEC, Caretas Digitales: Digital Identity in Central America, January 2021. Available at: https://www.ipandetec.org/wp-content/uploads/2021/05/IPNDTC_CARDIG2021_ingles.pdf

[57] Centre for Internet and Society, NHA Data Sharing Guidelines – Yet Another Policy in the Absence of a Data Protection Act, 29 September 2022. Available at: https://cis-india.org/internet-governance/blog/nha-data-sharing-guidelines

as well as sectorial regulation of the health sector and patient data - many of which are still in drafting stages and are not yet implemented -, ultimately questioning the extent to which these actually inform decision-making processes.[58]

Regulating industry and Public-Private Partnerships

Public-private partnerships in the digital healthcare sector are proliferating, but opportunities for scrutiny remain limited even in countries with robust access to information legislation. This 'government-industry complex' has largely evolved in a regulatory void. States have obligations to effectively regulate the role that industry should play in the health sector and the level of accountability and scrutiny they should be subject to.[59]

Over the years we've documented the involvement of industry across the healthcare sector from companies providing digital systems such as apps,[60] telemedicine[61] and the involvement of telcos in the delivery of m-Health[62] to big tech such as Google buying small companies processing health data,[63] Amazon Alexa being a tool for providing health-related information for the NHS,[64] and more recently the Covid-19 pandemic.[65]

We have seen exceptions to freedom of information laws being used to restrict access to information concerning healthcare public-private partnerships. In the UK, we were initially denied access to the full contract between Amazon and the UK National Health Service (NHS) on the grounds that the commercial interests of Amazon superseded the public interest in favour of disclosure.[66] After escalating the matter to the Information Commissioner's Office, we obtained a partial disclosure and a reassurance that the remaining unredacted sections were not relevant to patient data.[67] The fact that it took several months to obtain this reassurance is an illustration of the uphill battle of the time and resources involved in obtaining comprehensive information on the nature of public-private healthcare arrangements, and their data processing implications.

VII. Efforts taken by governments and third parties to uphold human rights

As noted elsewhere in this submission, there have been some encouraging developments with nearly 150 countries around the world having adopted comprehensive data protection laws to protect

[58] Asociación por los Derechos Civiles, Privacy is Health: A preliminary review of the legal framework and technological developments on electronic health records and telemedicine in Argentina, March 2021. Available at: https://adc.org.ar/wp-content/uploads/2021/06/ADC-Privacy-is-health.pdf
[59] Privacy International, Safeguards for Public-Private Surveillance Partnerships. Available at: https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships
[60] Privacy International, How digital health apps can exploit users' data, 4 March 2022. Available at: https://privacyinternational.org/long-read/4804/how-digital-health-apps-can-exploit-users-data
[61] Privacy International, Telemedicine and data exploitation, 28 October 2021. Available at: https://privacyinternational.org/long-read/4655/telemedicine-and-data-exploitation
[62] Privacy International, The use of SMS in the delivery of reproductive and maternal healthcare, 12 January 2022. Available at: https://privacyinternational.org/long-read/4735/use-sms-delivery-reproductive-and-maternal-healthcare
[63] Privacy International, The Google/Fitbit merger – Not on Our Watch. Available at: https://privacyinternational.org/campaigns/googlefitbit-merger-not-our-watch
[64] Privacy International, Amazon Alexa/NHS contract: ICO allows partial disclosure, 20 April 2021. Available at: https://privacyinternational.org/news-analysis/4486/amazon-alexanhs-contract-ico-allows-partial-disclosure
[65] Privacy International, Covid-19 response: Corporate Exploitation, 8 April 2020. Available at: https://privacyinternational.org/news-analysis/3592/covid-19-response-corporate-exploitation
[66] Privacy International, Alexa, what is hidden behind your contract with the NHS? 6 December 2019. Available at: https://privacyinternational.org/node/3298
[67] Privacy International, Amazon Alexa/NHS contract: ICO allows partial disclosure, 20 April 2021. Available at: https://privacyinternational.org/news-analysis/4486/amazon-alexanhs-contract-ico-allows-partial-disclosure

people and their data. There have been opportunities in many instances for CSOs to engage in those processes, such as in Pakistan, Argentina, India, Uganda and Kenya, to name a few. These processes have been on occasion accompanied by the development of laws in the health sector such as the consultation on Digital Health Act in Kenya and National Health Data Sharing Guidelines in India. However, efforts to regulate the use of data and technology in the health sector remain fragmented and uncoordinated.

We still too often observe that there are few instances of meaningful public consultation and participation in the development and/or the adoption of laws, policies and strategies developing digital technologies in the area of health. There are still many legislative processes which remain closed off from any external consultation. When there has been a consultation process, some of the main shortcomings we've identified include:

- It is made public far too late into the legislation process with little opportunity to meaningfully inform the process with many decisions already made in advance.
- The turnaround time is very limited which puts extra strain and stress on civil society organisations, who already have limited time and resources, to make the time for and prioritise engaging in these processes at the cost of other areas of work.
- It can take years and any changes in leadership, for example after elections, may mean starting the process from scratch, and requiring CSOs to repeat the same process all over again.

Beyond national level legislative processes, there have been some opportunities to engage with standard-setting bodies. For example, the WHO has taken some steps to engage a wider range of experts in certain processes such as by setting up a Working Group set-up to contribute to the development of the "Digital Documentation of COVID-19 Certificates: Vaccination Status" (DDCC:VS)[68], the running of some targeted consultations with CSOs and expert groups in the development of their guidance on Ethics and Governance of Artificial Intelligence for Health[69] and initial efforts to seek input into the development a Pandemic prevention, preparedness, and response accord.[70] Whilst these are important developments to highlight the implications associated with the use of technology in the health sector and identifying some of the minimum safeguards, there remains questions as to how these guidelines trickle down to the national level and serve as a standard for governments to uphold.

PI has sought to closely follow and engage with the discussions around the WHO's Pandemic prevention, preparedness, and response accord (Pandemic Treaty), despite the significant limitations to civil society participation in the process. In our submission to the working draft of the treaty we argued that the principles of human rights, equity, transparency, accountability, gender equality, non-discrimination and respect for diversity and rights of vulnerable populations must be strengthened to align with existing international and human rights obligations of governments and other non-state

[68] Privacy International, Covid-19 vaccination certificates: WHO sets minimum demands, governments must do even better, 9 August 2021. Available at: https://privacyinternational.org/advocacy/4607/covid-19-vaccination-certificates-who-sets-minimum-demands-governments-must-do-even

[69] Privacy International, Our analysis of the WHO report on Ethics and Governance of Artificial Intelligence for Health, 20 July 2021. Available at: https://privacyinternational.org/news-analysis/4594/our-analysis-who-report-ethics-and-governance-artificial-intelligence-health

[70] See: WHO, https://inb.who.int/; Privacy International, PI's contribution to the first public consultation for an International Pandemic Treaty, 12 April 2022. Available at: https://privacyinternational.org/advocacy/4838/pis-contribution-first-public-consultation-international-pandemic-treaty; Privacy International, PI's submission on the working draft of the WHO's Pandemic prevention, preparedness and response accord, 21 September 2022. Available at: https://privacyinternational.org/advocacy/4957/pis-submission-working-draft-whos-pandemic-prevention-preparedness-and-response

actors. We also recommended that the treaty elaborate further on the due diligence, effective regulation and robust oversight required of activities associated with use of data and technology.[71]

VIII. Conclusion and recommendations

The Special Rapporteur's thematic report is an important opportunity to highlight the wider human rights implicated in the use and deployment of technology in the health sector. In particular, we look forward to the Rapporteur's assessment as to whether digital health innovation is resulting in improvements to the quality and access to healthcare, which will help the healthcare sector to understand the ways in which individuals and communities are being impacted. This will further assist stakeholders to propose recommendations and solutions to overcome these issues.

We hope the UNSR will take the opportunity to integrate critical questions about the use of digital technologies in healthcare. These issues are becoming more pressing given some rapid developments in this domain during the Covid-19 pandemic, and a shift in policy-making leading to long-term investments.

We hope that the UN Special Rapporteur on the right to health will further explore the areas we have highlighted in our submission, and that the report develops recommendations to governments, companies and international organisations involved in the development of digital health.

Finally, we recommend that the report include recommendations aimed at:

- Promoting a comprehensive human rights-based approach in the design and deployment of digital health initiatives, as well as describing the necessary baseline measures to achieve this, including, for example 'human rights by design' and human rights impact assessments which integrate beneficiary perspectives and experiences,
- Establishing the need for a human rights-based approach to all AI applications in healthcare programmes,
- Ensuring that regulation and effective accountability mechanisms are in place to reign in, and/or heavily scrutinise, the involvement of the private sector in the delivery of healthcare services and access to healthcare infrastructure,
- Encouraging national human rights institutions to integrate questions of technology, security and privacy within their work on monitoring and promoting the right to health in their methodologies and strategies,
- Presenting an effective public policy around digital health which engenders trust and does not lead to a chilling effect on access, by preventing intrusive surveillance and monitoring practices,
- Recommending that international initiatives such as the Pandemic Treaty put human rights at the centre and reflect the need to ensure accountability and oversight of digital technologies introduced for the purposes of preventing and responding to future pandemics.

[71] Privacy International, Submission on the working draft of the WHO's Pandemic prevention, preparedness and response accord, https://privacyinternational.org/advocacy/4957/pis-submission-working-draft-whos-pandemic-prevention-preparedness-and-response

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471